

## **Guía de administración del sistema: servicios de seguridad**

Copyright © 2002, 2011, Oracle y/o sus subsidiarias. Todos los derechos reservados.

Este software y la documentación relacionada están sujetos a un contrato de licencia que incluye restricciones de uso y revelación, y se encuentran protegidos por la legislación sobre la propiedad intelectual. A menos que figure explícitamente en el contrato de licencia o esté permitido por la ley, no se podrá utilizar, copiar, reproducir, traducir, emitir, modificar, conceder licencias, transmitir, distribuir, exhibir, representar, publicar ni mostrar ninguna parte, de ninguna forma, por ningún medio. Queda prohibida la ingeniería inversa, desensamblaje o descompilación de este software, excepto en la medida en que sean necesarios para conseguir interoperabilidad según lo especificado por la legislación aplicable.

La información contenida en este documento puede someterse a modificaciones sin previo aviso y no se garantiza que se encuentre exenta de errores. Si detecta algún error, le agradeceremos que nos lo comuniqué por escrito.

Si este software o la documentación relacionada se entrega al Gobierno de EE.UU. o a cualquier entidad que adquiera licencias en nombre del Gobierno de EE.UU. se aplicará la siguiente disposición:

#### U.S. GOVERNMENT RIGHTS

Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065

Este software o hardware se ha desarrollado para uso general en diversas aplicaciones de gestión de la información. No se ha diseñado ni está destinado para utilizarse en aplicaciones de riesgo inherente, incluidas las aplicaciones que pueden causar daños personales. Si utiliza este software o hardware en aplicaciones de riesgo, usted será responsable de tomar todas las medidas apropiadas de prevención de fallos, copia de seguridad, redundancia o de cualquier otro tipo para garantizar la seguridad en el uso de este software o hardware. Oracle Corporation y sus subsidiarias declinan toda responsabilidad derivada de los daños causados por el uso de este software o hardware en aplicaciones de riesgo.

Oracle y Java son marcas comerciales registradas de Oracle y/o sus subsidiarias. Todos los demás nombres pueden ser marcas comerciales de sus respectivos propietarios.

Intel e Intel Xeon son marcas comerciales o marcas comerciales registradas de Intel Corporation. Todas las marcas comerciales de SPARC se utilizan con licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. AMD, Opteron, el logotipo de AMD y el logotipo de AMD Opteron son marcas comerciales o marcas comerciales registradas de Advanced Micro Devices. UNIX es una marca comercial registrada de The Open Group.

Este software o hardware y la documentación pueden ofrecer acceso a contenidos, productos o servicios de terceros o información sobre los mismos. Ni Oracle Corporation ni sus subsidiarias serán responsables de ofrecer cualquier tipo de garantía sobre el contenido, los productos o los servicios de terceros y renuncian explícitamente a ello. Oracle Corporation y sus subsidiarias no se harán responsables de las pérdidas, los costos o los daños en los que se incurra como consecuencia del acceso o el uso de contenidos, productos o servicios de terceros.

---

Copyright © 2002, 2011, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT RIGHTS. Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer des dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour ce type d'applications.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. UNIX est une marque déposée concédée sous licence par X/Open Company, Ltd.

# Contenido

---

<b>Prefacio .....</b>	<b>25</b>
 <b>Parte I Descripción general de la seguridad .....</b>	 <b>29</b>
<b>1 Servicios de seguridad (descripción general) .....</b>	<b>31</b>
Seguridad del sistema .....	32
Servicios criptográficos .....	33
Servicios de autenticación .....	34
Autenticación con cifrado .....	35
Auditoría .....	35
Política de seguridad .....	35
 <b>Parte II Seguridad de sistemas, archivos y dispositivos .....</b>	 <b>37</b>
<b>2 Gestión de seguridad de equipos (descripción general) .....</b>	<b>39</b>
Mejoras de la seguridad de equipos en la versión Solaris 10 .....	39
Control de acceso a un sistema informático .....	40
Mantenimiento de la seguridad física .....	40
Mantenimiento del control de inicio de sesión .....	41
Control de acceso a dispositivos .....	47
Política de dispositivos (descripción general) .....	48
Asignación de dispositivos (descripción general) .....	49
Control de acceso a recursos del equipo .....	50
Limitación y supervisión del superusuario .....	50
Configuración del control de acceso basado en roles para reemplazar al superusuario .....	50
Prevención del uso indebido involuntario de los recursos del equipo .....	51
Restricción de archivos ejecutables setuid .....	52

Uso de la herramienta automatizada de mejora de la seguridad .....	53
Uso de Oracle Solaris Security Toolkit .....	53
Uso de la configuración de seguridad predeterminada .....	53
Uso de funciones de gestión de recursos .....	54
Uso de zonas de Oracle Solaris .....	54
Supervisión del uso de los recursos del equipo .....	54
Supervisión de la integridad de archivos .....	55
Control de acceso a archivos .....	55
Protección de archivos con cifrado .....	55
Uso de listas de control de acceso .....	55
Uso compartido de archivos entre equipos .....	56
Restricción de acceso root a archivos compartidos .....	56
Control de acceso a la red .....	57
Mecanismos de seguridad de red .....	57
Autenticación y autorización para acceso remoto .....	58
Sistemas de cortafuegos .....	60
Cifrado y sistemas de cortafuegos .....	61
Comunicación de problemas de seguridad .....	62
<b>3 Control de acceso a sistemas (tareas) .....</b>	<b>63</b>
Control de acceso al sistema (mapa de tareas) .....	63
Protección de inicios de sesión y contraseñas (mapa de tareas) .....	64
Protección de inicios de sesión y contraseñas .....	64
▼ Cómo mostrar el estado de inicio de sesión de un usuario .....	64
▼ Cómo visualizar usuarios sin contraseñas .....	66
▼ Cómo deshabilitar temporalmente inicios de sesión de usuarios .....	66
▼ Cómo supervisar intentos de inicio de sesión fallidos .....	67
▼ Cómo supervisar todos los intentos de inicio de sesión fallidos .....	68
▼ Cómo crear una contraseña de marcación telefónica .....	69
▼ Cómo deshabilitar temporalmente inicios de sesión de marcación telefónica .....	71
Cambio del algoritmo de contraseña (mapa de tareas) .....	71
Cambio de algoritmo predeterminado para cifrado de contraseña .....	72
▼ Cómo especificar un algoritmo para cifrado de contraseña .....	72
▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS .....	73
▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS+ .....	74

▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP .....	74
▼ Cómo instalar un módulo de cifrado de contraseña de un tercero .....	75
Supervisión y restricción de superusuario (mapa de tareas) .....	76
Supervisión y restricción de superusuario .....	76
▼ Cómo supervisar quién está utilizando el comando su .....	76
▼ Cómo restringir y supervisar inicios de sesión de superusuario .....	77
SPARC: control de acceso a hardware del sistema (mapa de tareas) .....	79
Control de acceso a hardware del sistema .....	79
▼ Cómo requerir una contraseña para el acceso al hardware .....	79
▼ Cómo deshabilitar una secuencia de interrupción del sistema .....	80
<b>4 Control de acceso a dispositivos (tareas) .....</b>	<b>81</b>
Configuración de dispositivos (mapa de tareas) .....	81
Configuración de política de dispositivos (mapa de tareas) .....	82
Configuración de política de dispositivos .....	82
▼ Cómo ver una política de dispositivos .....	82
▼ Cómo cambiar la política de dispositivos en un dispositivo existente .....	83
▼ Cómo auditar cambios en la política de dispositivos .....	84
▼ Cómo recuperar información MIB-II IP de un dispositivo /dev/* .....	84
Gestión de asignación de dispositivos (mapa de tareas) .....	85
Gestión de asignación de dispositivos .....	86
▼ Cómo permitir que un dispositivo pueda asignarse .....	86
▼ Cómo autorizar a usuarios para que asignen un dispositivo .....	87
▼ Cómo ver la información de asignación de un dispositivo .....	88
▼ Asignación forzada de un dispositivo .....	88
▼ Desasignación forzada de un dispositivo .....	89
▼ Cómo cambiar los dispositivos que se pueden asignar .....	89
▼ Cómo auditar la asignación de dispositivos .....	90
Asignación de dispositivos (mapa de tareas) .....	91
Asignación de dispositivos .....	91
▼ Cómo asignar un dispositivo .....	91
▼ Cómo montar un dispositivo asignado .....	92
▼ Cómo desasignar un dispositivo .....	94
Protección de dispositivos (referencia) .....	95
Comandos de la política de dispositivos .....	95

Asignación de dispositivos .....	96
<b>5 Uso de la herramienta básica de creación de informes de auditoría (tareas) .....</b>	<b>105</b>
Herramienta básica de creación de informes de auditoría (descripción general) .....	105
Funciones de BART .....	106
Componentes de BART .....	106
Uso de BART (mapa de tareas) .....	108
Uso de BART (tareas) .....	109
Consideraciones de seguridad de BART .....	109
▼ Cómo crear un manifiesto .....	110
▼ Cómo personalizar un manifiesto .....	112
▼ Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo .....	115
▼ Cómo comparar manifiestos de diferentes sistemas .....	117
▼ Cómo personalizar un informe de BART especificando atributos de archivos .....	120
▼ Cómo personalizar un informe de BART mediante un archivo de reglas .....	121
Manifiestos, archivos de reglas e informes de BART (referencia) .....	122
Formato de archivo de manifiesto de BART .....	123
Formato de archivo de reglas de BART .....	124
Creación de informes de BART .....	125
<b>6 Control de acceso a archivos (tareas) .....</b>	<b>127</b>
Uso de permisos UNIX para proteger archivos .....	127
Comandos para visualizar y proteger archivos .....	127
Propiedad de archivos y directorios .....	128
Permisos de archivo UNIX .....	129
Permisos de archivo especiales (setuid, setgid y bit de permanencia) .....	129
Valor umask predeterminado .....	131
Modos de permiso de archivo .....	132
Uso de listas de control de acceso para proteger archivos UFS .....	134
Entradas de ACL para archivos UFS .....	135
Entradas de ACL para directorios UFS .....	136
Comandos para administrar ACL de UFS .....	136
Cómo impedir que los archivos ejecutables pongan en riesgo la seguridad .....	137
Protección de archivos (mapa de tareas) .....	138
Protección de archivos con permisos UNIX (mapa de tareas) .....	138

▼ Cómo visualizar información de archivos .....	138
▼ Cómo cambiar el propietario de un archivo local .....	139
▼ Cómo cambiar la propiedad de grupo de un archivo .....	140
▼ Cómo cambiar los permisos de archivo en modo simbólico .....	141
▼ Cómo cambiar permisos de archivo en modo absoluto .....	142
▼ Cómo cambiar permisos de archivo especiales en modo absoluto .....	143
Protección de archivos UFS con ACL (mapa de tareas) .....	144
▼ Cómo comprobar si un archivo tiene una ACL .....	144
▼ Cómo agregar entradas de ACL a un archivo .....	145
▼ Cómo copiar una ACL .....	147
▼ Cómo cambiar entradas de ACL en un archivo .....	147
▼ Cómo eliminar entradas de ACL de un archivo .....	148
▼ Cómo visualizar entradas de ACL de un archivo .....	148
Protección contra programas con riesgo de seguridad (mapa de tareas) .....	150
▼ Cómo buscar archivos con permisos de archivo especiales .....	150
▼ Cómo impedir que programas usen pilas ejecutables .....	151
<b>7 Uso de la herramienta automatizada de mejora de la seguridad (tareas) .....</b>	<b>153</b>
Herramienta automatizada de mejora de la seguridad (ASET) .....	153
Niveles de seguridad de ASET .....	154
Lista de tareas de ASET .....	155
Registro de ejecución de ASET .....	158
Informes de ASET .....	158
Archivos maestros de ASET .....	161
Archivo de entorno de ASET (asetenv) .....	162
Configuración de ASET .....	162
Restauración de archivos del sistema modificados por ASET .....	165
Operación de red con el sistema NFS .....	165
Variables de entorno de ASET .....	166
Ejemplos de archivos de ASET .....	170
Ejecución de ASET (mapa de tareas) .....	171
▼ Cómo ejecutar ASET interactivamente .....	172
▼ Cómo ejecutar ASET periódicamente .....	173
▼ Cómo detener la ejecución periódica de ASET .....	174
▼ Cómo recopilar informes de ASET en un servidor .....	174

Resolución de problemas de ASET .....	175
Mensajes de error de ASET .....	175
<b>Parte III Roles, perfiles de derechos y privilegios .....</b>	<b>179</b>
<b>8 Uso de roles y privilegios (descripción general) .....</b>	<b>181</b>
Novedades de RBAC .....	181
Control de acceso basado en roles (descripción general) .....	182
RBAC: una alternativa al modelo de superusuario .....	182
Elementos y conceptos básicos de RBAC en Oracle Solaris .....	184
Escalada de privilegios .....	188
Autorizaciones RBAC .....	188
Autorizaciones y privilegios .....	188
Aplicaciones con privilegios y RBAC .....	189
Perfiles de derechos de RBAC .....	190
Roles de RBAC .....	190
Shells de perfil y RBAC .....	192
Ámbito de servicio de nombres y RBAC .....	192
Consideraciones de seguridad al asignar directamente atributos de seguridad .....	192
Privilegios (descripción general) .....	193
Privilegios con protección de procesos del núcleo .....	193
Descripciones de privilegios .....	194
Diferencias administrativas en un sistema con privilegios .....	195
Privilegios y recursos del sistema .....	196
Cómo se implementan los privilegios .....	197
Cómo obtienen privilegios los procesos .....	198
Asignación de privilegios .....	199
Privilegios y dispositivos .....	201
Privilegios y depuración .....	202
<b>9 Uso del control de acceso basado en roles (tareas) .....</b>	<b>203</b>
Uso de RBAC (mapa de tareas) .....	203
Configuración de RBAC (mapa de tareas) .....	204
Configuración de RBAC .....	205



▼ Cómo planificar la implementación de RBAC .....	205
▼ Cómo crear y asignar un rol con la interfaz gráfica de usuario .....	207
▼ Cómo crear un rol desde la línea de comandos .....	210
▼ Cómo asignar un rol a un usuario local .....	213
▼ Cómo auditar roles .....	215
▼ Cómo convertir el usuario root en un rol .....	215
Uso de roles (mapa de tareas) .....	219
Uso de roles .....	219
▼ Cómo asumir un rol en una ventana de terminal .....	219
▼ Cómo asumir un rol en Solaris Management Console .....	222
Gestión de RBAC (mapa de tareas) .....	223
Gestión de RBAC .....	224
▼ Cómo cambiar la contraseña de un rol .....	224
▼ Cómo cambiar las propiedades de un rol .....	226
▼ Cómo crear o modificar un perfil de derechos .....	228
▼ Cómo cambiar las propiedades RBAC de un usuario .....	231
▼ Cómo agregar propiedades RBAC a las aplicaciones antiguas .....	233
<b>10 Control de acceso basado en roles (referencia) .....</b>	<b>237</b>
Contenido de los perfiles de derechos .....	237
Perfil de derechos de administrador principal .....	238
Perfil de derechos de administrador del sistema .....	239
Perfil de derechos de operador .....	239
Perfil de derechos de gestión de impresoras .....	240
Perfil de derechos de usuario de Solaris básico .....	240
Perfil de derechos "todos" .....	241
Orden de perfiles de derechos .....	241
Visualización del contenido de los perfiles de derechos .....	242
Denominación y delegación de autorizaciones .....	242
Convenciones de denominación de autorizaciones .....	242
Ejemplo de granularidad de autorizaciones .....	243
Autoridad de delegación en autorizaciones .....	243
Bases de datos que admiten RBAC .....	243
Relaciones entre bases de datos de RBAC .....	244
Bases de datos de RBAC y servicios de nombres .....	245

Base de datos user_attr .....	245
Base de datos auth_attr .....	246
Base de datos prof_attr .....	248
Base de datos exec_attr .....	249
Archivo policy.conf .....	250
Comandos de RBAC .....	251
Comandos que gestionan RBAC .....	251
Comandos que requieren autorizaciones .....	252
<b>11 Privilegios (tareas) .....</b>	<b>255</b>
Gestión y uso de privilegios (mapa de tareas) .....	255
Gestión de privilegios (mapa de tareas) .....	256
Gestión de privilegios .....	256
▼ Cómo determinar los privilegios de un proceso .....	256
▼ Cómo determinar los privilegios que necesita un programa .....	258
▼ Cómo agregar privilegios a un comando .....	260
▼ Cómo asignar privilegios a un usuario o rol .....	260
▼ Cómo limitar los privilegios de un usuario o rol .....	261
▼ Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios .....	263
Determinación de los privilegios (mapa de tareas) .....	264
Determinación de los privilegios asignados .....	264
▼ Cómo determinar los privilegios que se le asignaron directamente .....	265
▼ Cómo determinar los comandos con privilegios que puede ejecutar .....	266
▼ Cómo determinar los comandos con privilegios que puede ejecutar un rol .....	267
<b>12 Privilegios (referencia) .....</b>	<b>271</b>
Comandos administrativos para la gestión de privilegios .....	271
Archivos con información de privilegios .....	272
Privilegios y auditoría .....	273
Cómo evitar la escalada de privilegios .....	274
Aplicaciones antiguas y el modelo de privilegios .....	275

<b>Parte IV</b>	<b>Servicios criptográficos</b>	277
<b>13</b>	<b>Estructura criptográfica de Oracle Solaris (descripción general)</b>	279
	Novedades de la estructura criptográfica de Oracle Solaris	279
	Estructura criptográfica de Oracle Solaris	280
	Terminología de la estructura criptográfica de Oracle Solaris	281
	Ámbito de la estructura criptográfica de Oracle Solaris	282
	Comandos administrativos de la estructura criptográfica de Oracle Solaris	283
	Comandos de nivel de usuario de la estructura criptográfica de Oracle Solaris	283
	Firmas binarias para software de terceros	284
	Complementos de la estructura criptográfica de Oracle Solaris	284
	Zonas y servicios criptográficos	285
<b>14</b>	<b>Estructura criptográfica de Oracle Solaris (tareas)</b>	287
	Uso de la estructura criptográfica (mapa de tareas)	287
	Protección de archivos con la estructura criptográfica de Oracle Solaris (mapa de tareas)	288
	Protección de los archivos con la estructura criptográfica (tareas)	288
	▼ Cómo generar una clave simétrica con el comando <code>dd</code>	288
	▼ Cómo generar una clave simétrica con el comando <code>pktool</code>	290
	▼ Cómo calcular un resumen de un archivo	293
	▼ Cómo calcular un MAC de un archivo	295
	▼ Cómo cifrar y descifrar un archivo	296
	Administración de la estructura criptográfica (mapa de tareas)	299
	Administración de la estructura criptográfica (tareas)	299
	▼ Cómo mostrar los proveedores disponibles	300
	▼ Cómo agregar un proveedor de software	302
	▼ Cómo evitar el uso de un mecanismo de nivel de usuario	304
	▼ Cómo evitar el uso de un proveedor de software de núcleo	305
	▼ Cómo mostrar proveedores de hardware	308
	▼ Cómo deshabilitar funciones y mecanismos del proveedor de hardware	308
	▼ Cómo actualizar o reiniciar todos los servicios criptográficos	310
<b>15</b>	<b>Estructura de gestión de claves de Oracle Solaris</b>	313
	Administración de tecnologías de clave pública	313

Utilidades de la estructura de gestión de claves .....	314
Gestión de políticas KMF .....	314
Gestión de almacenes de claves KMF .....	315
Uso de la estructura de gestión de claves (mapa de tareas) .....	315
Uso de la estructura de gestión de claves (tareas) .....	316
▼ Cómo crear un certificado mediante el comando <code>pktool gencert</code> .....	316
▼ Cómo importar un certificado al almacén de claves .....	317
▼ Cómo exportar un certificado y una clave privada en formato PKCS #12 .....	318
▼ Cómo generar una frase de contraseña mediante el comando <code>pktool setpin</code> .....	320
<b>Parte V Servicios de autenticación y comunicación segura .....</b>	<b>321</b>
<b>16 Uso de servicios de autenticación (tareas) .....</b>	<b>323</b>
Descripción general de RPC segura .....	323
Servicios NFS y RPC segura .....	323
Cifrado DES con NFS seguro .....	324
Autenticación Kerberos .....	324
Autenticación Diffie-Hellman y RPC segura .....	324
Administración de RPC segura (mapa de tareas) .....	328
Administración de autenticación con RPC segura (tareas) .....	329
▼ Cómo reiniciar el servidor de claves RPC segura .....	329
▼ Cómo configurar una clave Diffie-Hellman para un host NIS+ .....	329
▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS+ .....	330
▼ Cómo configurar una clave Diffie-Hellman para un host NIS .....	331
▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS .....	332
▼ Cómo compartir archivos NFS con autenticación Diffie-Hellman .....	333
<b>17 Uso de PAM .....</b>	<b>335</b>
PAM (descripción general) .....	335
Ventajas del uso de PAM .....	335
Introducción a la estructura PAM .....	336
Cambios de PAM en Solaris 10 .....	337
PAM (tareas) .....	338
PAM (mapa de tareas) .....	339

Planificación de la implementación de PAM .....	339
▼ Cómo agregar un módulo PAM .....	340
▼ Cómo evitar el acceso de tipo .rhost desde sistemas remotos con PAM .....	341
▼ Cómo registrar los informes de errores de PAM .....	341
Configuración de PAM (referencia) .....	341
Sintaxis de archivo de configuración de PAM .....	342
Cómo funciona el apilamiento PAM .....	342
Ejemplo de apilamiento PAM .....	346
<b>18 Uso de SASL .....</b>	<b>349</b>
SASL (descripción general) .....	349
SASL (referencia) .....	350
Complementos de SASL .....	350
Variable de entorno de SASL .....	350
Opciones de SASL .....	351
<b>19 Uso de Oracle Solaris Secure Shell (tareas) .....</b>	<b>353</b>
Oracle Solaris Secure Shell (descripción general) .....	353
Autenticación de Oracle Solaris Secure Shell .....	354
Secure Shell en la empresa .....	356
Oracle Solaris Secure Shell y el proyecto OpenSSH .....	356
Oracle Solaris Secure Shell (mapa de tareas) .....	357
Configuración de Oracle Solaris Secure Shell (mapa de tareas) .....	358
Configuración de Oracle Solaris Secure Shell (tareas) .....	358
▼ Cómo configurar la autenticación basada en host para Secure Shell .....	358
▼ Cómo habilitar Secure Shell v1 .....	361
▼ Cómo configurar el reenvío del puerto en Secure Shell .....	361
Uso de Oracle Solaris Secure Shell (mapa de tareas) .....	362
Uso de Oracle Solaris Secure Shell (tareas) .....	363
▼ Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell .....	363
▼ Cómo cambiar la frase de contraseña de una clave privada de Secure Shell .....	365
▼ Cómo iniciar sesión en un host remoto con Secure Shell .....	366
▼ Cómo reducir indicadores de contraseñas en Secure Shell .....	367
▼ Cómo configurar el comando ssh-agent para que se ejecute automáticamente en el CDE .....	368

▼ Cómo utilizar el reenvío del puerto en Secure Shell .....	369
▼ Cómo copiar archivos con Secure Shell .....	371
▼ Cómo configurar conexiones predeterminadas a hosts fuera de un cortafuegos .....	372
<b>20 Oracle Solaris Secure Shell (referencia) .....</b>	<b>375</b>
Una sesión de Secure Shell típica .....	375
Características de la sesión en Secure Shell .....	376
Autenticación e intercambio de claves en Secure Shell .....	376
Ejecución de comandos y reenvío de datos en Secure Shell .....	377
Configuración de cliente y servidor en Secure Shell .....	378
Configuración de clientes en Secure Shell .....	378
Configuración de servidores en Secure Shell .....	378
Palabras clave en Secure Shell .....	378
Parámetros específicos de host Secure Shell .....	382
Secure Shell y variables de entorno de inicio de sesión .....	382
Mantenimiento de hosts conocidos en Secure Shell .....	383
Paquetes e inicialización de Secure Shell .....	384
Archivos de Secure Shell .....	384
Comandos de Secure Shell .....	387
<b>Parte VI Servicio Kerberos .....</b>	<b>391</b>
<b>21 Introducción al servicio Kerberos .....</b>	<b>393</b>
¿Qué es el servicio Kerberos? .....	393
Cómo funciona el servicio Kerberos .....	394
Autenticación inicial: el ticket de otorgamiento de tickets .....	395
Autenticaciones Kerberos posteriores .....	397
Aplicaciones remotas de Kerberos .....	398
Los principales de Kerberos .....	399
Dominios de Kerberos .....	399
Servidores Kerberos .....	400
Servicios de seguridad de Kerberos .....	401
Componentes de las distintas versiones de Kerberos .....	402
Componentes de Kerberos .....	402

Adiciones de Kerberos para la versión Solaris 10 5/08 .....	404
Adiciones de Kerberos para la versión Solaris 10 8/07 .....	404
Adiciones de Kerberos para la versión Solaris 10 6/06 .....	404
Mejoras de Kerberos en la versión Solaris 10 3/05 .....	405
Componentes de Kerberos en la versión Solaris 9 .....	407
Componentes SEAM 1.0.2 .....	407
Componentes de Kerberos en la versión Solaris 8 .....	408
Componentes SEAM 1.0.1 .....	408
Componentes SEAM 1.0 .....	409
<b>22 Planificación del servicio Kerberos .....</b>	<b>411</b>
¿Por qué planificar implementaciones Kerberos? .....	411
Planificación de dominios Kerberos .....	412
Nombres de dominio .....	412
Número de dominios .....	412
Jerarquía de dominios .....	413
Asignación de nombres de host en dominios .....	413
Nombres de principal de servicio y cliente .....	414
Puertos para KDC y servicios de administración .....	414
El número de KDC esclavos .....	415
Asignación de credenciales GSS a credenciales UNIX .....	416
Migración de usuario automática a dominio Kerberos .....	416
Qué sistema de propagación de base de datos se debe utilizar .....	417
Sincronización de reloj dentro de un dominio .....	417
Opciones de configuración de cliente .....	417
Mejora de seguridad de inicio de sesión de cliente .....	418
Opciones de configuración de KDC .....	418
Tipos de cifrado Kerberos .....	419
URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos .....	419
<b>23 Configuración del servicio Kerberos (tareas) .....</b>	<b>421</b>
Configuración del servicio Kerberos (mapa de tareas) .....	421
Configuración de servicios Kerberos adicionales (mapa de tareas) .....	422
Configuración de servidores KDC .....	423
▼ Cómo configurar manualmente un KDC maestro .....	423

▼ Cómo configurar un KDC para utilizar un servidor de datos LDAP .....	429
▼ Cómo configurar manualmente un KDC esclavo .....	437
▼ Cómo actualizar las claves del servicio de otorgamiento de tickets en un servidor maestro .....	440
Configuración de autenticación entre dominios .....	441
▼ Cómo establecer la autenticación entre dominios jerárquica .....	441
▼ Cómo establecer la autenticación entre dominios directa .....	442
Configuración de servidores de aplicaciones de red de Kerberos .....	444
▼ Cómo configurar un servidor de aplicaciones de red de Kerberos .....	444
Configuración de servidores NFS con Kerberos .....	446
▼ Cómo configurar servidores NFS con Kerberos .....	446
▼ Cómo crear una tabla de credenciales .....	448
▼ Cómo agregar una única entrada a la tabla de credenciales .....	448
▼ Cómo proporcionar asignación de credenciales entre dominios .....	449
▼ Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos ..	450
Configuración de clientes Kerberos .....	452
Configuración de clientes Kerberos (mapa de tareas) .....	452
▼ Cómo crear un perfil de instalación de cliente Kerberos .....	453
▼ Cómo configurar automáticamente un cliente Kerberos .....	454
▼ Cómo configurar interactivamente un cliente Kerberos .....	455
▼ Cómo configurar manualmente un cliente Kerberos .....	456
▼ Cómo deshabilitar la verificación del ticket de otorgamiento de tickets (TGT) .....	462
▼ Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario root .....	462
▼ Cómo configurar la migración automática de usuarios en un dominio Kerberos .....	464
Sincronización de relojes entre clientes Kerberos y KDC .....	466
Intercambio de un KDC maestro y un KDC esclavo .....	468
▼ Cómo configurar un KDC esclavo intercambiable .....	468
▼ Cómo intercambiar un KDC maestro y un KDC esclavo .....	468
Administración de la base de datos de Kerberos .....	473
Copia de seguridad y propagación de la base de datos de Kerberos .....	473
▼ Cómo realizar copias de seguridad de la base de datos de Kerberos .....	475
▼ Cómo restaurar la base de datos de Kerberos .....	476
▼ Cómo convertir una base de datos de Kerberos después de una actualización de servidor .....	476
▼ Cómo reconfigurar un KDC maestro para utilizar la propagación incremental .....	477



▼	Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental .....	479
▼	Cómo configurar un KDC esclavo para utilizar la propagación completa .....	480
▼	Cómo verificar que los servidores KDC estén sincronizados .....	484
▼	Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos .....	485
	Configuración de propagación en paralelo .....	486
	Pasos de configuración para la propagación en paralelo .....	486
	Administración del archivo intermedio .....	487
▼	Cómo eliminar un archivo intermedio .....	488
	Gestión de un KDC en un servidor de directorios LDAP .....	488
▼	Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos .....	488
▼	Cómo destruir un dominio en un servidor de directorios LDAP .....	489
	Aumento de la seguridad en servidores Kerberos .....	490
▼	Cómo habilitar sólo aplicaciones Kerberizadas .....	490
▼	Cómo restringir el acceso a servidores KDC .....	490
▼	Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas .....	491
<b>24</b>	<b>Mensajes de error y resolución de problemas de Kerberos .....</b>	<b>493</b>
	Mensajes de error de Kerberos .....	493
	Mensajes de error de la herramienta SEAM .....	493
	Mensajes de error comunes de Kerberos (A-M) .....	494
	Mensajes de error comunes de Kerberos (N-Z) .....	502
	Resolución de problemas de Kerberos .....	506
	Problemas con el formato del archivo <code>krb5.conf</code> .....	506
	Problemas al propagar la base de datos de Kerberos .....	506
	Problemas al montar un sistema de archivos NFS Kerberizado .....	507
	Problemas de autenticación como <code>root</code> .....	507
	Observación de asignación de credenciales GSS a credenciales UNIX .....	508
<b>25</b>	<b>Administración de las políticas y los principales de Kerberos (tareas) .....</b>	<b>509</b>
	Maneras de administrar las políticas y los principales de Kerberos .....	509
	Herramienta SEAM .....	510
	Equivalentes de línea de comandos de la herramienta SEAM .....	511
	El único archivo modificado por la herramienta SEAM .....	512
	Funciones de impresión y ayuda en pantalla de la herramienta SEAM .....	512

Trabajo con listas extensas en la herramienta SEAM .....	512
▼ Cómo iniciar la herramienta SEAM .....	513
Administración de los principales de Kerberos .....	514
Administración de los principales de Kerberos (mapa de tareas) .....	514
Automatización de la creación de nuevos principales de Kerberos .....	515
▼ Cómo ver la lista de los principales de Kerberos .....	516
▼ Cómo ver los atributos de un principal de Kerberos .....	518
▼ Cómo crear un nuevo principal de Kerberos .....	520
▼ Cómo duplicar un principal de Kerberos .....	523
▼ Cómo modificar un principal de Kerberos .....	523
▼ Cómo suprimir un principal de Kerberos .....	525
▼ Cómo configurar valores predeterminados para crear nuevos principales de Kerberos ..	525
▼ Cómo modificar los privilegios de administración de Kerberos .....	526
Administración de las políticas de Kerberos .....	528
Administración de las políticas de Kerberos (mapa de tareas) .....	528
▼ Cómo ver la lista de políticas de Kerberos .....	529
▼ Cómo ver los atributos de una política de Kerberos .....	531
▼ Cómo crear una nueva política de Kerberos .....	533
▼ Cómo duplicar una política de Kerberos .....	535
▼ Cómo modificar una política de Kerberos .....	535
▼ Cómo suprimir una política de Kerberos .....	536
Referencia de la herramienta SEAM .....	537
Descripción de los paneles de la herramienta SEAM .....	537
Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados .	540
Administración de los archivos keytab .....	542
Administración de archivos keytab (mapa de tareas) .....	543
▼ Cómo agregar un principal de servicio de Kerberos a un archivo keytab .....	543
▼ Cómo eliminar un principal de servicio de un archivo keytab .....	545
▼ Cómo visualizar la lista de claves (principales) en un archivo keytab .....	546
▼ Cómo deshabilitar temporalmente la autenticación de un servicio en un host .....	547
<b>26 Uso de aplicaciones Kerberos (tareas) .....</b>	<b>549</b>
Gestión de tickets de Kerberos .....	549
¿Debe preocuparse por los tickets? .....	549
Creación de un ticket de Kerberos .....	550

Visualización de tickets de Kerberos .....	551
Dstrucción de tickets de Kerberos .....	552
Gestión de contraseñas de Kerberos .....	553
Consejos para elegir una contraseña .....	553
Cambio de la contraseña .....	554
Otorgamiento de acceso a su cuenta .....	556
Comandos de usuario de Kerberos .....	558
Descripción general de comandos Kerberizados .....	558
Reenvío de tickets de Kerberos .....	561
Uso de comandos Kerberizados (ejemplos) .....	562
<b>27 El servicio Kerberos (referencia) .....</b>	<b>565</b>
Archivos de Kerberos .....	565
Comandos de Kerberos .....	567
Daemons de Kerberos .....	568
Terminología de Kerberos .....	569
Terminología específica de Kerberos .....	569
Terminología específica de la autenticación .....	569
Tipos de tickets .....	570
Cómo funciona el sistema de autenticación Kerberos .....	575
Cómo interactúa el servicio Kerberos con el DNS y el archivo <code>nsswitch.conf</code> .....	575
Obtención de acceso a un servicio con Kerberos .....	575
Obtención de una credencial para el servicio de otorgamiento de tickets .....	575
Obtención de una credencial para un servidor .....	577
Obtención de acceso a un servicio específico .....	578
Uso de los tipos de cifrado de Kerberos .....	579
Tabla de uso de <code>gsscred</code> .....	581
Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos .....	581
<b>Parte VII Auditoría de Oracle Solaris .....</b>	<b>583</b>
<b>28 Auditoría de Oracle Solaris (descripción general) .....</b>	<b>585</b>
¿Qué es la auditoría? .....	585
¿Cómo funciona la auditoría? .....	587

¿Cómo se relaciona la auditoría con la seguridad? .....	588
Conceptos y terminología de auditoría .....	588
Eventos de auditoría .....	590
Clases de auditoría y preselección .....	591
Registros de auditoría y tokens de auditoría .....	592
Módulos de complemento de auditoría .....	593
Registros de auditoría .....	593
Almacenamiento de la pista de auditoría .....	595
Examen de la pista de auditoría .....	595
Auditoría en un sistema con zonas de Oracle Solaris .....	596
Mejoras de la auditoría en la versión Solaris 10 .....	597
 <b>29 Planificación de la auditoría de Oracle Solaris</b> .....	 599
Planificación de auditoría de Oracle Solaris (mapa de tareas) .....	599
Planificación de la auditoría de Oracle Solaris (tareas) .....	600
▼ Cómo planificar auditoría en zonas .....	600
▼ Cómo planificar el almacenamiento para registros de auditoría .....	601
▼ Cómo planificar a quién y qué auditar .....	602
Determinación de política de auditoría .....	605
Políticas de auditoría para eventos síncronos y asíncronos .....	607
Control de costos de auditoría .....	609
Costo de mayor tiempo de procesamiento de datos de auditoría .....	609
Costo de análisis de datos de auditoría .....	609
Costo de almacenamiento de datos de auditoría .....	609
Auditoría eficaz .....	610
 <b>30 Gestión de la auditoría de Oracle Solaris (tareas)</b> .....	 613
Auditoría de Oracle Solaris (mapa de tareas) .....	613
Configuración de archivos de auditoría (mapa de tareas) .....	614
Configuración de archivos de auditoría (tareas) .....	615
▼ Cómo modificar el archivo audit_control .....	615
▼ Cómo configurar registros de auditoría syslog .....	617
▼ Cómo cambiar las características de auditoría de un usuario .....	620
▼ Cómo agregar un clase de auditoría .....	622
▼ Cómo cambiar una pertenencia a clase de un evento de auditoría .....	623

Configuración y habilitación del servicio de auditoría (mapa de tareas) .....	624
Configuración y habilitación del servicio de auditoría (tareas) .....	625
▼ Cómo crear particiones para los archivos de auditoría .....	625
▼ Cómo configurar el alias de correo electrónico audit_warn .....	629
▼ Cómo configurar la política de auditoría .....	629
▼ Cómo habilitar el servicio de auditoría .....	632
▼ Cómo deshabilitar el servicio de auditoría .....	634
▼ Cómo actualizar el servicio de auditoría .....	635
Configuración del servicio de auditoría en las zonas (tareas) .....	636
▼ Cómo configurar todas las zonas de forma idéntica para la auditoría .....	637
▼ Cómo configurar la auditoría por zona .....	639
Gestión de registros de auditoría (mapa de tareas) .....	640
Gestión de registros de auditoría .....	641
▼ Cómo visualizar formatos de registros de auditoría .....	641
▼ Cómo fusionar archivos de auditoría de la pista de auditoría .....	643
▼ Cómo seleccionar eventos de auditoría de la pista de auditoría .....	645
▼ Cómo visualizar el contenido de los archivos de auditoría binarios .....	647
▼ Cómo depurar un archivo de auditoría not_terminated .....	649
▼ Cómo evitar el desbordamiento de la pista de auditoría .....	650
Resolución de problemas de la auditoría de Oracle Solaris (tareas) .....	651
Resolución de problemas de la auditoría de Oracle Solaris (mapa de tareas) .....	651
▼ Cómo determinar que la auditoría de Oracle Solaris se está ejecutando .....	652
▼ Cómo reducir el volumen de los registros de auditoría que se producen .....	654
▼ Cómo auditar todos los comandos por usuarios .....	656
▼ Cómo buscar registros de auditoría de los cambios realizados en archivos específicos ....	658
▼ Cómo modificar una máscara de preselección de usuario .....	659
▼ Cómo evitar la auditoría de determinados eventos .....	661
▼ Cómo limitar el tamaño de los archivos de auditoría binarios .....	661
▼ Cómo auditar inicios de sesión de otros OSes .....	662
▼ Cómo auditar transferencias de archivos FTP y SFTP .....	662
<b>31 Auditoría de Oracle Solaris (referencia) .....</b>	<b>665</b>
Comandos de auditoría .....	665
Daemon auditd .....	666
Comando audit .....	667

Comando bsmrecord .....	667
Comando auditreduce .....	667
Comando praudit .....	669
Comando auditconfig .....	671
Archivos utilizados en el servicio de auditoría .....	671
Archivo system .....	672
Archivo syslog.conf .....	672
Archivo audit_class .....	672
Archivo audit_control .....	673
Archivo audit_event .....	674
Secuencia de comandos audit_startup .....	674
Base de datos audit_user .....	675
Secuencia de comandos audit_warn .....	676
Secuencia de comandos bsmconv .....	677
Perfiles de derechos para administración de auditoría .....	677
Auditoría y zonas de Oracle Solaris .....	678
Clases de auditoría .....	679
Definiciones de clases de auditoría .....	679
Sintaxis de la clase de auditoría .....	680
Complementos de auditoría .....	682
Política de auditoría .....	682
Características de auditoría de proceso .....	683
Pista de auditoría .....	683
Convenciones de nombres de archivos de auditoría binarios .....	684
Nombres de archivos de auditoría binarios .....	684
Indicadores de hora de archivos de auditoría binarios .....	685
Estructura de registro de auditoría .....	685
Análisis de registro de auditoría .....	686
Formatos de token de auditoría .....	686
Token acl .....	688
Token arbitrary (obsoleto) .....	688
Token arg .....	689
Token attribute .....	690
Token cmd .....	690
Token exec_args .....	691
Token exec_env .....	691

Token exit (obsoleto) .....	692
Token file .....	692
Token group (obsoleto) .....	692
Token groups .....	692
Token header .....	693
Token ip_addr .....	694
Token ip (obsoleto) .....	694
Token ipc .....	694
Token ipc_perm .....	695
Token iport .....	696
Token opaque (obsoleto) .....	696
Token path .....	696
Token path_attr .....	697
Token privilege .....	697
Token process .....	698
Token return .....	700
Token sequence .....	700
Token socket .....	701
Token subject .....	702
Token text .....	704
Token trailer .....	704
Token uauth .....	705
Token upriv .....	705
Token zonename .....	705
 <b>Glosario</b> .....	 707
 <b>Índice</b> .....	 719





# Prefacio

---

La *Guía de administración del sistema: servicios de seguridad* forma parte de un conjunto de varios volúmenes que tratan de manera exhaustiva la administración del Sistema operativo Oracle Solaris (Oracle Solaris). En esta guía, se da por sentado que ya instaló la versión actual y que configuró el software de red que tiene previsto usar. El Sistema operativo Oracle Solaris forma parte de la familia de productos Oracle Solaris, que incluye varias funciones, como Oracle Solaris Secure Shell.

---

**Nota** – Esta versión de Oracle Solaris es compatible con sistemas que usen arquitecturas de las familias de procesadores SPARC y x86. Los sistemas compatibles aparecen en *Listas de compatibilidad del sistema operativo Oracle Solaris*. Este documento indica las diferencias de implementación entre los tipos de plataforma.

En este documento, estos términos relacionados con x86 significan lo siguiente:

- x86 hace referencia a la familia más grande de productos compatibles con x86 de 64 y 32 bits.
- x64 hace referencia específicamente a CPU compatibles con x86 de 64 bits.
- 32-bit x86 destaca información específica de 32 bits acerca de sistemas basados en x86.

Para conocer cuáles son los sistemas admitidos, consulte [Listas de compatibilidad del sistema operativo Oracle Solaris](#).

---

## Usuarios a los que está destinada esta guía

Esta guía está dirigida a las personas responsables de administrar uno o varios sistemas que ejecutan Oracle Solaris. Para utilizar esta guía, se debe tener más de dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación sobre la administración de sistemas UNIX.

# Organización de las guías de administración del sistema

A continuación se enumeran los temas que abarcan las guías de administración del sistema.

Título de manual	Temas
<i>Guía de administración del sistema: administración básica</i>	Grupos y cuentas de usuario, asistencia para clientes y servidores, cierre e inicio de un sistema y administración de servicios
<i>Guía de administración del sistema: Administración avanzada</i>	Terminales y módems, recursos del sistema (cuotas de disco, cuentas y archivos crontab), procesos del sistema y resolución de problemas de software de Oracle Solaris
<i>System Administration Guide: Devices and File Systems</i>	Soportes extraíbles, discos y dispositivos, sistemas de archivos y copia de seguridad y restauración de datos
<i>Guía de administración del sistema: servicios IP</i>	Administración de redes TCP/IP, administración de direcciones IPv4 e IPv6, DHCP, IPsec, IKE, filtro IP, IP móvil, rutas múltiples de redes IP (IPMP) e IPQoS
<i>Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)</i>	Servicios de directorios y nombres DNS, NIS y LDAP, incluida la transición de NIS a LDAP y de NIS+ a LDAP
<i>System Administration Guide: Naming and Directory Services (NIS+)</i>	Servicios de directorios y nombres NIS+
<i>Guía de administración del sistema: servicios de red</i>	Servidores de caché web, servicios relacionados con el tiempo, sistemas de archivos de red (NFS y Autofs), correo, SLP y PPP
<i>System Administration Guide: Printing</i>	Tareas y temas de impresión, uso de servicios, herramientas, protocolos y tecnologías para configurar y administrar las impresoras y los servicios de impresión
<i>Guía de administración del sistema: servicios de seguridad</i>	Auditoría, administración de dispositivos, seguridad de archivos, BART, servicios Kerberos, PAM, estructura criptográfica de Oracle Solaris, privilegios, RBAC, SASL y Oracle Solaris Secure Shell
<i>Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris</i>	Tareas y proyectos de temas de gestión de recursos, contabilidad extendida, controles de recursos, planificación por reparto equitativo (FSS), control de memoria física utilizando el daemon de limitación de recursos (rcapd) y agrupaciones de recursos; virtualización con la tecnología de partición de software Zonas de Solaris y zonas con la marca lx
<i>Guía de administración de Oracle Solaris ZFS</i>	Creación y gestión de sistemas de archivos y agrupaciones de almacenamiento ZFS, instantáneas, clones, copias de seguridad, uso de listas de control de acceso (ACL) para proteger archivos ZFS, uso de ZFS en un sistema Oracle Solaris con zonas instaladas, volúmenes emulados, resolución de problemas y recuperación de datos

Título de manual	Temas
<i>Procedimientos de administradores de Oracle Solaris Trusted Extensions</i>	Administración de sistemas específica de un sistema Oracle Solaris Trusted Extensions
<i>Guía de configuración de Oracle Solaris Trusted Extensions</i>	A partir de la versión Solaris 10 5/08, se explica la forma de planificar, habilitar y configurar inicialmente la función Oracle Solaris Trusted Extensions

## Referencias relacionadas con el sitio web de otras empresas

En este documento, se proporcionan direcciones de Internet de terceros e información adicional relacionada.

Oracle no se hace responsable de la disponibilidad de los sitios web de terceros que se mencionen en este documento. Oracle no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles a través de dichos sitios o recursos. Oracle no será responsable de ningún daño o pérdida ocasionados o supuestamente ocasionados debido, directa o indirectamente, al uso de los contenidos, bienes o servicios disponibles en dichas sedes o a los que se pueda acceder a través de tales sedes o recursos.

## Acceso a Oracle Support

Los clientes de Oracle tienen acceso al soporte electrónico por medio de My Oracle Support. Para obtener información, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> o, si tiene alguna discapacidad auditiva, visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs>.

## Convenciones tipográficas

La siguiente tabla describe las convenciones tipográficas utilizadas en este manual.

TABLA P-1 Convenciones tipográficas

Tipos de letra	Significado	Ejemplo
AaBbCc123	Los nombres de los comandos, los archivos, los directorios y los resultados que el equipo muestra en pantalla	Edite el archivo <code>.login</code> .  Utilice el comando <code>ls -a</code> para mostrar todos los archivos.  <code>nombre_sistema%</code> tiene correo.
<b>AaBbCc123</b>	Lo que se escribe, en contraposición con la salida del equipo en pantalla	<code>nombre_sistema% su</code>  Contraseña:

TABLA P-1 Convenciones tipográficas (Continuación)		
Tipos de letra	Significado	Ejemplo
<i>aabbcc123</i>	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es <i>rm nombreachivo</i> .
<i>AaBbCc123</i>	Títulos de los manuales, términos nuevos y palabras destacables	Consulte el capítulo 6 de la <i>Guía del usuario</i> .  Una <i>copia en caché</i> es aquella que se almacena localmente.  <i>No</i> guarde el archivo.  <b>Nota:</b> Algunos elementos destacados aparecen en negrita en línea.

## Indicadores de los shells en los ejemplos de comandos

La tabla siguiente muestra los indicadores de sistema UNIX predeterminados y el indicador de superusuario de shells que se incluyen en los sistemas operativos Oracle Solaris. Tenga en cuenta que el indicador predeterminado del sistema que se muestra en los ejemplos de comandos varía según la versión de Oracle Solaris.

TABLA P-2 Indicadores de shell	
Shell	Indicador
Shell Bash, shell Korn y shell Bourne	\$
Shell Bash, shell Korn y shell Bourne para superusuario	#
Shell C	nombre_sistema%
Shell C para superusuario	nombre_sistema#

## P A R T E I

# Descripción general de la seguridad

Este manual se centra en las funciones que mejoran la seguridad en el Sistema operativo Oracle Solaris. El manual está pensado para administradores del sistema y usuarios de estas funciones de seguridad. El [Capítulo 1, “Servicios de seguridad \(descripción general\)”](#) presenta los temas que se tratarán en la guía.



## Servicios de seguridad (descripción general)

---

Para mantener la seguridad del Sistema operativo Oracle Solaris (SO Oracle Solaris), el software proporciona las siguientes funciones:

- “Seguridad del sistema” en la página 32: la capacidad para evitar la intrusión, proteger los recursos y dispositivos del equipo contra el uso inapropiado, y proteger los archivos contra la modificación maliciosa o involuntaria realizada por usuarios o intrusos.

Para ver una explicación de la seguridad del sistema local, consulte el [Capítulo 2, “Gestión de seguridad de equipos \(descripción general\)”](#).

- “Servicios criptográficos” en la página 33: la capacidad para codificar datos de manera que sólo el remitente y el receptor designado puedan leer el contenido, y para gestionar proveedores criptográficos y objetos de clave pública.
- “Servicios de autenticación” en la página 34: la capacidad para identificar a un usuario de manera segura, lo que requiere el nombre del usuario y alguna forma de prueba, normalmente, una contraseña.
- “Autenticación con cifrado” en la página 35: la capacidad para garantizar que las partes autenticadas se puedan comunicar sin interceptación, modificación ni falsificación.
- “Auditoría” en la página 35: la capacidad para identificar el origen de cambios de seguridad en el sistema, incluidos el acceso a archivos, las llamadas del sistema relacionadas con la seguridad y los errores de autenticación.
- “Política de seguridad” en la página 35: el diseño y la implementación de directrices de seguridad para un sistema o una red de sistemas.

# Seguridad del sistema

La seguridad del sistema garantiza que los recursos del sistema sean utilizados correctamente. Los controles de acceso pueden restringir quién tiene permitido el acceso a los recursos en el sistema. Entre las funciones de SO Oracle Solaris para la seguridad del sistema y el control de acceso, se incluyen:

- **Herramientas de administración de inicios de sesión:** comandos para supervisar y controlar la capacidad de un usuario para iniciar sesión. Consulte [“Protección de inicios de sesión y contraseñas \(mapa de tareas\)”](#) en la página 64.
- **Acceso a hardware:** comandos para limitar el acceso a la PROM y para restringir las personas que pueden iniciar el sistema. Consulte [“SPARC: control de acceso a hardware del sistema \(mapa de tareas\)”](#) en la página 79.
- **Acceso a recursos:** herramientas y estrategias para maximizar el uso adecuado de los recursos del equipo y, a la vez, minimizar el uso indebido de dichos recursos. Consulte [“Control de acceso a recursos del equipo”](#) en la página 50.
- **Control de acceso basado en roles (RBAC):** una arquitectura para crear cuentas de usuario restringidas especiales que tengan permitido realizar tareas administrativas específicas. Consulte [“Control de acceso basado en roles \(descripción general\)”](#) en la página 182.
- **Privilegios:** derechos discretos en procesos para realizar operaciones. Estos derechos de procesos se aplican en el núcleo. Consulte [“Privilegios \(descripción general\)”](#) en la página 193.
- **Gestión de dispositivos:** la *política* de dispositivos, además, protege los dispositivos que ya están protegidos con permisos UNIX. La *asignación* de dispositivos controla el acceso a dispositivos periféricos, como un micrófono o una unidad de CD-ROM. Al suprimir la asignación, las secuencias de comandos de limpieza de dispositivos pueden borrar datos del dispositivo. Consulte [“Control de acceso a dispositivos”](#) en la página 47.
- **Herramienta básica de creación de informes de auditoría (BART):** una instantánea, denominada *manifiesto*, de los atributos de archivo de los archivos en un sistema. Mediante la comparación de los manifiestos entre sistemas o en un sistema a lo largo del tiempo, se pueden supervisar cambios en los archivos a fin de reducir los riesgos de seguridad. Consulte el [Capítulo 5, “Uso de la herramienta básica de creación de informes de auditoría \(tareas\)”](#).
- **Permisos del archivo:** atributos de un archivo o directorio. Los permisos restringen los usuarios y grupos que tienen permiso para leer, escribir o ejecutar un archivo, o buscar en un directorio. Consulte el [Capítulo 6, “Control de acceso a archivos \(tareas\)”](#).
- **Secuencias de comandos para la mejora de la seguridad:** mediante el uso de secuencias de comandos, muchos parámetros y archivos del sistema se pueden ajustar para reducir los riesgos de seguridad. Consulte el [Capítulo 7, “Uso de la herramienta automatizada de mejora de la seguridad \(tareas\)”](#).



# Servicios criptográficos

La criptografía es la ciencia de cifrar y descifrar datos. La criptografía se utiliza para garantizar la integridad, la privacidad y la autenticidad. Integridad significa que los datos no han sido alterados. Privacidad significa que otros usuarios no pueden leer los datos. Autenticidad para datos significa que lo que se ha entregado es lo que se envió. Autenticación de usuario significa que el usuario ha suministrado una o más pruebas de identidad. Los mecanismos de autenticación verifican, matemáticamente, el origen de los datos o la prueba de la identidad. Los mecanismos de cifrado codifican datos, de manera que un observador casual no pueda leer los datos. Los servicios criptográficos proporcionan mecanismos de autenticación y cifrado para aplicaciones y usuarios.

Los algoritmos criptográficos utilizan el hashing, el encadenamiento y otras técnicas matemáticas para crear cifrados que son difíciles de descifrar. Los mecanismos de autenticación requieren que el destinatario y el remitente calculen un número idéntico de los datos. Los mecanismos de cifrado dependen de que el destinatario y el remitente compartan información sobre el método de cifrado. Esta información permite que sólo el receptor y el remitente descifren el mensaje. Oracle Solaris proporciona una estructura criptográfica centralizada y mecanismos de cifrado que están vinculados a aplicaciones particulares.

- **Estructura criptográfica de Oracle Solaris:** una estructura central de servicios criptográficos para consumidores en el nivel del núcleo y el nivel del usuario, que se basa en el siguiente estándar: Interfaz de señal criptográfica RSA Security Inc. PKCS #11 (Cryptoki). Utiliza contraseñas, IPsec y aplicaciones de terceros. La estructura centraliza fuentes de hardware y software para el cifrado. La biblioteca PKCS #11 proporciona una API para que los desarrolladores de terceros conecten los requisitos criptográficos para sus aplicaciones. Consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#).
- **Mecanismos de cifrado por aplicación:**
  - Para el uso de DES en RPC seguro, consulte [“Descripción general de RPC segura” en la página 323](#).
  - Para el uso de DES, 3DES, AES y ARCFOUR en el servicio Kerberos, consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).
  - Para el uso de RSA, DSA y cifrados, como Blowfish en Secure Shell, consulte el [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#).
  - Para el uso de algoritmos criptográficos en contraseñas, consulte [“Cambio del algoritmo de contraseña \(mapa de tareas\)” en la página 71](#).

A partir de la versión Solaris 10 8/07, la estructura de gestión de claves (KMF) proporciona una utilidad central para gestionar objetos de clave pública, incluidos las políticas, las claves y los certificados. KMF gestiona estos objetos para tecnologías de clave pública PKCS #11, NSS y OpenSSL. Consulte el [Capítulo 15, “Estructura de gestión de claves de Oracle Solaris”](#).

## Servicios de autenticación

La autenticación es un mecanismo que identifica a un usuario o un servicio según los criterios predefinidos. Los servicios de autenticación abarcan desde pares de nombre y contraseña simples hasta sistemas de desafío y respuesta más elaborados, por ejemplo, tarjetas de token y biometría. Los mecanismos de autenticación compleja dependen de que un usuario proporcione información que sólo él sepa y de que un dato personal se pueda verificar. Un nombre de usuario es un ejemplo de información que la persona sabe. Una tarjeta inteligente o una huella digital, por ejemplo, se pueden verificar. Entre las funciones de Oracle Solaris para autenticación, se incluyen:

- **RPC seguro:** un mecanismo de autenticación que utiliza el [protocolo de Diffie-Hellman](#) para proteger los montajes NFS y un servicio de nombres, como NIS o NIS+. Consulte [“Descripción general de RPC segura” en la página 323](#).
- **Módulo de autenticación conectable (PAM):** una estructura que permite que distintas tecnologías de autenticación se conecten en un servicio de entrada del sistema sin recompilar el servicio. Algunos de los servicios de entrada del sistema incluyen login y ftp. Consulte el [Capítulo 17, “Uso de PAM”](#).
- **Autenticación sencilla y capa de seguridad (SASL):** una estructura que proporciona servicios de autenticación y seguridad para protocolos de red. Consulte el [Capítulo 18, “Uso de SASL”](#).
- **Secure Shell:** un protocolo de inicio de sesión remoto seguro y transferencia que cifra comunicaciones en una red no segura. Consulte el [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#).
- **Servicio Kerberos:** una arquitectura de cliente y servidor que proporciona cifrado con autenticación. Consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).
- **Tarjeta inteligente de Solaris:** una tarjeta de plástico con un microprocesador y una memoria que se pueden usar con un lector de tarjetas para acceder a sistemas. Consulte la [Solaris Smartcard Administration Guide](#).

## Autenticación con cifrado

La autenticación con cifrado es la base de una comunicación segura. La autenticación ayuda a garantizar que el origen y el destino sean las partes deseadas. El cifrado codifica la comunicación en el origen y decodifica la comunicación en el destino. El cifrado impide que los intrusos puedan leer cualquier transmisión que logren interceptar. Entre las funciones de Oracle Solaris para la comunicación segura, se incluyen:

- **Secure Shell:** un protocolo para proteger transferencias de datos y sesiones de red de usuarios interactivos contra intrusiones, usurpaciones de sesión y ataques de tipo “Man-in-the-middle”. La autenticación compleja se proporciona mediante criptografía de clave pública. Los servicios de ventanas X y otros servicios de red se pueden enviar por túnel de manera segura mediante conexiones de Secure Shell para obtener una protección adicional. Consulte el [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#).
- **Servicio Kerberos:** una arquitectura de cliente y servidor que proporciona autenticación con cifrado. Consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).
- **Arquitectura de seguridad de protocolo de Internet (IPsec):** una arquitectura que proporciona protección de datagramas de IP. Las protecciones incluyen la confidencialidad, la integridad sólida de los datos, la autenticación de datos y la integridad de secuencia parcial. Consulte el [Capítulo 19, “Arquitectura de seguridad IP \(descripción general\)”](#) de *Guía de administración del sistema: servicios IP*.

## Auditoría

La auditoría es un concepto fundamental del mantenimiento y la seguridad del sistema. La auditoría es el proceso de examinar el historial de las acciones y los eventos en un sistema para determinar lo que ha sucedido. El historial se mantiene en un registro, donde se indica qué se hizo, cuándo se hizo, quién lo hizo y qué se afectó. Consulte el [Capítulo 28, “Auditoría de Oracle Solaris \(descripción general\)”](#).

## Política de seguridad

La política de seguridad de frases o [política](#) se utiliza en este manual para referirse a las instrucciones de seguridad de una organización. La política de seguridad de su sitio es el conjunto de reglas que definen la confidencialidad de la información que se está procesando y las medidas que se utilizan para proteger la información contra el acceso no autorizado. Las tecnologías de seguridad, como Secure Shell, autenticación, RBAC, autorización, privilegios y control de recursos, proporcionan medidas para proteger la información.

Algunas tecnologías de seguridad también utilizan la política de palabras cuando se describen aspectos específicos de su implementación. Por ejemplo, Oracle Solaris utiliza opciones de políticas de auditoría para configurar algunos aspectos de la política de auditoría. En la

siguiente tabla, se hace referencia al glosario, a las páginas del comando man y a información sobre las funciones que utilizan la política de palabras para describir aspectos específicos de su implementación.

TABLA 1-1    Uso de política en el SO Oracle Solaris

Definición del glosario	Páginas del comando man seleccionadas	Más información
política de auditoría	<code>audit_control(4)</code> , <code>audit_user(4)</code> , <code>auditconfig(1M)</code>	Capítulo 28, “Auditoría de Oracle Solaris (descripción general)”
política en la estructura criptográfica	<code>cryptoadm(1M)</code>	Capítulo 13, “Estructura criptográfica de Oracle Solaris (descripción general)”
política de dispositivos	<code>getdevpolicy(1M)</code>	“Control de acceso a dispositivos” en la página 47
política Kerberos	<code>krb5.conf(4)</code>	Capítulo 25, “Administración de las políticas y los principales de Kerberos (tareas)”
políticas de red	<code>ipfilter(5)</code> , <code>ifconfig(1M)</code> , <code>ike.config(4)</code> , <code>ipseccf(1M)</code> , <code>routeadm(1M)</code>	Parte IV, “Seguridad IP” de <i>Guía de administración del sistema: servicios IP</i>
política de contraseñas	<code>passwd(1)</code> , <code>nsswitch.conf(4)</code> , <code>crypt.conf(4)</code> , <code>policy.conf(4)</code>	“Mantenimiento del control de inicio de sesión” en la página 41
política para tecnologías de clave pública	<code>kmfcfg(1)</code>	Capítulo 15, “Estructura de gestión de claves de Oracle Solaris”
política RBAC	<code>rbac(5)</code> , <code>policy.conf(4)</code>	“Archivo <code>policy.conf</code> ” en la página 250

## P A R T E I I

# Seguridad de sistemas, archivos y dispositivos

En esta sección, se trata la seguridad que se puede configurar en un sistema que no está conectado a la red. En los capítulos, se discute sobre la planificación, la supervisión y el control del acceso al disco, a los archivos y a los dispositivos periféricos.

- Capítulo 2, “Gestión de seguridad de equipos (descripción general)”
- Capítulo 3, “Control de acceso a sistemas (tareas)”
- Capítulo 4, “Control de acceso a dispositivos (tareas)”
- Capítulo 5, “Uso de la herramienta básica de creación de informes de auditoría (tareas)”
- Capítulo 6, “Control de acceso a archivos (tareas)”
- Capítulo 7, “Uso de la herramienta automatizada de mejora de la seguridad (tareas)”



## Gestión de seguridad de equipos (descripción general)

---

Mantener protegida la información de un equipo constituye una responsabilidad importante de la administración del sistema. En este capítulo, se proporciona información general sobre la gestión de seguridad de equipos.

A continuación, se presenta la información general que se incluye en este capítulo.

- “Mejoras de la seguridad de equipos en la versión Solaris 10” en la página 39
- “Control de acceso a un sistema informático” en la página 40
- “Control de acceso a dispositivos” en la página 47
- “Control de acceso a recursos del equipo” en la página 50
- “Control de acceso a archivos” en la página 55
- “Control de acceso a la red” en la página 57
- “Comunicación de problemas de seguridad” en la página 62

### Mejoras de la seguridad de equipos en la versión Solaris 10

Desde la versión Solaris 9, se han agregado las siguientes funciones para mejorar la seguridad del sistema:

- El cifrado seguro de contraseña está disponible y se puede configurar. Para obtener más información, consulte “[Cifrado de contraseña](#)” en la página 43.
- La política de dispositivos se aplica con privilegios. Para obtener más información, consulte “[Política de dispositivos \(descripción general\)](#)” en la página 48.  
Para la asignación de dispositivos, es posible que versiones futuras de Oracle Solaris no admitan el directorio `/etc/security/dev`.
- La herramienta básica de creación de informes de auditoría (BART) puede supervisar la autenticidad de los archivos del sistema. Para obtener más información, consulte el [Capítulo 5, “Uso de la herramienta básica de creación de informes de auditoría \(tareas\)”](#).
- Los archivos pueden protegerse con el cifrado seguro. Para obtener más información, consulte “[Protección de archivos con cifrado](#)” en la página 55.

- Los privilegios aplican derechos de procesos en el nivel del núcleo. Para obtener más información, consulte [“Privilegios \(descripción general\)” en la página 193](#).
- La estructura criptográfica centraliza servicios criptográficos para proveedores y consumidores. Para obtener más información, consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#).
- La estructura PAM proporciona funcionalidad para muchos programas, como Secure Shell. Para obtener más información, consulte [“Cambios de PAM en Solaris 10” en la página 337](#).
- Acceso a los recursos del sistema para controlar la gestión de recursos y zonas de Oracle Solaris. Para obtener más información, consulte la [Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

## Control de acceso a un sistema informático

En el espacio de trabajo, todos los equipos conectados a un servidor pueden considerarse como un gran sistema multifacético. Usted es responsable de la seguridad de este sistema más grande. Debe proteger la red contra los desconocidos que intentan obtener acceso. También debe garantizar la integridad de los datos en los equipos de la red.

En el nivel de archivos, Oracle Solaris proporciona funciones de seguridad estándar que usted puede utilizar para proteger archivos, directorios y dispositivos. En los niveles de sistema y de red, los problemas de seguridad son generalmente los mismos. La primera línea de defensa de seguridad es controlar el acceso al sistema.

Puede controlar y supervisar el acceso al sistema con las siguientes medidas:

- [“Mantenimiento de la seguridad física” en la página 40](#)
- [“Mantenimiento del control de inicio de sesión” en la página 41](#)
- [“Control de acceso a dispositivos” en la página 47](#)
- [“Control de acceso a recursos del equipo” en la página 50](#)
- [“Control de acceso a archivos” en la página 55](#)
- [“Control de acceso a la red” en la página 57](#)
- [“Comunicación de problemas de seguridad” en la página 62](#)

## Mantenimiento de la seguridad física

Para controlar el acceso al sistema, debe mantener la seguridad física del entorno informático. Por ejemplo, un sistema cuya sesión está iniciada pero desatendida es vulnerable al acceso no autorizado. Un intruso puede obtener acceso al sistema operativo y a la red. El entorno y el hardware del equipo deben estar físicamente protegidos contra el acceso no autorizado.



Puede proteger un sistema SPARC contra el acceso no autorizado a la configuración de hardware. Utilice el comando `eeprom` para solicitar una contraseña para acceder a la PROM. Para obtener más información, consulte [“Cómo requerir una contraseña para el acceso al hardware” en la página 79](#).

## Mantenimiento del control de inicio de sesión

También debe prevenir los inicios de sesión no autorizados en un sistema o en la red. Puede realizar esto mediante la asignación de contraseñas o el control de inicios de sesión. Todas las cuentas de un sistema deben tener una contraseña. Una contraseña es un mecanismo de autenticación simple. Si una cuenta no tiene una contraseña, un intruso que adivina el nombre de un usuario puede acceder a toda la red. Un algoritmo de contraseña complejo protege contra ataques por fuerza bruta.

Cuando un usuario inicia sesión en un sistema, el comando `login` comprueba la base de datos adecuada del servicio de nombres o el servicio de directorios según la información que aparece en el archivo `/etc/nsswitch.conf`. Este archivo puede incluir las siguientes entradas:

- `files`: designa los archivos `/etc` en el sistema local
- `ldap`: designa el servicio de directorios LDAP en el servidor LDAP
- `nis`: designa la base de datos NIS en el servidor maestro NIS
- `nisplus`: designa la base de datos NIS+ en el servidor root NIS+

Para obtener una descripción del archivo `nsswitch.conf`, consulte la página del comando `man nsswitch.conf(4)`. Para obtener información sobre los servicios de nombres y los servicios de directorios, consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* o la *System Administration Guide: Naming and Directory Services (NIS+)*.

El comando `login` verifica el nombre de usuario y la contraseña proporcionados por el usuario. Si el nombre de usuario no está en el archivo de contraseñas, el comando `login` niega el acceso al sistema. Si la contraseña no es correcta para el nombre de usuario especificado, el comando `login` niega el acceso al sistema. Cuando el usuario proporciona un nombre de usuario válido y la contraseña correspondiente, se le otorga acceso al sistema.

Los módulos PAM pueden optimizar el inicio de sesión a las aplicaciones después de iniciar sesión correctamente en el sistema. Para obtener más información, consulte el [Capítulo 17, “Uso de PAM”](#).

Los sistemas Oracle Solaris disponen de mecanismos de autorización y autenticación sofisticados. Para ver una explicación de los mecanismos de autorización y autenticación en el nivel de red, consulte [“Autenticación y autorización para acceso remoto” en la página 58](#).

## Gestión de información de contraseñas

Cuando los usuarios inician sesión en un sistema, deben proporcionar un nombre de usuario y una contraseña. Aunque los nombres de usuario son de conocimiento público, las contraseñas deben mantenerse en secreto. Únicamente cada usuario individual debe conocer su contraseña. Debe solicitar a los usuarios que elijan sus contraseñas cuidadosamente. Los usuarios deben cambiar las contraseñas a menudo.

Las contraseñas se crean inicialmente al configurar una cuenta de usuario. Para mantener la seguridad de las cuentas de usuario, puede configurar la caducidad de las contraseñas para forzar a los usuarios a que cambien las contraseñas regularmente. También puede deshabilitar una cuenta de usuario mediante el bloqueo de la contraseña. Para obtener información detallada sobre la administración de contraseñas, consulte el [Capítulo 4, “Gestión de grupos y cuentas de usuario \(descripción general\)”](#) de *Guía de administración del sistema: administración básica* y la página del comando `passwd(1)`.

## Contraseñas locales

Si la red utiliza archivos locales para autenticar usuarios, la información de contraseñas se conserva en los archivos `/etc/passwd` y `/etc/shadow` del sistema. El nombre de usuario y otra información se conservan en el archivo `/etc/passwd`. La contraseña cifrada se conserva en un archivo *shadow* separado, `/etc/shadow`. Esta medida de seguridad impide que un usuario obtenga acceso a las contraseñas cifradas. Mientras que el archivo `/etc/passwd` está disponible para cualquier persona que pueda iniciar sesión en un sistema, únicamente un superusuario o un usuario con un rol equivalente puede leer el archivo `/etc/shadow`. Puede utilizar el comando `passwd` para cambiar la contraseña de un usuario en un sistema local.

## Contraseñas NIS y NIS+

Si la red utiliza NIS para autenticar a los usuarios, la información de contraseñas se conserva en el mapa de contraseñas NIS. NIS no admite la caducidad de las contraseñas. Puede utilizar el comando `passwd -r nis` para cambiar la contraseña de un usuario que está almacenada en un mapa de contraseñas NIS.

Si la red utiliza NIS+ para autenticar a los usuarios, la información de contraseñas se conserva en la base de datos NIS+. La información de la base de datos NIS+ se puede proteger mediante la restricción del acceso a los usuarios autorizados únicamente. Puede utilizar el comando `passwd -r nisplus` para cambiar la contraseña de un usuario que está almacenada en una base de datos NIS+.

## Contraseñas LDAP

El servicio de nombres LDAP de Oracle Solaris almacena información de contraseñas e información *shadow* en el contenedor `ou=people` del árbol de directorios LDAP. En el cliente del servicio de nombres LDAP de Oracle Solaris, puede utilizar el comando `passwd -r ldap` para cambiar la contraseña de un usuario. El servicio de nombres LDAP almacena la contraseña en el depósito LDAP.

La política de contraseñas se aplica en Sun Java System Directory Server. En concreto, el módulo `pam_ldap` del cliente sigue los controles de políticas de contraseña que se aplican en Sun Java System Directory Server. Para obtener más información, consulte [“Modelo de seguridad de servicios de nombres LDAP” de Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

## Cifrado de contraseña

El cifrado de contraseña seguro proporciona una barrera temprana contra un ataque. El software Oracle Solaris proporciona seis algoritmos de cifrado de contraseña. Los algoritmos [Blowfish](#), [MD5](#) y [SHA](#) proporcionan un cifrado de contraseña más sólido que el algoritmo UNIX.

## Identificadores de algoritmos de contraseña

Puede especificar la configuración de los algoritmos para su sitio en el archivo `/etc/security/policy.conf`. En el archivo `policy.conf`, los algoritmos se denominan según el identificador, como se muestra en la siguiente tabla. Para la asignación identificador-algoritmo, consulte el archivo `/etc/security/crypt.conf`.

TABLA 2-1 Algoritmos de cifrado de contraseña

Identificador	Descripción	Página del comando man de algoritmo
1	El algoritmo MD5 que es compatible con algoritmos MD5 en los sistemas BSD y Linux.	<a href="#">crypt_bsdmd5(5)</a>
2a	El algoritmo Blowfish que es compatible con el algoritmo Blowfish en los sistemas BSD.	<a href="#">crypt_bsdbf(5)</a>
md5	El algoritmo MD5 de Sun, que se considera más fuerte que la versión de MD5 de BSD y Linux.	<a href="#">crypt_sunmd5(5)</a>
5	El algoritmo SHA256. SHA es la sigla en inglés correspondiente al algoritmo de hash seguro. Este algoritmo es un miembro de la familia SHA-2. SHA256 admite contraseñas de 255 caracteres.	<a href="#">crypt_sha256(5)</a>
6	El algoritmo SHA512.	<a href="#">crypt_sha512(5)</a>
<code>__unix__</code>	El algoritmo de cifrado UNIX tradicional. Este algoritmo es el módulo predeterminado en el archivo <code>policy.conf</code> .	<a href="#">crypt_unix(5)</a>

## Configuración de algoritmos en el archivo `policy.conf`

A continuación, se muestra la configuración predeterminada de los algoritmos en el archivo `policy.conf`:

```
#
...
# crypt(3c) Algorithms Configuration
#
# CRYPT_ALGORITHMS_ALLOW specifies the algorithms that are allowed to
# be used for new passwords. This is enforced only in crypt_gensalt(3c).
#
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6

# To deprecate use of the traditional unix algorithm, uncomment below
# and change CRYPT_DEFAULT= to another algorithm. For example,
# CRYPT_DEFAULT=1 for BSD/Linux MD5.
#
#CRYPT_ALGORITHMS_DEPRECATE=__unix__

# The Solaris default is the traditional UNIX algorithm. This is not
# listed in crypt.conf(4) since it is internal to libc. The reserved
# name __unix__ is used to refer to it.
#
CRYPT_DEFAULT=__unix__
...
```

Al cambiar el valor para CRYPT\_DEFAULT, las contraseñas de los usuarios nuevos se cifran con el algoritmo que está asociado al valor nuevo.

Cuando los usuarios existentes cambian sus contraseñas, la manera en que se cifró la contraseña anterior afecta el algoritmo que se utiliza para cifrar la contraseña nueva. Por ejemplo, supongamos lo siguiente: CRYPT\_ALGORITHMS\_ALLOW=1,2a,md5,5,6 y CRYPT\_DEFAULT=1. La siguiente tabla muestra qué algoritmo se utilizaría para generar la contraseña cifrada.

Identificador = algoritmo de contraseña		
Contraseña inicial	Contraseña cambiada	Explicación
1 = crypt_bsmd5	Utiliza el mismo algoritmo	El identificador 1 también es el valor de CRYPT_DEFAULT. La contraseña del usuario se seguirá cifrando con el algoritmo crypt_bsmd5.
2a = crypt_bsdbf	Utiliza el mismo algoritmo	El identificador 2a está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_bsdbf.
md5 = crypt_md5	Utiliza el mismo algoritmo	El identificador md5 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_md5.
5 = crypt_sha256	Utiliza el mismo algoritmo	El identificador 5 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_sha256.
6 = crypt_sha512	Utiliza el mismo algoritmo	El identificador 6 está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, la contraseña nueva se cifra con el algoritmo crypt_sha512.

Identificador = algoritmo de contraseña		
Contraseña inicial	Contraseña cambiada	Explicación
__unix__ = crypt_unix	Utiliza el algoritmo crypt_bsdmd5	El identificador __unix__ no está en la lista CRYPT_ALGORITHMS_ALLOW. Por lo tanto, el algoritmo crypt_unix no se puede utilizar. La contraseña nueva se cifra con el algoritmo CRYPT_DEFAULT.

Para obtener más información sobre la configuración de las opciones de algoritmos, consulte la página del comando `man policy.conf(4)`. Para especificar algoritmos de cifrado de contraseña, consulte “[Cambio del algoritmo de contraseña \(mapa de tareas\)](#)” en la página 71.

## Cuentas especiales del sistema

La cuenta `root` es una de las diversas cuentas especiales del *sistema*. De estas cuentas, sólo a la cuenta `root` se le asigna una contraseña y se la puede utilizar para iniciar sesión. Con la cuenta `nuucp`, se puede iniciar sesión para realizar transferencias de archivos. Las otras cuentas del sistema sirven para proteger archivos o ejecutar procesos administrativos sin utilizar el poder total de `root`.



**Precaución** – Nunca cambie la configuración de contraseña de una cuenta del sistema. Una cuenta que tiene `NP` o `*LK*sys` en el segundo campo del archivo `shadow` indica una cuenta del sistema.

En la siguiente tabla, se muestran algunas cuentas del sistema junto con sus usos. Las cuentas del sistema realizan funciones especiales. Cada cuenta tiene un UID que es menor que 100.

TABLA 2-2 Cuentas del sistema y sus usos

Cuenta del sistema	GID	Uso
root	0	Prácticamente no tiene restricciones. Puede sustituir otros permisos y protecciones. La cuenta <code>root</code> tiene acceso a todo el sistema. La contraseña para el inicio de sesión de <code>root</code> debe estar protegida muy cuidadosamente. La cuenta <code>root</code> , superusuario, posee la mayoría de los comandos de Oracle Solaris.
daemon	1	Controla el procesamiento en segundo plano.
bin	2	Posee algunos de los comandos Oracle Solaris.
sys	3	Posee muchos archivos del sistema.
adm	4	Posee algunos archivos administrativos.
lp	71	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para la impresora.

TABLA 2-2 Cuentas del sistema y sus usos (Continuación)

Cuenta del sistema	GID	Uso
uucp	5	Posee los archivos de datos del objeto y los archivos de datos de cola de impresión para UUCP, el programa de copia de UNIX a UNIX.
nuucp	9	Utilizada por los sistemas remotos para iniciar sesión en el sistema e iniciar transferencias de archivos.

### Inicios de sesión remotos

Los inicios de sesión remotos ofrecen una vía tentadora para los intrusos. Oracle Solaris proporciona varios comandos para supervisar, limitar y deshabilitar los inicios de sesión remotos. Para conocer los procedimientos, consulte [“Protección de inicios de sesión y contraseñas \(mapa de tareas\)” en la página 64](#).

De manera predeterminada, con los inicios de sesión remotos, no se pueden controlar ni leer determinados dispositivos del sistema, como el mouse, el teclado, el búfer de trama o el dispositivo de audio. Para obtener más información, consulte la página del comando `man logindevperm(4)`.

### Inicios de sesión de acceso telefónico

Cuando se puede acceder a un equipo mediante un módem o un puerto de acceso telefónico, se puede agregar una capa adicional de seguridad. Se puede requerir una *contraseña de acceso telefónico* a los usuarios que acceden a un sistema mediante un módem o un puerto de acceso telefónico. Un usuario debe proporcionar esta contraseña adicional antes de que se le otorgue acceso al sistema.

Sólo los superusuarios pueden crear o cambiar una contraseña de acceso telefónico. Para garantizar la integridad del sistema, la contraseña se debe cambiar aproximadamente una vez al mes. El uso más eficaz de esta función es requerir una contraseña de acceso telefónico para obtener acceso a un sistema de puerta de enlace. Para configurar contraseñas de acceso telefónico, consulte [“Cómo crear una contraseña de marcación telefónica” en la página 69](#).

Para crear una contraseña de acceso telefónico, se utilizan dos archivos: `/etc/dialups` y `/etc/d_passwd`. El archivo `dialups` contiene una lista de puertos que requieren una contraseña de acceso telefónico. El archivo `d_passwd` contiene una lista de programas de shell que requieren una contraseña cifrada como contraseña adicional de acceso telefónico. La información de estos dos archivos se procesa de la siguiente manera:

- Si el shell de inicio de sesión del usuario en `/etc/passwd` coincide con una entrada en `/etc/d_passwd`, el usuario debe proporcionar una contraseña de acceso telefónico.
- Si el shell de inicio de sesión del usuario en `/etc/passwd` no se encuentra en `/etc/d_passwd`, el usuario debe proporcionar la contraseña predeterminada. La contraseña predeterminada es la entrada para `/usr/bin/sh`.

- Si el campo de shell de inicio de sesión en `/etc/passwd` está vacío, el usuario debe suministrar la contraseña predeterminada. La contraseña predeterminada es la entrada para `/usr/bin/sh`.
- Si `/etc/d_passwd` no tiene ninguna entrada para `/usr/bin/sh`, a los usuarios cuyo campo de shell de inicio de sesión en `/etc/passwd` está vacío o no coincide con ninguna entrada en `/etc/d_passwd` no se les solicitará una contraseña de acceso telefónico.
- Los inicios de sesión de acceso telefónico se deshabilitan si `/etc/d_passwd` tiene la entrada `/usr/bin/sh:*`: únicamente.

## Control de acceso a dispositivos

Los dispositivos periféricos conectados a un sistema informático presentan un riesgo de seguridad. Los micrófonos pueden captar conversaciones y transmitirlos a sistemas remotos. Los CD-ROM pueden dejar evidencia de información que el siguiente usuario del dispositivo de CD-ROM podrá leer. Se puede acceder a las impresoras de forma remota. Los dispositivos que son una parte integral del sistema también pueden presentar problemas de seguridad. Por ejemplo, las interfaces de red, como `hme0`, se consideran dispositivos integrales.

El software Oracle Solaris proporciona dos métodos de control de acceso a los dispositivos. La *política de dispositivos* restringe o impide el acceso a los dispositivos que son una parte integral del sistema. La política de dispositivos se aplica en el núcleo. La *asignación de dispositivos* restringe o impide el acceso a los dispositivos periféricos. La asignación de dispositivos se aplica en el momento de la asignación de usuarios.

La política de dispositivos utiliza privilegios para proteger dispositivos seleccionados en el núcleo. Por ejemplo, la política de dispositivos en las interfaces de red, como `hme`, requiere todos los privilegios de lectura o escritura.

La asignación de dispositivos utiliza autorizaciones para proteger dispositivos periféricos, como impresoras o micrófonos. De manera predeterminada, la asignación de dispositivos está deshabilitada. Una vez habilitada, la asignación de dispositivos puede configurarse para impedir el uso de un dispositivo o para requerir autorización para acceder al dispositivo. Cuando un dispositivo está asignado para su uso, ningún otro usuario puede acceder al dispositivo hasta que el usuario actual lo desasigne.

Un sistema Oracle Solaris puede configurarse en varias áreas para controlar el acceso a los dispositivos:

- **Configurar política de dispositivos:** en Oracle Solaris, puede requerir que el proceso que accede a un dispositivo determinado se esté ejecutando con un conjunto de privilegios. Los procesos sin estos privilegios no pueden utilizar el dispositivo. En el momento del inicio, el software Oracle Solaris configura la política de dispositivos. Los controladores de terceros se pueden configurar con la política de dispositivos durante la instalación. Después de la instalación, usted, como administrador, puede agregar la política de dispositivos a un dispositivo.
- **Permitir la asignación de dispositivos:** al habilitar la asignación de dispositivos, puede restringir el uso de un dispositivo a un usuario a la vez. Además, puede exigir que el usuario cumpla con algunos requisitos de seguridad. Por ejemplo, puede exigir que el usuario esté autorizado para utilizar el dispositivo.
- **Impedir que se utilicen los dispositivos:** puede impedir que cualquier usuario de un sistema informático utilice un dispositivo, como un micrófono. Un quiosco informático puede ser una buena opción para evitar que se utilicen determinados dispositivos.
- **Restringir un dispositivo a una zona determinada:** puede asignar el uso de un dispositivo a una zona no global. Para obtener más información, consulte [“Uso de dispositivos en zonas no globales”](#) de *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris*. Para obtener una explicación general de dispositivos y zonas, consulte [“Dispositivos configurados en zonas”](#) de *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris*.

## Política de dispositivos (descripción general)

El mecanismo de política de dispositivos permite especificar que los procesos que abran un dispositivo requieren determinados privilegios. Únicamente los procesos que se ejecutan con los privilegios especificados por la política de dispositivos pueden acceder a los dispositivos que están protegidos mediante la política de dispositivos. Oracle Solaris proporciona la política de dispositivos predeterminada. Por ejemplo, las interfaces de red, como `hme0`, requieren que los procesos que acceden a la interfaz se ejecuten con el privilegio `net_rawaccess`. El requisito se aplica en el núcleo. Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)”](#) en la página 193.

En versiones anteriores, los nodos de dispositivos estaban protegidos mediante permisos de archivo únicamente. Por ejemplo, sólo los miembros del grupo `sys` podían abrir los dispositivos que pertenecían al grupo `sys`. Ahora, los permisos de archivo no predicen quién puede abrir un dispositivo. En cambio, los dispositivos están protegidos mediante permisos de archivo y la política de dispositivos. Por ejemplo, el archivo `/dev/ip` tiene 666. Sin embargo, únicamente un proceso con los privilegios adecuados puede abrir el dispositivo.



La configuración de la política de dispositivos se puede auditar. El evento de auditoría AUE\_MODDEVPLCY registra los cambios en la política de dispositivos.

Para obtener más información sobre la política de dispositivos, consulte lo siguiente:

- [“Configuración de política de dispositivos \(mapa de tareas\)” en la página 82](#)
- [“Comandos de la política de dispositivos” en la página 95](#)
- [“Privilegios y dispositivos” en la página 201](#)

## Asignación de dispositivos (descripción general)

El mecanismo de asignación de dispositivos permite restringir el acceso a un dispositivo periférico, como un CD-ROM. El mecanismo se gestiona localmente. Si la asignación de dispositivos no está habilitada, los dispositivos periféricos se protegen únicamente mediante permisos de archivo. Por ejemplo, de manera predeterminada, los dispositivos periféricos están disponibles para los siguientes usos:

- Cualquier usuario puede leer y escribir en un disquete o CD-ROM.
- Cualquier usuario puede conectar un micrófono.
- Cualquier usuario puede acceder a una impresora conectada.

La asignación de dispositivos puede restringir un dispositivo a usuarios autorizados. La asignación de dispositivos también puede impedir que se acceda a un dispositivo en todo momento. Un usuario que asigna un dispositivo tiene el uso exclusivo de ese dispositivo hasta que lo desasigne. Cuando se desasigna un dispositivo, las secuencias de comandos device-clean borran los datos restantes. Puede escribir una secuencia de comandos device-clean para depurar la información de los dispositivos que no tienen una secuencia de comandos. Para ver un ejemplo, consulte [“Redacción de secuencias nuevas de comandos device-clean” en la página 103](#).

Se pueden auditar los intentos de asignación de un dispositivo, desasignación de un dispositivo y enumeración de los dispositivos asignables. Los eventos de auditoría forman parte de la clase de auditoría other.

Para obtener más información sobre la asignación de dispositivos, consulte lo siguiente:

- [“Gestión de asignación de dispositivos \(mapa de tareas\)” en la página 85](#)
- [“Asignación de dispositivos” en la página 96](#)
- [“Comandos de asignación de dispositivos” en la página 97](#)

## Control de acceso a recursos del equipo

Como administrador del sistema, usted puede controlar y supervisar la actividad del sistema. Puede definir límites sobre quién puede utilizar determinados recursos. Puede registrar el uso de recursos y supervisar quién los está utilizando. También puede configurar los sistemas para minimizar el uso indebido de los recursos.

### Limitación y supervisión del superusuario

El sistema requiere una contraseña root para el acceso del superusuario. En la configuración predeterminada, un usuario no puede iniciar sesión de manera remota en un sistema como root. Al iniciar sesión de manera remota, el usuario debe utilizar el nombre de usuario y, luego, el comando su para convertirse en root. Puede supervisar quién ha utilizado el comando su, en especial, aquellos usuarios que están intentando obtener acceso de superusuario. Para conocer los procedimientos para supervisar al superusuario y limitar el acceso al superusuario, consulte [“Supervisión y restricción de superusuario \(mapa de tareas\)” en la página 76.](#)

### Configuración del control de acceso basado en roles para reemplazar al superusuario

El control de acceso basado en roles (RBAC) está diseñado para limitar las capacidades del superusuario. El superusuario (usuario root) tiene acceso a todos los recursos del sistema. Con RBAC, puede reemplazar root con un conjunto de roles con poderes discretos. Por ejemplo, puede configurar un rol para manejar la creación de cuentas de usuario y otro rol para manejar la modificación de archivos del sistema. Una vez que haya establecido un rol para manejar una función o un conjunto de funciones, puede eliminar esas funciones de las capacidades de root.

Cada rol requiere que un usuario conocido inicie sesión con su nombre de usuario y contraseña. Después de iniciar sesión, el usuario asume el rol con una contraseña de rol específica. Como consecuencia, alguien que se entera de la contraseña root tiene una capacidad limitada para dañar el sistema. Para obtener más información sobre RBAC, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 182.](#)

## Prevención del uso indebido involuntario de los recursos del equipo

Puede prevenir que los usuarios y que usted realicen errores involuntarios de las siguientes formas:

- Puede evitar ejecutar un caballo de Troya si configura correctamente la variable PATH.
- Puede asignar un shell restringido a los usuarios. Un shell restringido previene los errores del usuario al guiar a los usuarios a las partes del sistema que necesitan para su trabajo. De hecho, mediante una configuración cuidadosa, usted puede asegurarse de que los usuarios sólo accedan a las partes del sistema que los ayudan a trabajar de manera eficiente.
- Puede establecer permisos restrictivos para los archivos a los que los usuarios no necesitan acceder.

### Configuración de la variable PATH

Debe asegurarse de configurar correctamente la variable PATH. De lo contrario, puede ejecutar accidentalmente un programa introducido por otra persona. El programa intruso puede dañar los datos o el sistema. Este tipo de programa, que crea un riesgo de seguridad, se conoce como *caballo de Troya*. Por ejemplo, es posible que se coloque un programa su sustituto en un directorio público y que usted, como administrador del sistema, ejecute el programa sustituto. Esa secuencia de comandos sería igual que el comando su habitual. Debido a que la secuencia de comandos se elimina sola después de la ejecución, habría pocas pruebas para mostrar que, en realidad, se ejecutó un caballo de Troya.

La variable PATH se configura automáticamente en el momento del inicio de sesión. La ruta se define con los archivos de inicio: `.login`, `.profile` y `.cshrc`. Si configura la ruta de búsqueda del usuario para que el directorio actual (`.`) esté en último lugar, estará protegido contra la ejecución de este tipo de caballo de Troya. La variable PATH para el superusuario no debe incluir el directorio actual.

La herramienta automatizada de mejora de la seguridad (ASET, Automated Security Enhancement Tool) examina los archivos de inicio para garantizar que la variable PATH esté configurada correctamente. ASET también garantiza que la variable PATH no contenga una entrada con un punto (`.`).

### Asignación de un shell restringido a los usuarios

El shell estándar permite que un usuario abra archivos, ejecute comandos, etc. El shell restringido limita la capacidad de un usuario para cambiar directorios y para ejecutar comandos. El shell restringido se invoca con el comando `/usr/lib/rsh`. Tenga en cuenta que el shell restringido no es el shell remoto, que es `/usr/sbin/rsh`.

El shell restringido se diferencia de un shell estándar de las siguientes formas:

- El usuario está limitado al directorio principal del usuario, de modo que no puede utilizar el comando `cd` para cambiar de directorios. Por lo tanto, el usuario no puede examinar los archivos del sistema.
- El usuario no puede cambiar la variable `PATH`, de manera que sólo puede utilizar comandos en la ruta definida por el administrador del sistema. El usuario tampoco puede ejecutar comandos o secuencias de comandos mediante un nombre completo de ruta.
- El usuario no puede redirigir la salida con `>` o `>>`.

El shell restringido permite limitar la capacidad de un usuario para desviarse hacia los archivos del sistema. El shell crea un entorno limitado para un usuario que necesita realizar tareas específicas. Sin embargo, el shell restringido no es completamente seguro y sólo tiene el propósito de impedir que los usuarios sin experiencia causen daños involuntariamente.

Para obtener información sobre el shell restringido, use el comando `man -s 1m rsh` para ver la página del comando `man rsh(1M)`.

## Restricción de acceso a datos de archivos

Dado que Oracle Solaris es un entorno multiusuario, la seguridad del sistema de archivos es el riesgo de seguridad más básico de un sistema. Puede utilizar las protecciones de archivos UNIX tradicionales para proteger los archivos. También puede utilizar las listas de control de acceso (ACL) más seguras.

Posiblemente desee permitir que algunos usuarios lean determinados archivos y conceder a otros usuarios permiso para cambiar o eliminar archivos. Es posible que existan datos que no desee que nadie más vea. En el [Capítulo 6, “Control de acceso a archivos \(tareas\)”](#), se describe cómo establecer permisos de archivo.

## Restricción de archivos ejecutables `setuid`

Los archivos ejecutables pueden constituir riesgos para la seguridad. Muchos programas ejecutables deben ejecutarse como `root`, es decir, como superusuario, para que funcionen correctamente. Estos programas `setuid` se ejecutan con el ID de usuario establecido en `0`. Cualquier persona que ejecuta estos programas lo hace con el ID `root`. Un programa que se ejecuta con el ID `root` crea un posible problema de seguridad si el programa no se escribió pensando en la seguridad.

Excepto para los ejecutables que Oracle envía con el bit `setuid` establecido en `root`, debe prohibir el uso de programas `setuid`. Si no puede prohibir el uso de programas `setuid`, debe restringir su uso. Una administración segura requiere pocos programas `setuid`.

Para obtener más información, consulte [“Cómo impedir que los archivos ejecutables pongan en riesgo la seguridad” en la página 137](#). Para ver los procedimientos, consulte [“Protección contra programas con riesgo de seguridad \(mapa de tareas\)” en la página 150](#).

## Uso de la herramienta automatizada de mejora de la seguridad

El paquete de seguridad ASET proporciona herramientas de administración automatizadas que permiten controlar y supervisar la seguridad del sistema. ASET proporciona tres niveles de seguridad: bajo, medio y alto. Usted especifica un nivel de seguridad de ASET. En cada nivel superior, las funciones de control de archivos de ASET aumentan para reducir el acceso a los archivos y reforzar la seguridad del sistema. Para obtener más información, consulte el [Capítulo 7, “Uso de la herramienta automatizada de mejora de la seguridad \(tareas\)”](#).

## Uso de Oracle Solaris Security Toolkit

Aunque ASET puede utilizarse para realizar un pequeño número de cambios de seguridad en un sistema, Oracle Solaris Security Toolkit proporciona un mecanismo flexible y extensible para minimizar, reforzar y proteger un sistema Oracle Solaris. Oracle Solaris Security Toolkit, conocido informalmente como kit de herramientas JASS, permite que el usuario realice modificaciones de seguridad en un sistema. La herramienta puede proporcionar un informe sobre el estado de seguridad de un sistema Oracle Solaris. La herramienta también tiene la capacidad para deshacer ejecuciones anteriores de la herramienta. El kit de herramientas JASS se puede descargar de [Oracle and Sun \(http://www.oracle.com/us/sun/index.htm\)](http://www.oracle.com/us/sun/index.htm). Haga clic en Sun Downloads: A-Z listing (Descargas de Sun: listado de la A a la Z) y, a continuación, busque la cadena Solaris Security Toolkit en el listado de descargas que aparece en orden alfabético.

El kit de herramientas se describe detalladamente en *Securing Systems with the Solaris Security Toolkit (Protección de sistemas con Solaris Security Toolkit)*, por Alex Noordergraaf y Glenn Brunette, ISBN 0-13-141071-7, junio de 2003. El manual forma parte de la serie Sun BluePrints, publicada por Sun Microsystems Press.

## Uso de la configuración de seguridad predeterminada

De manera predeterminada, cuando se instala la versión Solaris 10, se habilita un conjunto amplio de servicios de red. Para limitar la conectividad de red de un sistema, ejecute el comando `netservices limited`. Este comando activa una configuración de seguridad predeterminada (SBD). Con SBD, el único servicio de red que acepta solicitudes de red es el daemon `sshd`. Todos los demás servicios de red están deshabilitados o solamente manejan solicitudes locales. Puede habilitar servicios de red individuales, como `ftp`, con la utilidad de gestión de servicios (SMF). Para obtener más información, consulte las páginas del comando `man netservices(1M)` y `smf(5)`.

## Uso de funciones de gestión de recursos

El software Oracle Solaris ofrece funciones de gestión de recursos. Con estas funciones, usted puede asignar, programar, supervisar y limitar el uso de recursos por parte de aplicaciones en un entorno de consolidación de servidores. La estructura de control de recursos permite establecer restricciones a los recursos del sistema consumidos por los procesos. Estas restricciones ayudan a prevenir ataques de denegación del servicio por parte de una secuencia de comandos que intenta colapsar los recursos del sistema.

Con las funciones de gestión de recursos de Oracle Solaris, usted puede designar recursos para proyectos determinados. También puede adaptar dinámicamente los recursos disponibles. Para obtener más información, consulte la [Parte I, “Gestión de recursos” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

## Uso de zonas de Oracle Solaris

Las zonas de Oracle Solaris proporcionan un entorno de ejecución de aplicaciones en el que los procesos están aislados del resto del sistema dentro de una única instancia del SO Oracle Solaris. Este aislamiento evita que los procesos que se están ejecutando en una zona supervisen o afecten los procesos que se están ejecutando en otras zonas. Incluso un proceso que se está ejecutando con capacidades de superusuario no puede ver ni afectar la actividad de otras zonas.

Las zonas de Oracle Solaris son ideales para entornos que tienen varias aplicaciones en un único servidor. Para obtener más información, consulte la [Parte II, “Zonas” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

## Supervisión del uso de los recursos del equipo

Como administrador del sistema, debe supervisar la actividad del sistema. Debe conocer todos los aspectos de los equipos, incluidos los siguientes:

- ¿Cuál es la carga normal?
- ¿Quién tiene acceso al sistema?
- ¿Cuándo acceden los usuarios al sistema?
- ¿Qué programas se ejecutan generalmente en el sistema?

Con este tipo de conocimiento, puede utilizar las herramientas disponibles para auditar el uso del sistema y supervisar las actividades de usuarios individuales. La supervisión es muy útil cuando se sospecha que existe una infracción de seguridad. Para obtener más información sobre el servicio de auditoría, consulte el [Capítulo 28, “Auditoría de Oracle Solaris \(descripción general\)”](#).

## Supervisión de la integridad de archivos

Como administrador del sistema, debe garantizar que los archivos instalados en los sistemas que administra no hayan cambiado de manera inesperada. En las instalaciones de gran tamaño, una herramienta de comparación y elaboración de informes sobre la pila de software en cada uno de los sistemas permite realizar un seguimiento de los sistemas. La herramienta básica de creación de informes de auditoría (BART) permite validar exhaustivamente los sistemas mediante comprobaciones en el nivel de archivos de uno o varios sistemas a lo largo del tiempo. Los cambios en un *manifiesto* BART en varios sistemas, o en un sistema a lo largo del tiempo, pueden validar la integridad de los sistemas. BART permite crear y comparar manifiestos, y proporciona reglas para los informes de secuencias de comandos. Para obtener más información, consulte el [Capítulo 5, “Uso de la herramienta básica de creación de informes de auditoría \(tarear\)”](#).

## Control de acceso a archivos

Oracle Solaris es un entorno multiusuario. En un entorno multiusuario, todos los usuarios que iniciaron sesión en un sistema pueden leer los archivos que pertenecen a otros usuarios. Con los permisos de archivo adecuados, los usuarios también pueden utilizar archivos que pertenecen a otros usuarios. Para obtener más información, consulte el [Capítulo 6, “Control de acceso a archivos \(tarear\)”](#). Para obtener instrucciones paso a paso sobre cómo configurar permisos adecuados en los archivos, consulte [“Protección de archivos \(mapa de tareas\)”](#) en la página 138.

## Protección de archivos con cifrado

Para mantener un archivo seguro, puede impedir que otros usuarios accedan a él. Por ejemplo, nadie puede leer un archivo con permisos de `600`, excepto el propietario y el superusuario. De manera similar, un directorio con permisos de `700` es inaccesible. Sin embargo, alguien que adivine su contraseña o que descubra la contraseña `root` puede acceder a ese archivo. Además, el archivo inaccesible se conserva en una cinta de copia de seguridad cada vez que se realiza una copia de seguridad de los archivos del sistema en medios sin conexión.

La estructura criptográfica proporciona los comandos `digest`, `mac` y `encrypt` para proteger los archivos. Para obtener más información, consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#).

## Uso de listas de control de acceso

Las ACL pueden proporcionar un mayor control de los permisos de archivo. Puede agregar ACL cuando las protecciones de archivos UNIX tradicionales no son suficientes. Las protecciones de archivos UNIX tradicionales proporcionan permisos de lectura, escritura y ejecución para las tres clases de usuarios: propietario, grupo y otros usuarios. Una ACL proporciona un nivel de seguridad de archivos más específico.

Las ACL permiten definir los siguientes permisos de archivo:

- Permisos de propietario de archivo
- Permisos de archivo para el grupo del propietario
- Permisos de archivo para otros usuarios que están fuera del grupo del propietario
- Permisos de archivo para usuarios específicos
- Permisos de archivo para grupos específicos
- Permisos predeterminados para cada una de las categorías anteriores

Para obtener más información sobre el uso de las ACL, consulte [“Uso de listas de control de acceso para proteger archivos UFS” en la página 134.](#)

## Uso compartido de archivos entre equipos

Un servidor de archivos de red puede controlar qué archivos están disponibles para uso compartido. Un servidor de archivos de red también puede controlar qué clientes tienen acceso a los archivos y qué tipo de acceso está permitido para esos clientes. En general, el servidor de archivos puede otorgar acceso de lectura y escritura o acceso de sólo lectura a todos los clientes o a clientes específicos. El control de acceso se especifica cuando los recursos están disponibles con el comando `share`.

El archivo `/etc/dfs/dfstab` del servidor de archivos enumera los sistemas de archivos que el servidor pone a disposición de los clientes en la red. Para obtener más información sobre el uso compartido de sistemas de archivos, consulte [“Uso compartido de sistema de archivos automático” de \*Guía de administración del sistema: servicios de red\*.](#)

Al crear un recurso compartido NFS de un sistema de archivos ZFS, el sistema de archivos se comparte permanentemente hasta que se elimine el recurso compartido. SMF gestiona automáticamente el recurso compartido cuando el sistema se reinicia. Para obtener más información, consulte el [Capítulo 3, “Oracle Solaris ZFS y sistemas de archivos tradicionales” de \*Guía de administración de Oracle Solaris ZFS\*.](#)

## Restricción de acceso root a archivos compartidos

En general, al superusuario no se le permite el acceso root a los sistemas de archivos que se comparten en la red. El sistema NFS impide el acceso root a los sistemas de archivos montados cambiando el usuario del solicitante al usuario `nobody` con el ID de usuario `60001`. Los derechos de acceso del usuario `nobody` son los mismos que se otorgan al público. El usuario `nobody` tiene los derechos de acceso de un usuario sin credenciales. Por ejemplo, si el público sólo tiene permiso de ejecución para un archivo, el usuario `nobody` sólo puede ejecutar ese archivo.



Un servidor NFS puede otorgar capacidades de superusuario en un sistema de archivos compartidos por host. Para otorgar estos privilegios, utilice la opción `root=nombre de host` para el comando `share`. Debe utilizar esta opción con cuidado. Para ver una explicación de las opciones de seguridad con NFS, consulte el [Capítulo 6, “Acceso a los sistemas de archivos de red \(referencia\)”](#) de *Guía de administración del sistema: servicios de red*.

## Control de acceso a la red

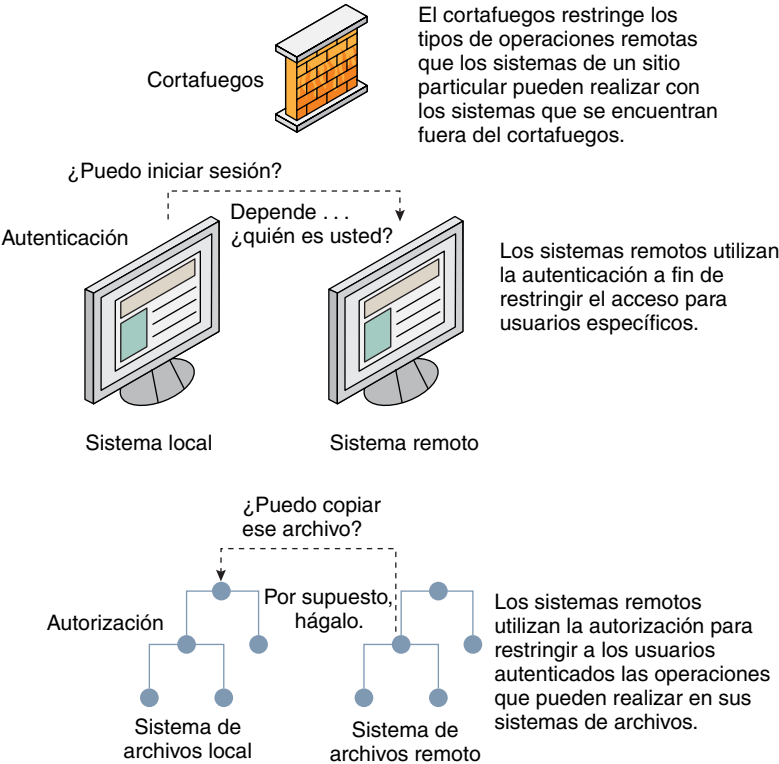
Los equipos suelen formar parte de una *red* de equipos. Una red permite que los equipos conectados intercambien información. Los equipos conectados a la red pueden acceder a datos y demás recursos de otros equipos de la red. Las redes de equipos crean un entorno informático potente y sofisticado. Sin embargo, las redes complican la seguridad de los equipos.

Por ejemplo, dentro de una red de equipos, los sistemas individuales permiten el uso compartido de información. El acceso no autorizado es un riesgo de seguridad. Debido a que muchas personas tienen acceso a una red, el acceso no autorizado es más probable, especialmente como consecuencia de errores del usuario. Un mal uso de contraseñas también puede originar el acceso no autorizado.

## Mecanismos de seguridad de red

La seguridad de red, generalmente, se basa en la limitación o el bloqueo de operaciones de sistemas remotos. En la siguiente figura, se describen las restricciones de seguridad que se pueden imponer en las operaciones remotas.

FIGURA 2-1 Restricciones de seguridad para operaciones remotas



## Autenticación y autorización para acceso remoto

La *autenticación* es una manera de restringir el acceso a usuarios específicos cuando acceden a un sistema remoto. La autenticación se puede configurar en el nivel del sistema y en el nivel de red. Después de que un usuario haya obtenido acceso a un sistema remoto, la *autorización* es una manera de limitar las operaciones que el usuario puede realizar. En la siguiente tabla, se muestran los servicios que proporcionan autenticación y autorización.

TABLA 2-3 Servicios de autenticación y autorización para acceso remoto

Servicio	Descripción	Para obtener más información
IPsec	IPsec proporciona autenticación basada en host y en certificado, y cifrado de tráfico de red.	<a href="#">Capítulo 19, “Arquitectura de seguridad IP (descripción general)” de Guía de administración del sistema: servicios IP</a>
Kerberos	Kerberos utiliza el cifrado para autenticar y autorizar a un usuario que está iniciando sesión en el sistema.	Para ver un ejemplo, consulte “ <a href="#">Cómo funciona el servicio Kerberos</a> ” en la página 394.

TABLA 2-3 Servicios de autenticación y autorización para acceso remoto (Continuación)

Servicio	Descripción	Para obtener más información
LDAP y NIS+	El servicio de directorios LDAP y el servicio de nombres NIS+ pueden proporcionar autenticación y autorización en el nivel de red.	<a href="#">Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP) y System Administration Guide: Naming and Directory Services (NIS+)</a>
Comandos de inicio de sesión remoto	Los comandos de inicio de sesión remoto permiten que los usuarios inicien sesión en un sistema remoto a través de la red y utilicen sus recursos. Algunos de los comandos de inicio de sesión remoto son <code>rlogin</code> , <code>rcp</code> y <code>ftp</code> . Si usted es un "host de confianza", la autenticación es automática. De lo contrario, se le pedirá que se autentique.	Capítulo 29, "Acceso a sistemas remotos (tareas)" de <a href="#">Guía de administración del sistema: servicios de red</a>
SASL	La autenticación sencilla y capa de seguridad (SASL) es una estructura que proporciona autenticación y servicios de seguridad opcionales a los protocolos de red. Los complementos permiten seleccionar el protocolo de autenticación adecuado.	"SASL (descripción general)" en la página 349
RPC segura	Las RPC seguras mejoran la seguridad de los entornos de red al autenticar a los usuarios que realizan solicitudes en equipos remotos. Puede utilizar un sistema de autenticación UNIX, DES o Kerberos para las RPC seguras.	"Descripción general de RPC segura" en la página 323
	Las RPC seguras también se pueden utilizar para proporcionar seguridad adicional en un entorno NFS. Un entorno NFS con RPC seguras se denomina NFS seguro. El NFS seguro utiliza la autenticación Diffie-Hellman para las claves públicas.	"Servicios NFS y RPC segura" en la página 323
Secure Shell	Secure Shell cifra el tráfico de red a través de una red no segura. Secure Shell proporciona autenticación mediante el uso de contraseñas, claves públicas, o ambos. Secure Shell utiliza autenticación RSA y DSA para las claves públicas.	"Oracle Solaris Secure Shell (descripción general)" en la página 353

Una posible alternativa a las RPC seguras es el mecanismo de *puerto con privilegios* de Oracle Solaris. A un puerto con privilegios se le asigna un número de puerto menor que 1024. Después de que un sistema cliente haya autenticado la credencial del cliente, el cliente crea una conexión al servidor mediante el puerto con privilegios. A continuación, el servidor verifica la credencial del cliente examinando el número de puerto de la conexión.

Es posible que los clientes que no están ejecutando el software Oracle Solaris no puedan comunicarse mediante el puerto con privilegios. Si los clientes no se pueden comunicar a través del puerto, se mostrará un mensaje de error similar al siguiente:

```
"Weak Authentication
NFS request from unprivileged port"
```

## Sistemas de cortafuegos

Puede configurar un sistema de cortafuegos para proteger los recursos de la red contra el acceso exterior. Un *sistema de cortafuegos* es un host seguro que actúa como una barrera entre la red interna y las redes externas. La red interna trata las otras redes como si no fueran de confianza. Debe considerar esta configuración como obligatoria entre la red interna y cualquier red externa, como Internet, con la que se comunica.

Un cortafuegos actúa como una puerta de enlace y como una barrera. Un cortafuegos actúa como una puerta de enlace que transfiere datos entre las redes. Un cortafuegos actúa como una barrera que bloquea la transferencia libre de datos desde y hacia la red. El cortafuegos requiere que un usuario de la red interna inicie sesión en el sistema de cortafuegos para acceder a hosts de redes remotas. De forma similar, un usuario de una red externa debe iniciar sesión en el sistema de cortafuegos antes de que se le otorgue acceso a un host de la red interna.

Un cortafuegos también puede ser útil entre algunas redes internas. Por ejemplo, puede configurar un cortafuegos o un equipo de puerta de enlace segura para restringir la transferencia de paquetes. La puerta de enlace puede prohibir el intercambio de paquetes entre dos redes, a menos que el equipo de puerta de enlace sea la dirección de origen o la dirección de destino del paquete. Un cortafuegos también se debe configurar para reenviar paquetes a protocolos determinados únicamente. Por ejemplo, puede permitir paquetes para transferir correo, pero no permitir paquetes para el comando `telnet` o `rlogin`. Cuando ASET se ejecuta con un nivel alto de seguridad, deshabilita el reenvío de paquetes de IP (protocolo de Internet).

Además, todos los correos electrónicos que se envían desde la red interna primero se envían al sistema de cortafuegos. A continuación, el cortafuegos transfiere el correo a un host de una red externa. El sistema de cortafuegos también recibe todos los correos electrónicos entrantes y los distribuye a los hosts de la red interna.



---

**Precaución** – Un cortafuegos impide que usuarios no autorizados accedan a los hosts de la red. Debe mantener una seguridad estricta y rigurosa en el cortafuegos, pero la seguridad en otros hosts de la red puede ser más flexible. Sin embargo, si un intruso logra entrar al sistema de cortafuegos, puede acceder a todos los otros hosts de la red interna.

---

Un sistema de cortafuegos no debe tener hosts de confianza. Un *host de confianza* es un host desde el cual un usuario puede iniciar sesión sin tener que proporcionar una contraseña. Un sistema de cortafuegos no debe compartir ninguno de sus sistemas de archivos ni montar sistemas de archivos de otros servidores.

Las siguientes tecnologías se pueden utilizar para proteger un sistema en un cortafuegos:

- ASET aplica un nivel alto de seguridad en un sistema de cortafuegos, como se describe en el [Capítulo 7, “Uso de la herramienta automatizada de mejora de la seguridad \(tareas\)”](#).
- Oracle Solaris Security Toolkit, conocido informalmente como kit de herramientas JASS, puede proteger un sistema Oracle Solaris en un cortafuegos. El kit de herramientas se puede obtener en el sitio web de descargas de Sun en [Oracle Sun \(http://www.oracle.com/us/sun/index.htm\)](http://www.oracle.com/us/sun/index.htm).
- IPsec y el filtro IP de Oracle Solaris pueden proporcionar protección de cortafuegos. Para obtener más información sobre cómo proteger el tráfico de red, consulte la [Parte IV, “Seguridad IP” de Guía de administración del sistema: servicios IP](#).

## Cifrado y sistemas de cortafuegos

La mayoría de las redes de área local transmiten datos entre equipos en bloques denominados *paquetes*. Mediante un procedimiento denominado *interceptación de paquetes*, los usuarios no autorizados que están afuera de la red pueden dañar o destruir los datos.

La interceptación de paquetes captura los paquetes antes de que lleguen a destino. A continuación, el intruso inserta datos arbitrarios en el contenido y envía los paquetes de vuelta en su curso original. En una red de área local, la interceptación de paquetes es imposible porque los paquetes llegan a todos los sistemas, incluido el servidor, al mismo tiempo. La interceptación de paquetes puede producirse en una puerta de enlace; por lo tanto, asegúrese de que todas las puertas de enlace de la red estén protegidas.

Los ataques más peligrosos afectan la integridad de los datos. Estos ataques implican cambiar el contenido de los paquetes o suplantar a un usuario. Los ataques que implican intrusiones no comprometen la integridad de los datos. Una intrusión registra conversaciones para reproducirlas más adelante. Una intrusión no implica suplantar a un usuario. Aunque los ataques de intrusión no afectan la integridad de los datos, afectan la privacidad. Puede proteger la privacidad de la información confidencial mediante el cifrado de los datos que se transmiten por la red.

- Para cifrar operaciones remotas a través de una red no segura, consulte el [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#).
- Para cifrar y autenticar datos a través de una red, consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).
- Para cifrar datagramas de IP, consulte el [Capítulo 19, “Arquitectura de seguridad IP \(descripción general\)” de Guía de administración del sistema: servicios IP](#).

## Comunicación de problemas de seguridad

Si experimenta una presunta infracción de seguridad, puede ponerse en contacto con el Equipo de Respuesta ante Emergencias Informáticas/Centro de Coordinación (CERT/CC). El CERT/CC es una Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) que se encuentra en el Instituto de Ingeniería de Software de Universidad Carnegie Mellon. Esta agencia puede ayudarlo con los problemas de seguridad que pueda tener. También puede derivarlo a otros equipos de respuesta ante emergencias informáticas que puedan ser más adecuados para sus necesidades específicas. Para conocer la información de contacto actual, consulte el sitio web de CERT/CC ([http://www.cert.org/contact\\_cert/](http://www.cert.org/contact_cert/)).

## Control de acceso a sistemas (tareas)

En este capítulo, se describen los procedimientos para controlar quién puede acceder a sistemas Oracle Solaris. A continuación, se presenta la información que se incluye en este capítulo.

- “Control de acceso al sistema (mapa de tareas)” en la página 63
- “Protección de inicios de sesión y contraseñas (mapa de tareas)” en la página 64
- “Cambio del algoritmo de contraseña (mapa de tareas)” en la página 71
- “Supervisión y restricción de superusuario (mapa de tareas)” en la página 76
- “SPARC: control de acceso a hardware del sistema (mapa de tareas)” en la página 79

Para obtener información general sobre la seguridad del sistema, consulte el [Capítulo 2, “Gestión de seguridad de equipos \(descripción general\)”](#).

### Control de acceso al sistema (mapa de tareas)

Un equipo es tan seguro como su punto de entrada más débil. El siguiente mapa de tareas muestra las áreas que debe supervisar y proteger.

Tarea	Descripción	Para obtener instrucciones
Supervisar, permitir y denegar inicios de sesión de usuarios	Supervisa la actividad poco común de inicio de sesión. Impide inicios de sesión temporalmente. Gestiona inicios de sesión de marcación telefónica.	<a href="#">“Protección de inicios de sesión y contraseñas (mapa de tareas)” en la página 64</a>
Proporcionar cifrado de contraseña más seguro	Especifica algoritmos para cifrar contraseñas de usuario. Instala algoritmos adicionales.	<a href="#">“Cambio del algoritmo de contraseña (mapa de tareas)” en la página 71</a>
Supervisar y restringir actividades de superusuarios	Supervisa periódicamente actividades de superusuarios. Impide el inicio de sesión remoto de un usuario root.	<a href="#">“Supervisión y restricción de superusuario (mapa de tareas)” en la página 76</a>
Impedir acceso a configuración de hardware	Mantiene a los usuarios comunes lejos de la PROM.	<a href="#">“SPARC: control de acceso a hardware del sistema (mapa de tareas)” en la página 79</a>

# Protección de inicios de sesión y contraseñas (mapa de tareas)

El siguiente mapa de tareas hace referencia a procedimientos que supervisan inicios de sesión de usuarios y que deshabilitan inicios de sesión de usuarios.

Tarea	Descripción	Para obtener instrucciones
Visualizar el estado de inicio de sesión de un usuario	Muestra amplia información sobre la cuenta de inicio de sesión de un usuario, por ejemplo, el nombre completo y la caducidad de las contraseñas.	<a href="#">“Cómo mostrar el estado de inicio de sesión de un usuario” en la página 64</a>
Buscar usuarios que no tienen contraseñas	Busca sólo aquellos usuarios cuyas cuentas no necesitan una contraseña.	<a href="#">“Cómo visualizar usuarios sin contraseñas” en la página 66</a>
Deshabilitar inicios de sesión temporalmente	Deniega inicios de sesión de usuario a un equipo como parte del cierre o mantenimiento de rutina del sistema.	<a href="#">“Cómo deshabilitar temporalmente inicios de sesión de usuarios” en la página 66</a>
Guardar intentos de inicio de sesión fallidos	Crea un registro de usuarios que no proporcionaron la contraseña correcta después de cinco intentos.	<a href="#">“Cómo supervisar intentos de inicio de sesión fallidos” en la página 67</a>
Guardar todos los intentos de inicio de sesión fallidos	Crea un registro de intentos fallidos para iniciar sesión.	<a href="#">“Cómo supervisar todos los intentos de inicio de sesión fallidos” en la página 68</a>
Crear una contraseña de marcación telefónica	Requiere una contraseña adicional para usuarios que inician sesión de manera remota mediante un módem o puerto de marcación telefónica.	<a href="#">“Cómo crear una contraseña de marcación telefónica” en la página 69</a>
Deshabilitar inicios de sesión de marcación telefónica temporalmente	Evita que los usuarios accedan telefónicamente de manera remota mediante un módem o puerto.	<a href="#">“Cómo deshabilitar temporalmente inicios de sesión de marcación telefónica” en la página 71</a>

## Protección de inicios de sesión y contraseñas

Puede limitar inicios de sesión remotos y solicitar a los usuarios que tengan contraseñas. También puede supervisar intentos de acceso fallidos y deshabilitar inicios de sesión temporalmente.

### ▼ Cómo mostrar el estado de inicio de sesión de un usuario

- 1
- Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)



## 2 Visualice el estado de inicio de sesión de un usuario mediante el comando `logins`.

```
# logins -x -l username
```

- x Muestra un conjunto ampliado de información de estado de inicio de sesión.
- l *nombre\_usuario* Muestra el estado de inicio de sesión para el usuario especificado. La variable *nombre\_usuario* es el nombre de inicio de sesión de un usuario. Varios nombres de inicio de sesión deben especificarse en una lista separada por comas.

El comando `logins` utiliza la base de datos de contraseñas adecuada para obtener el estado de inicio de sesión de un usuario. La base de datos puede ser el archivo `/etc/passwd` local o una base de datos de contraseñas para el servicio de nombres. Para obtener más información, consulte la página del comando `man logins(1M)`.

### Ejemplo 3-1 Visualización del estado de inicio de sesión de un usuario

En el ejemplo siguiente, se muestra el estado de inicio de sesión del usuario `rimmer`.

```
# logins -x -l rimmer
rimmer      500      staff          10      Annalee J. Rimmer
              /export/home/rimmer
              /bin/sh
PS 010103 10 7 -1
```

`rimmer` Identifica el nombre de inicio de sesión del usuario.

`500` Identifica el ID de usuario (UID).

`staff` Identifica el grupo principal del usuario.

`10` Identifica el ID de grupo (GID).

`Annalee J. Rimmer` Identifica el comentario.

`/export/home/rimmer` Identifica el directorio principal del usuario.

`/bin/sh` Identifica el shell de inicio de sesión.

`PS 010170 10 7 -1`

Especifica la información de caducidad de las contraseñas:

- Última fecha en la que se cambió la contraseña
- Número de días que son necesarios entre los cambios
- Número de días antes de que un cambio sea necesario
- Período de advertencia

## ▼ Cómo visualizar usuarios sin contraseñas

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Visualice todos los usuarios que no tienen contraseñas con el comando `logins`.

```
# logins -p
```

La opción `-p` muestra una lista de usuarios que no tienen contraseñas. El comando `logins` utiliza la base de datos de contraseñas del sistema local, a menos que un servicio de nombres esté habilitado.

#### Ejemplo 3–2 Visualización de usuarios sin contraseñas

En el siguiente ejemplo, el usuario `pmorph` no tiene una contraseña.

```
# logins -p
pmorph          501      other          1      Polly Morph
#
```

## ▼ Cómo deshabilitar temporalmente inicios de sesión de usuarios

Deshabilite temporalmente inicios de sesión de usuarios durante el cierre o el mantenimiento de rutina del sistema. Los inicios de sesión de superusuarios no se ven afectados. Para obtener más información, consulte la página del comando `man nologin(4)`.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Cree el archivo `/etc/nologin` en un editor de texto.

```
# vi /etc/nologin
```

### 3 Incluya un mensaje sobre la disponibilidad del sistema.

### 4 Cierre y guarde el archivo.

**Ejemplo 3-3** Deshabilitación de inicios de sesión de usuarios

En este ejemplo, se notifica a los usuarios que el sistema no está disponible.

```
# vi /etc/nologin
(Add system message here)

# cat /etc/nologin
***No logins permitted.***

***The system will be unavailable until 12 noon.***
```

También puede llevar el sistema al nivel de ejecución 0, modo de un solo usuario, para deshabilitar inicios de sesión. Para obtener información sobre cómo llevar el sistema al modo de un solo usuario, consulte el [Capítulo 10, “Cierre de un sistema \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**▼ Cómo supervisar intentos de inicio de sesión fallidos**

Este procedimiento captura intentos de inicio de sesión fallidos de ventanas de terminales. Este procedimiento no captura inicios de sesión fallidos de un intento de inicio de sesión o CDE.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Cree el archivo loginlog en el directorio /var/adm.**

```
# touch /var/adm/loginlog
```

**3 Establezca permisos de lectura y escritura para el usuario root en el archivo loginlog.**

```
# chmod 600 /var/adm/loginlog
```

**4 Cambie la pertenencia de grupo a sys en el archivo loginlog.**

```
# chgrp sys /var/adm/loginlog
```

**5 Verifique que el registro funcione.**

Por ejemplo, inicie sesión en el sistema cinco veces con la contraseña incorrecta. A continuación, visualice el archivo /var/adm/loginlog.

```
# more /var/adm/loginlog
jdoe:/dev/pts/2:Tue Nov  4 10:21:10 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:21 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:30 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:40 2010
jdoe:/dev/pts/2:Tue Nov  4 10:21:49 2010
#
```

El archivo `loginlog` contiene una entrada para cada intento fallido. Cada entrada contiene el nombre de inicio de sesión del usuario, el dispositivo TTY y la hora del intento fallido. Si una persona realiza menos de cinco intentos incorrectos, no se registran intentos fallidos.

Un archivo `loginlog` cada vez más grande puede indicar un intento de entrar ilegalmente al sistema del equipo. Por lo tanto, compruebe y borre el contenido de este archivo con regularidad. Para obtener más información, consulte la página del comando `man loginlog(4)`.

## ▼ Cómo supervisar todos los intentos de inicio de sesión fallidos

Este procedimiento captura en un archivo `syslog` todos los intentos de inicio de sesión fallidos.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Configure el archivo `/etc/default/login` con los valores deseados para `SYSLOG` y `SYSLOG_FAILED_LOGINS`.

Edite el archivo `/etc/default/login` para cambiar la entrada. Asegúrese de que `SYSLOG=YES` no tenga comentarios.

```
# grep SYSLOG /etc/default/login
# SYSLOG determines whether the syslog(3) LOG_AUTH facility
# should be used
SYSLOG=YES
...
SYSLOG_FAILED_LOGINS=0
#
```

### 3 Cree un archivo con los permisos correctos para mantener la información de registro.

#### a. Cree el archivo `authlog` en el directorio `/var/adm`.

```
# touch /var/adm/authlog
```

#### b. Establezca permisos de lectura y escritura para el usuario `root` en el archivo `authlog`.

```
# chmod 600 /var/adm/authlog
```

#### c. Cambie la pertenencia de grupo a `sys` en el archivo `authlog`.

```
# chgrp sys /var/adm/authlog
```

**4 Edite el archivo `syslog.conf` para registrar intentos de contraseña incorrectos.**

Los fallos deben enviarse al archivo `authlog`.

**a. Escriba la siguiente entrada en el archivo `syslog.conf`.**

Los campos en la misma línea de `syslog.conf` están separados por tabulaciones.

```
auth.notice      <Press Tab>  /var/adm/authlog
```

**b. Actualice la información de la configuración del daemon `syslog`.**

```
# svcadm refresh system/system-log
```

**5 Verifique que el registro funcione.**

Por ejemplo, como usuario común, inicie sesión en el sistema con la contraseña incorrecta. A continuación, en el rol de administrador principal o como superusuario, visualice el archivo `/var/adm/authlog`.

```
# more /var/adm/authlog
Nov  4 14:46:11 example1 login: [ID 143248 auth.notice]
Login failure on /dev/pts/8 from example2, stacey
#
```

**6 Supervise el archivo `/var/adm/authlog` de manera regular.****Ejemplo 3–4 Registro de intentos de acceso después de tres fallos de inicio de sesión**

Siga el procedimiento anterior, pero, en este caso, establezca el valor de `SYSLOG_FAILED_LOGINS` en 3, en el archivo `/etc/default/login`.

**Ejemplo 3–5 Cierre de conexión después de tres fallos de inicio de sesión**

Elimine el comentario de la entrada `RETRIES` en el archivo `/etc/default/login` y, luego, establezca el valor de `RETRIES` en 3. Las ediciones surten efecto inmediatamente. Después de tres reintentos de inicio en una sesión, el sistema cierra la conexión.

**▼ Cómo crear una contraseña de marcación telefónica**

**Precaución** – Al establecer una contraseña de marcación telefónica por primera vez, asegúrese de permanecer conectado, al menos, a un puerto. Pruebe la contraseña en un puerto diferente. Si cierra la sesión para probar la nueva contraseña, es posible que no pueda iniciar la sesión de nuevo. Si sigue conectado a otro puerto, puede volver y corregir el error.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Cree un archivo `/etc/dialups` que contenga una lista de dispositivos en serie.**

Incluya todos los puertos que se están protegiendo con contraseñas de marcación telefónica. El archivo `/etc/dialups` debe ser similar al siguiente:

```
/dev/term/a
/dev/term/b
/dev/term/c
```

**3 Cree un archivo `/etc/d_passwd` que contenga los programas de inicio de sesión que necesitan una contraseña de marcación telefónica.**

Incluya programas de shell que un usuario podría estar ejecutando en el inicio de sesión, por ejemplo, `uucico`, `sh`, `ksh` y `csh`. El archivo `/etc/d_passwd` debe ser similar al siguiente:

```
/usr/lib/uucp/uucico:encrypted-password:
/usr/bin/csh:encrypted-password:
/usr/bin/ksh:encrypted-password:
/usr/bin/sh:encrypted-password:
/usr/bin/bash:encrypted-password:
```

Más adelante, en el procedimiento, va a agregar la contraseña cifrada para cada programa de inicio de sesión.

**4 Establezca la propiedad en `root`, en los dos archivos.**

```
# chown root /etc/dialups /etc/d_passwd
```

**5 Establezca la propiedad de grupo en `root`, en los dos archivos.**

```
# chgrp root /etc/dialups /etc/d_passwd
```

**6 Establezca permisos de lectura y escritura para `root` en los dos archivos.**

```
# chmod 600 /etc/dialups /etc/d_passwd
```

**7 Cree las contraseñas cifradas.****a. Cree un usuario temporal.**

```
# useradd username
```

**b. Cree una contraseña para el usuario temporal.**

```
# passwd username
New Password:      <Type password>
Re-enter new Password:  <Retype password>
passwd: password successfully changed for username
```

**c. Capture la contraseña cifrada.**

```
# grep username /etc/shadow > username.temp
```

**d. Edite el archivo *nombre\_usuario.temp*.**

Elimine todos los campos, excepto la contraseña cifrada. El segundo campo contiene la contraseña cifrada.

Por ejemplo, en la siguiente línea, la contraseña cifrada es U9gp9SyA/JlSk.

```
temp:U9gp9SyA/JlSk:7967::::::7988:
```

**e. Elimine el usuario temporal.**

```
# userdel username
```

**8 Copie la contraseña cifrada del archivo *nombre\_usuario.temp* en el archivo */etc/d\_passwd*.**

Puede crear una contraseña diferente para cada shell de inicio de sesión. También puede utilizar la misma contraseña para cada shell de inicio de sesión.

**9 Informe la contraseña a los usuarios de marcación telefónica.**

Debe asegurarse de que sus medios para informar a los usuarios no puedan manipularse.

## ▼ **Cómo deshabilitar temporalmente inicios de sesión de marcación telefónica**

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Coloque la siguiente entrada de una sola línea en el archivo */etc/d\_passwd*:**

```
/usr/bin/sh:*
```

## **Cambio del algoritmo de contraseña (mapa de tareas)**

El siguiente mapa de tareas hace referencia a procedimientos para administrar algoritmos de contraseña.

Tarea	Para obtener instrucciones
Proporcionar cifrado de contraseña más seguro	<a href="#">“Cómo especificar un algoritmo para cifrado de contraseña” en la página 72</a>
Proporcionar cifrado de contraseña más seguro con un servicio de nombres	<a href="#">“Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS” en la página 73</a>
	<a href="#">“Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS+” en la página 74</a>
	<a href="#">“Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP” en la página 74</a>
Agregar nuevo módulo de cifrado de contraseña	<a href="#">“Cómo instalar un módulo de cifrado de contraseña de un tercero” en la página 75</a>

# Cambio de algoritmo predeterminado para cifrado de contraseña

De manera predeterminada, las contraseñas de usuario se cifran con el algoritmo `crypt_unix`. Puede utilizar un algoritmo de cifrado más seguro, como [MD5](#) o [Blowfish](#), cambiando el algoritmo de cifrado de contraseña predeterminado.

## ▼ Cómo especificar un algoritmo para cifrado de contraseña

En este procedimiento, la versión de BSD-Linux del algoritmo MD5 es el algoritmo de cifrado predeterminado que se utiliza cuando los usuarios cambian sus contraseñas. Este algoritmo es adecuado para una red mixta de equipos que ejecutan las versiones de Oracle Solaris, BSD y Linux de UNIX. Para obtener una lista de algoritmos de cifrado de contraseña e identificadores de algoritmo, consulte la [Tabla 2-1](#).

- 1

**Asuma el rol de administrador principal o conviértase en superusuario.**  
El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tarear\)” de Guía de administración del sistema: administración básica](#).
- 2

**Especifique el identificador para el algoritmo de cifrado seleccionado.**  
Escriba el identificador como el valor de la variable `CRYPT_DEFAULT` en el archivo `/etc/security/policy.conf`.



Puede que desee comentar el archivo para explicar su elección.

```
# cat /etc/security/policy.conf
...
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#
# Use the version of MD5 that works with Linux and BSD systems.
# Passwords previously encrypted with __unix__ will be encrypted with MD5
# when users change their passwords.
#
#
CRYPT_DEFAULT=__unix__
CRYPT_DEFAULT=1
```

En este ejemplo, la configuración de algoritmos garantiza que el algoritmo más débil, `crypt_unix`, nunca se utilice para cifrar una contraseña. Los usuarios cuyas contraseñas se cifraron con el módulo `crypt_unix` obtienen una contraseña cifrada con `crypt_bsdmd5` cuando cambian sus contraseñas.

Para obtener más información sobre la configuración de opciones de algoritmo, consulte la página del comando `man policy.conf(4)`.

### Ejemplo 3-6 Uso del algoritmo Blowfish para cifrado de contraseña

En este ejemplo, el identificador del algoritmo Blowfish, 2a, se especifica como el valor para la variable `CRYPT_DEFAULT` en el archivo `policy.conf`:

```
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6
#CRYPT_ALGORITHMS_DEPRECATE=__unix__
CRYPT_DEFAULT=2a
```

Esta configuración es compatible con los sistemas BSD que utilizan el algoritmo Blowfish.

## ▼ Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS

Cuando los usuarios en un dominio NIS cambian sus contraseñas, el cliente NIS consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El equipo cliente NIS cifra la contraseña.

- 1 **Especifique el algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente NIS.**
- 2 **Copie el archivo `/etc/security/policy.conf` modificado en cada equipo cliente del dominio NIS.**
- 3 **Para evitar confusiones, copie el archivo `/etc/security/policy.conf` modificado en el servidor root NIS y en los servidores esclavos.**

## ▼ **Cómo especificar un nuevo algoritmo de contraseña para un dominio NIS+**

Cuando los usuarios en un dominio NIS+ cambian sus contraseñas, el servicio de nombres NIS+ consulta la configuración de algoritmos en el archivo `/etc/security/policy.conf` del maestro NIS+. El maestro NIS+, que está ejecutando el daemon `rpc.nispasswd`, crea la contraseña cifrada.

- 1 **Especifique el algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del maestro NIS+.**
- 2 **Para evitar confusiones, copie el archivo `/etc/security/policy.conf` del maestro NIS+ en cada host del dominio NIS+.**

## ▼ **Cómo especificar un nuevo algoritmo de contraseña para un dominio LDAP**

Cuando el cliente LDAP se ha configurado correctamente, el cliente LDAP puede utilizar los nuevos algoritmos de contraseña. El cliente LDAP se comporta igual que el cliente NIS.

- 1 **Especifique un algoritmo de cifrado de contraseña en el archivo `/etc/security/policy.conf` del cliente LDAP.**
- 2 **Copie el archivo `policy.conf` modificado en cada equipo cliente del dominio LDAP.**
- 3 **Asegúrese de que el archivo `/etc/pam.conf` no utilice un módulo `pam_ldap`.**

Asegúrese de que un signo de comentario (`#`) preceda las entradas que incluyen `pam_ldap.so.1`. Además, no utilice la nueva opción `server_policy` con el módulo `pam_authok_store.so.1`.

Las entradas PAM en el archivo `pam.conf` del cliente permiten que la contraseña se cifre según la configuración local de algoritmos. Las entradas PAM también permiten que la contraseña se autentique.

Cuando los usuarios en el dominio LDAP cambian sus contraseñas, el cliente LDAP consulta su configuración local de algoritmos en el archivo `/etc/security/policy.conf`. El equipo cliente LDAP cifra la contraseña. A continuación, el cliente envía la contraseña cifrada, con una etiqueta `{crypt}`, al servidor. La etiqueta indica al servidor que la contraseña ya se ha cifrado. La contraseña se almacena, tal como está, en el servidor. Para la autenticación, el cliente recupera la contraseña almacenada desde el servidor. A continuación, el cliente compara la contraseña almacenada con la versión cifrada que el cliente acaba de generar a partir de la contraseña introducida del usuario.

---

**Nota** – Para aprovechar los controles de política de contraseña en el servidor LDAP, utilice la opción `server_policy` con las entradas `pam_authok_store` en el archivo `pam.conf`. Las contraseñas se cifran en el servidor mediante el mecanismo criptográfico de Sun Java System Directory Server. Para conocer el procedimiento, consulte el [Capítulo 11, “Configuración de Sun Java System Directory Server con clientes LDAP \(tareas\)”](#) de *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.

---

## ▼ Cómo instalar un módulo de cifrado de contraseña de un tercero

Un algoritmo de cifrado de contraseña de terceros se suele entregar como un módulo en un paquete de software. Al ejecutar el comando `pkgadd`, las secuencias de comandos del proveedor deben modificar el archivo `/etc/security/crypt.conf`. A continuación, debe modificar el archivo `/etc/security/policy.conf` para incluir el nuevo módulo y su identificador.

### 1 Agregue el software mediante el comando `pkgadd`.

Para obtener instrucciones detalladas sobre cómo agregar software, consulte [“Adición o eliminación de un paquete de software \(`pkgadd`\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Confirme que el módulo nuevo y el identificador de módulo se hayan agregado.

Lea la lista de algoritmos de cifrado en el archivo `/etc/security/crypt.conf`.

Por ejemplo, las siguientes líneas muestran que un módulo que implementa el algoritmo `crypt_rot13` se ha instalado.

```
# crypt.conf
#
md5 /usr/lib/security/$ISA/crypt_md5.so
rot13 /usr/lib/security/$ISA/crypt_rot13.so

# For *BSD - Linux compatibility
# 1 is MD5, 2a is Blowfish
1 /usr/lib/security/$ISA/crypt_bsdmd5.so
2a /usr/lib/security/$ISA/crypt_bsdbf.so
```

### 3 Agregue el identificador del algoritmo recién instalado al archivo `/etc/security/policy.conf`.

Las siguientes líneas muestran segmentos del archivo `policy.conf` que se deben modificar para agregar el identificador `rot13`.

```
# Copyright 1999-2002 Sun Microsystems, Inc. All rights reserved.
# ...
#ident "@(#)policy.conf 1.12 08/05/14 SMI"
# ...
# crypt(3c) Algorithms Configuration
```

```
CRYPT_ALGORITHMS_ALLOW=1,2a,md5,5,6,,rot13
#CRYPT_ALGORITHMS_DEPRECATED=__unix__
CRYPT_DEFAULT=md5
```

En este ejemplo, el algoritmo rot13 se usa si la contraseña actual está cifrada con el algoritmo crypt\_rot13. Las contraseñas de usuario nuevas se cifran con el algoritmo crypt\_sunmd5. La configuración de este algoritmo funciona en redes de Solaris únicamente.

## Supervisión y restricción de superusuario (mapa de tareas)

El siguiente mapa de tareas describe cómo supervisar y restringir el inicio de sesión de usuario root.

Tarea	Descripción	Para obtener instrucciones
Supervisar quién está utilizando el comando su	Analiza el archivo suLog de manera regular.	<a href="#">“Cómo supervisar quién está utilizando el comando su” en la página 76</a>
Visualizar actividad de superusuario en la consola	Supervisa intentos de acceso de superusuario a medida que se producen.	<a href="#">“Cómo restringir y supervisar inicios de sesión de superusuario” en la página 77</a>

## Supervisión y restricción de superusuario

Una alternativa al uso de la cuenta de superusuario es establecer el control de acceso basado en roles. El control de acceso basado en roles se denomina RBAC. Para obtener información general sobre RBAC, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 182](#). Para configurar RBAC, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#).

### ▼ Cómo supervisar quién está utilizando el comando su

El archivo suLog lista cada uso del comando su, no sólo los intentos de su que se utilizan para cambiar de usuario a superusuario.

- **Supervise el contenido del archivo /var/adm/suLog de manera regular.**

```
# more /var/adm/suLog
SU 12/20 16:26 + pts/0 stacey-root
SU 12/21 10:59 + pts/0 stacey-root
SU 01/12 11:11 + pts/0 root-rimmer
SU 01/12 14:56 + pts/0 pmorph-root
SU 01/12 14:57 + pts/0 pmorph-root
```

Las entradas muestran la información siguiente:

- La fecha y la hora en las que el comando se introdujo.
- Si el intento tuvo éxito. Un signo más (+) indica un intento con éxito. Un signo menos (-) indica un intento fallido.
- El puerto desde el que se ha ejecutado el comando.
- El nombre del usuario y el nombre de la identidad cambiada.

El registro de su en este archivo se habilita de manera predeterminada mediante la siguiente entrada en el archivo `/etc/default/su`:

```
SULOG=/var/adm/sulog
```

### Errores más frecuentes

Las entradas que incluyen ??? indican que el terminal de control para el comando su no se pueden identificar. Normalmente, las invocaciones del sistema del comando su antes de que el escritorio aparezca incluyen ???, como en `SU 10/10 08:08 + ??? root - root`. Después de que el usuario inicia una sesión de escritorio, el comando `ttynam` devuelve el valor del terminal de control a `sulog`: `SU 10/10 10:10 + pts/3 jdoe - root`.

Las entradas similares a las siguientes pueden indicar que el comando su no fue invocado en la línea de comandos: `SU 10/10 10:20 + ??? root - oracle`. Es posible que el usuario haya cambiado al rol `oracle` utilizando una GUI.

## ▼ Cómo restringir y supervisar inicios de sesión de superusuario

Este método detecta inmediatamente intentos de superusuarios de acceder al sistema local.

### 1 Consulte la entrada **CONSOLE** en el archivo `/etc/default/login`.

```
CONSOLE=/dev/console
```

De manera predeterminada, el dispositivo de consola se establece en `/dev/console`. Con este valor, `root` puede iniciar sesión en la consola. `root` no puede iniciar sesión de manera remota.

### 2 Verifique que **root** no pueda iniciar sesión de manera remota.

Desde un sistema remoto, intente iniciar sesión como superusuario.

```
mach2 % rlogin -l root mach1
Password: <Type root password of mach1>
Not on system console
Connection closed.
```

### 3 Supervise intentos de convertirse en superusuario.

De manera predeterminada, los intentos de convertirse en superusuario son impresos en la consola por la utilidad SYSLOG.

#### a. Abra una consola del terminal en el escritorio.

#### b. En otra ventana, utilice el comando `su` para convertirse en superusuario.

```
% su -  
Password:      <Type root password>  
#
```

Se imprime un mensaje en la consola del terminal.

```
Sep 7 13:22:57 mach1 su: 'su root' succeeded for jdoe on /dev/pts/6
```

### Ejemplo 3-7 Registro de intentos de acceso de superusuario

En este ejemplo, los intentos de superusuario no están siendo registrados por SYSLOG. Por lo tanto, el administrador está registrando esos intentos eliminando el comentario de la entrada `#CONSOLE=/dev/console` en el archivo `/etc/default/su`.

```
# CONSOLE determines whether attempts to su to root should be logged  
# to the named device  
#  
CONSOLE=/dev/console
```

Cuando un usuario intenta convertirse en superusuario, el intento se imprime en la consola del terminal.

```
SU 09/07 16:38 + pts/8 jdoe-root
```

### Errores más frecuentes

Para convertirse en superusuario de un sistema remoto cuando el archivo `/etc/default/login` contiene la entrada `CONSOLE` predeterminada, los usuarios deben, primero, iniciar sesión con su nombre de usuario. Después de iniciar sesión con su nombre de usuario, los usuarios pueden utilizar el comando `su` para convertirse en superusuario.

Si la consola muestra una entrada similar a `Mar 16 16:20:36 mach1 login: ROOT LOGIN /dev/pts/14 FROM mach2.Example.COM`, el sistema permite inicios de sesión root remotos. Para evitar el acceso remoto de superusuario, cambie la entrada `#CONSOLE=/dev/console` a `CONSOLE=/dev/console` en el archivo `/etc/default/login`.

# SPARC: control de acceso a hardware del sistema (mapa de tareas)

El mapa de tareas siguiente describe cómo proteger la PROM contra el acceso no deseado.

Tarea	Descripción	Para obtener instrucciones
Evitar que los usuarios cambien la configuración del hardware del sistema	Requiere una contraseña para modificar la configuración de la PROM.	<a href="#">“Cómo requerir una contraseña para el acceso al hardware” en la página 79</a>
Deshabilitar la secuencia de interrupción	Impide que los usuarios accedan a la PROM.	<a href="#">“Cómo deshabilitar una secuencia de interrupción del sistema” en la página 80</a>

## Control de acceso a hardware del sistema

Puede proteger el equipo físico mediante la solicitud de una contraseña para obtener acceso a la configuración del hardware. También puede proteger el equipo impidiendo que un usuario use la secuencia de interrupción para salir del sistema de ventanas.

### ▼ Cómo requerir una contraseña para el acceso al hardware

En un sistema x86, el equivalente a proteger la PROM es proteger el BIOS. Consulte los manuales del equipo para obtener información sobre cómo proteger el BIOS.

- 1 **Conviértase en superusuario o asuma un rol que incluya el perfil de seguridad de dispositivos, el perfil de mantenimiento y reparación, o el perfil de administrador del sistema.**

El perfil de administrador del sistema incluye el perfil de mantenimiento y reparación. Para crear un rol que incluya el perfil de administrador del sistema y para asignar el rol a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

- 2 **En una ventana de terminal, escriba el modo de seguridad de la PROM.**

```
# eeprom security-mode=command
```

Changing PROM password:

New password:       <Type password>

Retype new password:   <Retype password>

Seleccione el valor `command` o `full`. Para obtener más información, consulte la página del comando `man eeprom(1M)`.

Si, cuando escribe el comando anterior, no se le solicita una contraseña para la PROM, el sistema ya tiene una.

**3 (Opcional) Para cambiar la contraseña de la PROM, escriba el siguiente comando:**

```
# eeprom security-password=      Press Return
Changing PROM password:
New password:      <Type password>
Retype new password:      <Retype password>
```

El modo de seguridad y la contraseña nuevos de la PROM entran en vigor inmediatamente. Sin embargo, es más probable que se puedan observar en el próximo inicio.



**Precaución** – No olvide la contraseña de la PROM. El hardware no se puede utilizar sin esta contraseña.

---

## ▼ Cómo deshabilitar una secuencia de interrupción del sistema

Algunos sistemas del servidor tienen un conmutador de claves. Cuando el conmutador de claves se establece en la posición segura, el conmutador sustituye la configuración de interrupción de teclado del software. Por lo tanto, los cambios que realice con el siguiente procedimiento podrían no ser implementados.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Cambie el valor de KEYBOARD\_ABORT a disable.**

Elimine el comentario de la línea enable en el archivo /etc/default/kbd. Luego, agregue una línea disable:

```
# cat /etc/default/kbd
...
# KEYBOARD_ABORT affects the default behavior of the keyboard abort
# sequence, see kbd(1) for details. The default value is "enable".
# The optional value is "disable". Any other value is ignored.
...
#KEYBOARD_ABORT=enable
KEYBOARD_ABORT=disable
```

**3 Actualice los valores predeterminados del teclado.**

```
# kbd -i
```



## Control de acceso a dispositivos (tareas)

---

Este capítulo proporciona instrucciones paso a paso para proteger dispositivos, además de una sección de referencia. A continuación, se presenta la información que se incluye en este capítulo.

- “Configuración de dispositivos (mapa de tareas)” en la página 81
- “Configuración de política de dispositivos (mapa de tareas)” en la página 82
- “Gestión de asignación de dispositivos (mapa de tareas)” en la página 85
- “Asignación de dispositivos (mapa de tareas)” en la página 91
- “Protección de dispositivos (referencia)” en la página 95

Para obtener información general sobre la protección de dispositivos, consulte [“Control de acceso a dispositivos” en la página 47](#).

### Configuración de dispositivos (mapa de tareas)

El mapa de tareas siguiente hace referencia a las tareas para gestionar el acceso a los dispositivos.

Tarea	Para obtener instrucciones
Gestionar política de dispositivos	<a href="#">“Configuración de política de dispositivos (mapa de tareas)” en la página 82</a>
Gestionar asignación de dispositivos	<a href="#">“Gestión de asignación de dispositivos (mapa de tareas)” en la página 85</a>
Utilizar asignación de dispositivos	<a href="#">“Asignación de dispositivos (mapa de tareas)” en la página 91</a>

# Configuración de política de dispositivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos de configuración de dispositivos relativos a la política de dispositivos.

Tarea	Descripción	Para obtener instrucciones
Ver la política de dispositivos para los dispositivos del sistema	Muestra los dispositivos y su política de dispositivos.	<a href="#">“Cómo ver una política de dispositivos” en la página 82</a>
Requerir privilegio para uso de dispositivos	Utiliza privilegios para proteger un dispositivo.	<a href="#">“Cómo cambiar la política de dispositivos en un dispositivo existente” en la página 83</a>
Eliminar requisitos de privilegios de un dispositivo	Elimina o disminuye los privilegios necesarios para acceder a un dispositivo.	<a href="#">Ejemplo 4–3</a>
Auditar cambios en la política de dispositivos	Registra los cambios en la política de dispositivos en la pista de auditoría.	<a href="#">“Cómo auditar cambios en la política de dispositivos” en la página 84</a>
Acceder a /dev/arp	Obtiene información MIB-II IP de Oracle Solaris.	<a href="#">“Cómo recuperar información MIB-II IP de un dispositivo /dev/*” en la página 84</a>

## Configuración de política de dispositivos

La política de dispositivos restringe o impide el acceso a los dispositivos que son una parte integral del sistema. La política se aplica en el núcleo.

### ▼ Cómo ver una política de dispositivos

- Visualice la política de dispositivos para todos los dispositivos del sistema.

```
% getdevpolicy | more
DEFAULT
    read_priv_set=none
    write_priv_set=none
ip:*
    read_priv_set=net_rawaccess
    write_priv_set=net_rawaccess
...
```

#### Ejemplo 4–1 Visualización de la política de dispositivos para un dispositivo específico

En este ejemplo, se muestra la política de dispositivos para tres dispositivos.

```
% getdevpolicy /dev/allkmem /dev/ipsecesp /dev/hme
/dev/allkmem
    read_priv_set=all
```

```

        write_priv_set=all
/dev/ipsecesp
        read_priv_set=sys_net_config
        write_priv_set=sys_net_config
/dev/hme
        read_priv_set=net_rawaccess
        write_priv_set=net_rawaccess

```

## ▼ Cómo cambiar la política de dispositivos en un dispositivo existente

- 1 **Asuma un rol que incluya el perfil de derechos de seguridad de dispositivos o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de derechos de seguridad de dispositivos. También puede asignar el perfil de derechos de seguridad de dispositivos a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte el [Ejemplo 9-3](#).

- 2 **Agregue una política a un dispositivo.**

```
# update_drv -a -p policy device-driver
```

-a                      Especifica una *política* para *controlador\_dispositivo*.

-p *política*            Es la política de dispositivos para *controlador\_dispositivo*. La política de dispositivos especifica dos conjuntos de privilegios. Un conjunto es necesario para leer el dispositivo. El otro conjunto es necesario para escribir en el dispositivo.

*controlador\_dispositivo*    Es el controlador del dispositivo.

Para obtener más información, consulte la página del comando man [update\\_drv\(1M\)](#).

### Ejemplo 4-2    Cómo agregar una política a un dispositivo existente

En el ejemplo siguiente, la política de dispositivos se agrega al dispositivo ipnat.

```

# getdevpolicy /dev/ipnat
/dev/ipnat
    read_priv_set=none
    write_priv_set=none
# update_drv -a \
-p 'read_priv_set=net_rawaccess write_priv_set=net_rawaccess' ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
    read_priv_set=net_rawaccess
    write_priv_set=net_rawaccess

```

### Ejemplo 4-3 Eliminación de una política de un dispositivo

En el ejemplo siguiente, el conjunto de privilegios de lectura se elimina de la política de dispositivos para el dispositivo ipnat.

```
# getdevpolicy /dev/ipnat
/dev/ipnat
    read_priv_set=net_rawaccess
    write_priv_set=net_rawaccess
# update_drv -a -p write_priv_set=net_rawaccess ipnat
# getdevpolicy /dev/ipnat
/dev/ipnat
    read_priv_set=none
    write_priv_set=net_rawaccess
```

## ▼ Cómo auditar cambios en la política de dispositivos

De manera predeterminada, la clase de auditoría as incluye el evento de auditoría AUE\_MODDEVPLCY.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Preseleccione la clase de auditoría que incluye el evento de auditoría AUE\_MODDEVPLCY.

Agregue la clase as a la línea flags del archivo audit\_control. El archivo tendría un aspecto similar al siguiente:

```
# audit_control file
dir:/var/audit
flags:lo,as
minfree:20
naflags:lo
```

Para obtener instrucciones detalladas, consulte “[Cómo modificar el archivo audit\\_control](#)” en la [página 615](#).

## ▼ Cómo recuperar información MIB-II IP de un dispositivo /dev/\*

Las aplicaciones que recuperan información MIB-II IP de Oracle Solaris deben abrir /dev/arp, no /dev/ip.

1 **Determine la política de dispositivos en /dev/ip y /dev/arp.**

```
% getdevpolicy /dev/ip /dev/arp
/dev/ip
    read_priv_set=net_rawaccess
    write_priv_set=net_rawaccess
/dev/arp
    read_priv_set=none
    write_priv_set=none
```

Tenga en cuenta que se requiere el privilegio net\_rawaccess para la lectura y escritura en /dev/ip. No se requieren privilegios para /dev/arp.

2 **Abra /dev/arp y utilice los módulos tcp y udp.**

No se requieren privilegios. Este método es equivalente a abrir /dev/ip y utilizar los módulos arp, tcp y udp. Como la apertura de /dev/ip requiere ahora un privilegio, es preferible usar el método /dev/arp.

# Gestión de asignación de dispositivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para habilitar y configurar la asignación de dispositivos. La asignación de dispositivos está deshabilitada de manera predeterminada. Después de habilitar la asignación de dispositivos, consulte [“Asignación de dispositivos \(mapa de tareas\)” en la página 91](#).

Tarea	Descripción	Para obtener instrucciones
Permitir que un dispositivo pueda asignarse	Permite que un dispositivo se asigne a un usuario a la vez.	“Cómo permitir que un dispositivo pueda asignarse” en la página 86
Autorizar a los usuarios a asignar un dispositivo	Asigna autorizaciones de asignación de dispositivos a los usuarios.	“Cómo autorizar a usuarios para que asignen un dispositivo” en la página 87
Ver los dispositivos asignables del sistema	Muestra los dispositivos que se pueden asignar y el estado del dispositivo.	“Cómo ver la información de asignación de un dispositivo” en la página 88
Asignar de manera forzada un dispositivo	Asigna un dispositivo a un usuario que tiene una necesidad inmediata.	“Asignación forzada de un dispositivo” en la página 88
Desasignar de manera forzada un dispositivo	Desasigna un dispositivo que está asignado actualmente a un usuario.	“Desasignación forzada de un dispositivo” en la página 89
Cambiar las propiedades de asignación de un dispositivo	Cambia los requisitos para asignar un dispositivo.	“Cómo cambiar los dispositivos que se pueden asignar” en la página 89
Crear una secuencia de comandos device-clean	Depura datos de un dispositivo físico.	“Redacción de secuencias nuevas de comandos device-clean” en la página 103

Tarea	Descripción	Para obtener instrucciones
Deshabilitar asignación de dispositivos	Elimina las restricciones de asignación de todos los dispositivos.	<a href="#">“Cómo deshabilitar el servicio de auditoría” en la página 634</a>
Auditar asignación de dispositivos	Registra la asignación de dispositivos en la pista de auditoría.	<a href="#">“Cómo auditar la asignación de dispositivos” en la página 90</a>

# Gestión de asignación de dispositivos

La asignación de dispositivos restringe o impide el acceso a dispositivos periféricos. Se aplican restricciones en el momento de asignación de usuarios. De manera predeterminada, los usuarios deben tener autorización para acceder a dispositivos asignables.

## ▼ Cómo permitir que un dispositivo pueda asignarse

Si ya ha ejecutado el comando `bsmconv` para habilitar la auditoría, la asignación de dispositivos ya está habilitada en el sistema. Para obtener más información, consulte la página del comando `man bsmconv(1M)`.

1 **Asuma un rol que incluya el perfil de derechos de control de auditoría o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de derechos de control de auditoría. También puede asignar el perfil de derechos de control de auditoría a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte el [Ejemplo 9-3](#).

2 **Habilite la asignación de dispositivos.**

```
# bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: move aside /etc/rc3.d/S81volmgt.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation files.

The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

**Nota** – Este comando deshabilita el daemon de gestión de volúmenes (`/etc/rc3.d/S81volmgt`).

## ▼ **Cómo autorizar a usuarios para que asignen un dispositivo**

### **1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### **2 Cree un perfil de derechos que incluya la autorización y los comandos adecuados.**

Generalmente, debe crear un perfil de derechos que incluya la autorización `solaris.device.allocate`. Siga las instrucciones de [“Cómo crear o modificar un perfil de derechos”](#) en la [página 228](#). Otorgue al perfil de derechos las propiedades adecuadas, como las siguientes:

- Nombre del perfil de derechos: Device Allocation
- Autorizaciones otorgadas: `solaris.device.allocate`
- Comandos con atributos de seguridad: `mount` con el privilegio `sys_mount` y `umount` con el privilegio `sys_mount`

### **3 Cree un rol para el perfil de derechos.**

Siga las instrucciones de [“Cómo crear y asignar un rol con la interfaz gráfica de usuario”](#) en la [página 207](#). Utilice las siguientes propiedades del rol como guía:

- Nombre del rol: `devicealloc`
- Nombre completo del rol: Device Allocator
- Descripción del rol: Allocates and mounts allocated devices
- Perfil de derechos: Device Allocation

Este perfil de derechos debe estar en la parte superior de la lista de perfiles incluidos en el rol.

### **4 Asigne el rol a todos los usuarios que tienen permiso para asignar un dispositivo.**

### **5 Enseñe a los usuarios cómo utilizar la asignación de dispositivos.**

Para ver ejemplos de cómo asignar medios extraíbles, consulte [“Cómo asignar un dispositivo”](#) en la [página 91](#).

Como el daemon de gestión de volúmenes (`vol`) no se está ejecutando, los medios extraíbles no se montan automáticamente. Para ver ejemplos de cómo montar un dispositivo asignado, consulte [“Cómo montar un dispositivo asignado”](#) en la [página 92](#).

## ▼ Cómo ver la información de asignación de un dispositivo

### Antes de empezar

La asignación de dispositivos debe estar habilitada para que este procedimiento se realice correctamente. Para habilitar la asignación de dispositivos, consulte [“Cómo permitir que un dispositivo pueda asignarse” en la página 86](#).

#### 1 Asuma un rol que incluya el perfil de derechos de seguridad de dispositivos o conviértase en superusuario.

El rol de administrador principal incluye el perfil de derechos de seguridad de dispositivos. También puede asignar el perfil de derechos de seguridad de dispositivos a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte el [Ejemplo 9-3](#).

#### 2 Visualice información sobre los dispositivos asignables en el sistema.

```
# list_devices device-name
```

Donde *nombre\_dispositivo* es uno de los siguientes:

- `audio[n]`: micrófono y altavoz.
- `fd[n]`: unidad de disquete.
- `sr[n]`: unidad de CD-ROM.
- `st[n]`: unidad de cinta.

### Errores más frecuentes

Si el comando `list_devices` devuelve un mensaje de error similar al siguiente, es posible que la asignación de dispositivos no esté habilitada o que usted no cuente con permisos suficientes para recuperar la información.

```
list_devices: No device maps file entry for specified device.
```

Para que el comando se ejecute correctamente, habilite la asignación de dispositivos y asuma un rol con la autorización `solaris.device.revoke`.

## ▼ Asignación forzada de un dispositivo

La asignación forzada se utiliza cuando alguien ha olvidado desasignar un dispositivo. La asignación forzada también se puede utilizar cuando un usuario tiene una necesidad inmediata de un dispositivo.

### Antes de empezar

El usuario o el rol deben tener la autorización `solaris.device.revoke`.

#### 1 Determine si tiene las autorizaciones adecuadas en el rol.

```
$ auths
solaris.device.allocate solaris.device.revoke
```



## 2 Asigne de manera forzada el dispositivo al usuario que lo necesita.

En este ejemplo, la unidad de cinta se asigna de manera forzada al usuario jdoe.

```
$ allocate -U jdoe
```

## ▼ Desasignación forzada de un dispositivo

Los dispositivos que un usuario ha asignado no se desasignan automáticamente cuando finaliza el proceso o cuando el usuario cierra la sesión. La desasignación forzada se utiliza cuando un usuario ha olvidado desasignar un dispositivo.

### Antes de empezar

El usuario o el rol deben tener la autorización `solaris.device.revoke`.

## 1 Determine si tiene las autorizaciones adecuadas en el rol.

```
$ auths
solaris.device.allocate solaris.device.revoke
```

## 2 Desasigne el dispositivo de manera forzada.

En este ejemplo, la impresora se desasigna de manera forzada. La impresora ahora está disponible para que otro usuario la asigne.

```
$ deallocate -f /dev/lp/printer-1
```

## ▼ Cómo cambiar los dispositivos que se pueden asignar

## 1 Asuma un rol que incluya el perfil de derechos de seguridad de dispositivos o conviértase en superusuario.

El rol de administrador principal incluye el perfil de derechos de seguridad de dispositivos. También puede asignar el perfil de derechos de seguridad de dispositivos a un rol que cree. Para crear el rol y asignarlo a un usuario, consulte el [Ejemplo 9-3](#).

## 2 Especifique si se requiere autorización o especifique la autorización `solaris.device.allocate`.

Cambie el quinto campo en la entrada del dispositivo del archivo `device_allocate`.

```
audio;audio;reserved;reserved;solaris.device.allocate;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris.device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Donde `solaris.device.allocate` indica que un usuario debe tener la autorización `solaris.device.allocate` para utilizar el dispositivo.

**Ejemplo 4-4** Permiso para que cualquier usuario asigne un dispositivo

En el ejemplo siguiente, cualquier usuario del sistema puede asignar cualquier dispositivo. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió al símbolo arroba (@).

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;@;/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;@;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;@;/etc/security/lib/sr_clean
...
```

**Ejemplo 4-5** Prevención de uso de algunos dispositivos periféricos

En el ejemplo siguiente, el dispositivo de audio no se puede utilizar. El quinto campo en la entrada del dispositivo de audio del archivo `device_allocate` se cambió a un asterisco (\*).

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;*/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;solaris device.allocate;/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;solaris device.allocate;/etc/security/lib/sr_clean
...
```

**Ejemplo 4-6** Prevención de uso de todos los dispositivos periféricos

En el ejemplo siguiente, no se puede utilizar ningún dispositivo periférico. El quinto campo en cada entrada de dispositivo del archivo `device_allocate` se cambió a un asterisco (\*).

```
$ whoami
devicesec
$ vi /etc/security/device_allocate
audio;audio;reserved;reserved;*/etc/security/lib/audio_clean
fd0;fd;reserved;reserved;*/etc/security/lib/fd_clean
sr0;sr;reserved;reserved;*/etc/security/lib/sr_clean
...
```

**▼ Cómo auditar la asignación de dispositivos**

De manera predeterminada, los comandos de asignación de dispositivos se encuentran en la clase de auditoría `other`.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

## 2 Preseleccione la clase `ot` para la auditoría.

Agregue la clase `ot` a la línea `flags` del archivo `audit_control`. El archivo tendría un aspecto similar al siguiente:

```
# audit_control file
dir:/var/audit
flags:lo,ot
minfree:20
naflags:lo
```

Para obtener instrucciones detalladas, consulte [“Cómo modificar el archivo `audit\_control`” en la página 615](#).

# Asignación de dispositivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos que muestran a los usuarios cómo asignar dispositivos.

Tarea	Descripción	Para obtener instrucciones
Asignar un dispositivo	Permite que el usuario utilice un dispositivo y, al mismo tiempo, impide que otros usuarios lo utilicen.	<a href="#">“Cómo asignar un dispositivo” en la página 91</a>
Montar un dispositivo asignado	Permite que un usuario visualice un dispositivo que requiere montaje, como un CD-ROM o un disquete.	<a href="#">“Cómo montar un dispositivo asignado” en la página 92</a>
Desasignar un dispositivo	Permite que un dispositivo asignable esté disponible para que lo utilice otro usuario.	<a href="#">“Cómo desasignar un dispositivo” en la página 94</a>

# Asignación de dispositivos

La asignación de dispositivos reserva el uso de un dispositivo a un usuario a la vez. Los dispositivos que requieren un punto de montaje deben montarse.

## ▼ Cómo asignar un dispositivo

### Antes de empezar

La asignación de dispositivos debe estar habilitada, como se describe en [“Cómo permitir que un dispositivo pueda asignarse” en la página 86](#). Si se requiere autorización, el usuario debe contar con la autorización.

## 1 Asigne el dispositivo.

Especifique el nombre del dispositivo.

```
% allocate device-name
```

## 2 Verifique que el dispositivo esté asignado.

Ejecute el comando idéntico.

```
% allocate device-name
allocate. Device already allocated.
```

### Ejemplo 4-7 Asignación de un micrófono

En este ejemplo, el usuario `jdoe` asigna un micrófono: `audio`.

```
% whoami
jdoe
% allocate audio
```

### Ejemplo 4-8 Asignación de una impresora

En este ejemplo, un usuario asigna una impresora. Nadie más puede imprimir en `printer-1` hasta que el usuario la haya desasignado o hasta que la impresora se asigne de manera forzada a otro usuario.

```
% allocate /dev/lp/printer-1
```

Para ver un ejemplo de una desasignación forzada, consulte [“Desasignación forzada de un dispositivo” en la página 89](#).

### Ejemplo 4-9 Asignación de una unidad de cinta

En este ejemplo, el usuario `jdoe` asigna una unidad de cinta: `st0`.

```
% whoami
jdoe
% allocate st0
```

#### Errores más frecuentes

Si el comando `allocate` no puede asignar el dispositivo, se muestra un mensaje de error en la ventana de consola. Para obtener una lista de los mensajes de error de asignación, consulte la página del comando `man allocate(1)`.

## ▼ Cómo montar un dispositivo asignado

#### Antes de empezar

El usuario o el rol asignaron el dispositivo. Para montar un dispositivo, el usuario o rol deben tener los privilegios necesarios. Para otorgar los privilegios necesarios, consulte [“Cómo autorizar a usuarios para que asignen un dispositivo” en la página 87](#).

### 1 Asuma un rol que permita asignar y montar un dispositivo.

```
% su - role-name
Password: <Type role-name password>
$
```

**2 Cree y proteja un punto de montaje en el directorio principal del rol.**

Únicamente debe realizar este paso la primera vez que necesita un punto de montaje.

```
$ mkdir mount-point ; chmod 700 mount-point
```

**3 Enumere los dispositivos asignables.**

```
$ list_devices -l
List of allocatable devices
```

**4 Asigne el dispositivo.**

Especifique el nombre del dispositivo.

```
$ allocate device-name
```

**5 Monte el dispositivo.**

```
$ mount -o ro -F filesystem-type device-path mount-point
```

Donde

`-o ro` Indica que el dispositivo se montará en el modo de sólo lectura. Utilice `-o rw` para indicar que debe poder escribir en el dispositivo.

`-F tipo_sistema de archivos` Indica el formato del sistema de archivos del dispositivo. Generalmente, un CD-ROM se formatea con un sistema de archivos HSFS. Un disquete suele formatearse con un sistema de archivos PCFS.

`ruta_dispositivo` Indica la ruta del dispositivo. La salida del comando `list_devices -l` incluye `ruta_dispositivo`.

`punto_montaje` Indica el punto de montaje creado en el [Paso 2](#).

**Ejemplo 4-10 Asignación de una unidad de disquete**

En este ejemplo, un usuario asume un rol que permite asignar y montar una unidad de disquete: `fd0`. El disquete se formatea con un sistema de archivos PCFS.

```
% roles
devicealloc
% su - devicealloc
Password: <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: fd0 type: fd files: /dev/diskette /dev/rdiskette /dev/fd0a
...
$ allocate fd0
```

```
$ mount -o ro -F pcfs /dev/diskette /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
List of the contents of diskette
```

#### Ejemplo 4-11 Asignación de una unidad de CD-ROM

En este ejemplo, un usuario asume un rol que permite asignar y montar una unidad de CD-ROM: `sr0`. La unidad está formateada como un sistema de archivos HSFS.

```
% roles
devicealloc
% su - devicealloc
Password:      <Type devicealloc password>
$ mkdir /home/devicealloc/mymnt
$ chmod 700 /home/devicealloc/mymnt
$ list_devices -l
...
device: sr0 type: sr files: /dev/sr0 /dev/rsr0 /dev/dsk/c0t2d0s0 ...
...
$ allocate sr0
$ mount -o ro -F hsfs /dev/sr0 /home/devicealloc/mymnt
$ cd /home/devicealloc/mymnt ; ls
List of the contents of CD-ROM
```

#### Errores más frecuentes

Si el comando `mount` no puede montar el dispositivo, se muestra un mensaje de error: `mount: insufficient privileges`. Compruebe lo siguiente:

- Asegúrese de estar ejecutando el comando `mount` en un shell de perfil. Si asumió un rol, el rol tiene un shell de perfil. Si es un usuario y se le asignó un perfil con el comando `mount`, debe crear un shell de perfil. Los comandos `pfsh`, `pfksh` y `pfcs` crean un shell de perfil.
- Asegúrese de ser el propietario del punto de montaje especificado. Debe tener acceso de lectura, escritura y ejecución al punto de montaje.

Póngase en contacto con el administrador si todavía no puede montar el dispositivo asignado.

## ▼ Cómo desasignar un dispositivo

La desasignación permite que otros usuarios asignen y utilicen el dispositivo cuando usted haya terminado.

#### Antes de empezar

Debe haber asignado el dispositivo.

**1 Si el dispositivo está montado, desmóntelo.**

```
$ cd $HOME
$ umount mount-point
```

**2 Desasigne el dispositivo.**

```
$ deallocate device-name
```

**Ejemplo 4–12 Desasignación de un micrófono**

En este ejemplo, el usuario jdoe desasigna el micrófono: audio.

```
% whoami
jdoe
% deallocate audio
```

**Ejemplo 4–13 Desasignación de una unidad de CD-ROM**

En este ejemplo, el rol de asignador de dispositivos desasigna una unidad de CD-ROM. Después de que se imprime el mensaje, se expulsa el CD-ROM.

```
$ whoami
devicealloc
$ cd /home/devicealloc
$ umount /home/devicealloc/mymnt
$ ls /home/devicealloc/mymnt
$
$ deallocate sr0
/dev/sr0:      326o
/dev/rsr0:     326o
...
sr_clean: Media in sr0 is ready. Please, label and store safely.
```

## Protección de dispositivos (referencia)

Los dispositivos en Oracle Solaris están protegidos por una política de dispositivos. Los dispositivos periféricos se pueden proteger mediante la asignación de dispositivos. La política de dispositivos se aplica por el núcleo. La asignación de dispositivos se habilita de manera opcional y se aplica en el nivel de usuario.

## Comandos de la política de dispositivos

Los comandos de gestión de dispositivos administran la política de dispositivos en archivos locales. La política de dispositivos puede incluir requisitos de privilegios. Sólo el superusuario o un rol con capacidades equivalentes puede gestionar los dispositivos.

En la siguiente tabla, se muestran los comandos de gestión de dispositivos.

TABLA 4-1 Comandos de gestión de dispositivos

Comando	Finalidad	Página del comando man
devfsadm	Administra los dispositivos y los controladores de dispositivos en un sistema en ejecución. También carga la política de dispositivos.  El comando devfsadm permite la limpieza de enlaces /dev sin referencia a dispositivos de disco, cinta, puerto, audio y pseudodispositivos. Los dispositivos para un controlador con nombre también se pueden volver a configurar.	<a href="#">devfsadm(1M)</a>
getdevpolicy	Muestra la política asociada con uno o varios dispositivos. Cualquier usuario puede ejecutar este comando.	<a href="#">getdevpolicy(1M)</a>
add_drv	Agrega un nuevo controlador de dispositivos a un sistema en ejecución. Contiene opciones para agregar la política de dispositivos al nuevo dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.	<a href="#">add_drv(1M)</a>
update_drv	Actualiza los atributos de un controlador de dispositivos existente. Contiene opciones para actualizar la política de dispositivos para el dispositivo. Generalmente, este comando se invoca en una secuencia de comandos cuando se está instalando un controlador de dispositivos.	<a href="#">update_drv(1M)</a>
rem_drv	Elimina un dispositivo o un controlador de dispositivos.	<a href="#">rem_drv(1M)</a>

## Asignación de dispositivos

La asignación de dispositivos puede proteger su sitio contra pérdida de datos, virus informáticos y otras infracciones de seguridad. A diferencia de la política de dispositivos, la asignación de dispositivos es opcional. Los dispositivos no se pueden asignar hasta que se ejecute la secuencia de comandos bsmconv. La asignación de dispositivos utiliza autorizaciones para limitar el acceso a los dispositivos asignables.



## Componentes de la asignación de dispositivos

Los componentes del mecanismo de asignación de dispositivos son los siguientes:

- Los comandos `allocate`, `deallocate`, `dminfo` y `list_devices`. Para obtener más información, consulte “Comandos de asignación de dispositivos” en la página 97.
- Secuencias de comandos `device-clean` para cada dispositivo asignable.

Estos comandos y las secuencias de comandos utilizan los siguientes archivos locales para implementar la asignación de dispositivos:

- El archivo `/etc/security/device_allocate`. Para obtener más información, consulte la página del comando `man device_allocate(4)`.
- El archivo `/etc/security/device_maps`. Para obtener más información, consulte la página del comando `man device_maps(4)`.
- Un archivo de bloqueo, en el directorio `/etc/security/dev`, para cada dispositivo asignable.
- Los atributos modificados de los archivos de bloqueo que están asociados con cada dispositivo asignable.

**Nota** – Es posible que versiones futuras de Oracle Solaris no admitan el directorio `/etc/security/dev`.

## Comandos de asignación de dispositivos

Con opciones de mayúsculas, los comandos `allocate`, `deallocate` y `list_devices` son comandos administrativos. De lo contrario, estos comandos son comandos de usuario. En la siguiente tabla, se muestran los comandos de asignación de dispositivos.

TABLA 4-2 Comandos de asignación de dispositivos

Comando	Finalidad	Página del comando man
<code>bsmconv</code>	<p>Crea las bases de datos para manejar la asignación de dispositivos. También permite el servicio de auditoría. Debe ser superusuario o tener el rol de administrador principal.</p> <p><code>devalloc_adm</code>: permite que los dispositivos puedan asignarse, de modo que los usuarios individuales puedan asignar un dispositivo para uso privado. Impide la asignación de dispositivos; por lo tanto, impide el uso de dispositivos periféricos en un sistema. Elimina los dispositivos de la lista de dispositivos asignables.</p> <p>Si no desea utilizar la auditoría, puede utilizar el comando <code>devalloc_adm</code> para habilitar la asignación de dispositivos.</p>	<a href="#">bsmconv(1M)</a>

TABLA 4-2 Comandos de asignación de dispositivos (Continuación)		
Comando	Finalidad	Página del comando man
dminfo	Busca un dispositivo asignable por tipo de dispositivo, nombre del dispositivo y nombre de ruta completa.	<a href="#">dminfo(1M)</a>
list_devices	Muestra el estado de los dispositivos asignables.  Muestra todos los archivos especiales del dispositivo que están asociados con los dispositivos enumerados en el archivo device_maps.	<a href="#">list_devices(1)</a>
list_devices -U	Muestra los dispositivos asignables o los que están asignados al ID de usuario especificado. Esta opción permite comprobar cuáles dispositivos son asignables y cuáles están asignados a otro usuario. Debe tener la autorización solaris.device.revoke.	
allocate	Reserva un dispositivo asignable para que lo utilice un usuario.  De manera predeterminada, un usuario debe tener la autorización solaris.device.allocate para poder asignar un dispositivo. Puede modificar el archivo device_allocate para que no requiera autorización del usuario. De esa manera, cualquier usuario del sistema puede solicitar la asignación del dispositivo para su uso.	<a href="#">allocate(1)</a>
deallocate	Elimina la reserva de asignación de un dispositivo.	<a href="#">deallocate(1)</a>

### Autorizaciones para los comandos de asignación

De manera predeterminada, los usuarios deben tener la autorización `solaris.device.allocate` para reservar un dispositivo asignable. Para crear un perfil de derechos a fin de incluir la autorización `solaris.device.allocate`, consulte [“Cómo autorizar a usuarios para que asignen un dispositivo” en la página 87](#).

Los administradores deben tener la autorización `solaris.device.revoke` para cambiar el estado de asignación de un dispositivo. Por ejemplo, la opción `-U` para los comandos `allocate` y `list_devices`, y la opción `-F` para el comando `deallocate` requieren la autorización `solaris.device.revoke`.

Para obtener más información, consulte [“Comandos que requieren autorizaciones” en la página 252](#).

### Estado de error de asignación

Un dispositivo está en un *estado de error de asignación* cuando el comando `deallocate` no puede realizar la desasignación o cuando el comando `allocate` no puede realizar la asignación. Cuando un dispositivo asignable se encuentra en un estado de error de asignación, se debe

desasignar de manera forzada. Sólo el superusuario o un rol con el perfil de derechos de gestión de dispositivos o de seguridad de dispositivos puede manejar un estado de error de asignación.

El comando `deallocate` con la opción `-F` fuerza la desasignación. O bien, puede usar `allocate -U` para asignar el dispositivo a un usuario. Una vez que el dispositivo está asignado, puede investigar los mensajes de error que aparecen. Después de corregir los problemas con el dispositivo, puede desasignarlo de manera forzada.

## Archivo `device_maps`

Los mapas de dispositivos se crean al configurar la asignación de dispositivos. El comando `bsmconv` crea un archivo `/etc/security/device_maps` predeterminado cuando el servicio de auditoría está habilitado. Este archivo `device_maps` inicial se puede personalizar para su sitio. El archivo `device_maps` incluye los nombres de los dispositivos, los tipos de dispositivos y los archivos especiales de los dispositivos que están asociados con cada dispositivo asignable.

El archivo `device_maps` define las asignaciones de archivos especiales para cada dispositivo, que en muchos casos no son intuitivas. Este archivo permite que los programas descubran qué archivos especiales de dispositivos se deben asignar a determinados dispositivos. Puede utilizar el comando `dminfo`, por ejemplo, para recuperar el nombre del dispositivo, el tipo de dispositivo y los archivos especiales del dispositivo que se deben especificar al configurar un dispositivo asignable. El comando `dminfo` utiliza el archivo `device_maps` para comunicar esta información.

Cada dispositivo se representa con una entrada de una línea con el formato:

*device-name:device-type:device-list*

### EJEMPLO 4-14 Ejemplo de entrada `device_maps`

El siguiente es un ejemplo de una entrada en un archivo `device_maps` para una unidad de disquete, `fd0`:

```
fd0:\
    fd:\
        /dev/diskette /dev/rdiskette /dev/fd0a /dev/rfd0a \
/dev/fd0b /dev/rfd0b /dev/fd0c /dev/fd0 /dev/rfd0c /dev/rfd0:\
```

Las líneas en el archivo `device_maps` pueden finalizar con una barra diagonal inversa (`\`) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (`#`) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

<i>nombre_dispositivo</i>	Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte <a href="#">“Cómo ver la información de asignación de un dispositivo” en la página 88</a> .
---------------------------	--

<i>tipo_dispositivo</i>	Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como <i>st</i> , <i>fd</i> o <i>audio</i> . El campo <i>tipo_dispositivo</i> agrupa lógicamente dispositivos relacionados.
<i>lista_dispositivo</i>	Muestra los archivos especiales del dispositivo que están asociados con el dispositivo físico. <i>lista_dispositivo</i> debe contener todos los archivos especiales que permiten el acceso a un dispositivo determinado. Si la lista está incompleta, un usuario malintencionado podrá obtener o modificar información privada. Las entradas válidas para el campo <i>lista_dispositivo</i> reflejan los archivos del dispositivo que están ubicados en el directorio <i>/dev</i> .

## Archivo `device_allocate`

El comando `bsmconv` crea un archivo `/etc/security/device_allocate` inicial cuando el servicio de auditoría está habilitado. Este archivo `device_allocate` inicial se puede utilizar como punto de partida. Puede modificar el archivo `/etc/security/device_allocate` para cambiar los dispositivos de asignables a no asignables, o para agregar dispositivos nuevos. A continuación, se presenta un ejemplo del archivo `device_allocate`.

```
st0;st;;;/etc/security/lib/st_clean
fd0;fd;;;/etc/security/lib/fd_clean
sr0;sr;;;/etc/security/lib/sr_clean
audio;audio;;;*/etc/security/lib/audio_clean
```

Una entrada en el archivo `device_allocate` no significa que el dispositivo es asignable, a menos que la entrada indique específicamente que el dispositivo es asignable. En el archivo `device_allocate` de ejemplo, observe el asterisco (\*) en el quinto campo de la entrada del dispositivo de audio. Un asterisco en el quinto campo indica al sistema que el dispositivo no es asignable. Por lo tanto, el dispositivo no se puede utilizar. Si hay otros valores o si no hay ningún valor en este campo, el dispositivo se puede utilizar.

En el archivo `device_allocate`, cada dispositivo se representa con una entrada de una línea con el formato:

```
device-name;device-type;reserved;reserved;auths;device-exec
```

Las líneas en el archivo `device_allocate` pueden finalizar con una barra diagonal inversa (\) para continuar una entrada en la línea siguiente. También se pueden incluir comentarios. Un signo de almohadilla (#) indica que hay comentarios en todo el texto subsiguiente hasta la siguiente línea nueva que no está inmediatamente precedida por una barra diagonal inversa. En todos los campos, se permiten espacios iniciales y finales. Los campos se definen del modo siguiente:

<i>nombre_dispositivo</i>	Especifica el nombre del dispositivo. Para obtener una lista de los nombres actuales de dispositivos, consulte <a href="#">“Cómo ver la información de asignación de un dispositivo” en la página 88</a> .
---------------------------	--

<i>tipo_dispositivo</i>	Especifica el tipo de dispositivo genérico. El nombre genérico es el nombre para la clase de dispositivos, como <i>st</i> , <i>fd</i> y <i>sr</i> . El campo <i>tipo_dispositivo</i> agrupa lógicamente dispositivos relacionados. Cuando permita que un dispositivo pueda asignarse, recupere el nombre del dispositivo del campo <i>tipo_dispositivo</i> en el archivo <i>device_maps</i> .
<i>reserved</i>	Sun reserva para uso futuro los dos campos marcados como <i>reserved</i> .
<i>autorizaciones</i>	Especifica si el dispositivo es asignable. Un asterisco (*) en este campo indica que el dispositivo no es asignable. Una cadena de autorización, o un campo vacío, indica que el dispositivo es asignable. Por ejemplo, la cadena <i>solaris.device.allocate</i> en el campo <i>autorizaciones</i> indica que se necesita la autorización <i>solaris.device.allocate</i> para poder asignar el dispositivo. Un símbolo arroba (@) en este archivo indica que cualquier usuario puede asignar el dispositivo.
<i>ejec_dispositivo</i>	Proporciona el nombre de ruta de una secuencia de comandos que se debe invocar para tratamiento especial, como limpieza y protección contra la reutilización del objeto durante el proceso de asignación. La secuencia de comandos <i>ejec_dispositivo</i> se ejecuta cuando el comando <i>deallocate</i> se ejecuta en el dispositivo.

Por ejemplo, la entrada siguiente para el dispositivo *sr0* indica que un usuario que cuente con la autorización *solaris.device.allocate* puede asignar la unidad de CD-ROM:

```
sr0;sr;reserved;reserved;solaris.device.allocate;/etc/security/lib/sr_clean
```

Puede decidir aceptar los servicios predeterminados y sus características definidas. Después de instalar un dispositivo nuevo, puede modificar las entradas. Los dispositivos que requieren asignación antes de su uso deben definirse en los archivos *device\_allocate* y *device\_maps* del sistema de ese dispositivo. En la actualidad, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM y los chips de audio se consideran asignables. Estos tipos de dispositivos tienen secuencias de comandos *device-clean*.

---

**Nota** – Las unidades de cinta Xylogics o Archive también utilizan la secuencia de comandos *st\_clean* proporcionada para los dispositivos SCSI. Debe crear sus propias secuencias de comandos *device-clean* para otros dispositivos, como módems, terminales, tabletas gráficas y otros dispositivos asignables. La secuencia de comandos debe cumplir con los requisitos de reutilización de objetos para ese tipo de dispositivo.

---

## Secuencias de comandos *device-clean*

La asignación de dispositivos cumple parte de lo que se conoce como requisito de reutilización de objetos. Las secuencias de comandos *device-clean* abordan el requisito de seguridad que establece que todos los datos utilizables deben depurarse de un dispositivo físico antes de volver

a utilizarlo. Los datos se limpian antes de que otro usuario asigne el dispositivo. De manera predeterminada, las unidades de cinta de cartucho, las unidades de disquete, las unidades de CD-ROM y los dispositivos de audio requieren secuencias de comandos `device-clean`. Oracle Solaris proporciona las secuencias de comandos. Esta sección describe qué acciones realizan las secuencias de comandos `device-clean`.

## Secuencia de comandos `device-clean` para cintas

La secuencia de comandos `st_clean` admite tres dispositivos de cinta:

- Cinta SCSI de ¼ de pulgada
- Cinta Archive de ¼ de pulgada
- Cinta de carrete abierto de ½ pulgada

La secuencia de comandos `st_clean` utiliza la opción `rewoffl` del comando `mt` para limpiar el dispositivo. Para obtener más información, consulte la página del comando `man mt(1)`. Si la secuencia de comandos se ejecuta durante el inicio del sistema, la secuencia consulta al dispositivo para determinar si está en línea. Si el dispositivo está en línea, la secuencia de comandos determina si el dispositivo tiene medios. Los dispositivos de cinta de ¼ de pulgada que tienen medios se colocan en el estado de error de asignación. El estado de error de asignación fuerza al administrador a limpiar manualmente el dispositivo.

Durante el funcionamiento normal del sistema, cuando el comando `deallocate` se ejecuta en modo interactivo, se le indica al usuario que extraiga los medios. La desasignación se retrasa hasta que los medios se hayan extraído del dispositivo.

## Secuencias de comandos `device-clean` para disquetes y unidades de CD-ROM

Las siguientes secuencias de comandos `device-clean` se proporcionan para disquetes y unidades de CD-ROM:

- **Secuencia de comandos `fd_clean`:** secuencia de comandos `device-clean` para disquetes.
- **Secuencia de comandos `sr_clean`:** secuencia de comandos `device-clean` para unidades de CD-ROM.

Las secuencias de comandos utilizan el comando `eject` para extraer los medios de la unidad. Si el comando `eject` falla, el dispositivo se coloca en el estado de error de asignación. Para obtener más información, consulte la página del comando `man eject(1)`.

## Secuencia de comandos `device-clean` para audio

Los dispositivos de audio se limpian con una secuencia de comandos `audio_clean`. La secuencia de comandos realiza una llamada del sistema `ioctl AUDIO_GETINFO` para leer el dispositivo. A continuación, la secuencia de comandos realiza una llamada del sistema `ioctl AUDIO_SETINFO` para restablecer la configuración del dispositivo a los valores predeterminados.

## Redacción de secuencias nuevas de comandos device-clean

Si agrega más dispositivos asignables al sistema, posiblemente deba crear sus propias secuencias de comandos device-clean. El comando `dealocate` pasa un parámetro a las secuencias de comandos device-clean. El parámetro, que se muestra aquí, es una cadena que contiene el nombre del dispositivo. Para obtener más información, consulte la página del comando `man device_allocate(4)`.

*clean-script* - [I|i|f|S] *device-name*

Si las secuencias de comandos device-clean devuelven “0”, son correctas; si devuelven valores mayores que “0”, fallaron. Las opciones -I, -f y -S determinan el modo de ejecución de la secuencia de comandos:

- I     Se necesita durante el inicio del sistema únicamente. Todas las salidas deben ir a la consola del sistema. Si no se pueden expulsar de manera forzada los medios o si la expulsión falla, el dispositivo debe pasar al estado de error de asignación.
- i     Similar a la opción -I, excepto que se suprime la salida.
- f     Se utiliza para la limpieza forzada. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos. Una secuencia de comandos con esta opción debe intentar completar la limpieza si se produce un error en una parte de ésta.
- S     Se utiliza para la limpieza estándar. La opción es interactiva y asume que el usuario está disponible para responder a las peticiones de datos.





## Uso de la herramienta básica de creación de informes de auditoría (tareas)

---

En este capítulo, se describe cómo crear un manifiesto de los archivos de un sistema y cómo utilizar dicho manifiesto para comprobar la integridad del sistema. La herramienta básica de creación de informes de auditoría (BART, Basic Audit Reporting Tool) permite validar exhaustivamente los sistemas mediante comprobaciones en el nivel de archivo de un sistema a lo largo del tiempo.

A continuación, se presenta la información que se incluye en este capítulo:

- “Herramienta básica de creación de informes de auditoría (descripción general)” en la página 105
- “Uso de BART (tareas)” en la página 109
- “Manifiestos, archivos de reglas e informes de BART (referencia)” en la página 122

### Herramienta básica de creación de informes de auditoría (descripción general)

BART es una herramienta de seguimiento de archivos que funciona por completo en el nivel del sistema de archivos. BART le permite reunir de manera rápida, sencilla y confiable información sobre los componentes de la pila de software que está instalada en los sistemas implementados. Con BART, puede reducir significativamente los costos de administración de una red de sistemas al simplificar tareas administrativas que requieren mucho tiempo.

BART le permite determinar los cambios que se produjeron en el nivel de archivo de un sistema, en relación con un punto de partida conocido. Puede utilizar BART para crear un manifiesto de *control* o punto de partida a partir de un sistema instalado y configurado totalmente. De esta manera, puede comparar este punto de partida con una instantánea del sistema en un momento posterior y generar un informe que enumera los cambios en el nivel de archivo que se produjeron en el sistema desde su instalación.

El comando `bart` es un comando UNIX estándar. Puede redirigir la salida del comando `bart` a un archivo para un procesamiento posterior.

## Funciones de BART

BART se ha diseñado pensando en una sintaxis simple que es potente y flexible a la vez. La herramienta permite generar manifiestos de un sistema determinado a lo largo del tiempo. Así, cuando sea necesario validar los archivos del sistema, usted puede generar un informe mediante la comparación de los manifiestos antiguos y los nuevos. Otra forma de utilizar BART es generar manifiestos de varios sistemas similares y ejecutar comparaciones entre los sistemas. La diferencia principal entre BART y las herramientas de auditoría existentes es que BART es flexible, tanto en términos de la información sobre la cual se realiza un seguimiento como de la información que se comunica.

Entre los usos y los beneficios adicionales de BART, se incluyen los siguientes:

- Ofrece un método eficaz y sencillo para catalogar un sistema que ejecuta el software Oracle Solaris en el nivel de archivos.
- Permite definir los archivos que se van a supervisar y ofrece la posibilidad de modificar perfiles cuando es necesario. Esta flexibilidad permite supervisar las personalizaciones locales y volver a configurar software de manera fácil y eficaz.
- Garantiza que los sistemas ejecuten software confiable.
- Permite supervisar los cambios en el nivel de archivo de un sistema a lo largo del tiempo, lo cual puede ayudar a encontrar archivos dañados o poco comunes.
- Ayuda a solucionar problemas de rendimiento del sistema.

## Componentes de BART

BART tiene dos componentes principales y un componente opcional:

- Manifiesto de BART
- Informe de BART
- Archivo de reglas de BART

### Manifiesto de BART

Puede utilizar el comando `bart create` para tomar una instantánea de nivel de archivo de un sistema en un momento determinado. La salida es un catálogo de archivos y atributos de archivos denominado *manifiesto*. El manifiesto muestra información sobre todos los archivos o sobre archivos específicos de un sistema. Contiene información sobre los atributos de los archivos, que puede incluir información de identificación exclusiva, como una suma de comprobación MD5. Para obtener más información sobre la suma de comprobación MD5, consulte la página del comando `man md5(3EXT)`. Un manifiesto se puede almacenar y transferir entre sistemas cliente y del servidor.

---

**Nota** – BART *no* traspasa los límites del sistema de archivos, con la excepción de los sistemas de archivos del mismo tipo. Esta restricción hace que la salida del comando `bart create` sea más predecible. Por ejemplo, sin argumentos, el comando `bart create` cataloga todos los sistemas de archivos en el directorio root (`/`). Sin embargo, no se catalogan los sistemas de archivos NFS o TMPFS ni los CD-ROM montados. Al crear un manifiesto, no intente auditar los sistemas de archivos de una red. Tenga en cuenta que, al usar BART para supervisar los sistemas de archivos conectados a la red, se puede consumir una gran cantidad de recursos para generar manifiestos de poco valor.

---

Para obtener más información sobre los manifiestos de BART, consulte [“Formato de archivo de manifiesto de BART” en la página 123](#).

## Informe de BART

La herramienta de creación de informes tiene tres entradas: los dos manifiestos que se compararán y un archivo de reglas opcional proporcionado por el usuario que indica las discrepancias que deben marcarse.

El comando `bart compare` se usa para comparar dos manifiestos, un *manifiesto de control* y un *manifiesto de prueba*. Estos manifiestos se deben preparar con los mismos sistemas de archivos, las mismas opciones y el mismo archivo de reglas que se utilizan con el comando `bart create`.

La salida del comando `bart compare` es un informe que enumera las discrepancias por archivo entre los dos manifiestos. Una *discrepancia* es un cambio en cualquier atributo para un archivo determinado que se cataloga para ambos manifiestos. Las adiciones o eliminaciones de entradas de archivos entre los dos manifiestos también se consideran discrepancias.

Hay dos niveles de control al informar discrepancias:

- Al generar un manifiesto
- Al producir informes

Estos niveles de control son intencionales, ya que generar un manifiesto es más costoso que informar discrepancias entre dos manifiestos. Una vez que haya creado los manifiestos, puede compararlos desde perspectivas distintas ejecutando el comando `bart compare` con archivos de reglas diferentes.

Para obtener más información sobre los informes de BART, consulte [“Creación de informes de BART” en la página 125](#).

## Archivo de reglas de BART

El *archivo de reglas* es un archivo de texto que usted puede utilizar opcionalmente como entrada para el comando `bart`. Este archivo utiliza reglas de inclusión y de exclusión. Un archivo de reglas se utiliza para crear manifiestos e informes personalizados. Un archivo de reglas le

permite expresar con una sintaxis concisa los conjuntos de archivos que desea catalogar y los atributos que desea supervisar para un conjunto de archivos determinado. Cuando se comparan manifiestos, el archivo de reglas ayuda a marcar las discrepancias entre los manifiestos. Usar un archivo de reglas es un método eficaz para reunir información específica sobre los archivos de un sistema.

Para crear un archivo de reglas, se utiliza un editor de texto. Con un archivo de reglas, puede realizar las siguientes tareas:

- Utilizar el comando `bart create` para crear un manifiesto que muestre información sobre todos los archivos o sobre archivos específicos de un sistema.
- Utilizar el comando `bart compare` para generar un informe que supervise atributos específicos de un sistema de archivos.

**Nota** – Puede crear varios archivos de reglas con propósitos diferentes. Sin embargo, si crea un manifiesto usando un archivo de reglas, debe utilizar el mismo archivo de reglas cuando compare los manifiestos. Si no utiliza el mismo archivo de reglas al comparar manifiestos creados con un archivo de reglas, la salida del comando `bart compare` enumera muchas discrepancias no válidas.

Un archivo de reglas también puede contener errores de sintaxis y otra información ambigua como resultado de errores del usuario. Si un archivo de reglas contiene información errónea, también se notifican estos errores del usuario.

El uso de un archivo de reglas para supervisar atributos de archivos y archivos específicos de un sistema requiere planificación. Antes de crear un archivo de reglas, decida qué archivos y atributos de archivos del sistema desea supervisar. Según lo que esté intentando realizar, puede utilizar un archivo de reglas para crear manifiestos o comparar manifiestos, o con otra finalidad.

Para obtener más información sobre el archivo de reglas de BART, consulte [“Formato de archivo de reglas de BART” en la página 124](#) y la página del comando `man bart_rules(4)`.

## Uso de BART (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Crear un manifiesto de BART	Genera una lista de información sobre cada archivo instalado en un sistema.	<a href="#">“Cómo crear un manifiesto” en la página 110</a>

Tarea	Descripción	Para obtener instrucciones
Crear un manifiesto de BART personalizado	<p>Genera una lista de información sobre archivos específicos instalados en un sistema de una de las siguientes formas:</p> <ul style="list-style-type: none"> <li>■ Especificando un subárbol</li> <li>■ Especificando un nombre de archivo</li> <li>■ Mediante un archivo de reglas</li> </ul>	<p><a href="#">“Cómo personalizar un manifiesto” en la página 112</a></p> <p><a href="#">Ejemplo 5-2</a></p> <p><a href="#">Ejemplo 5-3</a></p> <p><a href="#">Ejemplo 5-4</a></p>
Comparar manifiestos de BART	<p>Genera un informe que compara los cambios en un sistema a lo largo del tiempo.</p> <p>O bien, genera un informe que compara uno o varios sistemas con el sistema de control.</p>	<p><a href="#">“Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo” en la página 115</a></p> <p><a href="#">“Cómo comparar manifiestos de diferentes sistemas” en la página 117</a></p>
(Opcional) Personalizar un informe de BART	<p>Genera un informe de BART personalizado de una de las siguientes formas:</p> <ul style="list-style-type: none"> <li>■ Especificando atributos.</li> <li>■ Mediante un archivo de reglas.</li> </ul>	<p><a href="#">“Cómo personalizar un informe de BART especificando atributos de archivos” en la página 120</a></p> <p><a href="#">“Cómo personalizar un informe de BART mediante un archivo de reglas” en la página 121</a></p>

## Uso de BART (tareas)

Puede ejecutar el comando `bart` como un usuario común, un superusuario o un usuario que asume el rol de administrador principal. Si ejecuta el comando `bart` como un usuario común, sólo podrá catalogar y supervisar archivos para los que tiene permiso de acceso, como los archivos en el directorio principal. La ventaja de convertirse en superusuario al ejecutar el comando `bart` es que los manifiestos que crea contienen información sobre archivos ocultos y privados que posiblemente desee supervisar. Si necesita catalogar y supervisar información sobre archivos con permisos restringidos, por ejemplo, el archivo `/etc/passwd` o `/etc/shadow`, ejecute el comando `bart` como superusuario. Para obtener más información sobre el uso del control de acceso basado en roles, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 182](#).

## Consideraciones de seguridad de BART

Si ejecuta el comando `bart` como superusuario, la salida es legible para todos los usuarios. Esta salida puede contener nombres de archivos que deberían ser privados. Si se convierte en superusuario al ejecutar el comando `bart`, tome las medidas adecuadas para proteger la salida. Por ejemplo, utilice opciones que generen archivos de salida con permisos restrictivos.

---

**Nota** – Los procedimientos y ejemplos que se presentan en este capítulo muestran el comando `bart` ejecutado por el superusuario. A menos que se especifique lo contrario, la ejecución del comando `bart` como superusuario es opcional.

---

## ▼ Cómo crear un manifiesto

Puede crear un manifiesto de un sistema inmediatamente después de la instalación inicial del software Oracle Solaris. Este tipo de manifiesto proporciona un punto de partida para comparar los cambios realizados en el mismo sistema a lo largo del tiempo. O bien, puede utilizar este manifiesto para compararlo con los manifiestos para diferentes sistemas. Por ejemplo, si toma una instantánea de cada sistema de la red y, a continuación, compara cada manifiesto de prueba con el manifiesto de control, puede determinar rápidamente lo que necesita hacer para sincronizar el sistema de prueba con la configuración de punto de partida.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Después de instalar el software Oracle Solaris, cree un manifiesto de control y redirija la salida a un archivo.

```
# bart create options > control-manifest
```

- R Especifica el directorio root para el manifiesto. Todas las rutas especificadas por las reglas se interpretan en relación con este directorio. Todas las rutas informadas en el manifiesto están relacionadas con este directorio.
- I Acepta una lista de archivos individuales para catalogarlos, ya sea en la línea de comandos o leídos de la entrada estándar.
- r Nombre del archivo de reglas para este manifiesto. Tenga en cuenta que, cuando – se utiliza con la opción -r, el archivo de reglas se lee desde la entrada estándar.
- n Desactiva firmas de contenido para todos los archivos regulares en la lista de archivos. Esta opción se puede utilizar mejorar el rendimiento. De manera alternativa, puede utilizar esta opción si se espera que cambie el contenido de la lista de archivos, como en el caso de los archivos de registro del sistema.

### 3 Examine el contenido del manifiesto.

### 4 Guarde el manifiesto para uso futuro.

Elija un nombre significativo para el manifiesto. Por ejemplo, utilice el nombre del sistema y la fecha en que se creó el manifiesto.

## Ejemplo 5-1 Creación de un manifiesto que muestra información sobre cada archivo de un sistema

Si ejecuta el comando `bart create` sin ninguna opción, se cataloga la información sobre cada archivo instalado en el sistema. Utilice este tipo de manifiesto como un punto de partida al instalar muchos sistemas desde una imagen central. O bien, utilice este tipo de manifiesto para realizar comparaciones cuando desee asegurarse de que las instalaciones sean idénticas.

Por ejemplo:

```
# bart create
! Version 1.0
! Thursday, December 04, 2003 (16:17:39)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 1024 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea47 0 0
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f8dc04d 0 10
/.java/.userPrefs D 512 40700 user::rwx,group:---,mask:---
other:--- 3f8dc06b 010
/.java/.userPrefs/.user.lock.root F 0 100600 user::rw-
group:---,mask:---,other:--- 3f8dc06b 0 10 -
/.java/.userPrefs/.userRootModFile.root F 0 100600 user::rw-,
group:---,mask:---,other:--- 3f8dc0a1 0 10 -
.
.
.
/var/sadm/pkg/SUNWdtmad/install/depend F 932 100644 user::rw-,
group:r--,mask:r--,other:r-- 3c23a19e 0 0 -
/var/sadm/pkg/SUNWdtmad/pkginfo F 594 100644 user::rw-
group:r--,mask:r--,other:r-- 3f81e416 0 0 -
/var/sadm/pkg/SUNWdtmad/save D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e416 0 0
/var/sadm/pkg/SUNWdtmaz D 512 40755 user::rwx,group::r-x
mask:r-x,other:r-x 3f81e41b 0 0
/var/sadm/pkg/TSIpgxw/save D 512 40755 user::rwx
group:r-x,mask:r-x,other:r-x 3f81e892 0 0
.
.
.
```

Cada manifiesto costa de un encabezado y entradas. Cada entrada de archivo de manifiesto consiste en una sola línea, según el tipo de archivo. Por ejemplo, para cada entrada de manifiesto en la salida anterior, el tipo F especifica un archivo y el tipo D especifica un directorio. También se muestra información sobre el tamaño, el contenido, el ID de usuario, el ID de grupo y los permisos. Las entradas de archivos en la salida se ordenan por versiones codificadas de los nombres de archivos, a fin de manejar correctamente los caracteres especiales. Todas las entradas se ordenan de manera ascendente por nombre de archivo. En todos los nombres de

archivos no estándar, como los que contienen caracteres de tabulación o de línea nueva incrustados, los caracteres no estándar se escriben entre comillas antes de ordenar las entradas.

Las líneas que empiezan por ! proporcionan metadatos sobre el manifiesto. La línea de versión del manifiesto indica la versión de especificación del manifiesto. La línea de fecha muestra la fecha en la que se creó el manifiesto, en formato de fecha. Consulte la página del comando `man date(1)`. La herramienta de comparación de manifiestos ignora algunas líneas. Las líneas ignoradas incluyen líneas en blanco, líneas que contienen sólo espacios en blanco y comentarios que empiezan por #.

## ▼ Cómo personalizar un manifiesto

Puede personalizar un manifiesto de una de las siguientes formas:

- Especificando un subárbol

Crear un manifiesto para un subárbol individual de un sistema es una forma eficaz de supervisar cambios en archivos específicos, en lugar de todo el contenido de un directorio grande. Puede crear un manifiesto de punto de partida de un subárbol específico del sistema y, luego, crear periódicamente manifiestos de prueba del mismo subárbol. Utilice el comando `bart compare` para comparar el manifiesto de control con el manifiesto de prueba. Al utilizar esta opción, puede supervisar eficazmente sistemas de archivos importantes para determinar si algún archivo se vio comprometido por un intruso.

- Especificando un nombre de archivo

Dado que la creación de un manifiesto que cataloga todo el sistema requiere más tiempo, ocupa más espacio y es más costosa, posiblemente elija utilizar esta opción del comando `bart` cuando sólo desee mostrar información sobre un archivo o sobre archivos específicos de un sistema.

- Mediante un archivo de reglas

Puede utilizar un archivo de reglas para crear manifiestos personalizados que muestren información sobre archivos específicos y subárboles específicos de un sistema determinado. También puede utilizar un archivo de reglas para supervisar atributos de archivos específicos. Usar un archivo de reglas para crear y comparar manifiestos le ofrece flexibilidad para especificar varios atributos para más de un archivo o subárbol. Mientras que, desde la línea de comandos, sólo puede especificar una definición global de atributos que se aplica a todos los archivos para cada manifiesto que cree o cada informe que genere.

### 1 Determine los archivos que desea catalogar y supervisar.



## 2 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

## 3 Después de instalar el software Oracle Solaris, cree un manifiesto personalizado mediante una de las siguientes opciones:

- Especificando un subárbol:

```
# bart create -R root-directory
```

- Especificando un nombre de archivo o nombres de archivos:

```
# bart create -I filename...
```

Por ejemplo:

```
# bart create -I /etc/system /etc/passwd /etc/shadow
```

- Mediante un archivo de reglas:

```
# bart create -r rules-file
```

## 4 Examine el contenido del manifiesto.

## 5 Guarde el manifiesto para uso futuro.

### Ejemplo 5–2 Creación de un manifiesto especificando un subárbol

En este ejemplo, se muestra cómo crear un manifiesto que contiene información sobre los archivos del subárbol `/etc/ssh` únicamente.

```
# bart create -R /etc/ssh
! Version 1.0
! Saturday, November 29, 2003 (14:05:36)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81eab9 0 3
/ssh_config F 861 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81e504 0 3 422453ca0e2348cd9981820935600395
/ssh_host_dsa_key F 668 100600 user::rw-,group::---,mask:---,
other:--- 3f81eab9 0 0 5cc28cdc97e833069fd41ef89e4d9834
/ssh_host_dsa_key.pub F 602 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eab9 0 0 16118c736995a4e4754f5ab4f28cf917
/ssh_host_rsa_key F 883 100600 user::rw-,group::---,mask:---,
other:--- 3f81eaa2 0 0 6ff17aa968ecb20321c448c89a8840a9
```

```
/ssh_host_rsa_key.pub F 222 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81eaa2 0 0 9ea27617efc76058cb97aa2caa6dd65a
.
.
.
```

### Ejemplo 5-3 Personalización de un manifiesto especificando un nombre de archivo

En este ejemplo, se muestra cómo crear un manifiesto que únicamente presenta información sobre los archivos `/etc/passwd` y `/etc/shadow` de un sistema.

```
# bart create -I /etc/passwd /etc/shadow
! Version 1.0
! Monday, December 15, 2003 (16:28:55)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/passwd F 542 100444 user::r--,group::r--,mask:r--,
other:r-- 3fcfd45b 0 3 d6
84554f85d1de06219d80543174ad1a
/etc/shadow F 294 100400 user::r--,group::---,mask:---,
other:--- 3f8dc5a0 0 3 fd
c3931c1ae5ee40341f3567b7cf15e2
```

En comparación, la siguiente es la salida estándar del comando `ls -al` para los archivos `/etc/passwd` y `/etc/shadow` del mismo sistema.

```
# ls -al /etc/passwd
-r--r--r-- 1 root sys 542 Dec 4 17:42 /etc/passwd

# ls -al /etc/shadow
-r----- 1 root sys 294 Oct 15 16:09 /etc/shadow
```

### Ejemplo 5-4 Personalización de un manifiesto mediante un archivo de reglas

En este ejemplo, se muestra cómo crear un manifiesto mediante un archivo de reglas para catalogar sólo los archivos del directorio `/etc`. El mismo archivo de reglas incluye directivas que el comando `bart compare` utilizará para supervisar los cambios al atributo `acl` del archivo `/etc/`.

- Use un editor de texto para crear un archivo de reglas que catalogue sólo los archivos del directorio `/etc`.

```
# List information about all the files in the /etc directory.

CHECK all
/etc
```

```
# Check only acl changes in the /etc/system file

IGNORE all
CHECK acl
/etc/system
```

Para obtener más información sobre la creación de un archivo de reglas, consulte [“Archivo de reglas de BART” en la página 107](#).

- Cree un manifiesto de control mediante el archivo de reglas que ha creado.

```
# bart create -r etc.rules-file > etc.system.control-manifest
! Version 1.0
! Thursday, December 11, 2003 (21:51:32)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/etc/system F 1883 100644 user::rw-,group::r--,mask:r--,
other:r-- 3f81db61 0 3
```

- Cree un manifiesto de prueba cada vez que desee supervisar cambios realizados en el sistema. Prepare el manifiesto de prueba de manera idéntica al manifiesto de control utilizando las mismas opciones de `bart` y el mismo archivo de reglas.
- Compare los manifiestos utilizando el mismo archivo de reglas.

## ▼ Cómo comparar manifiestos para el mismo sistema a lo largo del tiempo

Utilice este procedimiento si desea supervisar cambios en el nivel de archivo realizados en el mismo sistema a lo largo del tiempo. Este tipo de manifiesto puede ayudar a encontrar archivos dañados o poco comunes, detectar infracciones de seguridad o solucionar problemas de rendimiento en un sistema.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

### 2 Después de instalar el software Oracle Solaris, cree un manifiesto de control de los archivos que desea supervisar en el sistema.

```
# bart create -R /etc > control-manifest
```

- 3 Cree un manifiesto de prueba que esté preparado de manera idéntica al manifiesto de control cada vez que desee supervisar cambios realizados en el sistema.

```
# bart create -R /etc > test-manifest
```

- 4 Compare el manifiesto de control con el manifiesto de prueba.

```
# bart compare options control-manifest test-manifest > bart-report
```

-r Nombre del archivo de reglas para esta comparación. Cuando la opción -r se utiliza con -, las directivas se leen desde la entrada estándar.

-i Permite que el usuario defina directivas IGNORE globales de la línea de comandos.

-p Modo programático que genera una salida estándar no localizada para el análisis programático.

*manifiesto\_control* Salida del comando bart create para el sistema de control.

*manifiesto\_prueba* Salida del comando bart create del sistema de prueba.

- 5 Examine el informe de BART para encontrar rarezas.

### Ejemplo 5-5 Comparación de manifiestos para el mismo sistema a lo largo del tiempo

En este ejemplo, se muestra cómo supervisar los cambios que se produjeron en el directorio /etc entre dos puntos en el tiempo. Este tipo de comparación permite determinar rápidamente si hay archivos importantes del sistema que se vieron comprometidos.

- Cree un manifiesto de control.

```
# bart create -R /etc > system1.control.121203
! Version 1.0
! Friday, December 12, 2003 (08:34:51)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:--- 3f81f14d
0 1 d41
d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb7
.
```

- Cree un manifiesto de prueba cuando desee supervisar cambios realizados en el directorio /etc.

```
# bart create -R /etc > system1.test.121503
Version 1.0
! Monday, December 15, 2003 (08:35:28)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 4096 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9dfb4 0 3
/.cpr_config F 2236 100644 user::rw-,group::r--,mask:r--,other:r--
3fd9991f 0 0
67cfa2c830b4ce3e112f38c5e33c56a2
/.group.lock F 0 100600 user::rw-,group::---,mask:---,other:---
3f81f14d 0 1 d41d8cd98f00b204e9800998ecf8427e
/.java D 512 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3f81dcb5 0 2
/.java/.systemPrefs D 512 40755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f81dcb70 2
/.java/.systemPrefs/.system.lock F 0 100644 user::rw-,group::r--
,mask:r--,other:
r-- 3f81dcb5 0 2 d41d8cd98f00b204e9800998ecf8427e
/.java/.systemPrefs/.systemRootModFile F 0 100644 user::rw-,
group::r--,mask:r--,
other:r-- 3f81dd0b 0 2 d41d8cd98f00b204e9800998ecf8427e
.
.
.
```

- Compare el manifiesto de control con el manifiesto de prueba.

```
# bart compare system1.control.121203 system1.test.121503
/vfstab:
mode control:100644 test:100777
acl control:user::rw-,group::r--,mask:r--,other:r-- test:user::rwx,
group::rwx,mask:rwx,other:rwx
```

La salida anterior indica que los permisos en el archivo `vfstab` han cambiado desde que se creó el manifiesto de control. Este informe se puede utilizar para investigar si la propiedad, la fecha, el contenido o cualquier otro atributo del archivo han cambiado. Contar con este tipo de información fácilmente disponible puede ayudarlo a averiguar quién podría haber alterado el archivo y cuándo se podría haber producido el cambio.

## ▼ Cómo comparar manifiestos de diferentes sistemas

Puede ejecutar comparaciones entre sistemas, lo cual le permite determinar rápidamente si existen diferencias en el nivel de archivo entre un sistema de punto de partida y los otros

sistemas. Por ejemplo, si ha instalado una versión determinada del software Oracle Solaris en un sistema de punto de partida y desea saber si hay otros sistemas que tengan paquetes idénticos instalados, puede crear manifiestos para esos sistemas y, luego, comparar los manifiestos de prueba con el manifiesto de control. Este tipo de comparación muestra las discrepancias existentes en el contenido del archivo para cada sistema de prueba que se compare con el sistema de control.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Después de instalar el software Oracle Solaris, cree un manifiesto de control.**

```
# bart create options > control-manifest
```

**3 Guarde el manifiesto de control.**

**4 En el sistema de prueba, utilice las mismas opciones de bart para crear un manifiesto y redirija la salida a un archivo.**

```
# bart create options > test1-manifest
```

Elija un nombre significativo y único para el manifiesto de prueba.

**5 Guarde el manifiesto de prueba en una ubicación central en el sistema hasta que esté preparado para comparar manifiestos.**

**6 Si desea comparar manifiestos, copie el manifiesto de control en la ubicación del manifiesto de prueba. O bien, copie el manifiesto de prueba al sistema de control.**

Por ejemplo:

```
# cp manifiesto_control/red/servidor_prueba/bart/manifiestos
```

Si el sistema de prueba no es un sistema montado en NFS, use FTP o algún otro medio confiable para copiar el manifiesto de control al sistema de prueba.

**7 Compare el manifiesto de control con el manifiesto de prueba y redirija la salida a un archivo.**

```
# bart compare control-manifest test1-manifest > test1.report
```

**8 Examine el informe de BART para encontrar rarezas.**

**9 Repita los pasos 4 a 9 para cada manifiesto de prueba que desee comparar con el manifiesto de control.**

Use las mismas opciones de bart para cada sistema de prueba.

## Ejemplo 5-6 Comparación de manifiestos de diferentes sistemas con el manifiesto de un sistema de control

En este ejemplo, se describe cómo supervisar los cambios en el contenido del directorio `/usr/bin` comparando un manifiesto de control con un manifiesto de prueba de un sistema diferente.

- Cree un manifiesto de control.

```
# bart create -R /usr/bin > control-manifest.121203
!Version 1.0
! Friday, December 12, 2003 (09:19:00)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9e925 0 2
/.s F 14200 104711 user::rwx,group::--x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dc71 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
/activation-client F 9172 100755 user::rwx,group::r-x,mask:r-x,
other:r-x 3f5cb907 0 1 b3836ad1a656324a6e1bd01edcba28f0
/adb F 9712 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5736 0 2 5e026413175f65fb239ee628a8870eda
/addbib F 11080 100555 user::r-x,group::r-x,mask:r-x,other:r-x
3f6b5803 0 2 a350836c36049febf185f78350f27510
.
.
.
```

- Cree un manifiesto de prueba para cada sistema que desee comparar con el sistema de control.

```
# bart create -R /usr/bin > system2-manifest.121503
! Version 1.0
! Friday, December 15, 2003 (13:30:58)
# Format:
#fname D size mode acl dirmtime uid gid
#fname P size mode acl mtime uid gid
#fname S size mode acl mtime uid gid
#fname F size mode acl mtime uid gid contents
#fname L size mode acl lnmtime uid gid dest
#fname B size mode acl mtime uid gid devnode
#fname C size mode acl mtime uid gid devnode
/ D 13312 40755 user::rwx,group::r-x,mask:r-x,other:r-x 3fd9ea9c 0 2
/.s F 14200 104711 user::rwx,group::--x,mask:--x,other:--x
3f8dbfd6 0 1 8ec7e52d8a35ba3b054a6394cbf71cf6
/ControlPanel L 28 120777 - 3f81dc71 0 1 jre/bin/ControlPanel
/HtmlConverter L 25 120777 - 3f81dc71 0 1 bin/HtmlConverter
/acctcom F 28300 100555 user::r-x,group::r-x,mask:r-x,other:
```

```
r-x 3f6b5750 0 2 d6e99b19c847ab4ec084d9088c7c7608
```

```
.
```

- Si desea comparar manifiestos, copie los manifiestos en la misma ubicación.

```
# cp control-manifest /net/system2.central/bart/manifests
```

- Compare el manifiesto de control con el manifiesto de prueba.

```
# bart compare control-manifest system2.test > system2.report
```

```
/su:
```

```
gid control:3 test:1
```

```
/ypcat:
```

```
mtime control:3fd72511 test:3fd9eb23
```

La salida anterior indica que el ID de grupo del archivo su en el directorio `/usr/bin` no es el mismo que el del sistema de control. Esta información puede ser útil para determinar si se instaló en el sistema de prueba una versión diferente del software o si es posible que alguien haya alterado el archivo.

## ▼ Cómo personalizar un informe de BART especificando atributos de archivos

Este procedimiento es opcional y explica cómo personalizar un informe de BART especificando atributos de archivos de la línea de comandos. Si crea un manifiesto de punto de partida que muestra información sobre todos los archivos o sobre archivos específicos del sistema, puede ejecutar el comando `bart compare` y especificar atributos diferentes cada vez que necesite supervisar los cambios realizados en un directorio, un subdirectorio o en archivos determinados. Puede ejecutar distintos tipos de comparaciones para los mismos manifiestos especificando atributos de archivos diferentes de la línea de comandos.

### 1 Determine qué atributos de archivos desea supervisar.

### 2 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

### 3 Después de instalar el software Oracle Solaris, cree un manifiesto de control.

### 4 Cree un manifiesto de prueba cuando desee supervisar cambios.

Prepare el manifiesto de prueba de manera idéntica al manifiesto de control.



## 5 Compare los manifiestos.

Por ejemplo:

```
# bart compare -i dirmtime,lnmtime,mtime control-manifest.121503 \
test-manifest.010504 > bart.report.010504
```

Tenga en cuenta que una coma separa cada atributo que especifique en la sintaxis de la línea de comandos.

## 6 Examine el informe de BART para encontrar rarezas.

# ▼ Cómo personalizar un informe de BART mediante un archivo de reglas

Este procedimiento también es opcional y explica cómo personalizar un informe de BART mediante un archivo de reglas como entrada para el comando `bart compare`. Mediante un archivo de reglas, puede personalizar un informe de BART, lo cual le ofrece flexibilidad para especificar varios atributos para más de un archivo o subárbol. Puede ejecutar distintas comparaciones para los mismos manifiestos mediante archivos de reglas diferentes.

## 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

## 2 Determine qué archivos y atributos de archivos desea supervisar.

## 3 Use un editor de texto para crear un archivo de reglas con las directivas adecuadas.

## 4 Después de instalar el software Oracle Solaris, cree un manifiesto de control mediante el archivo de reglas que ha creado.

```
# bart create -r rules-file > control-manifest
```

## 5 Cree un manifiesto de prueba que esté preparado de manera idéntica al manifiesto de control.

```
# bart create -r rules-file > test-manifest
```

## 6 Compare el manifiesto de control con el manifiesto de prueba usando el mismo archivo de reglas.

```
# bart compare -r rules-file control-manifest test-manifest > bart.report
```

## 7 Examine el informe de BART para encontrar rarezas.

### Ejemplo 5-7 Personalización de un informe de BART mediante un archivo de reglas

El siguiente archivo de reglas incluye directivas para los comandos `bart create` y `bart compare`. El archivo de reglas le indica al comando `bart create` que muestre información sobre el contenido del directorio `/usr/bin`. Además, el archivo de reglas le indica al comando `bart compare` que sólo realice un seguimiento de los cambios de tamaño y contenido en el mismo directorio.

```
# Check size and content changes in the /usr/bin directory.  
# This rules file only checks size and content changes.  
# See rules file example.
```

```
IGNORE all  
CHECK size contents  
/usr/bin
```

- Cree un manifiesto de control mediante el archivo de reglas que ha creado.

```
# bart create -r bartrules.txt > usr_bin.control-manifest.121003
```

- Cree un manifiesto de prueba cada vez que desee supervisar cambios realizados en el directorio `/usr/bin`.

```
# bart create -r bartrules.txt > usr_bin.test-manifest.121103
```

- Compare los manifiestos utilizando el mismo archivo de reglas.

```
# bart compare -r bartrules.txt usr_bin.control-manifest \  
usr_bin.test-manifest
```

- Examine la salida del comando `bart compare`.

```
/usr/bin/gunzip: add  
/usr/bin/ypcat:  
delete
```

En la salida anterior, el comando `bart compare` informó una discrepancia en el directorio `/usr/bin`. Esta salida indica que se eliminó el archivo `/usr/bin/ypcat` y se agregó el archivo `/usr/bin/gunzip`.

## Manifiestos, archivos de reglas e informes de BART (referencia)

En esta sección, se incluye la siguiente información de referencia:

- [“Formato de archivo de manifiesto de BART” en la página 123](#)
- [“Formato de archivo de reglas de BART” en la página 124](#)
- [“Creación de informes de BART” en la página 125](#)

En esta sección, se describe el formato de archivos que BART utiliza y crea.

## Formato de archivo de manifiesto de BART

Cada entrada de archivo de manifiesto consiste en una sola línea, según el tipo de archivo. Cada entrada comienza con *fname*, que es el nombre del archivo. Para evitar problemas de análisis causados por caracteres especiales incrustados en los nombres de archivos, estos últimos se codifican. Para obtener más información, consulte [“Formato de archivo de reglas de BART” en la página 124](#).

Los campos que se enumeran a continuación representan los siguientes atributos de archivos:

<i>type</i>	Tipo de archivo con los siguientes valores posibles: <ul style="list-style-type: none"> <li>▪ B para un nodo de dispositivo de bloques</li> <li>▪ C para un nodo de dispositivo de caracteres</li> <li>▪ D para un directorio</li> <li>▪ F para un archivo</li> <li>▪ L para un enlace simbólico</li> <li>▪ P para una conducción</li> <li>▪ S para un socket</li> </ul>
<i>size</i>	Tamaño del archivo en bytes.
<i>mode</i>	Número octal que representa los permisos del archivo.
<i>acl</i>	Atributos de ACL del archivo. Para un archivo con atributos de ACL, contiene la salida de <code>acltotext()</code> .
<i>uid</i>	ID de usuario numérico del propietario de esta entrada.
<i>gid</i>	ID de grupo numérico del propietario de esta entrada.
<i>dirmtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los directorios.
<i>lnmtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los enlaces.
<i>mtime</i>	Hora de la última modificación, en segundos, desde las 00:00:00 UTC del 1 de enero de 1970, para los archivos.
<i>contents</i>	Valor de suma de comprobación del archivo. Este atributo sólo se especifica para los archivos regulares. Si desactiva la comprobación del contexto, o si las sumas de comprobación no se pueden calcular, el valor de este campo es –.
<i>dest</i>	Destino de un enlace simbólico.
<i>devnode</i>	Valor del nodo de dispositivo. Este atributo es sólo para archivos del dispositivo de caracteres y archivos del dispositivo de bloques.

Para obtener más información sobre manifiestos de BART, consulte la página del comando `man bart_manifest(4)`.

## Formato de archivo de reglas de BART

Los archivos de entrada del comando `bart` son archivos de texto. Estos archivos constan de líneas que especifican qué archivos se deben incluir en el manifiesto y qué atributos de archivos se deben incluir en el informe. El mismo archivo de entrada se puede utilizar en ambas partes de la funcionalidad de BART. La herramienta ignora las líneas que empiezan por `#`, las líneas en blanco y las líneas que contienen espacios en blanco.

Los archivos de entrada tienen tres tipos de directivas:

- Directiva de subárbol, con modificadores de coincidencia de modelos opcionales
- Directiva CHECK
- Directiva IGNORE

### EJEMPLO 5-8 Formato de archivo de reglas

```
<Global CHECK/IGNORE Directives>
<subtree1> [pattern1..]
<IGNORE/CHECK Directives for subtree1>

<subtree2> [pattern2..]
<subtree3> [pattern3..]
<subtree4> [pattern4..]
<IGNORE/CHECK Directives for subtree2, subtree3, subtree4>
```

---

**Nota** – Todas las directivas se leen en orden; las directivas más recientes posiblemente reemplacen las directivas más antiguas.

---

Hay una directiva de subárbol por línea. La directiva *debe* comenzar por un nombre de ruta absoluto, seguido de cero o más sentencias de coincidencia de modelos.

## Atributos de archivo de reglas

El comando `bart` utiliza las sentencias CHECK e IGNORE para definir qué atributos se deben seguir o ignorar. Cada atributo tiene una palabra clave asociada.

Las *palabras clave* de los atributos son las siguientes:

- `acl`
- `all`
- `contents`
- `dest`
- `devnode`
- `dirmtime`
- `gid`

- `lnmtime`
- `mode`
- `mtime`
- `size`
- `type`
- `uid`

La palabra clave `all` se refiere a todos los atributos del archivo.

## Sintaxis de comillas

El idioma de especificación del archivo de reglas que BART utiliza es la sintaxis de comillas estándar de UNIX para representar nombres de archivos no estándar. Los caracteres incrustados de tabulación, espacio, línea nueva o caracteres especiales se codifican en sus formas octales para permitir que la herramienta lea nombres de archivos. Esta sintaxis de comillas no uniforme evita que determinados nombres de archivos, como los que contienen un retorno de carro incrustado, se procesen correctamente en una canalización de comando. El idioma de especificación de reglas permite la expresión de criterios de filtrado de nombres de archivos complejos, que sería difícil de describir, y poco eficaz, al utilizar la sintaxis de shell sola.

Para obtener más información sobre el archivo de reglas de BART o la sintaxis de comillas utilizada por BART, consulte la página del comando `man bart\_rules\(4\)`.

## Creación de informes de BART

En el modo predeterminado, el comando `bart compare`, como se muestra en el ejemplo siguiente, comprueba todos los archivos instalados en el sistema, con la excepción de las indicaciones de hora modificadas del directorio (`dirmtime`):

```
CHECK all
IGNORE  dirmtime
```

Si proporciona un archivo de reglas, las directivas globales `CHECK all` e `IGNORE dirmtime`, en ese orden, se anteponen automáticamente al archivo de reglas.

## Salida de BART

Se devolvieron los siguientes valores de salida:

- 0      Éxito
- 1      Error no fatal durante el procesamiento de archivos, como problemas de permisos
- >1    Error fatal, como una opción de línea de comandos no válida

El mecanismo de creación de informes ofrece dos tipos de salidas, detallada y programática:

- La salida detallada es la salida predeterminada, y se localiza y se presenta en varias líneas. La salida detallada está internacionalizada y en lenguaje natural. Cuando el comando `bart compare` compara dos manifiestos el sistema, se genera una lista de diferencias de archivos.

Por ejemplo:

*filename attribute control:xxxx test:yyyy*

*nombre\_archivo*      Nombre del archivo que difiere entre el manifiesto de control y el manifiesto de prueba.

*atributo*              Nombre del atributo de archivo que difiere entre los manifiestos que se comparan. *xxxx* es el valor del atributo del manifiesto de control y *yyyy* es el valor del atributo del manifiesto de prueba. Cuando las discrepancias de varios atributos se producen en un mismo archivo, cada diferencia se indica en una línea separada.

A continuación, se muestra un ejemplo de la salida predeterminada para el comando `bart compare`. Las diferencias del atributo son para el archivo `/etc/passwd`. La salida indica que los atributos `size`, `mtime` y `contents` han cambiado.

```
/etc/passwd:
size      control:74      test:81
mtime control:3c165879 test:3c165979
contents  control:daca28ae0de97afd7a6b91fde8d57afa
test:84b2b32c4165887355317207b48a6ec7
```

- La salida programática se genera si se utiliza la opción `-p` al ejecutar el comando `bart compare`. Esta salida se genera en una forma adecuada para la manipulación programática. Otros programas pueden analizar fácilmente la salida programática; esta salida está diseñada para utilizarse como entrada para otras herramientas.

Por ejemplo:

*filename attribute control-val test-val [attribute control-val test-val]\**

*nombre\_archivo*              Igual que el atributo *nombre\_archivo* en el formato predeterminado

*atributo val\_control val\_prueba*      Una descripción de los atributos de archivos que difieren entre los manifiestos de control y de prueba para cada archivo

Para ver una lista de atributos admitidos por el comando `bart`, consulte [“Atributos de archivo de reglas” en la página 124](#).

Para obtener más información sobre BART, consulte la página del comando `man bart(1M)`.

## Control de acceso a archivos (tareas)

---

En este capítulo, se describe cómo proteger archivos en Oracle Solaris. Asimismo, se describe cómo proteger el sistema contra archivos cuyos permisos podrían ponerlo en peligro.

---

**Nota** – Para proteger los archivos ZFS con listas de control de acceso (ACL), consulte el [Capítulo 8](#), “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de *Guía de administración de Oracle Solaris ZFS*.

---

A continuación, se presenta la información que se incluye en este capítulo.

- “Uso de permisos UNIX para proteger archivos” en la página 127
- “Uso de listas de control de acceso para proteger archivos UFS” en la página 134
- “Cómo impedir que los archivos ejecutables pongan en riesgo la seguridad” en la página 137
- “Protección de archivos (mapa de tareas)” en la página 138
- “Protección de archivos con permisos UNIX (mapa de tareas)” en la página 138
- “Protección de archivos UFS con ACL (mapa de tareas)” en la página 144
- “Protección contra programas con riesgo de seguridad (mapa de tareas)” en la página 150

### Uso de permisos UNIX para proteger archivos

Los archivos se pueden proteger mediante permisos de archivo UNIX y mediante ACL. Los archivos con bits de permanencia y los archivos que son ejecutables requieren medidas de seguridad especiales.

### Comandos para visualizar y proteger archivos

En esta tabla, se describen los comandos para supervisar y proteger archivos y directorios.

TABLA 6-1 Comandos para proteger archivos y directorios

Comando	Descripción	Página del comando man
ls	Muestra los archivos en un directorio e información sobre los archivos.	<a href="#">ls(1)</a>
chown	Cambia la propiedad de un archivo.	<a href="#">chown(1)</a>
chgrp	Cambia la propiedad de grupo de un archivo.	<a href="#">chgrp(1)</a>
chmod	Cambia permisos en un archivo. Puede utilizar el modo simbólico, que utiliza letras y símbolos, o el modo absoluto, que utiliza números octales, para cambiar los permisos en un archivo.	<a href="#">chmod(1)</a>

## Propiedad de archivos y directorios

Los permisos de archivo UNIX tradicionales pueden asignar propiedad a tres clases de usuarios:

- **usuario:** el propietario del archivo o directorio, que, normalmente, es el usuario que creó el archivo. El propietario de un archivo puede decidir quién tiene derecho a leer el archivo, escribir en el archivo (realizar cambios en él) o, si el archivo es un comando, ejecutar el archivo.
- **grupo:** los miembros de un grupo de usuarios.
- **otros:** todos los demás usuarios que no son los propietarios del archivo y no son miembros del grupo.

El propietario del archivo, normalmente, puede asignar o modificar permisos de archivo. Además, los usuarios o roles con capacidades administrativas, como superusuario o el rol de administrador principal, pueden cambiar la propiedad de un archivo. Para sustituir la directiva del sistema, consulte el [Ejemplo 6-2](#).

Un archivo puede ser uno de siete tipos. Cada tipo se muestra con un símbolo:

- (símbolo menos)	Texto o programa
<b>b</b>	Archivo especial de bloques
<b>c</b>	Archivo especial de caracteres
<b>d</b>	Directorio
<b>l</b>	Enlace simbólico
<b>s</b>	Socket
<b>D</b>	Puerta
<b>P</b>	Conducción con nombre (FIFO)



## Permisos de archivo UNIX

En la siguiente tabla, se muestran y se describen los permisos que puede otorgar a cada clase de usuario para un archivo o directorio.

**TABLA 6-2** Permisos de archivos y directorios

Símbolo	Permiso	Objeto	Descripción
r	Lectura	Archivo	Los usuarios designados pueden abrir y leer el contenido de un archivo.
		Directorio	Los usuarios designados pueden enumerar archivos en el directorio.
w	Escritura	Archivo	Los usuarios designados pueden modificar el contenido del archivo o eliminar el archivo.
		Directorio	Los usuarios designados pueden agregar archivos o enlaces en el directorio. También pueden eliminar archivos o enlaces en el directorio.
x	Ejecución	Archivo	Los usuarios designados pueden ejecutar el archivo si es un programa o una secuencia de comandos de shell. También pueden ejecutar el programa con una de las llamadas del sistema <code>exec(2)</code> .
		Directorio	Los usuarios designados pueden abrir o ejecutar archivos en el directorio. También pueden hacer que el directorio y los directorios debajo de él sean los actuales.
-	Denegado	Archivo y directorio	Los usuarios designados no pueden leer, escribir ni ejecutar el archivo.

Estos permisos de archivo se aplican a archivos regulares y a archivos especiales, como dispositivos, sockets y conducciones con nombre (FIFO).

Para un enlace simbólico, los permisos que se aplican son los permisos del archivo al que el enlace hace referencia.

Puede proteger los archivos de un directorio y sus subdirectorios estableciendo permisos de archivo restrictivos en ese directorio. Tenga en cuenta que, sin embargo, el superusuario tiene acceso a todos los archivos y directorios en el sistema.

## Permisos de archivo especiales (setuid, setgid y bit de permanencia)

Tres tipos de permisos especiales están disponibles para archivos ejecutables y directorios públicos: `setuid`, `setgid` y bit de permanencia. Cuando estos permisos se establecen, cualquier usuario que ejecuta ese archivo ejecutable asume el ID del propietario (o grupo) del archivo ejecutable.

Debe ser extremadamente cuidadoso cuando define permisos especiales, porque los permisos especiales constituyen un riesgo de seguridad. Por ejemplo, un usuario puede obtener capacidades de superusuario mediante la ejecución de un programa que establece el ID de usuario (UID) en 0, que es el UID de root. Además, todos los usuarios pueden establecer permisos especiales para archivos que poseen, lo cual constituye otro problema de seguridad.

Debe supervisar el sistema para detectar cualquier uso no autorizado de los permisos `setuid` y `setgid` con intención de obtener capacidades de superusuario. Un permiso sospechoso concede la propiedad de un programa administrativo a un usuario en lugar de a root o bin. Para buscar y mostrar todos los archivos que utilizan este permiso especial, consulte [“Cómo buscar archivos con permisos de archivo especiales” en la página 150](#).

## Permiso `setuid`

Cuando el permiso `setuid` se establece en un archivo ejecutable, se otorga acceso a un proceso que ejecuta este archivo según el propietario del archivo. El acceso *no* se basa en el usuario que está ejecutando el archivo ejecutable. Este permiso especial permite a un usuario acceder a los archivos y directorios que, normalmente, están disponibles sólo para el propietario.

Por ejemplo, el permiso `setuid` del comando `passwd` hace posible que los usuarios cambien contraseñas. Un comando `passwd` con permiso `setuid` sería de la siguiente manera:

```
-r-sr-sr-x  3 root    sys      28144 Jun 17 12:02 /usr/bin/passwd
```

Este permiso especial presenta un riesgo de seguridad. Algunos usuarios determinados pueden buscar una manera de mantener los permisos que se les otorgan mediante el proceso `setuid`, incluso después de que el proceso ha terminado de ejecutarse.

---

**Nota** – El uso de permisos `setuid` con los UID reservados (de 0 a 100) de un programa podría no establecer el UID efectivo correctamente. Utilice una secuencia de comandos de shell o evite el uso de los UID reservados con permisos `setuid`.

---

## Permiso `setgid`

El permiso `setgid` es similar al permiso `setuid`. Se cambia el ID de grupo (GID) efectivo del proceso al grupo que posee el archivo y se le concede acceso a un usuario según los permisos que se otorgan a ese grupo. El comando `/usr/bin/mail` tiene permisos `setgid`:

```
-r-x--s--x  1 root    mail     67504 Jun 17 12:01 /usr/bin/mail
```

Cuando el permiso `setgid` se aplica a un directorio, los archivos que se crearon en ese directorio pertenecen al grupo al que pertenece el directorio. Los archivos no pertenecen al grupo al que pertenece el proceso de creación. Cualquier usuario que tiene permisos de escritura y ejecución en el directorio puede crear un archivo allí. Sin embargo, el archivo pertenece al grupo que posee el directorio, no al grupo al que pertenece el usuario.

Debe supervisar el sistema para detectar cualquier uso no autorizado del permiso `setgid` con intención de obtener capacidades de superusuario. Un permiso sospechoso otorga acceso de grupo a tal programa a un grupo poco común en lugar de a `root` o `bin`. Para buscar y mostrar todos los archivos que utilizan este permiso, consulte [“Cómo buscar archivos con permisos de archivo especiales” en la página 150](#).

## Bit de permanencia

El *bit de permanencia* es un bit de permiso que protege los archivos dentro de un directorio. Si el directorio tiene el bit de permanencia establecido, un archivo sólo puede ser eliminado por el propietario del archivo, el propietario del directorio o un usuario con privilegios. El usuario `root` y el rol de administrador principal son ejemplos de usuarios con privilegios. El bit de permanencia impide que un usuario elimine los archivos de otros usuarios de directorios públicos, como `/tmp`:

```
drwxrwxrwt 7 root sys 400 Sep 3 13:37 tmp
```

Asegúrese de definir el bit de permanencia manualmente al configurar un directorio público en un sistema de archivos TMPFS. Para obtener instrucciones, consulte el [Ejemplo 6-5](#).

## Valor umask predeterminado

Al crear un archivo o directorio, se crea con un conjunto predeterminado de permisos. Los valores predeterminados del sistema son abiertos. Un archivo de texto tiene permisos `666`, que conceden permisos de lectura y escritura a todos los usuarios. Un directorio y un archivo ejecutable tienen permisos `777`, que conceden permisos de lectura, escritura y ejecución a todos los usuarios. Normalmente, los usuarios sustituyen los valores predeterminados del sistema en los archivos `/etc/profile`, `.cshrc` o `.login`.

El valor asignado por el comando `umask` se obtiene del valor predeterminado. Este proceso tiene el efecto de denegar permisos de la misma forma que el comando `chmod` los otorga. Por ejemplo, el comando `chmod 022` otorga permiso de escritura para grupo y otros. El comando `umask 022` deniega permiso de escritura para grupo y otros.

En la siguiente tabla, se muestran algunos valores `umask` típicos y el efecto que tienen en un archivo ejecutable.

**TABLA 6-3** Valores `umask` para niveles de seguridad diferentes

Nivel de seguridad	Valor <code>umask</code>	Permisos no permitidos
Permisivo (744)	022	w para grupo y otros
Moderado (740)	027	w para grupo, rwx para otros
Moderado (741)	026	w para grupo, rw para otros

TABLA 6-3 Valores umask para niveles de seguridad diferentes (Continuación)

Nivel de seguridad	Valor umask	Permisos no permitidos
Grave (700)	077	rwX para grupo y otros

Para obtener más información sobre el establecimiento del valor umask, consulte la página del comando `man umask(1)`.

## Modos de permiso de archivo

El comando `chmod` permite cambiar los permisos en un archivo. Debe ser superusuario o el propietario de un archivo o directorio para cambiar los permisos.

Puede utilizar el comando `chmod` para definir permisos en uno de los dos modos siguientes:

- **Modo absoluto:** use números para representar permisos de archivo. Al cambiar los permisos mediante el modo absoluto, representa los permisos para cada triplo con un número de modo octal. El modo absoluto es el método que se utiliza con más frecuencia para establecer permisos.
- **Modo simbólico:** utilice combinaciones de letras y símbolos para agregar o eliminar permisos.

En la siguiente tabla, se muestran los valores octales para configurar permisos de archivo en modo absoluto. Use estos números en conjuntos de tres para definir permisos para propietario, grupo y otros, en ese orden. Por ejemplo, el valor 644 establece permisos de lectura y escritura para propietario, y permisos de sólo lectura para grupo y otros.

TABLA 6-4 Establecimiento de permisos de archivo en modo absoluto

Valor octal	Permisos de archivo establecidos	Descripción de permisos
0	- - -	Sin permisos
1	- - X	Sólo permiso de ejecución
2	- W -	Sólo permiso de escritura
3	- W X	Permisos de escritura y ejecución
4	r - -	Sólo permiso de lectura
5	r - X	Permisos de lectura y ejecución
6	r W -	Permisos de lectura y escritura
7	r W X	Permisos de lectura, escritura y ejecución

En la siguiente tabla, se muestran los símbolos para establecer permisos de archivo en modo simbólico. Los símbolos pueden especificar los permisos de qué usuarios se van a definir o cambiar, la operación que se va a realizar y los permisos que se están asignando o cambiando.

**TABLA 6-5** Establecimiento de permisos de archivo en modo simbólico

Símbolo	Función	Descripción
u	<i>who</i>	Usuario (propietario)
g	<i>who</i>	Grupo
o	<i>who</i>	Otros
a	<i>who</i>	Todos
=	<i>operator</i>	Asignación
+	<i>operator</i>	Adición
-	<i>operator</i>	Eliminación
r	<i>permissions</i>	Lectura
w	<i>permissions</i>	Escritura
x	<i>permissions</i>	Ejecución
l	<i>permissions</i>	Bloqueo obligatorio, bit <code>setgid</code> está activado, bit de ejecución de grupo está desactivado
s	<i>permissions</i>	Bit <code>setuid</code> o <code>setgid</code> está activado
t	<i>permissions</i>	Bit de permanencia está activado, bit de ejecución para otros está activado

Las designaciones *who operator permissions* en la columna de función especifican los símbolos que cambian los permisos en el archivo o directorio.

*who* Especifica los permisos de qué usuarios se van a cambiar.

*operator* Especifica la operación que se va a realizar.

*permissions* Especifica qué permisos se van a cambiar.

Puede definir permisos especiales en un archivo en modo absoluto o modo simbólico. No obstante, debe utilizar el modo simbólico para definir o eliminar permisos `setuid` en un directorio. En el modo absoluto, los permisos especiales se establecen agregando un nuevo valor octal a la izquierda del tripo de permiso. En la siguiente tabla, se muestran los valores octales para definir permisos especiales en un archivo.

TABLA 6-6 Establecimiento de permisos de archivo especiales en modo absoluto

Valor octal	Permisos de archivo especiales
1	Bit de permanencia
2	setgid
4	setuid

## Uso de listas de control de acceso para proteger archivos UFS

La protección de archivos UNIX tradicionales proporciona permisos de lectura, escritura y ejecución para las tres clases de usuario: propietario de archivo, grupo de archivos y otros. En un sistema de archivos UFS, una lista de control de acceso (ACL) proporciona una mayor seguridad para los archivos, ya que le permite hacer lo siguiente:

- Definir permisos de archivo para el propietario del archivo, el grupo, otros y usuarios y grupos específicos.
- Definir permisos predeterminados para cada una de las categorías anteriores.

**Nota** – Para las ACL en el sistema de archivos ZFS y las ACL en archivos NFSv4, consulte el [Capítulo 8, “Uso de listas de control de acceso y atributos para proteger archivos Oracle Solaris ZFS” de Guía de administración de Oracle Solaris ZFS](#).

Por ejemplo, si desea que todos los usuarios de un grupo puedan leer un archivo, puede, simplemente, conceder permisos de lectura de grupo en ese archivo. Ahora, suponga que desea que sólo una persona en el grupo pueda escribir en ese archivo. UNIX estándar no proporciona ese nivel de seguridad de archivo. Sin embargo, una ACL sí lo hace.

En un sistema de archivos UFS, las entradas de la ACL se establecen en un archivo mediante el comando `setfacl`. Las entradas de la ACL de UFS constan de los siguientes campos separados por dos puntos:

<i>entry-type</i> : <i>[uid gid]:perms</i>	
<i>entry-type</i>	Es el tipo de entrada de ACL en la que se deben definir permisos de archivo. Por ejemplo, <i>entry-type</i> puede ser <i>user</i> (el propietario de un archivo) o <i>mask</i> (la máscara de la ACL). Para obtener un listado de entradas de ACL, consulte la <a href="#">Tabla 6-7</a> y la <a href="#">Tabla 6-8</a> .
<i>uid</i>	Es el nombre de usuario o el ID de usuario (UID).
<i>gid</i>	Es el nombre de grupo o el ID de grupo (GID).
<i>perms</i>	Representa los permisos que se establecen en <i>entry-type</i> . <i>perms</i> se puede indicar con los caracteres simbólicos <i>rwX</i> o un número octal. Estos son los mismos

números que se utilizan con el comando `chmod`.

En el siguiente ejemplo, una entrada de la ACL establece permisos de lectura y escritura para el usuario `stacey`.

```
user:stacey:rw-
```



**Precaución** – Los atributos del sistema de archivos UFS, como las ACL, sólo se admiten en sistemas de archivos UFS. Por lo tanto, si restaura o copia archivos con entradas de la ACL en el directorio `/tmp`, que suele estar montado como un sistema de archivos TMPFS, las entradas de la ACL se perderán. Utilice el directorio `/var/tmp` para el almacenamiento temporal de los archivos UFS.

## Entradas de ACL para archivos UFS

En la siguiente tabla, se muestran las entradas de la ACL válidas que puede usar cuando configura ACL en archivos. Las tres primeras entradas de la ACL proporcionan la protección de archivos UNIX básica.

**TABLA 6-7** Entradas de ACL para archivos UFS

Entrada de ACL	Descripción
<code>u[ser]::perms</code>	Permisos de propietario de archivo.
<code>g[roup]::perms</code>	Permisos de grupo de archivos.
<code>o[ther]::perms</code>	Permisos para usuarios no sean el propietario del archivo ni miembros del grupo de archivos.
<code>m[ask]::perms</code>	La máscara de la ACL. La entrada de máscara indica el número máximo de permisos que están permitidos para usuarios (excepto el propietario) y para grupos. La máscara es una forma rápida de cambiar permisos en todos los usuarios y grupos.  Por ejemplo, la entrada de máscara <code>mask:r - -</code> indica que los usuarios y los grupos no pueden tener más que permisos de lectura, aunque sus cuentas indiquen que tienen permisos de escritura y ejecución.
<code>u[ser]:uid:perms</code>	Permisos para un usuario específico. Para <i>uid</i> , puede especificar un nombre de usuario o un UID numérico.
<code>g[roup]:gid:perms</code>	Permisos para un grupo específico. Para <i>gid</i> , puede especificar un nombre de grupo o un GID numérico.

## Entradas de ACL para directorios UFS

Además de las entradas de la ACL que se describen en la [Tabla 6–7](#), puede definir entradas de ACL predeterminadas en un directorio. Los archivos o directorios creados en un directorio que tiene entradas de ACL predeterminadas tendrán las mismas entradas de ACL que las entradas de ACL predeterminadas. En la [Tabla 6–8](#), se muestran las entradas de ACL predeterminadas para directorios.

Al definir entradas de ACL predeterminadas para usuarios y grupos específicos en un directorio por primera vez, también debe establecer entradas de ACL predeterminadas para el propietario del archivo, el grupo de archivos, otros y la máscara de la ACL. Estas entradas son obligatorias. Son las primeras cuatro entradas de la ACL predeterminadas de la tabla siguiente.

**TABLA 6–8** Entradas de ACL predeterminadas para directorios UFS

Entrada de ACL predeterminada	Descripción
<code>d[efault]:u[ser]::perms</code>	Permisos de propietario de archivo predeterminados.
<code>d[efault]:g[roup]::perms</code>	Permisos de grupo de archivos predeterminados.
<code>d[efault]:o[ther]:perms</code>	Permisos predeterminados para usuarios no sean el propietario del archivo ni miembros del grupo de archivos.
<code>d[efault]:m[ask]:perms</code>	Máscara de ACL predeterminada.
<code>d[efault]:u[ser]:uid:perms</code>	Permisos predeterminados para un usuario específico. Para <i>uid</i> , puede especificar un nombre de usuario o un UID numérico.
<code>d[efault]:g[roup]:gid:perms</code>	Permisos predeterminados para un grupo específico. Para <i>gid</i> , puede especificar un nombre de grupo o un GID numérico.

## Comandos para administrar ACL de UFS

Los siguientes comandos administran ACL en archivos o directorios UFS.

- comando `setfacl` Establece, agrega, modifica y elimina entradas de la ACL. Para obtener más información, consulte la página del comando `man setfacl(1)`.
- comando `getfacl` Muestra entradas de la ACL. Para obtener más información, consulte la página del comando `man getfacl(1)`.



# Cómo impedir que los archivos ejecutables pongan en riesgo la seguridad

Varios errores de seguridad están relacionados con las pilas ejecutables predeterminadas cuando los permisos están establecidos en lectura, escritura y ejecución. Si bien las pilas con permisos de ejecución están permitidas, la mayoría de los programas pueden funcionar correctamente sin utilizar pilas ejecutables.

La variable `noexec_user_stack` permite especificar si las asignaciones de pilas son ejecutables. La variable está disponible a partir de la versión Solaris 2.6. De manera predeterminada, esta variable está establecida en cero, excepto en aplicaciones de 64 bits, que proporciona un comportamiento compatible con ABI. Si la variable está establecida en un valor que no es cero, el sistema marca la pila de cada uno de los procesos del sistema como que se puede leer y escribir, pero no ejecutar.

Una vez que esta variable se define, se envía una señal SIGSEGV a los programas que intentan ejecutar el código en sus pilas. Esta señal, normalmente, tiene como resultado la terminación del programa con un volcado del núcleo central. Esos programas también generan un mensaje de advertencia que incluye el nombre del programa ofensivo, el ID de proceso y el UID real del usuario que ejecutó el programa. Por ejemplo:

```
a.out[347] attempt to execute code on stack by uid 555
```

El mensaje es registrado por el daemon `syslog` cuando la utilidad `syslog kern` está establecida en el nivel `notice`. Este registro está establecido de manera predeterminada en el archivo `syslog.conf`, lo que significa que el mensaje se envía a la consola y al archivo `/var/adm/messages`. Para obtener más información, consulte las páginas del comando `man syslogd(1M)` y `syslog.conf(4)`.

El mensaje `syslog` es útil para observar posibles problemas de seguridad. El mensaje también identifica programas válidos que dependen de pilas ejecutables cuyo funcionamiento correcto ha sido impedido al establecer esta variable. Si no desea que se registre ningún mensaje, establezca la variable `noexec_user_stack_log` en cero, en el archivo `/etc/system`. Aunque los mensajes no se registran, la señal SIGSEGV puede continuar para hacer que el programa en ejecución finalice con un volcado del núcleo central.

Puede utilizar la función `mprotect()` si desea que los programas marquen de forma explícita sus pilas como ejecutables. Para obtener más información, consulte la página del comando `man mprotect(2)`.

Debido a las limitaciones de hardware, la capacidad de capturar y generar informes de problemas de pilas ejecutables no está disponible en la mayoría de los sistemas basados en x86. Los sistemas de la familia de productos AMD64 pueden capturar e informar problemas de pilas ejecutables.

# Protección de archivos (mapa de tareas)

El siguiente mapa de tareas hace referencia a conjuntos de procedimientos para proteger archivos.

Tarea	Descripción	Para obtener instrucciones
Usar permisos UNIX para proteger archivos	Permite visualizar permisos UNIX en archivos. Protege archivos con permisos UNIX.	<a href="#">“Protección de archivos con permisos UNIX (mapa de tareas)” en la página 138</a>
Usar ACL para proteger archivos	Agrega ACL para proteger archivos en un nivel más granular que los permisos UNIX.	<a href="#">“Protección de archivos UFS con ACL (mapa de tareas)” en la página 144</a>
Proteger el sistema contra archivos que implican un riesgo de seguridad	Busca archivos ejecutables que tienen una propiedad sospechosa. Deshabilita archivos que pueden dañar el sistema.	<a href="#">“Protección contra programas con riesgo de seguridad (mapa de tareas)” en la página 150</a>

# Protección de archivos con permisos UNIX (mapa de tareas)

El siguiente mapa de tareas indica procedimientos que enumeran permisos de archivo, cambian permisos de archivo y protegen archivos con permisos de archivo especiales.

Tarea	Para obtener instrucciones
Visualizar información de archivos	<a href="#">“Cómo visualizar información de archivos” en la página 138</a>
Cambiar propiedad de archivos	<a href="#">“Cómo cambiar el propietario de un archivo local” en la página 139</a> <a href="#">“Cómo cambiar la propiedad de grupo de un archivo” en la página 140</a>
Cambiar permisos de archivo	<a href="#">“Cómo cambiar los permisos de archivo en modo simbólico” en la página 141</a> <a href="#">“Cómo cambiar permisos de archivo en modo absoluto” en la página 142</a> <a href="#">“Cómo cambiar permisos de archivo especiales en modo absoluto” en la página 143</a>

## ▼ Cómo visualizar información de archivos

Visualice información sobre todos los archivos en un directorio mediante el comando `ls`.

- **Escriba el siguiente comando para mostrar un listado largo de todos los archivos en el directorio actual.**

`% ls -la`

`-l` Muestra el formato largo que incluye la propiedad de usuario, la propiedad de grupo y los permisos de archivo.

- a Muestra todos los archivos, incluidos los archivos ocultos que empiezan con un punto (.).

### Ejemplo 6-1 Visualización de información de archivos

En el siguiente ejemplo, se muestra una lista parcial de los archivos en el directorio /sbin.

```
% cd /sbin
% ls -la
total 13456
drwxr-xr-x  2 root    sys      512 Sep  1 14:11 .
drwxr-xr-x 29 root    root     1024 Sep  1 15:40 ..
-r-xr-xr-x  1 root    bin     218188 Aug 18 15:17 autopush
lrwxrwxrwx  1 root    root       21 Sep  1 14:11 bpgetfile -> ...
-r-xr-xr-x  1 root    bin    505556 Aug 20 13:24 dhcpagent
-r-xr-xr-x  1 root    bin   456064 Aug 20 13:25 dhcpinfo
-r-xr-xr-x  1 root    bin   272360 Aug 18 15:19 fdisk
-r-xr-xr-x  1 root    bin   824728 Aug 20 13:29 hostconfig
-r-xr-xr-x  1 root    bin   603528 Aug 20 13:21 ifconfig
-r-xr-xr-x  1 root    sys    556008 Aug 20 13:21 init
-r-xr-xr-x  2 root    root   274020 Aug 18 15:28 jsh
-r-xr-xr-x  1 root    bin   238736 Aug 21 19:46 mount
-r-xr-xr-x  1 root    sys     7696 Aug 18 15:20 mountall
.
```

Cada una de las líneas muestra información sobre un archivo en el siguiente orden:

- Tipo de archivo, por ejemplo, d. Para obtener una lista de tipos de archivo, consulte [“Propiedad de archivos y directorios” en la página 128](#).
- Permisos, por ejemplo, r-xr-xr-x. Para obtener una descripción, consulte [“Propiedad de archivos y directorios” en la página 128](#).
- Número de enlaces físicos, por ejemplo, 2.
- Propietario del archivo, por ejemplo, root.
- Grupo del archivo, por ejemplo, bin.
- Tamaño del archivo, en bytes, por ejemplo, 7696.
- Fecha de creación del archivo o la última fecha en la que el archivo se modificó, por ejemplo, Aug 18 15:20.
- Nombre del archivo, por ejemplo, mountall.

## ▼ Cómo cambiar el propietario de un archivo local

El propietario del archivo, el rol de administrador principal o el superusuario pueden cambiar la propiedad de cualquier archivo.

**1 Visualice los permisos en un archivo.**

```
% ls -l example-file
-rw-r--r-- 1 janedoe staff 112640 May 24 10:49 example-file
```

**2 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

**3 Cambie el propietario del archivo.**

```
# chown stacey example-file
```

**4 Verifique que el propietario del archivo haya cambiado.**

```
# ls -l example-file
-rw-r--r-- 1 stacey staff 112640 May 26 08:50 example-file
```

**Ejemplo 6–2 Cómo permitir que los usuarios cambien la propiedad de sus propios archivos**

**Consideración de seguridad:** necesita una buena razón para cambiar el valor de la variable `rstchown` a cero. Este valor permite a un usuario cambiar la propiedad de sus archivos a otro nombre de usuario.

En este ejemplo, el valor de la variable `rstchown` se define en cero, en el archivo `/etc/system`. Este valor permite al propietario de un archivo utilizar el comando `chown` para cambiar la propiedad del archivo a otro usuario. Este valor también permite al propietario utilizar el comando `chgrp` para establecer la propiedad de grupo de un archivo en un grupo al que el propietario no pertenece. El cambio entra en vigor cuando se reinicia el sistema.

```
set rstchown = 0
```

Para obtener más información, consulte las páginas del comando `man chown(1)` y `chgrp(1)`.

Además, tenga en cuenta que los sistemas de archivos montados en NFS tienen otras restricciones para cambiar propiedades y grupos. Para obtener más información sobre la restricción del acceso a sistemas montados en NFS, consulte el [Capítulo 6, “Acceso a los sistemas de archivos de red \(referencia\)” de Guía de administración del sistema: servicios de red.](#)

**▼ Cómo cambiar la propiedad de grupo de un archivo****1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica.](#)

**2 Cambie la propiedad de grupo de un archivo.**

```
$ chgrp scifi example-file
```

Para obtener información sobre la configuración de grupos, consulte el [Capítulo 4, “Gestión de grupos y cuentas de usuario \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*.

**3 Verifique que la propiedad de grupo del archivo haya cambiado.**

```
$ ls -l example-file
-rw-r--r-- 1 stacey  scifi  112640 June 20 08:55  example-file
```

Consulte también el [Ejemplo 6-2](#).

## ▼ Cómo cambiar los permisos de archivo en modo simbólico

**1 Si no es el propietario del archivo o directorio, conviértase en superusuario o adopte un rol equivalente.**

Sólo el propietario o el superusuario actuales pueden utilizar el comando `chmod` para cambiar los permisos de archivo de un archivo o directorio.

**2 Cambie permisos en modo simbólico.**

```
% chmod who operator permissions filename
```

*quién*                      Especifica los permisos de qué usuarios se van a cambiar.

*operador*                  Especifica la operación que se va a realizar.

*permisos*                  Especifica qué permisos se van a cambiar. Para obtener la lista de símbolos válidos, consulte la [Tabla 6-5](#).

*nombre\_archivo*          Especifica el archivo o directorio.

**3 Verifique que los permisos del archivo hayan cambiado.**

```
% ls -l filename
```

**Ejemplo 6-3 Cambio de permisos en modo simbólico**

En el siguiente ejemplo, el permiso de lectura se quita de otros.

```
% chmod o-r example-file1
```

En el siguiente ejemplo, los permisos de lectura y ejecución se agregan para usuario, grupo y otros.

```
$ chmod a+rx example-file2
```

En el siguiente ejemplo, los permisos de lectura, escritura y ejecución se asignan a grupo.

```
$ chmod g=rwx example-file3
```

## ▼ Cómo cambiar permisos de archivo en modo absoluto

- 1 Si no es el propietario del archivo o directorio, conviértase en superusuario o adopte un rol equivalente.

Sólo el propietario o el superusuario actuales pueden utilizar el comando `chmod` para cambiar los permisos de archivo de un archivo o directorio.

- 2 Cambie permisos en modo absoluto.

```
% chmod nnn filename
```

*nnn* Especifica los valores octales que representan los permisos para el propietario de archivo, el grupo de archivos y otros, en ese orden. Para obtener la lista de valores octales válidos, consulte la [Tabla 6-4](#).

*nombre\_archivo* Especifica el archivo o directorio.

---

**Nota** – Al utilizar el comando `chmod` para cambiar los permisos de grupo de archivos en un archivo con entradas de ACL, tanto los permisos de grupo de archivos como la máscara de la ACL se cambian a los nuevos permisos. Tenga en cuenta que los nuevos permisos de la máscara de la ACL pueden cambiar los permisos para otros usuarios y grupos que tienen entradas de ACL en el archivo. Utilice el comando `getfacl` para asegurarse de que los permisos adecuados se establezcan para todas las entradas de la ACL. Para obtener más información, consulte la página del comando `man getfacl(1)`.

---

- 3 Verifique que los permisos del archivo hayan cambiado.

```
% ls -l filename
```

### Ejemplo 6-4 Cambio de permisos en modo absoluto

En el siguiente ejemplo, los permisos de un directorio público se cambian de 744 (lectura, escritura, ejecución; sólo lectura; y sólo lectura) a 755 (lectura, escritura, ejecución; lectura y ejecución; y lectura y ejecución).

```
# ls -ld public_dir
drwxr--r-- 1 jdoe staff 6023 Aug 5 12:06 public_dir
# chmod 755 public_dir
# ls -ld public_dir
```

```
drwxr-xr-x 1 jdoe staff 6023 Aug 5 12:06 public_dir
```

En el siguiente ejemplo, los permisos de una secuencia de comandos de shell ejecutable se cambian de lectura y escritura a lectura, escritura y ejecución.

```
% ls -l my_script
-rw----- 1 jdoe staff 6023 Aug 5 12:06 my_script
% chmod 700 my_script
% ls -l my_script
-rwx----- 1 jdoe staff 6023 Aug 5 12:06 my_script
```

## ▼ Cómo cambiar permisos de archivo especiales en modo absoluto

- 1 Si no es el propietario del archivo o directorio, conviértase en superusuario o adopte un rol equivalente.

Sólo el propietario actual o un usuario con capacidades de superusuario pueden utilizar el comando `chmod` para cambiar los permisos especiales en un archivo o directorio.

- 2 Cambie permisos especiales en modo absoluto.

```
% chmod nnnn filename
```

*nnnn* Especifica los valores octales que cambian los permisos en el archivo o directorio. El valor octal que se encuentra más a la izquierda establece los permisos especiales en el archivo. Para obtener la lista de valores octales válidos para permisos especiales, consulte la [Tabla 6-6](#).

*nombre\_archivo* Especifica el archivo o directorio.

---

**Nota** – Al utilizar el comando `chmod` para cambiar los permisos de grupo de archivos en un archivo con entradas de ACL, tanto los permisos de grupo de archivos como la máscara de la ACL se cambian a los nuevos permisos. Tenga en cuenta que los nuevos permisos de la máscara de ACL pueden cambiar los permisos para otros usuarios y grupos que tienen entradas de ACL en el archivo. Utilice el comando `getfacl` para asegurarse de que los permisos adecuados se establezcan para todas las entradas de la ACL. Para obtener más información, consulte la página del comando `man getfacl(1)`.

---

- 3 Verifique que los permisos del archivo hayan cambiado.

```
% ls -l filename
```

### Ejemplo 6-5 Establecimiento de permisos de archivo especiales en modo absoluto

En el ejemplo siguiente, el permiso `setuid` está establecido en el archivo `dbprog`.

```
# chmod 4555 dbprog
# ls -l dbprog
-r-sr-xr-x  1 db      staff      12095 May  6 09:29 dbprog
```

En el ejemplo siguiente, el permiso setgid está establecido en el archivo dbprog2.

```
# chmod 2551 dbprog2
# ls -l dbprog2
-r-xr-s--x  1 db      staff      24576 May  6 09:30 dbprog2
```

En el siguiente ejemplo, el permiso de bit de permanencia está establecido en el directorio public\_dir.

```
# chmod 1777 public_dir
# ls -ld public_dir
drwxrwxrwt  2 jdoe    staff      512 May 15 15:27 public_dir
```

## Protección de archivos UFS con ACL (mapa de tareas)

El siguiente mapa de tareas indica procedimientos que enumeran las ACL en un archivo UFS, cambian las ACL y copian las ACL en otro archivo.

Tarea	Para obtener instrucciones
Determinar si un archivo tiene una ACL	<a href="#">“Cómo comprobar si un archivo tiene una ACL” en la página 144</a>
Agregar una ACL a un archivo	<a href="#">“Cómo agregar entradas de ACL a un archivo” en la página 145</a>
Copiar una ACL	<a href="#">“Cómo copiar una ACL” en la página 147</a>
Modificar una ACL	<a href="#">“Cómo cambiar entradas de ACL en un archivo” en la página 147</a>
Eliminar las ACL de un archivo	<a href="#">“Cómo eliminar entradas de ACL de un archivo” en la página 148</a>
Visualizar las ACL en un archivo	<a href="#">“Cómo visualizar entradas de ACL de un archivo” en la página 148</a>

### ▼ Cómo comprobar si un archivo tiene una ACL

- Compruebe si un archivo tiene una ACL.

```
% ls -l filename
donde nombre_archivo especifica el archivo o directorio.
```

En el resultado, un signo más (+) a la derecha del campo de modo indica que el archivo tiene una ACL.



**Nota** – A menos que haya agregado entradas de ACL que amplíen los permisos de archivo UNIX, se considerará que un archivo tiene una ACL “trivial” y no se mostrará el signo más (+).

**Ejemplo 6-6** Comprobación para determinar si un archivo tiene una ACL

En el ejemplo siguiente, el archivo `ch1.sgm` tiene una ACL. La ACL se indica con el signo más (+) a la derecha del campo de modo.

```
% ls -l ch1.sgm
-rwxr-----+ 1 stacey  techpubs      167 Nov 11 11:13 ch1.sgm
```

▼ **Cómo agregar entradas de ACL a un archivo**

**1** Establezca una ACL en un archivo mediante el comando `setfacl`.

<pre>% setfacl -s user::perms,group::perms,other::perms,mask::perms,acl-entry-list filename ...</pre>	
<pre>-s</pre>	Establece una ACL en el archivo. Si un archivo ya tiene una ACL, se sustituye. Esta opción requiere, al menos, las entradas <code>user::</code> , <code>group::</code> y <code>other::</code> .
<pre>user::perms</pre>	Especifica los permisos de propietario de archivo.
<pre>group::perms</pre>	Especifica los permisos de propiedad de grupo.
<pre>other::perms</pre>	Especifica los permisos para usuarios que no sean el propietario del archivo ni miembros del grupo.
<pre>mask::perms</pre>	Especifica los permisos para la máscara de la ACL. La máscara indica el número máximo de permisos que están permitidos para los usuarios (excepto el propietario) y para grupos.
<pre>lista_entrada_acl</pre>	Especifica la lista de una o más entradas de ACL para definir para usuarios y grupos específicos en el archivo o directorio. También puede definir entradas de ACL predeterminadas en un directorio. La <a href="#">Tabla 6-7</a> y la <a href="#">Tabla 6-8</a> muestran las entradas de ACL válidas.
<pre>nombre_archivo ...</pre>	Especifica uno o más archivos o directorios en los cuales se establecerá la ACL. Varios nombres de archivo ( <i>nombre_archivo</i> ) se separan con espacios.



**Precaución** – Si una ACL ya existe en el archivo, la opción `-s` sustituye toda la ACL con la nueva ACL.

Para obtener más información, consulte la página del comando `man setfacl(1)`.

**2 Verifique que las entradas de la ACL se hayan establecido en el archivo.**

```
% getfacl filename
```

Para obtener más información, consulte [“Cómo comprobar si un archivo tiene una ACL” en la página 144.](#)

**Ejemplo 6-7 Definición de una ACL en un archivo**

En el ejemplo siguiente, los permisos de propietario de archivo están establecidos en lectura y escritura, los permisos de grupo de archivos están establecidos en sólo lectura y otros permisos están establecidos en ninguno en el archivo `ch1.sgm`. Además, al usuario `anusha` se le conceden permisos de lectura y escritura en el archivo. Los permisos de máscara de ACL están establecidos en lectura y escritura, lo que significa que ningún usuario ni grupo pueden tener permisos de ejecución.

```
% setfacl -s user::rw-,group::r--,other:---,mask:rw-,user:anusha:rw- ch1.sgm
% ls -l
total 124
-rw-r-----+ 1 stacey techpubs 34816 Nov 11 14:16 ch1.sgm
-rw-r--r-- 1 stacey techpubs 20167 Nov 11 14:16 ch2.sgm
-rw-r--r-- 1 stacey techpubs 8192 Nov 11 14:16 notes
% getfacl ch1.sgm
# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:rw-    #effective:rw-
group::r--         #effective:r--
mask:rw-
other:---
```

En el ejemplo siguiente, los permisos de propietario de archivo están establecidos en lectura, escritura y ejecución, los permisos de grupo de archivos están establecidos en sólo lectura y otros permisos están establecidos en ninguno. Además, los permisos de máscara de la ACL están establecidos en lectura en el archivo `ch2.sgm`. Por último, al usuario `anusha` se le conceden permisos de lectura y escritura. Sin embargo, debido a la máscara de la ACL, los permisos para `anusha` son de sólo lectura.

```
% setfacl -s u::7,g::4,o:0,m:4,u:anusha:7 ch2.sgm
% getfacl ch2.sgm
# file: ch2.sgm
# owner: stacey
# group: techpubs
user::rwx
user:anusha:rwx    #effective:r--
group::r--         #effective:r--
mask:r--
other:---
```

## ▼ Cómo copiar una ACL

- Copie la ACL de un archivo a otro archivo redirigiendo el resultado de `getfacl`.

```
% getfacl filename1 | setfacl -f - filename2
```

*nombre\_archivo1*      Especifica el archivo desde el que se va a copiar la ACL.

*nombre\_archivo2*      Especifica el archivo en el cual se establecerá la ACL copiada.

### Ejemplo 6-8 Copia de una ACL

En el ejemplo siguiente, la ACL en `ch2.sgm` se copia a `ch3.sgm`.

```
% getfacl ch2.sgm | setfacl -f - ch3.sgm
```

## ▼ Cómo cambiar entradas de ACL en un archivo

- 1 Modifique entradas de ACL en un archivo mediante el comando `setfacl`.

```
% setfacl -m acl-entry-list filename ...
```

`-m`      Modifica la entrada de ACL existente.

*lista\_entrada\_acl*      Especifica la lista de una o más entradas de ACL para modificar en el archivo o directorio. También puede modificar las entradas de ACL predeterminadas en un directorio. La [Tabla 6-7](#) y la [Tabla 6-8](#) muestran las entradas de ACL válidas.

*nombre\_archivo ...*      Especifica uno o más archivos o directorios, separados por un espacio.

- 2 Verifique que las entradas de la ACL se hayan modificado en el archivo.

```
% getfacl filename
```

### Ejemplo 6-9 Modificación de entradas de ACL en un archivo

En el ejemplo siguiente, los permisos para el usuario `anusha` se modifican a lectura y escritura.

```
% setfacl -m user:anusha:6 ch3.sgm
% getfacl ch3.sgm
# file: ch3.sgm
# owner: stacey
# group: techpubs
user::rw-
user::anusha:rw-      #effective:r--
group::r-              #effective:r--
mask:r--
other:r-
```

En el siguiente ejemplo, los permisos predeterminados para el grupo `staff` se modifican a lectura en el directorio `book`. Además, los permisos de máscara de ACL predeterminados se modifican a lectura y escritura.

```
% setfacl -m default:group:staff:4,default:mask:6 book
```

## ▼ Cómo eliminar entradas de ACL de un archivo

### 1 Elimine entradas de ACL de un archivo.

```
% setfacl -d acl-entry-list filename ...
```

`-d` Elimina las entradas de ACL especificadas.

`lista_entrada_acl` Especifica la lista de entradas de ACL (sin especificar los permisos) para eliminar del archivo o directorio. Sólo puede eliminar las entradas de la ACL y las entradas de la ACL predeterminadas para usuarios y grupos específicos. La [Tabla 6-7](#) y la [Tabla 6-8](#) muestran las entradas de ACL válidas.

`nombre_archivo ...` Especifica uno o más archivos o directorios, separados por un espacio.

Como alternativa, puede utilizar el comando `setfacl -s` para eliminar todas las entradas de la ACL en un archivo y reemplazarlas con las nuevas entradas de la ACL que se han especificado.

### 2 Verifique que las entradas de la ACL se hayan eliminado del archivo.

```
% getfacl filename
```

## Ejemplo 6-10 Eliminación de entradas de ACL en un archivo

En el siguiente ejemplo, el usuario `anusha` se elimina del archivo `ch4.sgm`.

```
% setfacl -d user:anusha ch4.sgm
```

## ▼ Cómo visualizar entradas de ACL de un archivo

### ● Visualice entradas de la ACL de un archivo mediante el comando `getfacl`.

```
% getfacl [-a | -d] filename ...
```

`-a` Muestra el nombre de archivo, el propietario de archivo, el grupo de archivos y las entradas de la ACL para el archivo o directorio especificado.

- d Muestra el nombre de archivo, el propietario de archivo, el grupo de archivos y las entradas de la ACL predeterminadas, si existen, para el directorio especificado.
- nombre\_archivo ...* Especifica uno o más archivos o directorios, separados por un espacio.
- Si especifica varios nombres de archivo en la línea de comandos, las entradas de la ACL se muestran con una línea en blanco entre cada entrada.

### Ejemplo 6–11 Visualización de entradas de ACL de un archivo

En el ejemplo siguiente, se muestran todas las entradas de la ACL para el archivo `ch1.sgm`. La nota `#effective`: junto a las entradas de usuario y grupo indica cuáles son los permisos después de ser modificados por la máscara de la ACL.

```
% getfacl ch1.sgm

# file: ch1.sgm
# owner: stacey
# group: techpubs
user::rw-
user:anusha:r-      #effective:r--
group::rw-          #effective:rw-
mask:rw-
other:---
```

En el ejemplo siguiente, se muestran las entradas de la ACL predeterminadas para el directorio `book`.

```
% getfacl -d book

# file: book
# owner: stacey
# group: techpubs
user::rwx
user:anusha:r-x      #effective:r-x
group::rwx           #effective:rwx
mask:rwx
other:---
default:user::rw-
default:user:anusha:r--
default:group::rw-
default:mask:rw-
default:other:---
```

# Protección contra programas con riesgo de seguridad (mapa de tareas)

El siguiente mapa de tareas indica procedimientos que buscan ejecutables riesgosos en el sistema y que impiden que los programas se aprovechen de una pila ejecutable.

Tarea	Descripción	Para obtener instrucciones
Buscar archivos con permisos especiales	Localiza archivos con el bit <code>setuid</code> establecido, pero que no son propiedad del usuario <code>root</code> .	<a href="#">“Cómo buscar archivos con permisos de archivo especiales” en la página 150</a>
Evitar que pilas ejecutables se desborden	Impide que los programas se aprovechen de una pila ejecutable.	<a href="#">“Cómo impedir que programas usen pilas ejecutables” en la página 151</a>
Evitar el registro de mensajes de pilas ejecutables	Desactiva el registro de mensajes de pilas ejecutables.	<a href="#">Ejemplo 6-13</a>

## ▼ Cómo buscar archivos con permisos de archivo especiales

Debe supervisar el sistema para detectar cualquier uso no autorizado de los permisos `setuid` y `setgid` en los programas. Los permisos `setuid` y `setgid` permiten a los usuarios comunes adquirir capacidades de superusuario. Un archivo ejecutable sospechoso concede propiedad a un usuario en lugar de a `root` o `bin`.

1 **Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

2 **Busque archivos con permisos `setuid` mediante el comando `find`.**

<code># find <i>directorio</i> -user root -perm -4000 -exec ls -ldb {} \;</code>	<code>&gt;/tmp/<i>filename</i></code>
<code>find <i>directorio</i></code>	Comprueba todas las rutas montadas a partir del <i>directorio</i> ) especificado, que puede ser <code>root</code> ( <code>/</code> ), <code>sys</code> , <code>bin</code> o <code>mail</code> .
<code>-user root</code>	Muestra archivos que sólo son propiedad de <code>root</code> .
<code>-perm -4000</code>	Muestra archivos sólo con permisos establecidos en <code>4000</code> .
<code>-exec ls -ldb</code>	Muestra el resultado del comando <code>find</code> en formato <code>ls -ldb</code> .
<code>/tmp/<i>nombre_archivo</i></code>	Es el archivo que contiene los resultados del comando <code>find</code> .

**3 Muestra los resultados en /tmp/nombre\_archivo.**

```
# more /tmp/filename
```

Para obtener más información sobre los permisos `setuid`, consulte [“Permiso `setuid`” en la página 130](#).

**Ejemplo 6–12 Búsqueda de archivos con permisos `setuid`**

El resultado del siguiente ejemplo muestra que un usuario en un grupo denominado `rar` ha realizado una copia personal de `/usr/bin/sh` y ha establecido los permisos como `setuid` en `root`. Como resultado, el programa `/usr/rar/bin/sh` se ejecuta con permisos `root`.

Este resultado se ha guardado para referencia futura al mover el directorio `/var/tmp/ckprm` al directorio `/export/sysreports/ckprm`.

```
# find / -user root -perm -4000 -exec ls -ldb {} \; > /var/tmp/ckprm
# cat /var/tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
# mv /var/tmp/ckprm /export/sysreports/ckprm
```

**▼ Cómo impedir que programas usen pilas ejecutables**

Para obtener una descripción de los riesgos de seguridad de las pilas ejecutables, consulte [“Cómo impedir que los archivos ejecutables pongan en riesgo la seguridad” en la página 137](#).

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

**2 Edite el archivo `/etc/system` y agregue la siguiente línea:**

```
set noexec_user_stack=1
```

**3 Reinicie el sistema.**

```
# init 6
```

### **Ejemplo 6–13**    Deshabilitación del registro de mensajes de pilas ejecutables

En este ejemplo, el registro de mensajes de pilas ejecutables se deshabilita y el sistema se reinicia.

```
# cat /etc/system
set noexec_user_stack=1
set noexec_user_stack_log=0
# init 6
```



## Uso de la herramienta automatizada de mejora de la seguridad (tareas)

---

En este capítulo, se describe cómo utilizar la herramienta automatizada de mejora de la seguridad (ASET) para supervisar o restringir el acceso a archivos y directorios del sistema.

A continuación, se muestra una lista de las instrucciones paso a paso que se incluyen en este capítulo.

- [“Herramienta automatizada de mejora de la seguridad \(ASET\)” en la página 153](#)
- [“Ejecución de ASET \(mapa de tareas\)” en la página 171](#)
- [“Resolución de problemas de ASET” en la página 175](#)

Para obtener una herramienta más completa que ASET, utilice Oracle Solaris Security Toolkit. Oracle Solaris Security Toolkit proporciona una estructura para endurecer y minimizar un sistema Oracle Solaris. El kit incluye una herramienta de creación de perfiles, una herramienta de elaboración de informes y una capacidad para deshacer. Para obtener más información, consulte [“Uso de Oracle Solaris Security Toolkit” en la página 53](#).

## Herramienta automatizada de mejora de la seguridad (ASET)

El SO Oracle Solaris incluye la herramienta automatizada de mejora de la seguridad (ASET). ASET ayuda a supervisar y controlar la seguridad del sistema al realizar automáticamente tareas que, de otro modo, tendría que realizar usted manualmente.

El paquete de seguridad de ASET proporciona herramientas de administración automatizadas que le permiten controlar y supervisar la seguridad del sistema. Se especifica un nivel de seguridad en el cual se desea ejecutar ASET. Los niveles de seguridad son bajo, medio y alto. En cada nivel superior, las funciones de control de archivos de ASET aumentan para reducir el acceso a archivos y reforzar la seguridad del sistema.

Hay siete tareas que ASET ejecuta. Cada tarea realiza comprobaciones y ajustes específicos en los archivos del sistema. Las tareas de ASET refuerzan los permisos de archivo, comprueban el contenido de archivos del sistema esenciales para detectar fallos de seguridad y supervisan áreas

cruciales. ASET también puede proteger una red aplicando los requisitos básicos de un sistema de cortafuegos a un sistema que sirve como sistema de puerta de enlace. Consulte [“Configuración de cortafuegos” en la página 157](#).

ASET usa archivos maestros para la configuración. Los archivos maestros, los informes y otros archivos de ASET están en el directorio `/usr/aset`. Estos archivos se pueden cambiar para ajustarse a los requisitos concretos del sitio.

Cada tarea genera un informe. El informe indica los fallos de seguridad detectados y los cambios que la tarea ha realizado en los archivos del sistema. Cuando se ejecuta en el mayor nivel de seguridad, ASET intenta modificar todos los fallos de seguridad del sistema. Si ASET no puede corregir un problema de seguridad potencial, informa la existencia del problema.

Puede iniciar una sesión de ASET usando el comando `/usr/aset/aset` de forma interactiva. Como alternativa, puede configurar ASET para que se ejecute periódicamente colocando una entrada en el archivo `crontab`.

Las tareas de ASET hacen un uso intensivo del disco. Las tareas pueden interferir con actividades regulares. Para minimizar el impacto en el rendimiento del sistema, programe ASET para que se ejecute cuando el nivel de actividad del sistema sea el más bajo. Por ejemplo, ejecute ASET una vez cada 24 h o 48 h a medianoche.

## Niveles de seguridad de ASET

ASET se puede establecer para que funcione en uno de los tres niveles de seguridad: bajo, medio o alto. En cada nivel superior, las funciones de control de archivos de ASET aumentan para reducir el acceso a archivos y reforzar la seguridad del sistema. Estas funciones incluyen desde la supervisión de la seguridad del sistema sin limitar el acceso a archivos de los usuarios hasta el refuerzo cada vez mayor de los permisos de acceso hasta que el sistema sea completamente seguro.

En la siguiente tabla, se describen estos tres niveles de seguridad.

Nivel de seguridad	Descripción
Bajo	Garantiza que los atributos de los archivos del sistema estén establecidos en valores de versión estándar. ASET realiza varias comprobaciones y, a continuación, informa posibles fallos de seguridad. En este nivel, ASET no realiza ninguna acción, por lo que no afecta los servicios del sistema.
Medio	Proporciona un control de seguridad adecuado para la mayoría de los entornos. ASET modifica algunos de los valores de los archivos y parámetros del sistema. Restringe el acceso al sistema para reducir los riesgos de ataques contra la seguridad. Informa fallos de seguridad y cualquier modificación que ha hecho para restringir el acceso. En este nivel, no afecta los servicios del sistema.

Nivel de seguridad	Descripción
Alto	Proporciona un sistema altamente seguro. ASET ajusta muchos archivos del sistema y valores de parámetros para que tengan permisos de acceso mínimos. La mayoría de las aplicaciones y los comandos del sistema siguen funcionando con normalidad. Sin embargo, en este nivel, las consideraciones de seguridad tienen prioridad sobre otro comportamiento del sistema.

**Nota** – ASET no cambia los permisos de un archivo para que el archivo sea menos seguro, a menos que usted disminuya el nivel de seguridad. También puede revertir intencionalmente el sistema a la configuración que existía antes de ejecutar ASET.

## Lista de tareas de ASET

En esta sección, se trata qué hace ASET. Debe comprender cada tarea de ASET. Al comprender los objetivos de ASET, las operaciones que ASET realiza y los componentes del sistema a los que ASET afecta, puede interpretar y utilizar los informes de manera efectiva.

Los archivos de informe de ASET contienen mensajes que describen lo más específico posible los problemas que han sido detectados por cada tarea de ASET. Estos mensajes pueden ayudar a diagnosticar y corregir estos problemas. Sin embargo, el uso satisfactorio de ASET asume que usted posee una visión general de la administración del sistema y los componentes del sistema. Si es un administrador inexperto, puede consultar otra documentación de administración del sistema Oracle Solaris. Puede leer páginas del comando `man` relacionadas para prepararse para la administración de ASET.

La utilidad `taskstat` identifica las tareas que se han completado. La utilidad también identifica las tareas que aún se están ejecutando. Cada tarea finalizada produce un archivo de informe. Para obtener una descripción completa de la utilidad `taskstat`, consulte [taskstat\(1M\)](#).

## Ajuste de permisos de archivos del sistema

Esta tarea establece los permisos en los archivos del sistema en el nivel de seguridad que usted designa. Esta tarea se ejecuta cuando el sistema se instala. Si más tarde decide modificar los niveles previamente establecidos, ejecute esta tarea de nuevo. En seguridad baja, los permisos se establecen en valores que son apropiados para un entorno abierto de uso compartido de información. En seguridad media, los permisos se ajustan para generar la seguridad adecuada para la mayoría de los entornos. En seguridad alta, los permisos se ajustan para restringir el acceso estrictamente.

Cualquier modificación que esta tarea realiza en permisos de archivos del sistema o en valores de parámetros se informa en el archivo `tune.rpt`. Para ver un ejemplo de los archivos que ASET consulta cuando define los permisos, consulte [“Ejemplos de archivos de ajuste” en la página 170](#).

## Comprobaciones de archivos del sistema

Esta tarea examina los archivos del sistema y compara cada archivo con una descripción de ese archivo en un archivo maestro. El archivo maestro se crea la primera vez que ASET ejecuta esta tarea. El archivo maestro contiene los valores del sistema de archivos aplicados por checklist para el nivel de seguridad especificado.

Una lista de directorios cuyos archivos se comprobarán se define para cada nivel de seguridad. Puede utilizar la lista predeterminada o puede modificar la lista especificando directorios diferentes para cada nivel.

Para cada archivo, se comprueban los siguientes criterios:

- Propietario y grupo
- Bits de permiso
- Tamaño y suma de comprobación
- Número de enlaces
- Hora de última modificación

Cualquier discrepancia que ASET encuentra se informa en el archivo `cklist.rpt`. Este archivo contiene los resultados de la comparación de los valores del tamaño del archivo del sistema, el permiso y la suma de comprobación con el archivo maestro.

## Comprobaciones de usuario y grupo

Esta tarea comprueba la coherencia y la integridad de grupos y cuentas de usuario. La tarea utiliza las definiciones de los archivos `passwd` y `group`. Esta tarea comprueba los archivos de contraseña locales y NIS o NIS+. Los problemas de los archivos de contraseña para NIS+ se informan, pero no se corrigen.

Esta tarea comprueba las siguientes infracciones:

- ID o nombres duplicados
- Entradas en formato incorrecto
- Cuentas sin contraseña
- Directorios de inicio de sesión no válidos
- Cuenta nobody
- Contraseña de grupo nula
- Un signo más (+) en el archivo `/etc/passwd` en un servidor NIS o un servidor NIS+

Las discrepancias se informan en el archivo `usrg rp.rpt`.

## Comprobación de archivos de configuración del sistema

Durante esta tarea, ASET comprueba varias tablas del sistema, la mayoría de las cuales están en el directorio `/etc`.

Estos archivos son los siguientes:

- /etc/default/login
- /etc/hosts.equiv
- /etc/inetd.conf
- /etc/aliases
- /var/adm/utmpx
- /.rhosts
- /etc/vfstab
- /etc/dfs/dfstab
- /etc/ftpd/ftpusers

ASET realiza varias comprobaciones y modificaciones en estos archivos. ASET informa los problemas en el archivo `sysconf.rpt`.

## Comprobación de variables de entorno

Esta tarea comprueba cómo las variables de entorno `PATH` y `UMASK` están definidas para `root` y otros usuarios. La tarea comprueba los archivos `/.profile`, `/.login` y `/.cshrc`.

Los resultados de la comprobación de la seguridad del entorno se informan en el archivo `env.rpt`.

## Comprobación de eeprom

Esta tarea comprueba el valor del parámetro de seguridad `eeprom` para garantizar que el parámetro esté establecido en el nivel de seguridad adecuado. Puede establecer el parámetro de seguridad `eeprom` en `none`, `command` o `full`.

ASET no cambia este valor, pero informa sus recomendaciones en el archivo `eeprom.rpt`.

## Configuración de cortafuegos

Esta tarea garantiza que el sistema se pueda utilizar de forma segura como un relé de red. Esta tarea protege una red interna contra redes públicas externas mediante la configuración de un sistema dedicado como un cortafuegos, que se describe en [“Sistemas de cortafuegos” en la página 60](#). El sistema de cortafuegos separa dos redes. En este caso, cada red se acerca a la otra red como una red que no es de confianza. La tarea de configuración de cortafuegos deshabilita el reenvío de paquetes de protocolo de Internet (IP). El cortafuegos también oculta la información de enrutamiento a la red externa.

La tarea de cortafuegos se ejecuta en todos los niveles de seguridad, pero sólo toma acción en el nivel superior. Si desea ejecutar ASET en el nivel de seguridad alto, pero nota que el sistema no requiere protección de cortafuegos, puede eliminar la tarea de cortafuegos. Elimine la tarea mediante la edición del archivo `asetenv`.

Los cambios realizados se informan en el archivo `firewall.rpt`.

## Registro de ejecución de ASET

ASET genera un registro de ejecución ya sea si se ejecuta de manera interactiva o en segundo plano. De manera predeterminada, ASET genera el archivo de registro en el resultado estándar. El registro de ejecución confirma que ASET se ejecutó a la hora designada y que, además, contiene los mensajes de error de ejecución. El comando `aset -n` indica al registro que sea enviado por correo electrónico a un usuario designado. Para obtener una lista completa de las opciones de ASET, consulte la página del comando `man aset(1M)`.

### Ejemplo de un archivo de registro de ejecución de ASET

ASET running at security level low

Machine=example; Current time = 0325\_08:00

aset: Using /usr/aset as working directory

Executing task list...

```
firewall
env
sysconfig
usrgrp
tune
cklist
eeprom
```

All tasks executed. Some background tasks may still be running.

Run /usr/aset/util/taskstat to check their status:

```
$/usr/aset/util/taskstat      aset_dir
```

Where aset\_dir is ASET's operating directory, currently=/usr/aset

When the tasks complete, the reports can be found in:

```
/usr/aset/reports/latest/*.rpt
```

You can view them by:

```
more /usr/aset/reports/latest/*.rpt
```

El registro de ejecución primero muestra el sistema y la hora a la que se ejecutó ASET. A continuación, el registro de ejecución muestra las tareas a medida que se iniciaron.

ASET invoca un proceso en segundo plano para cada una de estas tareas, que se describen en “[Lista de tareas de ASET](#)” en la [página 155](#). La tarea se incluye en el registro de ejecución cuando se inicia. Este listado no indica que la tarea ha finalizado. Para comprobar el estado de las tareas en segundo plano, utilice el comando `taskstat`.

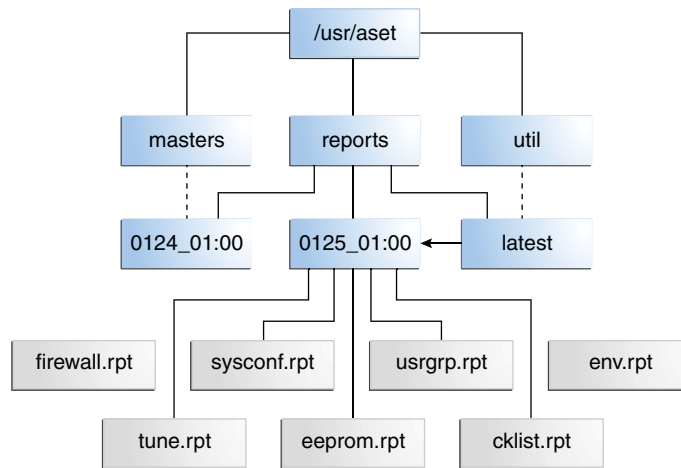
## Informes de ASET

Todos los archivos de informe que se generan a partir de las tareas de ASET se almacenan en subdirectorios en el directorio `/usr/aset/reports`. Esta sección describe la estructura del directorio `/usr/aset/reports` y proporciona directrices sobre la gestión de los archivos de informe.

ASET coloca los archivos de informe en subdirectorios que se especifican para indicar la fecha y la hora en las que se generan los informes. Esta convención permite mantener un rastro ordenado de registros que documentan el estado del sistema a medida que el estado varía entre las ejecuciones de ASET. Puede supervisar y comparar estos informes para determinar la solidez de la seguridad de su sistema.

En la siguiente figura, se muestra un ejemplo de la estructura del directorio `reports`.

FIGURA 7-1 Estructura del directorio `reports` de ASET



Este ejemplo muestra dos subdirectorios de informes.

- 0124\_01:00
- 0125\_01:00

Los nombres de subdirectorio indican la fecha y la hora en que los informes se han generado. Cada nombre de subdirectorio de informes tiene el siguiente formato:

*monthdate\_hour:minute*

*mes, fecha, hora y minuto*, y todos tienen números de dos dígitos. Por ejemplo, 0125\_01:00 representa el 25 de enero, a la 1 a. m.

Cada uno de los dos subdirectorios de informes contiene una recopilación de los informes que se generan a partir de una ejecución de ASET.

El directorio `latest` es un enlace simbólico que siempre hace referencia al subdirectorio que contiene los informes más recientes. Por lo tanto, para consultar los informes más recientes que

ASET ha generado, puede ir al directorio `/usr/aset/reports/latest`. Hay un archivo de informe en este directorio para cada una de las tareas que ASET realizó durante su ejecución más reciente.

### Formato de los archivos de informe de ASET

Cada archivo de informe se nombra después de la tarea que genera el informe. La siguiente tabla enumera las tareas y sus informes.

TABLA 7-1 Tareas e informes resultantes de ASET

Tareas	Informe
Ajuste de permisos de archivos del sistema (tune)	tune.rpt
Comprobaciones de archivos del sistema (cklist)	cklist.rpt
Comprobaciones de usuarios y grupos (usrgrp)	usrgrp.rpt
Comprobación de archivos de configuración del sistema (sysconf)	sysconf.rpt
Comprobación de variables de entorno (env)	env.rpt
Comprobación eeprom (eeprom)	eeprom.rpt
Configuración de cortafuegos (firewall)	firewall.rpt

Dentro de cada archivo de informe, los mensajes son encerrados entre paréntesis por una línea de carátula inicial y una final. A veces, una tarea finaliza prematuramente. Por ejemplo, una tarea puede finalizar de manera prematura cuando un componente de ASET se elimina o se daña accidentalmente. En tales casos, el archivo de informe contiene, por lo general, un mensaje casi al final que indica el motivo de la terminación prematura.

A continuación, se muestra un ejemplo de archivo de informe, `usrgrp.rpt`.

```
*** Begin User and Group Checking ***

Checking /etc/passwd ...
Warning! Password file, line 10, no passwd
:sync::1:1:::/bin/sync
..end user check; starting group check ...
Checking /etc/group...
*** End User And group Checking ***
```

### Examen de archivos de informe de ASET

Después de ejecutar inicialmente o volver a configurar ASET, debe examinar los archivos de informe detenidamente. La reconfiguración incluye la modificación del archivo `asetenv` o los archivos maestros en el subdirectorio `masters`, o el cambio del nivel de seguridad en el que funciona ASET.



Los informes registran cualquier error que se ha introducido al reconfigurar ASET. Al analizar los informes detenidamente, puede reaccionar y resolver problemas a medida que surgen.

## Comparación de archivos de informe de ASET

Después de supervisar los archivos de informe por un período durante el cual no hay cambios de configuración ni actualizaciones del sistema, puede notar que el contenido de los informes empieza a estabilizarse. Cuando los informes contienen poca información inesperada, puede usar la utilidad `diff` para comparar informes.

## Archivos maestros de ASET

Los archivos maestros de ASET, `tune.high`, `tune.low`, `tune.med` y `uid_alias`, se encuentran en el directorio `/usr/aset/masters`. ASET utiliza los archivos maestros para definir niveles de seguridad. Para obtener más información, consulte la página del comando `man asetmasters(4)`.

## Archivos de ajuste

Los archivos maestros `tune.low`, `tune.med` y `tune.high` definen los niveles de seguridad disponibles de ASET. Los archivos especifican los atributos de los archivos del sistema en cada nivel y se utilizan para fines de comparación y referencia.

## Archivo `uid_alias`

El archivo `uid_alias` contiene una lista de varias cuentas de usuario que comparten el mismo ID de usuario (UID). Normalmente, ASET advierte sobre el uso de varias cuentas de usuario porque esta práctica disminuye la responsabilidad. Puede permitir excepciones a esta regla mostrando las excepciones en el archivo `uid_alias`. ASET no informa entradas en el archivo `passwd` con UID duplicados si estas entradas están especificadas en el archivo `uid_alias`.

Evite tener varias cuentas de usuario que comparten el mismo UID. Debe considerar otros métodos para lograr el objetivo. Por ejemplo, si desea que varios usuarios compartan un conjunto de permisos, puede crear una cuenta de grupo. También puede crear un rol. El uso compartido de UID debe ser el último recurso, ya que se debe utilizar sólo cuando otros métodos no pueden cumplir sus objetivos.

Puede utilizar la variable de entorno `UID_ALIASES` para especificar un archivo de alias alternativo. El archivo predeterminado es `/usr/aset/masters/uid_alias`.

## Archivos de lista de comprobación

Los archivos maestros que son utilizados por las comprobaciones de los archivos del sistema se generan cuando se ejecuta ASET por primera vez. Los archivos maestros también se generan al ejecutar ASET después de cambiar el nivel de seguridad.

Las siguientes variables de entorno definen los archivos que son comprobados por esta tarea:

- CKLISTPATH\_LOW
- CKLISTPATH\_MED
- CKLISTPATH\_HIGH

## Archivo de entorno de ASET (asetenv)

El archivo de entorno, `asetenv`, contiene una lista de variables de entorno que afectan las tareas de ASET. Algunas de estas variables se pueden cambiar para modificar la operación de ASET. Para obtener detalles sobre el archivo `asetenv`, consulte [asetenv\(4\)](#).

## Configuración de ASET

En esta sección, se explica cómo está configurada ASET. Además, se describe el entorno en el que funciona ASET.

ASET requiere una administración y una configuración mínimas. En la mayoría de los casos, puede ejecutar ASET con los valores predeterminados. Sin embargo, puede ajustar algunos de los parámetros que afectan el funcionamiento y el comportamiento de ASET para maximizar su beneficio. Antes de cambiar los valores predeterminados, debe comprender cómo funciona ASET y cómo afecta los componentes del sistema.

ASET depende de cuatro archivos de configuración para controlar el comportamiento de sus tareas:

- `/usr/aset/asetenv`
- `/usr/aset/masters/tune.low`
- `/usr/aset/masters/tune.med`
- `/usr/aset/masters/tune.high`

## Modificación del archivo de entorno (asetenv)

El archivo `/usr/aset/asetenv` tiene dos secciones principales:

- Una sección de variables de entorno configurable por el usuario
- Una sección de variables de entorno interna

Puede modificar la sección de parámetros configurable por el usuario. Sin embargo, la configuración en la sección de variables de entorno interna es sólo para uso interno. Estos valores no se deben modificar.

Puede editar las entradas de la sección configurable por el usuario para realizar lo siguiente:

- Seleccionar las tareas que desea ejecutar

- Especificar los directorios para la tarea de comprobaciones de archivos del sistema
- Programar la ejecución de ASET
- Especificar un archivo de alias de UID
- Ampliar las comprobaciones a las tablas NIS+

## Selección de las tareas para ejecutar: TASKS

Cada una de las tareas que ASET realiza supervisa un área particular del sistema de seguridad. En la mayoría de los entornos del sistema, todas las tareas son necesarias para proporcionar una cobertura de seguridad equilibrada. Sin embargo, puede decidir eliminar una o más tareas.

Por ejemplo, la tarea de cortafuegos se ejecuta en todos los niveles de seguridad, pero actúa sólo en el nivel de seguridad alto. Es posible que desee ejecutar ASET en el nivel de seguridad alto, pero no necesita la protección de cortafuegos.

Puede configurar ASET para que se ejecute en el nivel de seguridad alto sin la función de cortafuegos. Para ello, edite la lista TASKS de variables de entorno en el archivo `asetenv`. De manera predeterminada, la lista TASKS contiene todas las tareas de ASET. Para eliminar una tarea, elimine la variable de entorno relacionada con la tarea del archivo. En este caso, debe eliminar la variable de entorno `firewall` de la lista. La próxima vez que ASET se ejecuta, la tarea excluida no se realiza.

En el ejemplo siguiente, se muestra la lista TASKS con todas las tareas de ASET.

```
TASKS="env sysconfig usrgrp tune cklist eepprom firewall"
```

## Especificación de directorios para la tarea de comprobaciones de archivos del sistema: CKLISTPATH

La comprobación de archivos del sistema comprueba los atributos de los archivos de los directorios del sistema seleccionados. Defina qué directorios comprobar mediante las siguientes variables de entorno.

La variable `CKLISTPATH_LOW` define los directorios que se deben comprobar en el nivel de seguridad bajo. Las variables de entorno `CKLISTPATH_MED` y `CKLISTPATH_HIGH` funcionan de manera similar para los niveles de seguridad medio y alto.

La lista de directorios definida mediante una variable de entorno en un nivel de seguridad más bajo debe ser un subconjunto de la lista de directorios definida en el siguiente nivel superior. Por ejemplo, todos los directorios que se especifican para `CKLISTPATH_LOW` deben estar incluidos en `CKLISTPATH_MED`. De forma similar, todos los directorios que se especifican para `CKLISTPATH_MED` deben estar incluidos en `CKLISTPATH_HIGH`.

Las comprobaciones que se realizan en estos directorios no son recursivas. ASET sólo comprueba los directorios que se encuentran explícitamente enumerados en la variable de entorno. No comprueba los subdirectorios.

Puede editar estas definiciones de variables de entorno para agregar o eliminar directorios que desea que ASET compruebe. Tenga en cuenta que estas listas de comprobación sólo son útiles para los archivos del sistema que normalmente no cambian día a día. El directorio principal de un usuario, por ejemplo, es, generalmente, demasiado dinámico para ser candidato para una lista de comprobación.

## Programación de la ejecución de ASET: PERIODIC\_SCHEDULE

Puede iniciar ASET interactivamente o puede utilizar la opción `-p` para solicitar que las tareas de ASET se ejecuten a una hora programada. Puede ejecutar ASET periódicamente, en un momento en que la demanda del sistema es leve. Por ejemplo, ASET consulta a `PERIODIC_SCHEDULE` para determinar la frecuencia para ejecutar las tareas de ASET y a qué hora ejecutar las tareas. Para obtener instrucciones detalladas sobre la configuración de ASET para que se ejecute periódicamente, consulte [“Cómo ejecutar ASET periódicamente” en la página 173](#).

El formato de `PERIODIC_SCHEDULE` sigue el formato de las entradas `crontab`. Para obtener más información, consulte [`crontab\(1\)`](#).

## Especificación de un archivo de alias: UID\_ALIASES

La variable `UID_ALIASES` especifica un archivo de alias que muestra los UID compartidos. El archivo predeterminado es `/usr/aset/masters/uid_aliases`.

## Ampliación de comprobaciones a tablas NIS+: YPCHECK

La variable de entorno `YPCHECK` especifica si ASET también debe comprobar las tablas de archivos de configuración del sistema. `YPCHECK` es una variable booleana. Sólo puede especificar `true` o `false` para `YPCHECK`. El valor predeterminado es `false`, que deshabilita la comprobación de tablas NIS+.

Para comprender cómo funciona esta variable de entorno, tenga en cuenta su efecto en el archivo `passwd`. Cuando se configura como `false`, ASET comprueba el archivo `passwd` local. Cuando se configura como `true`, la tarea también comprueba la tabla `passwd` NIS+ para el dominio del sistema.

---

**Nota** – Aunque ASET repara automáticamente los archivos locales, sólo informa problemas potenciales en las tablas NIS+. No cambia las tablas.

---

## Modificación de archivos de ajuste

ASET utiliza los tres archivos de ajuste maestros, `tune.low`, `tune.med` y `tune.high`, para facilitar o reforzar el acceso a archivos del sistema esenciales. Estos archivos maestros se encuentran en el directorio `/usr/aset/masters`. Puede modificar los archivos para que se ajusten a su entorno. Para obtener más ejemplos, consulte [“Ejemplos de archivos de ajuste” en la página 170](#).

El archivo `tune . low` define los permisos en valores que son adecuados para la configuración predeterminada del sistema. El archivo `tune . med` restringe aún más estos permisos. El archivo `tune . med` también incluye entradas que no están presentes en `tune . low`. El archivo `tune . high` restringe los permisos mucho más.

---

**Nota** – Modifique los valores en los archivos de ajuste agregando o eliminando entradas de archivos. No puede establecer efectivamente un permiso en un valor menos restrictivo que la configuración actual. Las tareas de ASET no flexibilizan los permisos, a menos que disminuya la seguridad del sistema a un nivel inferior.

---

## Restauración de archivos del sistema modificados por ASET

Cuando ASET se ejecuta por primera vez, guarda y archiva los archivos del sistema originales. La utilidad `aset . restore` restablece estos archivos. Esta utilidad también anula la programación de ASET, si la herramienta actualmente está programada para una ejecución periódica. El comando `aset . restore` se encuentra en `/usr/aset`, el directorio operativo de ASET.

Los cambios que se realizan en archivos del sistema se pierden al ejecutar el comando `aset . restore`.

Debe utilizar el comando `aset . restore` en los siguientes casos:

- Cuando desee eliminar los cambios de ASET y restaurar el sistema original.  
En caso de que desee desactivar ASET permanentemente, puede eliminar ASET de la programación de `cron` si el comando `aset` se ha agregado previamente a `crontab` de `root`. Para obtener instrucciones sobre cómo utilizar `cron` para eliminar la ejecución automática, consulte [“Cómo detener la ejecución periódica de ASET” en la página 174](#).
- Tras un breve período de experimentar con ASET, para restaurar el estado original del sistema.
- Cuando algunas funciones principales del sistema no funcionan correctamente, y sospecha que ASET es la causante del problema.

## Operación de red con el sistema NFS

Por lo general, ASET se utiliza en modo independiente, incluso en un sistema que forma parte de una red. Como administrador del sistema para su sistema independiente, es responsable de la seguridad del sistema. Por lo tanto, es responsable de la ejecución y gestión de ASET para proteger el sistema.

También puede utilizar ASET en el entorno distribuido NFS. Como administrador de la red, es responsable de instalar, ejecutar y administrar varias tareas administrativas para todos sus clientes. Para facilitar la gestión de ASET entre varios sistemas cliente, puede realizar cambios de configuración que se aplican de forma global a todos los clientes. Al aplicar globalmente los cambios, elimina la necesidad de tener que iniciar sesión en cada sistema para repetir los cambios de configuración.

Cuando decide cómo configurar ASET en los sistemas conectados a la red, debe considerar quién desea que controle la seguridad. Es posible que desee que los usuarios controlen parte de la seguridad en sus propios sistemas. Es posible que desee centralizar la responsabilidad para el control de la seguridad.

## **Establecimiento de una configuración global para cada nivel de seguridad**

Es posible que surja una situación en la que desee definir más de una configuración de red. Por ejemplo, puede que desee establecer una configuración para los clientes que están designados con un nivel de seguridad bajo. Puede que desee establecer otra configuración para los clientes con nivel de seguridad medio e incluso otra configuración con nivel de seguridad alto.

Si necesita crear una configuración de red independiente de ASET para cada nivel de seguridad, puede crear tres configuraciones de ASET en el servidor. En este caso, cree una configuración para cada nivel. Luego, exporte cada configuración a los clientes con el nivel de seguridad adecuado. Algunos componentes de ASET que son comunes a las tres configuraciones pueden compartirse mediante enlaces.

## **Recopilación de informes de ASET**

No sólo puede centralizar los componentes de ASET en un servidor, sino que también puede configurar un directorio central en un servidor para recopilar todos los informes de ASET. Los clientes pueden acceder al servidor con o sin privilegios de superusuario. Para obtener instrucciones sobre la configuración de un mecanismo de recopilación, consulte [“Cómo recopilar informes de ASET en un servidor” en la página 174](#).

Mediante la configuración de la recopilación de informes en un servidor, puede revisar informes para todos los clientes desde una ubicación. Puede utilizar este método sin importar si un cliente tiene o no tiene privilegios de superusuario. Como alternativa, puede dejar el directorio de informes en el sistema local si desea que los usuarios supervisen sus propios informes de ASET.

## **Variables de entorno de ASET**

A continuación, se muestra una lista de las variables de entorno de ASET y los valores que las variables especifican.

ASETDIR	Especifica el directorio de trabajo de ASET.
ASETSECLEVEL	Especifica el nivel de seguridad.
PERIODIC_SCHEDULE	Especifica la programación periódica.
TASKS	Especifica qué tareas de ASET se deben ejecutar.
UID_ALIASES	Especifica un archivo de alias.
YPCHECK	Determina si se van a ampliar las comprobaciones a las asignaciones NIS y las tablas NIS+.
CKLISTPATH_LOW	Es la lista de directorios para el nivel de seguridad bajo.
CKLISTPATH_MED	Es el directorio para el nivel de seguridad medio.
CKLISTPATH_HIGH	Es la lista de directorios para el nivel de seguridad alto.

Las variables de entorno que se muestran en las secciones siguientes se encuentran en el archivo `/usr/aset/asetenv`. Las variables `ASETDIR` y `ASETSECLEVEL` son opcionales. Las variables sólo se pueden establecer mediante el shell con el comando `/usr/aset/aset`. Las demás variables de entorno se pueden establecer editando el archivo.

## Variable de entorno ASETDIR

`ASETDIR` especifica un directorio de trabajo de ASET.

Desde el shell C, escriba:

```
% setenv ASETDIR pathname
```

Desde el shell Bourne o el shell Korn, escriba:

```
$ ASETDIR=pathname
$ export ASETDIR
```

Establezca *nombre\_ruta* en el nombre de ruta completo del directorio de trabajo de ASET.

## Variable de entorno ASETSECLEVEL

La variable `ASETSECLEVEL` especifica un nivel de seguridad en el que se ejecutan las tareas de ASET.

Desde el shell C, escriba:

```
% setenv ASETSECLEVEL level
```

Desde el shell Bourne o el shell Korn, escriba:

```
$ ASETSECLEVEL=level
$ export ASETSECLEVEL
```

En estos comandos, el nivel (*level*) se puede establecer en uno de los siguientes valores:

low	Nivel de seguridad bajo
med	Nivel de seguridad medio
high	Nivel de seguridad alto

## Variable de entorno PERIODIC\_SCHEDULE

El valor de PERIODIC\_SCHEDULE sigue el mismo formato que el archivo `crontab`. Especifique el valor de la variable como una cadena de cinco campos entre comillas dobles, cada uno separado por un espacio:

*"minutes hours day-of-month month day-of-week"*

*minutos\_horas* Especifica la hora de inicio en cantidad de minutos (de 0 a 59) después de la hora y la hora (de 0 a 23).

*día\_del\_mes* Especifica el día del mes cuando ASET se debe ejecutar, con valores de 1 a 31.

*mes* Especifica el mes del año cuando ASET se debe ejecutar, con valores de 1 a 12.

*día\_de\_semana* Especifica el día de la semana cuando ASET se debe ejecutar, con valores de 0 a 6. El domingo es el día 0.

Las siguientes reglas se aplican al crear una programación periódica para ASET:

- Puede especificar una lista de valores, cada uno delimitado por una coma, para cualquier campo.
- Puede especificar un valor como un número o puede especificar el valor como un rango. Un rango es un par de números que están unidos por un guión. Un rango indica que las tareas de ASET se deben ejecutar a cada hora que se incluye en el rango.
- Puede especificar un asterisco (\*) como el valor de cualquier campo. Un asterisco especifica todos los valores posibles del campo.

La entrada predeterminada para la variable PERIODIC\_SCHEDULE hace que ASET se ejecute todos los días a las 12:00 de la noche:

```
PERIODIC_SCHEDULE="0 0 * * *"
```



## Variable de entorno TASKS

La variable TASKS enumera las tareas que realiza ASET. De manera predeterminada, se enumeran las siete tareas:

```
TASKS="env sysconfig usrgrp tune cklist eeprom firewall"
```

## Variable de entorno UID\_ALIASES

La variable UID\_ALIASES especifica un archivo de alias. Si está presente, ASET consulta este archivo para obtener una lista de varios alias permitidos. El formato es

UID\_ALIASES=*nombre\_ruta*, donde *nombre\_ruta* es el nombre de ruta completo del archivo de alias.

El valor predeterminado es el siguiente:

```
UID_ALIASES=${ASETDIR}/masters/uid_aliases
```

## Variable de entorno YPCHECK

La variable YPCHECK amplía la tarea de comprobación de las tablas del sistema para incluir las tablas NIS o NIS+. La variable YPCHECK es una variable booleana, que se puede establecer en true o false.

El valor predeterminado es false, que limita la comprobación a tablas del sistema locales:

```
YPCHECK=false
```

## Variables de entorno CKLISTPATH\_level

Las tres variables de la ruta de la lista de comprobación enumeran los directorios que serán comprobados por la tarea de comprobaciones de archivos del sistema. Las siguientes definiciones de las variables están definidas de manera predeterminada. Las definiciones ilustran la relación entre las variables en diferentes niveles:

```
CKLISTPATH_LOW=${ASETDIR}/tasks:${ASETDIR}/util:${ASETDIR}/masters:/etc
CKLISTPATH_MED=${CKLISTPATH_LOW}:/usr/bin:/usr/ucb
CKLISTPATH_HIGH=${CKLISTPATH_MED}:/usr/lib:/sbin:/usr/sbin:/usr/ucblib
```

Los valores de las variables de entorno de la ruta de la lista de comprobación son similares a los valores de las variables de la ruta del shell. Al igual que las variables de la ruta del shell, las variables de entorno de la ruta de la lista de comprobación son listas de nombres de directorios. Los nombres de directorios están separados por dos puntos. Utilice un signo igual (=) para conectar el nombre de variable con su valor.

## Ejemplos de archivos de ASET

Esta sección tiene ejemplos de algunos archivos de ASET, incluidos los archivos de ajuste y el archivo de alias.

### Ejemplos de archivos de ajuste

ASET contiene tres archivos de ajuste. Cada entrada de un archivo de ajuste ocupa una línea. Los campos de una entrada están en el siguiente orden:

*pathname mode owner group type*

<i>nombre_ruta</i>	El nombre de ruta completa del archivo.
<i>modo</i>	Un número de 5 dígitos que representa la configuración de permisos.
<i>propietario</i>	El propietario del archivo.
<i>grupo</i>	El propietario del grupo del archivo.
<i>tipo</i>	El tipo de archivo.

Las siguientes reglas se aplican al editar los archivos de ajuste:

- Puede utilizar caracteres comodín de shell regulares, como un asterisco ( *\** ) y un signo de interrogación ( *?* ), en el nombre de la ruta de varias referencias. Para obtener más información, consulte [sh\(1\)](#).
- El modo (*mode*) representa el valor menos restrictivo. Si el valor actual ya es más restrictivo que el valor especificado, ASET no reduce la configuración de los permisos. Por ejemplo, si el valor especificado es *00777*, el permiso permanece sin cambios, porque *00777* siempre es menos restrictivo que cualquier valor actual.  
Este proceso representa cómo ASET maneja la configuración del modo. El proceso es diferente si el nivel de seguridad se está reduciendo o si está eliminando ASET. Cuando reduce el nivel de seguridad desde el nivel de la ejecución anterior o cuando desea restaurar los archivos del sistema al estado en el que estaban antes de que ASET se ejecutara por primera vez, ASET reconoce lo que está haciendo y disminuye el nivel de protección.
- Debe utilizar nombres para propietario (*owner*) y grupo (*group*) en lugar de ID numéricos.
- Puede utilizar un signo de interrogación ( *?* ) en el lugar de propietario (*owner*), grupo (*group*) y tipo (*type*) para evitar que ASET cambie los valores existentes de estos parámetros.
- El tipo (*type*) puede ser *symlink*, directorio o archivo. Un *symlink* es un enlace simbólico.
- Los archivos de ajuste con nivel de seguridad más alto restablecen los permisos de archivo para que sean, al menos, tan restrictivos como los permisos de archivo en niveles más bajos. Asimismo, en los niveles de seguridad más altos, se agregan archivos adicionales a la lista.
- Un archivo puede coincidir con más de una entrada de archivo de ajuste. Por ejemplo, *etc/passwd* coincide con las entradas *etc/pass\** y *etc/\**.

- Cuando dos entradas tienen permisos diferentes, el permiso de archivo se establece en el valor más restrictivo. En el ejemplo siguiente, el permiso del archivo `/etc/passwd` se establece en `00755`, que es el más restrictivo de `00755` y `00770`.  

```
/etc/pass* 00755 ? ? file
/etc/* 00770 ? ? file
```
- Si dos entradas tienen diferentes designaciones de propietario (*owner*) o grupo (*group*), la última entrada tiene prioridad. En el siguiente ejemplo, el propietario de `/usr/sbin/chroot` está establecido en `root`.  

```
/usr/sbin/chroot 00555 bin bin file
/usr/sbin/chroot 00555 root bin file
```

### Ejemplos de archivos de alias

El archivo de alias contiene una lista de alias que comparten el mismo ID de usuario.

Cada entrada tiene el siguiente formato:

```
uid=alias1 =alias2=alias3=. . .
uid      UID compartido.
aliasn    Cuentas de usuario que comparten un UID.
```

Por ejemplo, la siguiente entrada indica el UID `0`. El UID es compartido por las cuentas `sysadm` y `root`:

```
0=root=sysadm
```

## Ejecución de ASET (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Ejecutar ASET desde la línea de comandos	Protege el sistema en el nivel de ASET que especifica. Muestra el registro de ejecución para ver los cambios.	<a href="#">“Cómo ejecutar ASET interactivamente” en la página 172</a>
Ejecutar ASET en modo de proceso por lotes a intervalos regulares	Configura un trabajo cron para garantizar que ASET protege el sistema.	<a href="#">“Cómo ejecutar ASET periódicamente” en la página 173</a>
Detener la ejecución de ASET en modo de proceso por lotes	Elimina el trabajo cron de ASET.	<a href="#">“Cómo detener la ejecución periódica de ASET” en la página 174</a>
Almacenar los informes de ASET en un servidor	Recopila informes de ASET de los clientes para supervisarlos en una ubicación central.	<a href="#">“Cómo recopilar informes de ASET en un servidor” en la página 174</a>

Para establecer las variables de ASET, consulte [“Variables de entorno de ASET” en la página 166](#). Para configurar ASET, consulte [“Configuración de ASET” en la página 162](#).

## ▼ Cómo ejecutar ASET interactivamente

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Ejecute ASET de forma interactiva mediante el comando `aset`.

```
# /usr/aset/aset -l level -d pathname
```

*nivel* Especifica el nivel de seguridad. Los valores válidos son `low`, `medium` o `high`. La configuración predeterminada es `low`. Para obtener información detallada sobre los niveles de seguridad, consulte [“Niveles de seguridad de ASET” en la página 154](#).

*nombre\_ruta* Especifica el directorio de trabajo de ASET. El valor predeterminado es `/usr/aset`.

### 3 Verifique que ASET se esté ejecutando al observar el registro de ejecución de ASET que se muestra en la pantalla.

El mensaje de registro de ejecución identifica las tareas que se están ejecutando.

## Ejemplo 7-1 Ejecución de ASET interactivamente

En el siguiente ejemplo, ASET se ejecuta a un nivel de seguridad bajo con el directorio de trabajo predeterminado.

```
# /usr/aset/aset -l low
===== ASET Execution Log =====

ASET running at security level low

Machine = jupiter; Current time = 0111_09:26

aset: Using /usr/aset as working directory

Executing task list ...
    firewall
    env
    sysconf
    usrgrp
    tune
    cklist
    eepprom
```

All tasks executed. Some background tasks may still be running.

Run `/usr/aset/util/taskstat` to check their status:  
`/usr/aset/util/taskstat [aset_dir]`

where `aset_dir` is ASET's operating directory, currently `/usr/aset`.

When the tasks complete, the reports can be found in:  
`/usr/aset/reports/latest/*.rpt`

You can view them by:  
`more /usr/aset/reports/latest/*.rpt`

## ▼ Cómo ejecutar ASET periódicamente

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Si es necesario, configure la hora a la que desea que ASET se ejecute periódicamente.

Debe hacer que ASET se ejecute cuando la demanda del sistema es leve. La variable de entorno `PERIODIC_SCHEDULE` en el archivo `/usr/aset/asetenv` se utiliza para configurar la hora a la que se va a ejecutar ASET periódicamente. De manera predeterminada, la hora está establecida todos los días a medianoche.

Si desea configurar una hora diferente, edite la variable `PERIODIC_SCHEDULE` en el archivo `/usr/aset/asetenv`. Para obtener información detallada acerca de la configuración de la variable `PERIODIC_SCHEDULE`, consulte [“Variable de entorno `PERIODIC\_SCHEDULE`” en la página 168](#).

### 3 Agregue una entrada al archivo `crontab` mediante el comando `aset`.

```
# /usr/aset/aset -p
```

La opción `-p` inserta una línea en el archivo `crontab` que empieza la ejecución de ASET a la hora determinada por la variable de entorno `PERIODIC_SCHEDULE` en el archivo `/usr/aset/asetenv`.

### 4 Visualice la entrada `crontab` para verificar cuándo está programada la ejecución de ASET.

```
# crontab -l root
```

## ▼ Cómo detener la ejecución periódica de ASET

- 1 **Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Edite el archivo `crontab`.**

```
# crontab -e root
```

- 3 **Elimine la entrada de ASET.**

- 4 **Guarde los cambios y salga.**

- 5 **Visualice la entrada `crontab` para verificar que la entrada de ASET se haya eliminado.**

```
# crontab -l root
```

## ▼ Cómo recopilar informes de ASET en un servidor

- 1 **Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Configure un directorio en el servidor:**

- a. **Cambie al directorio `/usr/aset`.**

```
mars# cd /usr/aset
```

- b. **Cree un directorio `rptdir`.**

```
mars# mkdir rptdir
```

- c. **Cambie al directorio `rptdir` y cree un directorio `client_rpt`.**

Este paso crea un subdirectorio `client_rpt` para un cliente. Repita este paso para cada cliente cuyos informes debe recopilar.

```
mars# cd rptdir
mars# mkdir client_rpt
```

En el ejemplo siguiente, el directorio `all_reports` y los subdirectorios `pluto_rpt` y `neptune_rpt` se crean.

```
mars# cd /usr/aset
mars# mkdir all_reports
mars# cd all_reports
mars# mkdir pluto_rpt
mars# mkdir neptune_rpt
```

### 3 Agregue los directorios *client\_rpt* al archivo */etc/dfs/dfstab*.

Los directorios deben tener opciones de lectura y escritura.

Por ejemplo, las siguientes entradas en el archivo `dfstab` se comparten con permisos de lectura y escritura.

```
share -F nfs -o rw=pluto /usr/aset/all_reports/pluto_rpt
share -F nfs -o rw=neptune /usr/aset/all_reports/neptune_rpt
```

### 4 Haga que los recursos en el archivo *dfstab* estén disponibles para los clientes.

```
# shareall
```

### 5 En cada cliente, monte el subdirectorio del cliente desde el servidor en el punto de montaje, */usr/aset/masters/reports*.

```
# mount server:/usr/aset/client_rpt /usr/aset/masters/reports
```

### 6 Edite el archivo */etc/vfstab* para montar el directorio automáticamente en el momento de inicio.

La siguiente entrada de ejemplo en `/etc/vfstab` en `neptune` muestra el directorio que se montará desde `mars`, `/usr/aset/all_reports/neptune_rpt`, y el punto de montaje en `neptune`, `/usr/aset/reports`. En el momento de inicio, los directorios que se muestran en `vfstab` se montan automáticamente.

```
mars:/usr/aset/all_reports/neptune.rpt /usr/aset/reports nfs - yes hard
```

## Resolución de problemas de ASET

En esta sección, se describen los mensajes de error generados por ASET.

### Mensajes de error de ASET

ASET failed: no mail program found.

**Causa:** Se indica a ASET que envíe el registro de ejecución a un usuario, pero no se puede encontrar ningún programa de correo.

**Solución:** Instale un programa de correo.

Usage: aset [-n user[@host]] in /bin/mail or /usr/ucb/mail.

Cannot decide current and previous security levels.

**Causa:** ASET no puede determinar cuáles son los niveles de seguridad para las invocaciones actuales y anteriores.

**Solución:** Asegúrese de que el nivel de seguridad actual se establezca mediante la opción de línea de comandos o la variable de entorno ASETSECLEVEL. Además, asegúrese de que la última línea de ASETDIR/archives/asetseclevel.arch refleje correctamente el nivel de seguridad anterior. Si estos valores no están establecidos o son incorrectos, introduzca los valores correctos.

ASET working directory undefined.

To specify, set ASETDIR environment variable or use command line option -d.

ASET startup unsuccessful.

**Causa:** El directorio de trabajo de ASET no está definido o el directorio está definido incorrectamente. El directorio de trabajo es el directorio operativo.

**Solución:** Utilice la variable de entorno ASETDIR o la opción de línea de comandos -d para corregir el error, y reinicie ASET.

ASET working directory \$ASETDIR missing.

ASET startup unsuccessful.

**Causa:** El directorio de trabajo de ASET no está definido o el directorio está definido incorrectamente. El directorio de trabajo es el directorio operativo. Este problema puede ser debido a que la variable ASETDIR hace referencia a un directorio inexistente. O la opción de línea de comandos -d puede hacer referencia a un directorio inexistente.

**Solución:** Asegúrese de que se haga referencia correctamente al directorio correspondiente, es decir, el directorio que contiene la jerarquía de directorios de ASET.

Cannot expand \$ASETDIR to full pathname.

**Causa:** ASET no puede expandir el nombre del directorio proporcionado por la variable ASETDIR o la opción de línea de comandos -d a un nombre de ruta completa.

**Solución:** Asegúrese de que el nombre del directorio sea correcto. Asegúrese de que el directorio haga referencia a un directorio existente al que el usuario tenga acceso.



aset: invalid/undefined security level.

To specify, set ASETSECLEVEL environment variable or use command line option -l, with argument= low/med/high.

**Causa:** El nivel de seguridad no está definido o está definido incorrectamente. Sólo los valores low, med o high son aceptables.

**Solución:** Utilice la variable ASETSECLEVEL o la opción de línea de comandos -l para especificar uno de los tres valores.

ASET environment file asetenv not found in \$ASETDIR.

ASET startup unsuccessful.

**Causa:** ASET no puede encontrar un archivo asetenv en su directorio de trabajo.

**Solución:** Asegúrese de que haya un archivo asetenv en el directorio de trabajo de ASET. Para obtener detalles sobre este archivo, consulte la página del comando man [asetenv\(4\)](#).

filename doesn't exist or is not readable.

**Causa:** El archivo al que se hace referencia por el nombre de archivo (*filename*) no existe o no se puede leer. Este problema se puede producir cuando está utilizando la opción -u. La opción permite especificar un archivo que contiene una lista de usuarios a los que desea comprobar.

**Solución:** Asegúrese de que el argumento para la opción -u exista y que el argumento se pueda leer.

ASET task list TASKLIST undefined.

**Causa:** La lista de tareas de ASET, que debe estar definida en el archivo asetenv, no está definida. Este mensaje puede significar que el archivo asetenv es incorrecto.

**Solución:** Examine el archivo asetenv. Asegúrese de que la lista de tareas esté definida en la sección User Configurable. Compruebe, además, otras partes del archivo para asegurarse de que el archivo esté intacto. Para obtener el contenido de un archivo asetenv válido, consulte la página del comando man [asetenv\(4\)](#).

ASET task list \$TASKLIST missing.

ASET startup unsuccessful.

**Causa:** La lista de tareas de ASET, que debe estar definida en el archivo asetenv, no está definida. Este mensaje puede significar que el archivo asetenv es incorrecto.

**Solución:** Examine el archivo asetenv. Asegúrese de que la lista de tareas esté definida en la sección User Configurable. Compruebe, además, otras partes del archivo para asegurarse de que el archivo esté intacto. Para obtener el contenido de un archivo asetenv válido, consulte la página del comando man [asetenv\(4\)](#).

Schedule undefined for periodic invocation.

No tasks executed or scheduled. Check asetenv file.

**Causa:** La programación de ASET se solicita mediante la opción -p, pero la variable de entorno PERIODIC\_SCHEDULE no está definida en el archivo asetenv.

**Solución:** Compruebe la sección User Configurable del archivo asetenv para asegurarse de que la variable esté definida. Asegúrese de que la variable se encuentre en el formato adecuado.

Warning! Duplicate ASET execution scheduled.

Check crontab file.

**Causa:** ASET está programada para ejecutarse más de una vez. En otras palabras, la programación se solicita mientras una programación ya está en efecto. Este mensaje no indica necesariamente un error si se desea más de una programación. En esta instancia, los mensajes sólo sirven como una advertencia. Si desea más de una programación, debe utilizar el formato de programación adecuado con el comando crontab. Para obtener más información, consulte la página del comando `man crontab(1)`.

**Solución:** Verifique, mediante el comando `crontab`, que la programación correcta esté en efecto. Asegúrese de que no haya ninguna entrada `crontab` innecesaria para ASET.

## P A R T E   I I I

# Roles, perfiles de derechos y privilegios

En esta sección, se tratan el control de acceso basado en roles (RBAC, Role-Based Access Control) y la gestión de derechos de procesos. Los componentes de RBAC incluyen roles, perfiles de derechos y autorizaciones. La gestión de derechos de procesos se implementa a través de privilegios. Los privilegios se utilizan junto con RBAC para proporcionar una alternativa de administración más segura que la administración de un sistema con un superusuario.

- Capítulo 8, “Uso de roles y privilegios (descripción general)”
- Capítulo 9, “Uso del control de acceso basado en roles (tareas)”
- Capítulo 10, “Control de acceso basado en roles (referencia)”
- Capítulo 11, “Privilegios (tareas)”
- Capítulo 12, “Privilegios (referencia)”



## Uso de roles y privilegios (descripción general)

---

El control de acceso basado en roles (RBAC) y los privilegios de Oracle Solaris proporcionan una alternativa más segura al modelo de superusuario. En este capítulo, se proporciona información general sobre RBAC y los privilegios.

A continuación, se presenta la información general que se incluye en este capítulo.

- “Control de acceso basado en roles (descripción general)” en la página 182
- “Privilegios (descripción general)” en la página 193

## Novedades de RBAC

**Solaris 10 8/07:** a partir de esta versión, se introdujeron los controles de recursos `project.max-locked-memory` y `zone.max-locked-memory`. Si el privilegio `PRIV_PROC_LOCK_MEMORY` se asigna a un usuario o una zona no global, es posible configurar estos controles de recursos para evitar que el usuario o la zona bloqueen toda la memoria. Para ver una explicación más detallada, consulte [“Privilegios y recursos del sistema” en la página 196](#).

**Solaris 10 10/08:** en esta versión, se reorganizaron las autorizaciones `solaris.admin.usermgr` para permitir la *separación de tareas*, un requisito en las instalaciones de seguridad elevada. Para cumplir con la separación de tareas, se necesitan dos cuentas para crear una cuenta de usuario. Si desea configurar el software para cumplir este requisito, consulte [“Creación de perfiles de derechos que aplican la separación de tareas” de Guía de configuración de Oracle Solaris Trusted Extensions](#). También en esta versión, la guía describe cómo cambiar la contraseña de un rol en [“Cómo cambiar la contraseña de un rol” en la página 224](#).

**Solaris 10 9/10:** en esta versión, se agrega el privilegio `net_access` al conjunto básico de privilegios. Para obtener una descripción del privilegio, consulte la página del comando `man privileges(5)`.

## Control de acceso basado en roles (descripción general)

El control de acceso basado en roles (RBAC) es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al superusuario. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede dividir las capacidades de superusuario entre varios administradores. La gestión de derechos de procesos se implementa a través de *privilegios*. La gestión de derechos de usuarios se implementa a través de RBAC.

- Para ver una explicación de la gestión de derechos de procesos, consulte [“Privilegios \(descripción general\)” en la página 193](#).
- Para obtener información sobre las tareas de RBAC, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#).
- Para obtener información de referencia, consulte el [Capítulo 10, “Control de acceso basado en roles \(referencia\)”](#).

## RBAC: una alternativa al modelo de superusuario

En los sistemas UNIX convencionales, el usuario `root`, también conocido como superusuario, es omnipotente. Los programas que se ejecutan como `root`, o los programas `setuid`, son omnipotentes. El usuario `root` puede leer y escribir en cualquier archivo, ejecutar todos los programas y enviar señales de terminación a cualquier proceso. De hecho, cualquier persona que puede convertirse en superusuario puede modificar el cortafuegos de un sitio, modificar la pista de auditoría, leer registros confidenciales y apagar toda la red. Un programa `setuid` usurpado puede realizar cualquier tarea en el sistema.

El control de acceso basado en roles (RBAC) ofrece una alternativa más segura al modelo de superusuario del tipo "todo o nada". Con RBAC, puede aplicar una política de seguridad en un nivel más específico. RBAC utiliza el principio de seguridad del *privilegio mínimo*. Privilegio mínimo significa que un usuario dispone exactamente de la cantidad de privilegios necesaria para realizar un trabajo. Los usuarios comunes tienen privilegios suficientes para utilizar sus aplicaciones, comprobar el estado de sus trabajos, imprimir archivos, crear archivos nuevos, etc. Las capacidades que van más allá de las capacidades de los usuarios comunes se agrupan en perfiles de derechos. Los usuarios que realizarán trabajos que requieren algunas de las capacidades de superusuario asumen un rol que incluye el perfil de derechos adecuado.

RBAC recopila las capacidades de superusuario en *perfiles de derechos*. Estos perfiles de derechos se asignan a cuentas de usuario especiales denominadas *roles*. Luego, un usuario puede asumir un rol para realizar un trabajo que requiere algunas de las capacidades de superusuario. Se incluyen perfiles de derechos predefinidos con el software Oracle Solaris. Usted crea los roles y asigna los perfiles.

Los perfiles de derechos pueden proporcionar capacidades amplias. Por ejemplo, el perfil de derechos de administrador principal es equivalente al superusuario. Los perfiles de derechos

también se pueden definir de manera limitada. Por ejemplo, el perfil de derechos de gestión de cron se encarga de los trabajos at y cron. Al crear roles, puede optar por crear roles con capacidades amplias o roles con capacidades limitadas, o ambos.

En el modelo RBAC, el superusuario crea uno o más roles. Los roles se basan en perfiles de derechos. El superusuario luego asigna los roles a los usuarios en los que confía para realizar las tareas del rol. Los usuarios inician sesión con su nombre de usuario. Después del inicio de sesión, los usuarios asumen roles que pueden ejecutar comandos administrativos restringidos y herramientas de la interfaz gráfica de usuario (GUI).

La flexibilidad en la configuración de los roles posibilita una variedad de políticas de seguridad. Aunque se incluyen pocos roles con Oracle Solaris, es posible configurar fácilmente tres roles recomendados. Los roles se basan en perfiles de derechos con el mismo nombre:

- **Administrador principal:** un rol poderoso que es equivalente al usuario root o superusuario.
- **root:** un rol poderoso que es equivalente al usuario root. Sin embargo, este usuario root no puede iniciar sesión. Un usuario común debe iniciar sesión y, a continuación, asumir el rol root asignado.
- **Administrador del sistema:** un rol menos poderoso para la administración que no está relacionado con la seguridad. Este rol puede gestionar sistemas de archivos, correo e instalación de software. Sin embargo, este rol no puede definir contraseñas.
- **Operador:** rol de administrador junior para operaciones como copias de seguridad y gestión de impresoras.

---

**Nota** – El perfil de derechos de copia de seguridad de medios proporciona acceso a todo el sistema de archivos raíz. Por lo tanto, si bien los perfiles de derechos de copia de seguridad de medios y operador están diseñados para un administrador junior, debe asegurarse de que el usuario es de confianza.

---

No es necesario implementar estos tres roles. Los roles representan una función de las necesidades de seguridad de una organización. Los roles se pueden configurar para administradores con fines especiales en áreas como administración de cortafuegos, redes o seguridad. Otra estrategia es crear un rol de administrador poderoso único junto con un rol de usuario avanzado. El rol de usuario avanzado sería para los usuarios que tienen permiso para corregir partes de sus propios sistemas.

El modelo de superusuario y el modelo RBAC pueden coexistir. La siguiente tabla resume las gradaciones de superusuario a usuario común restringido que son posibles en el modelo RBAC. La tabla incluye las acciones administrativas que se pueden supervisar en ambos modelos. Para obtener un resumen del efecto de los privilegios solamente en un sistema, consulte la [Tabla 8–2](#).

TABLA 8-1    Modelo de superusuario y modelo RBAC con privilegios

Capacidades de usuario en un sistema	Modelo de superusuario	Modelo RBAC
Puede convertirse en superusuario con capacidades completas de superusuario	Sí	Sí
Puede iniciar sesión como usuario con capacidades completas de usuario	Sí	Sí
Puede convertirse en superusuario con capacidades limitadas	No	Sí
Puede iniciar sesión como usuario y tener capacidades de superusuario, esporádicamente	Sí, sólo con los programas setuid	Sí, con los programas setuid y con RBAC
Puede iniciar sesión como usuario con capacidades administrativas, pero sin capacidades completas de superusuario	No	Sí, con RBAC y con los privilegios y autorizaciones asignados directamente
Puede iniciar sesión como usuario con menos capacidades que un usuario común	No	Sí, con RBAC y con los privilegios eliminados
Puede supervisar las acciones de superusuario	Sí, mediante la auditoría del comando su	Sí, mediante la auditoría de los comandos de shell de perfil  Además, si el usuario root está deshabilitado, el nombre del usuario que asumió el rol root está en la pista de auditoría

## Elementos y conceptos básicos de RBAC en Oracle Solaris

El modelo RBAC en Oracle Solaris introduce los siguientes elementos:

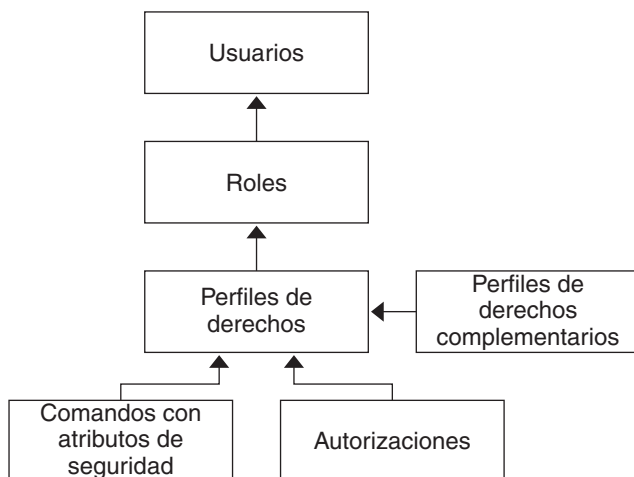
- **Autorización:** un permiso para que un usuario o un rol realice una clase de acciones que requieren derechos adicionales. Por ejemplo, la política de seguridad en la instalación otorga a los usuarios comunes la autorización `solaris.device.cdrom`. Esta autorización permite a los usuarios leer y escribir en un dispositivo de CD-ROM. Para obtener una lista de autorizaciones, consulte el archivo `/etc/security/auth_attr`.
- **Privilegio:** un derecho perfectamente definido que se puede otorgar a un comando, un usuario, un rol o un sistema. Los privilegios permiten que un proceso se realice correctamente. Por ejemplo, el privilegio `proc_exec` permite a un proceso llamar `execve()`. Los usuarios comunes tienen privilegios básicos. Para ver sus privilegios básicos, ejecute el comando `ppriv -vl basic`.



- **Atributos de seguridad:** un atributo que permite a un proceso efectuar una operación. En un entorno UNIX típico, un atributo de seguridad permite a un proceso efectuar una operación que, de lo contrario, está prohibida para los usuarios comunes. Por ejemplo, los programas `setuid` y `setgid` tienen atributos de seguridad. En el modelo RBAC, las operaciones que los usuarios comunes realizan pueden requerir atributos de seguridad. Además de los programas `setuid` y `setgid`, las autorizaciones y los privilegios también son atributos de seguridad en el modelo RBAC. Por ejemplo, un usuario con la autorización `solaris.device.allocate` puede asignar un dispositivo para uso exclusivo. Un proceso con el privilegio `sys_time` puede manipular la hora del sistema.
- **Aplicación con privilegios:** una aplicación o un comando que puede anular los controles del sistema mediante la comprobación de *atributos de seguridad*. En un entorno UNIX típico y en el modelo RBAC, los programas que usan `setuid` y `setgid` son aplicaciones con privilegios. En el modelo RBAC, los programas que necesitan privilegios o autorizaciones para ejecutarse correctamente también son aplicaciones con privilegios. Para obtener más información, consulte “Aplicaciones con privilegios y RBAC” en la página 189.
- **Perfil de derechos:** una recopilación de capacidades administrativas que se pueden asignar a un rol o a un usuario. Un perfil de derechos puede constar de autorizaciones, comandos con atributos de seguridad y otros perfiles de derechos. Los perfiles de derechos ofrecen una forma práctica de agrupar los atributos de seguridad.
- **Rol:** una identidad especial para ejecutar aplicaciones con privilegios. Sólo los usuarios asignados pueden asumir la identidad especial. En un sistema que se ejecuta por roles, el superusuario resulta innecesario. Las capacidades de superusuario se distribuyen en roles diferentes. Por ejemplo, en un sistema de dos roles, las tareas de seguridad serían gestionadas por un rol de seguridad. El segundo rol se ocuparía de las tareas de administración del sistema que no están relacionadas con la seguridad. Los roles pueden ser más específicos. Por ejemplo, un sistema podría incluir roles administrativos independientes para gestionar la estructura criptográfica, las impresoras, la hora del sistema, los sistemas de archivos y la auditoría.

La siguiente figura muestra cómo trabajan juntos los elementos de RBAC.

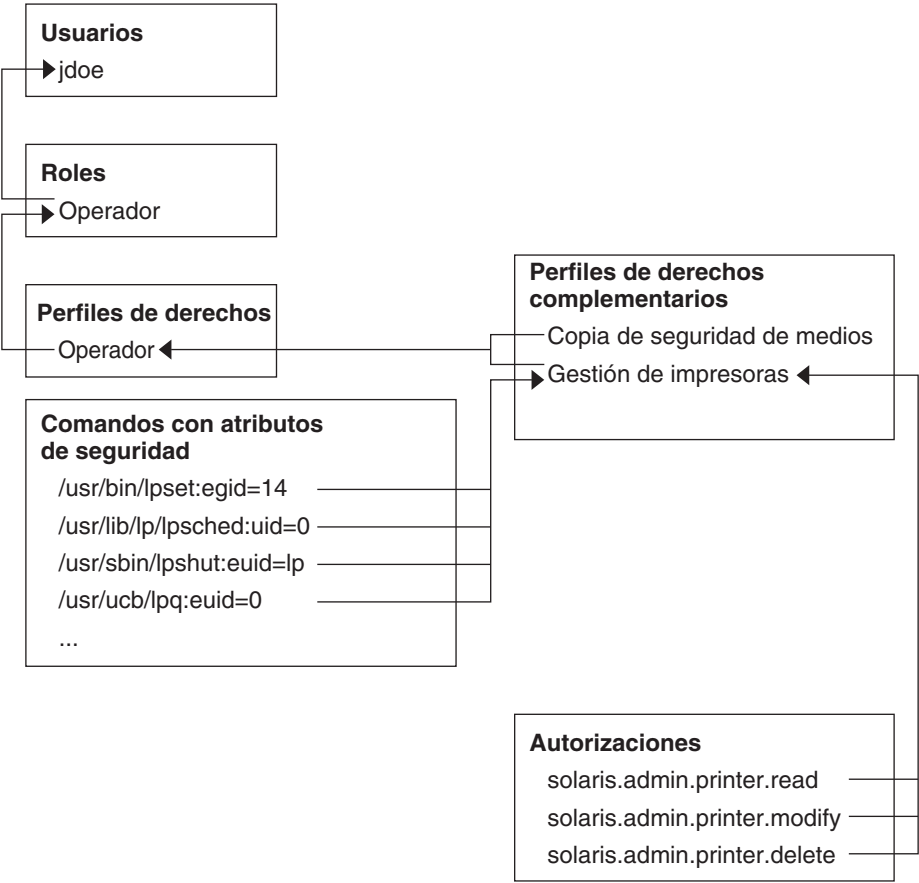
FIGURA 8-1 Relaciones entre elementos de RBAC en Oracle Solaris



En RBAC, se asignan roles a los usuarios. Cuando un usuario asume un rol, las capacidades del rol están disponibles. Los roles obtienen sus capacidades de los perfiles de derechos. Los perfiles de derechos pueden contener autorizaciones, privilegios asignados directamente, comandos con privilegios y otros perfiles de derechos complementarios. Los comandos con privilegios son comandos que se ejecutan con atributos de seguridad.

La siguiente figura utiliza el rol de seguridad de la red y el perfil de derechos de seguridad de la red para demostrar las relaciones de RBAC.

FIGURA 8-2 Ejemplo de relaciones entre elementos de RBAC en Oracle Solaris



El rol de seguridad de la red se utiliza para la gestión de IPsec, wifi y enlaces de red. El rol se asigna al usuario `jdoe`. Para asumir el rol, `jdoe` puede cambiar a dicho rol y, a continuación, suministrar la contraseña del rol.

El perfil de derechos de seguridad de la red se asignó al rol de seguridad de la red. El perfil de derechos de seguridad de la red contiene perfiles complementarios que se evalúan en orden: seguridad de wifi de red, seguridad de enlaces de red y gestión de IPsec de red. Estos perfiles complementarios desempeñan las principales tareas del rol.

El perfil de derechos de seguridad de la red tiene tres autorizaciones asignadas directamente, ningún privilegio asignado directamente y dos comandos con atributos de seguridad. Los perfiles de derechos complementarios tienen autorizaciones asignadas directamente y dos de ellas tienen comandos con atributos de seguridad. En el rol de seguridad de la red, `jdoe` tiene todas las autorizaciones asignadas en estos perfiles y puede ejecutar todos los comandos con atributos de seguridad en estos perfiles. `jdoe` puede administrar la seguridad de la red.

## Escalada de privilegios

Oracle Solaris proporciona a los administradores mucha flexibilidad al configurar la seguridad. Tal como está instalado, el software no permite la [escalonamiento de privilegios](#). La escalada de privilegios se produce cuando un usuario o un proceso obtienen más derechos administrativos de los que inicialmente se les iban a otorgar. En este sentido, un privilegio comprende cualquier atributo de seguridad, no sólo privilegios.

El software Oracle Solaris incluye atributos de seguridad que están asignados al usuario root únicamente. Con otras protecciones de seguridad implementadas, es posible que un administrador asigne atributos que están diseñados para el usuario root en otras cuentas, pero dicha asignación se debe realizar con cuidado.

Por ejemplo, el perfil de derechos de restauración de medios existe, pero no es parte de ningún otro perfil de derechos. Debido a que la restauración de medios proporciona acceso a todo el sistema de archivos raíz, su uso constituye una posible escalada de privilegios. Se podrían restaurar medios alternativos o archivos modificados deliberadamente. De manera predeterminada, sólo el usuario root tiene este perfil de derechos.

Para conocer las escaladas que afectan el atributo de seguridad del privilegio, consulte [“Cómo evitar la escalada de privilegios” en la página 274](#).

## Autorizaciones RBAC

Una *autorización* es un derecho perfectamente definido que se puede otorgar a un rol o a un usuario. Las autorizaciones aplican políticas en el nivel de aplicación del usuario.

Aunque las autorizaciones pueden asignarse directamente a un rol o a un usuario, se recomienda incluirlas en un perfil de derechos. El perfil de derechos luego se agrega a un rol, y el rol se asigna a un usuario. Para ver un ejemplo, consulte la [Figura 8–2](#).

Las aplicaciones compatibles con RBAC pueden comprobar las autorizaciones de un usuario antes de otorgar acceso a la aplicación o a operaciones específicas dentro de la aplicación. Esta comprobación reemplaza la verificación en las aplicaciones UNIX convencionales para `UID=0`. Para obtener más información sobre las autorizaciones, consulte las siguientes secciones:

- [“Denominación y delegación de autorizaciones” en la página 242](#)
- [“Base de datos `auth\_attr`” en la página 246](#)
- [“Comandos que requieren autorizaciones” en la página 252](#)

## Autorizaciones y privilegios

Los privilegios aplican la política de seguridad en el núcleo. La diferencia entre las autorizaciones y los privilegios reside en el nivel en el que se aplica la política de seguridad. Sin el privilegio adecuado, el núcleo puede evitar que un proceso realice operaciones con

privilegios. Sin las autorizaciones adecuadas, es posible que se le impida a un usuario utilizar una aplicación con privilegios o realizar operaciones que conlleven riesgos de seguridad dentro de una aplicación con privilegios. Para ver una explicación más detallada de los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#).

## Aplicaciones con privilegios y RBAC

Las aplicaciones y los comandos que pueden anular los controles del sistema se consideran aplicaciones con privilegios. Los atributos de seguridad, como `UID=0`, los privilegios y las autorizaciones hacen que una aplicación sea una aplicación con privilegios.

### Aplicaciones que comprueban UID y GID

Las aplicaciones con privilegios que comprueban la existencia de `root` (`UID=0`) o algún otro UID o GID especial han estado presentes en el entorno UNIX desde hace tiempo. El mecanismo de perfiles de derechos permite aislar comandos que requieren un ID específico. En lugar de cambiar el ID de un comando al que cualquiera puede acceder, puede colocar el comando con atributos de seguridad de ejecución en un perfil de derechos. Un usuario o un rol con ese perfil de derechos luego pueden ejecutar el programa sin tener que convertirse en superusuario.

Los ID se pueden especificar como reales o efectivos. Se prefiere la asignación de ID efectivos en lugar de la asignación de ID reales. Los ID efectivos son equivalentes a la función `setuid` en los bits de permisos de archivo. Los ID efectivos también identifican el UID para auditoría. Sin embargo, dado que algunos programas y secuencias de comandos de shell requieren un UID real de `root`, también es posible definir UID reales. Por ejemplo, el comando `pkgadd` requiere un UID real en lugar de uno efectivo. Si un ID efectivo no es suficiente para ejecutar un comando, debe cambiar el ID por un ID real. Para conocer el procedimiento, consulte [“Cómo crear o modificar un perfil de derechos” en la página 228](#).

### Aplicaciones que comprueban privilegios

Las aplicaciones con privilegios pueden comprobar el uso de privilegios. El mecanismo de perfiles de derechos de RBAC permite especificar los privilegios para comandos específicos. En lugar de requerir capacidades de superusuario para utilizar una aplicación o un comando, puede aislar el comando con atributos de seguridad de ejecución en un perfil de derechos. Un usuario o un rol con ese perfil de derechos luego pueden ejecutar el comando sólo con los privilegios que el comando necesita para una ejecución correcta.

Entre los comandos que comprueban la existencia de privilegios, se incluyen los siguientes:

- Comandos de Kerberos, como `kadmin`, `kprop` y `kdb5_util`.
- Comandos de redes, como `ifconfig`, `routeadm` y `snoop`.
- Comandos de archivos y sistemas de archivos, como `chmod`, `chgrp` y `mount`.
- Comandos que controlan procesos, como `kill`, `pcrd` y `rcapadm`.

Para agregar comandos con privilegios en un perfil de derechos, consulte [“Cómo crear o modificar un perfil de derechos” en la página 228](#). Para determinar los comandos que comprueban privilegios en un perfil concreto, consulte [“Determinación de los privilegios asignados” en la página 264](#).

## Aplicaciones que comprueban autorizaciones

Oracle Solaris proporciona además comandos que comprueban autorizaciones. Por definición, el usuario `root` tiene todas las autorizaciones. Por lo tanto, el usuario `root` puede ejecutar cualquier aplicación. Entre las aplicaciones que comprueban la existencia de autorizaciones, se incluyen las siguientes:

- Todo el conjunto de herramientas de Solaris Management Console.
- Comandos de administración de auditoría, como `auditconfig` y `auditreduce`.
- Comandos de administración de impresoras, como `lpadmin` y `lpfilter`.
- Comandos relacionados con trabajos por lotes, como `at`, `atq`, `batch` y `crontab`.
- Comandos orientados a dispositivos, como `allocate`, `deallocate`, `list_devices` y `cdrw`.

Para probar las autorizaciones de una secuencia de comandos o un programa, consulte el [Ejemplo 9–24](#). Para escribir un programa que requiere autorizaciones, consulte [“About Authorizations” de \*Developer’s Guide to Oracle Solaris Security\*](#).

## Perfiles de derechos de RBAC

Un *perfil de derechos* es una recopilación de valores de sustitución del sistema que se pueden asignar a un rol o a un usuario. Un perfil de derechos puede incluir autorizaciones, comandos con atributos de seguridad asignados y otros perfiles de derechos. La información del perfil de derechos se divide entre las bases de datos `prof_attr` y `exec_attr`. El nombre y las autorizaciones del perfil de derechos están en la base de datos `prof_attr`. El nombre y los comandos del perfil de derechos con atributos de seguridad asignados están en la base de datos `exec_attr`.

Para obtener más información sobre los perfiles de derechos, consulte las siguientes secciones:

- [“Contenido de los perfiles de derechos” en la página 237](#)
- [“Base de datos `prof\_attr`” en la página 248](#)
- [“Base de datos `exec\_attr`” en la página 249](#)

## Roles de RBAC

Un *rol* es un tipo especial de cuenta de usuario desde la que puede ejecutar aplicaciones con privilegios. Los roles se crean del mismo modo general que las cuentas de usuario. Los roles tiene un directorio principal, una asignación de grupo, una contraseña, etc. Los perfiles de

derechos y las autorizaciones otorgan al rol capacidades administrativas. Los roles no pueden heredar capacidades de otros roles u otros usuarios. Los roles discretos dividen las capacidades de superusuario y, por lo tanto, permiten prácticas administrativas más seguras.

Cuando un usuario asume un rol, los atributos del rol reemplazan todos los atributos de usuario. La información del rol se almacena en las bases de datos `passwd`, `shadow` y `user_attr`. La información del rol se puede agregar a la base de datos `audit_user`. Para obtener información detallada acerca de cómo configurar roles, consulte las siguientes secciones:

- [“Cómo planificar la implementación de RBAC” en la página 205](#)
- [“Cómo crear un rol desde la línea de comandos” en la página 210](#)
- [“Cómo cambiar las propiedades de un rol” en la página 226](#)

Un rol se puede asignar a más de un usuario. Todos los usuarios que pueden asumir el mismo rol tienen el mismo directorio principal, trabajan en el mismo entorno y tienen acceso a los mismos archivos. Los usuarios pueden asumir roles desde la línea de comandos. Para ello, deben ejecutar el comando `su` y proporcionar el nombre del rol y la contraseña. Los usuarios también pueden asumir un rol en la herramienta de Solaris Management Console.

Un rol no puede iniciar sesión directamente. Un usuario inicia sesión y, a continuación, asume un rol. Tras asumir un rol, el usuario no puede asumir otro rol sin salir primero de su rol actual. Tras salir del rol, el usuario puede asumir otro rol.

Para impedir el inicio de sesión anónimo de `root` puede cambiar el usuario `root` a un rol, tal como se muestra en [“Cómo convertir el usuario `root` en un rol” en la página 215](#). Si se audita el comando de shell de perfil, `pfexec`, la pista de auditoría contiene el UID real del usuario que inició sesión, los roles que el usuario asumió y las acciones que el rol realizó. Para auditar operaciones de roles en el sistema o un usuario concreto, consulte [“Cómo auditar roles” en la página 215](#).

No se incluyen roles predefinidos con el software Oracle Solaris. Sin embargo, los perfiles de derechos que se envían con el software están diseñados para asignarlos a roles. Por ejemplo, el perfil de derechos de administrador principal se puede utilizar para crear el rol de administrador principal.

- Para configurar el rol de administrador principal, consulte [“Uso de las herramientas de gestión de Solaris con RBAC \(mapa de tareas\)” de Guía de administración del sistema: administración básica](#).
- Para configurar otros roles, consulte [“Cómo crear y asignar un rol con la interfaz gráfica de usuario” en la página 207](#).
- Para crear roles en la línea de comandos, consulte [“Gestión de RBAC \(mapa de tareas\)” en la página 223](#).

## Shells de perfil y RBAC

Los roles pueden ejecutar aplicaciones con privilegios desde el programa de ejecución de Solaris Management Console o desde un [shell de perfil](#). Un *shell de perfil* es un shell especial que reconoce los atributos de seguridad que se incluyen en un perfil de derechos. Los shells de perfil se inician cuando el usuario ejecuta el comando `su` para asumir un rol. Los shells de perfil son `pfsh`, `pfcs` y `pfksh`. Los shells se corresponden con el shell Bourne (`sh`), el shell C (`cs`) y el shell Korn (`ksh`), respectivamente.

Los usuarios a los que se asignó directamente un perfil de derechos deben invocar un shell de perfil para ejecutar los comandos con atributos de seguridad. Para conocer las consideraciones de seguridad y facilidad de uso, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 192](#).

Todos los comandos que se ejecutan en un shell de perfil pueden auditarse. Para obtener más información, consulte [“Cómo auditar roles” en la página 215](#).

## Ámbito de servicio de nombres y RBAC

El ámbito de servicio de nombres es un concepto importante para comprender RBAC. El ámbito de un rol puede estar limitado a un host individual. El ámbito también puede incluir todos los hosts gestionados por un servicio de nombres, como NIS, NIS+ o LDAP. El ámbito de servicio de nombres de un sistema se especifica en el archivo `/etc/nsswitch.conf`. Las consultas se detienen en la primera coincidencia. Por ejemplo, si un perfil de derechos existe en dos ámbitos de servicio de nombres, sólo se utilizan las entradas del primer ámbito de servicio de nombres. Si `files` es la primera coincidencia, el ámbito del rol se limita al host local.

## Consideraciones de seguridad al asignar directamente atributos de seguridad

Por lo general, un usuario obtiene capacidades administrativas a través de un rol. Las autorizaciones y los comandos con privilegios se agrupan en un perfil de derechos. El perfil de derechos se incluye en un rol, y el rol se asigna a un usuario.

La asignación directa de perfiles de derechos y atributos de seguridad también es posible:

- Se pueden asignar directamente perfiles de derechos, privilegios y autorizaciones a usuarios.
- Se pueden asignar directamente privilegios y autorizaciones a usuarios y roles.

Sin embargo, la asignación directa de privilegios no es una práctica segura. Los usuarios y los roles con un privilegio asignado directamente pueden anular la política de seguridad cada vez que el núcleo necesite este privilegio. Una práctica más segura es asignar el privilegio como atributo de seguridad de un comando en un perfil de derechos. Luego, ese privilegio sólo estará disponible para ese comando y un usuario que tenga ese perfil de derechos.



Dado que las autorizaciones funcionan en el nivel de usuario, la asignación directa de autorizaciones puede resultar menos riesgosa que la asignación directa de privilegios. Sin embargo, las autorizaciones pueden permitir a un usuario realizar tareas de seguridad elevada, por ejemplo, asignar indicadores de auditoría.

Un perfil de derechos que se asigna directamente a un usuario presenta problemas de facilidad de uso más que problemas de seguridad. Los comandos con atributos de seguridad en el perfil de derechos sólo se pueden ejecutar correctamente en un shell de perfil. El usuario no se debe olvidar de abrir un shell de perfil y, a continuación, debe escribir los comandos en ese shell. Un rol al cual se asigna un perfil de derechos obtiene un shell de perfil automáticamente. Por lo tanto, los comandos se ejecutan correctamente en el shell del rol.

## Privilegios (descripción general)

La gestión de derechos de procesos permite restringir procesos en el nivel de comando, usuario, rol o sistema. Oracle Solaris implementa la gestión de derechos de procesos a través de *privilegios*. Los privilegios disminuyen el riesgo de seguridad asociado a un usuario o un proceso que tiene capacidades completas de superusuario en un sistema. Los privilegios y RBAC ofrecen un modelo alternativo eficaz al modelo de superusuario tradicional.

- Para obtener más información sobre RBAC, consulte [“Control de acceso basado en roles \(descripción general\)” en la página 182](#).
- Para obtener información sobre cómo administrar privilegios, consulte [Capítulo 11, “Privilegios \(tareas\)”](#).
- Para obtener información de referencia sobre privilegios, consulte [Capítulo 12, “Privilegios \(referencia\)”](#).

## Privilegios con protección de procesos del núcleo

Un privilegio es un derecho perfectamente definido que un proceso requiere para realizar una operación. El derecho se aplica en el núcleo. Un programa que funciona dentro de los límites del *conjunto básico* de privilegios de Oracle Solaris funciona dentro de los límites de la política de seguridad del sistema. Los programas `setuid` son ejemplos de programas que funcionan fuera de los límites de la política de seguridad del sistema. Mediante el uso de privilegios, los programas eliminan la necesidad de realizar llamadas a `setuid`.

Los privilegios enumeran de forma discreta los tipos de operaciones que son posibles en un sistema. Los programas se pueden ejecutar con los privilegios exactos que permiten que el programa funcione correctamente. Por ejemplo, un programa que define la fecha y escribe la fecha en un archivo administrativo puede necesitar los privilegios `file_dac_write` y `sys_time`. Esta capacidad elimina la necesidad de ejecutar cualquier programa como `root`.

Históricamente, los sistemas no adoptaron el modelo de privilegios. En su lugar, los sistemas utilizaron el modelo de superusuario. En el modelo de superusuario, los procesos se ejecutan como `root` o como usuario. Los procesos de usuario se limitaban a trabajar en los directorios y

los archivos del usuario. Los procesos root podían crear directorios y archivos en cualquier parte del sistema. Un proceso que requería la creación de un directorio fuera del directorio del usuario se ejecutaba con un UID=0, es decir, como root. La política de seguridad dependía del control de acceso discrecional (DAC, Discretionary Access Control) para proteger los archivos del sistema. Los nodos del dispositivo estaban protegidos por DAC. Por ejemplo, sólo los miembros del grupo sys podían abrir los dispositivos que pertenecían al grupo sys.

Sin embargo, los programas `setuid`, los permisos de archivo y las cuentas administrativas son vulnerables al uso indebido. Las acciones que un proceso `setuid` puede realizar son más numerosas que las acciones que requiere para completar su operación. Un programa `setuid` puede verse comprometido por un intruso que luego se ejecuta como usuario root omnipotente. De modo similar, cualquier usuario con acceso a la contraseña root puede poner en peligro todo el sistema.

En cambio, un sistema que aplica la política con privilegios permite una gradación entre las capacidades de usuario y las capacidades de root. Es posible otorgar a un usuario privilegios para realizar actividades que van más allá de las capacidades de los usuarios comunes, y root puede limitarse a menos privilegios que los que root posee actualmente. Con RBAC, un comando que se ejecuta con privilegios se puede aislar en un perfil de derechos y asignar a un usuario o rol. La [Tabla 8-1](#) resume la gradación entre las capacidades de usuario y las capacidades de root que proporciona el modelo RBAC con privilegios.

El modelo de privilegios proporciona mayor seguridad que el modelo de superusuario. Los privilegios que se eliminaron de un proceso no se pueden utilizar. Los privilegios de proceso impiden que un programa o una cuenta administrativa obtengan acceso a todas las capacidades. Los privilegios de proceso pueden proporcionar una protección adicional para los archivos confidenciales, en donde las protecciones de DAC solamente pueden utilizarse para obtener acceso.

Los privilegios pueden restringir programas y procesos a las capacidades que el programa necesita únicamente. Esta capacidad se denomina *principio de privilegio mínimo*. En un sistema que implementa este principio, un intruso que captura un proceso tiene acceso sólo a aquellos privilegios que tiene el proceso. El resto del sistema no corre peligro.

## Descripciones de privilegios

Los privilegios se agrupan de manera lógica de acuerdo con el área del privilegio.

- **Privilegios FILE:** los privilegios que comienzan con la cadena `file` funcionan en los objetos del sistema de archivos. Por ejemplo, el privilegio `file_dac_write` anula el control de acceso discrecional al escribir en los archivos.
- **Privilegios IPC:** los privilegios que comienzan con la cadena `ipc` anulan los controles de acceso a objetos IPC. Por ejemplo, el privilegio `ipc_dac_read` permite a un proceso leer memoria compartida remota que está protegida por DAC.

- Privilegios **NET**: los privilegios que comienzan con la cadena `net` otorgan acceso a funcionalidades de red específicas. Por ejemplo, el privilegio `net_rawaccess` permite a un dispositivo conectarse con la red.
- Privilegios **PROC**: los privilegios que comienzan con la cadena `proc` permiten a los procesos modificar propiedades restringidas del propio proceso. Los privilegios **PROC** incluyen privilegios que tienen un efecto muy limitado. Por ejemplo, el privilegio `proc_clock_highres` permite a un proceso usar temporizadores de alta resolución.
- Privilegios **SYS**: los privilegios que comienzan con la cadena `sys` otorgan a los procesos acceso sin restricciones a distintas propiedades del sistema. Por ejemplo, el privilegio `sys_linkdir` permite a un proceso establecer y anular enlaces físicos a directorios.

Algunos privilegios tienen un efecto limitado en el sistema y otros tienen un efecto amplio. La definición del privilegio `proc_taskid` indica su efecto limitado:

```
proc_taskid
    Allows a process to assign a new task ID to the calling process.
```

La definición del privilegio `file_setid` indica su efecto amplio:

```
net_rawaccess
    Allow a process to have direct access to the network layer.
```

La página del comando `man privileges(5)` proporciona descripciones de cada privilegio. El comando `ppriv -lv` imprime una descripción de cada privilegio con formato estándar.

## Diferencias administrativas en un sistema con privilegios

Un sistema tiene privilegios posee varias diferencias visibles con un sistema que no tiene privilegios. La siguiente tabla muestra algunas de las diferencias.

**TABLA 8-2** Diferencias visibles entre un sistema con privilegios y un sistema sin privilegios

Función	Sin privilegios	Con privilegios
Daemons	Los daemons se ejecutan como <code>root</code> .	Los daemons se ejecutan como el daemon de usuario.  Por ejemplo, los siguientes daemons tienen asignados los privilegios adecuados y se ejecutan como daemon: <code>lockd</code> , <code>nfsd</code> y <code>rpcbind</code> .
Propiedad de archivos de registro	Los archivos de registro son propiedad de <code>root</code> .	Los archivos de registro ahora son propiedad de daemon, que creó el archivo de registro. El usuario <code>root</code> no es propietario del archivo.

TABLA 8-2 Diferencias visibles entre un sistema con privilegios y un sistema sin privilegios (Continuación)

Función	Sin privilegios	Con privilegios
Mensajes de error	Los mensajes de error hacen referencia al superusuario.  Por ejemplo, chroot: not superuser.	Los mensajes de error reflejan el uso de privilegios.  Por ejemplo, el mensaje de error equivalente para el error chroot es chroot: exec failed.
Programas setuid	Los programas usan setuid para completar las tareas que los usuarios comunes no tienen permiso para realizar.	Muchos programas setuid se modificaron para ejecutarse con privilegios.  Por ejemplo, las siguientes utilidades usan privilegios: ufsdump, ufsrestore, rsh, rlogin, rcp, rdist, ping, traceroute y newtask.
Permisos de archivo	Los permisos de dispositivo están controlados por DAC. Por ejemplo, los miembros del grupo sys pueden abrir /dev/ip.	Los permisos de archivo (DAC) no predicen quién puede abrir un dispositivo. Los dispositivos están protegidos con DAC y la política de dispositivos.  Por ejemplo, el archivo /dev/ip tiene 666 permisos, pero únicamente un proceso con los privilegios adecuados puede abrir el dispositivo. Los sockets sin formato siguen protegidos por DAC.
Eventos de auditoría	La auditoría del uso del comando su comprende varias funciones administrativas.	La auditoría del uso de privilegios comprende la mayoría de las funciones administrativas. Las clases de auditoría pm y as incluyen eventos de auditoría que configuran la política de dispositivos y eventos de auditoría que establecen privilegios.
Procesos	Los procesos están protegidos por el propietario del proceso.	Los procesos están protegidos por privilegios. Los privilegios de proceso y los indicadores de proceso están visibles como una nueva entrada en el directorio /proc/<pid>, priv.
Depuración	Ninguna referencia a privilegios en los volcados del núcleo central.	La sección de notas ELF de los volcados del núcleo central incluye información sobre los indicadores y privilegios de proceso en las notas NT_PRPRIV y NT_PRPRIVINFO.  La utilidad ppriv y otras utilidades muestran el número adecuado de conjuntos con tamaño apropiado. Las utilidades asignan correctamente los bits de los conjuntos de bits a los nombres de privilegio.

## Privilegios y recursos del sistema

A partir de la versión Solaris 10 8/07, los controles de recursos `project.max-locked-memory` y `zone.max-locked-memory` se pueden utilizar para limitar el consumo de memoria de los procesos que tienen asignado el privilegio `PRIV_PROC_LOCK_MEMORY`. Este privilegio permite a un proceso bloquear páginas en la memoria física.

Si asigna el privilegio `PRIV_PROC_LOCK_MEMORY` a un perfil de derechos, puede otorgar a los procesos que tienen este privilegio la posibilidad de bloquear toda la memoria. Como protección, defina un control de recursos para evitar que el usuario del privilegio bloquee toda la memoria. Para los procesos con privilegios que se ejecutan en una zona no global, defina el

control de recursos `zone.max-locked-memory`. Para los procesos con privilegios que se ejecutan en un sistema, cree un proyecto y defina el control de recursos `project.max-locked-memory`. Para obtener información sobre estos controles de recursos, consulte el [Capítulo 6, “Controles de recursos \(descripción general\)”](#) de *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris* y el [Capítulo 17, “Configuración de zonas no globales \(descripción general\)”](#) de *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris*.

## Cómo se implementan los privilegios

Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede usar un determinado privilegio. El núcleo calcula automáticamente el *conjunto vigente* de privilegios. Puede modificar el *conjunto heredable* inicial de privilegios. Un programa que está codificado para utilizar privilegios puede reducir el *conjunto permitido* de privilegios del programa. Puede reducir el *conjunto límite* de privilegios.

- **Conjunto vigente de privilegios o E (effective):** es el conjunto de privilegios que actualmente está en vigor. Un proceso puede agregar los privilegios que están en el conjunto permitido al conjunto vigente. Un proceso también puede eliminar privilegios de E.
- **Conjunto permitido de privilegios o P (permitted):** es el conjunto de privilegios que está disponible para su uso. Los privilegios pueden estar disponibles para un programa a través de herencia o mediante asignación. Un perfil de ejecución es una forma de asignar privilegios a un programa. El comando `setuid` asigna todos los privilegios que tiene `root` a un programa. Se pueden eliminar privilegios del conjunto permitido, pero no se pueden agregar privilegios al conjunto. Los privilegios que se quitan de P se eliminan automáticamente de E.

Un programa *para privilegios* elimina los privilegios que un programa nunca utiliza de su conjunto permitido. De esta forma, el programa ni ningún proceso malicioso pueden utilizar privilegios innecesarios. Para obtener más información sobre los programas para privilegios, consulte el [Capítulo 2, “Developing Privileged Applications”](#) de *Developer’s Guide to Oracle Solaris Security*.

- **Conjunto heredable de privilegios o I (inheritable):** es el conjunto de privilegios que un proceso puede heredar a través de una llamada a `exec`. Después de la llamada a `exec`, los conjuntos permitido y vigente son iguales, excepto en el caso especial de un programa `setuid`.

En un programa `setuid`, después de la llamada a `exec`, el conjunto heredable se ve restringido primero por el conjunto límite. Luego, el conjunto de privilegios que se heredaron (I), menos los privilegios que estaban en el conjunto límite (L), se asignan a P y E para ese proceso.

- **Conjunto límite de privilegios o L (limit):** es el límite externo de los privilegios que están disponibles para un proceso y sus procesos secundarios. De manera predeterminada, el conjunto límite incluye todos los privilegios. Los procesos pueden reducir el conjunto límite, pero nunca pueden ampliarlo. L se utiliza para restringir I. Por lo tanto, L restringe P y E cuando se ejecuta exec.

Si se asignó a un usuario un perfil que incluye un programa con privilegios asignados, el usuario normalmente puede ejecutar ese programa. En un sistema sin modificaciones, los privilegios asignados del programa están dentro del conjunto límite del usuario. Los privilegios que se asignaron al programa pasan a formar parte del conjunto permitido del usuario. Para ejecutar el programa con privilegios asignados, el usuario debe ejecutar el programa desde un shell de perfil.

El núcleo reconoce un *conjunto básico de privilegios*. En un sistema sin modificaciones, cada conjunto heredable inicial del usuario es equivalente al conjunto básico en el inicio de sesión. Puede modificar el conjunto heredable inicial del usuario. No puede modificar el conjunto básico.

En un sistema sin modificaciones, los conjuntos de privilegios de un usuario en el inicio de sesión tendrían un aspecto similar al siguiente:

```
E (Effective): basic
I (Inheritable): basic
P (Permitted): basic
L (Limit): all
```

Por lo tanto, en el inicio de sesión, todos los usuarios tienen el conjunto básico en su conjunto heredable, su conjunto permitido y su conjunto vigente. El conjunto límite de un usuario contiene todos los privilegios. Para poner más privilegios en el conjunto vigente del usuario, debe asignar un perfil de derechos al usuario. El perfil de derechos incluiría los comandos en los que agregó privilegios. También puede asignar privilegios directamente al usuario o el rol, aunque dicha asignación de privilegios puede ser riesgosa. Para ver una explicación de los riesgos, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 192](#).

## Cómo obtienen privilegios los procesos

Los procesos pueden heredar privilegios. O bien se pueden asignar privilegios a los procesos. Un proceso hereda privilegios de su proceso principal. En el inicio de sesión, el conjunto heredable inicial de privilegios del usuario determina los privilegios que están disponibles para los procesos del usuario. Todos los procesos secundarios del inicio de sesión inicial del usuario heredan ese conjunto.

También puede asignar directamente privilegios a programas, usuarios y roles. Cuando un programa requiere privilegios, puede asignar los privilegios al archivo ejecutable del programa en un perfil de derechos. A los usuarios o roles que tienen permiso para ejecutar el programa se

les asigna el perfil que incluye el programa. En el inicio de sesión o cuando se indica un shell de perfil, el programa se ejecuta con privilegios al escribir el archivo ejecutable del programa en el shell de perfil. Por ejemplo, un rol que incluye el perfil de gestión del acceso a objetos puede ejecutar el comando `chmod` con el privilegio `file_chown`.

Cuando un rol o un usuario ejecutan un programa al que se asignó directamente un privilegio adicional, el privilegio asignado se agrega al conjunto heredable del rol o el usuario. Los procesos secundarios del programa al que se asignaron privilegios heredan los privilegios del proceso principal. Si el proceso secundario requiere más privilegios que el proceso principal, esos privilegios se deben asignar directamente al proceso secundario.

Los programas que están codificados para utilizar privilegios se denominan programas para privilegios. Un programa *para privilegios* activa el uso de privilegios y desactiva el uso de privilegios durante la ejecución del programa. Para lograr un funcionamiento correcto en un entorno de producción, se deben asignar al programa los privilegios que el programa activa y desactiva.

Para ver ejemplos de código para privilegios, consulte el [Capítulo 2, “Developing Privileged Applications”](#) de *Developer’s Guide to Oracle Solaris Security*. Para asignar privilegios a un programa que los requiera, consulte [“Cómo agregar privilegios a un comando”](#) en la página 260.

## Asignación de privilegios

Como administrador del sistema, usted es responsable de asignar privilegios. Por lo general, puede asignar el privilegio a un comando en un perfil de derechos. El perfil de derechos luego se asigna a un rol o un usuario. Solaris Management Console proporciona la interfaz gráfica de usuario (GUI) para asignar privilegios. Los privilegios también se pueden asignar mediante comandos, como `smuser` y `smrole`. Para obtener más información acerca de cómo utilizar la interfaz gráfica de usuario para asignar privilegios, consulte el [Capítulo 9, “Uso del control de acceso basado en roles \(tarear\)”](#).

Los privilegios también se pueden asignar directamente a un usuario. Si confía en que un subconjunto de usuarios puede utilizar un privilegio de forma responsable a lo largo de sus sesiones, puede asignar el privilegio directamente. Los privilegios que tienen un efecto limitado, como `proc_clock_highres`, son buenos candidatos para la asignación directa. Los privilegios que tienen efectos de largo alcance, como `file_dac_write`, son malos candidatos para la asignación directa.

También es posible denegar privilegios a un usuario o un sistema. Se debe tener cuidado al eliminar privilegios del conjunto heredable inicial o el conjunto límite de un usuario o un sistema.

## **Ampliación de los privilegios de un usuario o rol**

Los usuarios y roles tienen un conjunto heredable de privilegios y un conjunto límite de privilegios. El conjunto límite no se puede ampliar, ya que incluye inicialmente todos los privilegios. El conjunto heredable inicial se puede ampliar para usuarios, roles y sistemas. Un privilegio que no está en el conjunto heredable también se puede asignar a un proceso.

La asignación de privilegios por proceso es la manera más precisa de agregar privilegios. Para ampliar la cantidad de operaciones con privilegios que puede realizar un usuario, debe permitir que el usuario asuma un rol. Se asignarán perfiles al rol que incluyen comandos con privilegios agregados. Cuando el usuario asume el rol, obtiene el shell de perfil del rol. Al escribir en el shell del rol, los comandos de los perfiles del rol se ejecutan con los privilegios agregados.

También puede asignar un perfil al usuario en lugar de un rol que el usuario asumirá. El perfil incluirá comandos con privilegios agregados. Cuando el usuario abre un shell de perfil, como `pfksh`, puede ejecutar los comandos del perfil con privilegios. En un shell común, los comandos no se ejecutan con privilegios. El proceso con privilegios sólo se puede ejecutar en un shell con privilegios.

Ampliar el conjunto heredable inicial de privilegios para usuarios, roles o sistemas es una manera más riesgosa de asignar privilegios. Todos los privilegios del conjunto heredable están en el conjunto permitido y vigente. Todos los comandos que el usuario o el rol escriben en un shell puede utilizar los privilegios asignados directamente. Los privilegios asignados directamente permiten un usuario o rol realizar fácilmente operaciones que pueden estar fuera de los límites de sus responsabilidades administrativas.

Al aumentar el conjunto heredable inicial de privilegios en un sistema, todos los usuarios que inician sesión en el sistema tienen un conjunto más grande de privilegios básicos. Esa asignación directa permite a todos los usuarios del sistema realizar fácilmente operaciones que probablemente están fuera de los límites de los usuarios comunes.

---

**Nota** – El conjunto límite no se puede ampliar, ya que incluye inicialmente todos los privilegios.

---

## **Restricción de los privilegios de un usuario o rol**

Al eliminar privilegios, puede impedir que los usuarios y los roles realicen determinadas tareas. Puede eliminar privilegios del conjunto heredable inicial y del conjunto límite. Debe probar con cuidado la eliminación de privilegios antes de distribuir un conjunto heredable inicial o un conjunto límite que es menor que el conjunto predeterminado. Al eliminar privilegios del conjunto heredable inicial, puede impedir que los usuarios inicien sesión. Cuando se eliminan privilegios del conjunto límite, es posible que se produzca un error en un programa `setuid` antiguo porque el programa necesita un privilegio que se eliminó.



## Asignación de privilegios a una secuencia de comandos

Las secuencias de comandos son ejecutables, como los comandos. Por lo tanto, en un perfil de derechos, puede agregar privilegios a una secuencia de comandos del mismo modo que puede agregar privilegios a un comando. La secuencia de comandos se ejecuta con los privilegios agregados cuando un usuario o rol al que se asignó el perfil ejecuta la secuencia de comandos en un shell de perfil. Si la secuencia de comandos contiene comandos que requieren privilegios, los comandos con privilegios agregados también deben estar en el perfil.

Los programas para privilegios pueden restringir los privilegios por proceso. Su función con un programa para privilegios consiste en asignar al archivo ejecutable sólo los privilegios que necesita el programa. Luego, prueba el programa para ver si el programa realiza sus tareas correctamente. También comprueba que el programa no abuse de su uso de privilegios.

## Privilegios y dispositivos

El modelo de privilegios utiliza privilegios para proteger las interfaces del sistema que están protegidas solamente mediante permisos de archivo en el modelo de superusuario. En un sistema con privilegios, los permisos de archivo son demasiado débiles para proteger las interfaces. Un privilegio como `proc_owner` puede anular los permisos de archivo y, a continuación, proporcionar acceso completo a todo el sistema.

Por lo tanto, la propiedad del directorio de dispositivos no es suficiente para abrir un dispositivo. Por ejemplo, a los miembros del grupo `sys` ya no se les permite abrir automáticamente el dispositivo `/dev/ip`. Los permisos de archivo en `/dev/ip` son `0666`, pero se requiere el privilegio `net_rawaccess` para abrir el dispositivo.

La política de dispositivos se controla mediante privilegios. El comando `getdevpolicy` muestra la política para cada dispositivo. El comando de configuración de dispositivos, `devfsadm`, instala la política de dispositivos. El comando `devfsadm` vincula los conjuntos de privilegios con `open` para la lectura o escritura de dispositivos. Para obtener más información, consulte las páginas del comando `man getdevpolicy(1M)` y `devfsadm(1M)`.

La política de dispositivos ofrece más flexibilidad en el momento de otorgar permiso para abrir dispositivos. Puede requerir privilegios distintos o más privilegios que la política de dispositivos predeterminada. Los requisitos de privilegios se pueden modificar para la política de dispositivos y para el propio controlador. Puede modificar los privilegios al instalar, agregar o actualizar un controlador de dispositivos.

Los comandos `add_drv` y `update_drv` pueden modificar entradas de la política de dispositivos y privilegios específicos del controlador. Para cambiar la política de dispositivos, debe ejecutar el proceso con el conjunto completo de privilegios. Para obtener más información, consulte las páginas de comando `man add_drv(1M)` y `update_drv(1M)`.

## Privilegios y depuración

Oracle Solaris proporciona herramientas para depurar errores en privilegios. El comando `ppriv` y el comando `truss` proporcionan los resultados de la depuración. Para ver ejemplos, consulte la página del comando `man ppriv(1)`. Para conocer el procedimiento, consulte [“Cómo determinar los privilegios que necesita un programa” en la página 258](#).

# Uso del control de acceso basado en roles (tareas)

En este capítulo, se describen las tareas para distribuir las capacidades de superusuario mediante roles discretos. Los mecanismos que los roles pueden utilizar incluyen perfiles de derechos, autorizaciones y privilegios. A continuación, se muestra una lista de los mapas de tareas que se incluyen en este capítulo.

- “Uso de RBAC (mapa de tareas)” en la página 203
- “Configuración de RBAC (mapa de tareas)” en la página 204
- “Uso de roles (mapa de tareas)” en la página 219
- “Gestión de RBAC (mapa de tareas)” en la página 223

Para obtener una descripción general de RBAC, consulte “Control de acceso basado en roles (descripción general)” en la página 182. Para obtener información de referencia, consulte el Capítulo 10, “Control de acceso basado en roles (referencia)”. Para usar privilegios con RBAC o sin RBAC, consulte el Capítulo 11, “Privilegios (tareas)”.

## Uso de RBAC (mapa de tareas)

Para utilizar RBAC, es necesario planificar, configurar RBAC y conocer cómo asumir un rol. Una vez que se haya familiarizado con los roles, puede personalizar aún más RBAC para utilizar nuevas operaciones. El siguiente mapa de tareas hace referencia a estas tareas principales.

Tarea	Descripción	Para obtener instrucciones
Planificar y configurar RBAC	Configure RBAC en su sitio.	“Configuración de RBAC (mapa de tareas)” en la página 204
Usar roles	Asuma roles desde la línea de comandos y en la interfaz gráfica de usuario de Solaris Management Console.	“Uso de roles (mapa de tareas)” en la página 219

Tarea	Descripción	Para obtener instrucciones
Personalizar RBAC	Personalice RBAC para su sitio.	<a href="#">“Gestión de RBAC (mapa de tareas)” en la página 223</a>

## Configuración de RBAC (mapa de tareas)

Para utilizar RBAC de manera eficaz, se requiere planificación. Utilice el siguiente mapa de tareas para planificar e implementar inicialmente RBAC en su sitio.

Tarea	Descripción	Para obtener instrucciones
1. Planificar la implementación de RBAC	Implica examinar las necesidades de seguridad de su sitio y decidir cómo utilizará RBAC en su sitio.	<a href="#">“Cómo planificar la implementación de RBAC” en la página 205</a>
2. Aprender a utilizar Solaris Management Console	Implica familiarizarse con Solaris Management Console.	Capítulo 2, “Trabajo con Solaris Management Console (tareas)” de <i>Guía de administración del sistema: administración básica</i>
3. Configurar el primer usuario y rol	Utiliza las herramientas de configuración de RBAC en Solaris Management Console para crear un usuario y un rol, y para asignar el rol al usuario.	<a href="#">“Uso de las herramientas de gestión de Solaris con RBAC (mapa de tareas)” de Guía de administración del sistema: administración básica</a>
4. (Opcional) Crear otros usuarios que puedan asumir roles	Garantiza que existan usuarios que pueden asumir un rol administrativo.	<a href="#">“Uso de las herramientas de gestión de Solaris con RBAC (mapa de tareas)” de Guía de administración del sistema: administración básica</a>
5. (Recomendada) Crear otros roles y asignarlos a usuarios	Utiliza las herramientas de RBAC para crear roles para determinadas áreas administrativas y para asignar los roles a usuarios.	<a href="#">“Cómo crear y asignar un rol con la interfaz gráfica de usuario” en la página 207</a>
		Ejemplo 9–5
		<a href="#">“Cómo crear un rol desde la línea de comandos” en la página 210</a>
	Utiliza la línea de comandos para crear roles y para asignar los roles a usuarios.	<a href="#">“Cómo asignar un rol a un usuario local” en la página 213</a>
6. (Recomendada) Auditar acciones de roles	Permite preseleccionar una clase de auditoría que incluye el evento de auditoría que registra las acciones de roles.	<a href="#">“Cómo auditar roles” en la página 215</a>
7. (Opcional) Convertir el usuario root en un rol	Impide el inicio de sesión anónimo de root, que representa una vulnerabilidad de seguridad.	<a href="#">“Cómo convertir el usuario root en un rol” en la página 215</a>

# Configuración de RBAC

RBAC se puede configurar con las siguientes utilidades:

- **Interfaz gráfica de usuario de Solaris Management Console:** el método preferido para realizar tareas relacionadas con RBAC es por medio de la interfaz gráfica de usuario. Las herramientas de la consola para gestionar los elementos de RBAC se incluyen en el conjunto de la herramienta Users.
- **Comandos de Solaris Management Console:** con las interfaces de línea de comandos de Solaris Management Console, como `smrole`, puede trabajar en cualquier servicio de nombres. Los comandos de Solaris Management Console requieren autenticación para conectarse con el servidor. Como resultado, estos comandos no resultan prácticos para usar en secuencias de comandos.
- **Comandos locales:** con el conjunto de interfaces de línea de comandos `user*` y `role*`, como `useradd`, puede trabajar en archivos locales solamente. Los comandos que funcionan en archivos locales deben ser ejecutados por un superusuario o por un rol con los privilegios adecuados.

## ▼ Cómo planificar la implementación de RBAC

RBAC puede ser una parte integral de la manera en que una organización gestiona sus recursos de información. La planificación requiere un conocimiento exhaustivo de las capacidades de RBAC, así como de los requisitos de seguridad de la organización.

### 1 Aprenda los conceptos básicos de RBAC.

Lea [“Control de acceso basado en roles \(descripción general\)”](#) en la página 182. Usar RBAC para administrar un sistema es muy diferente a utilizar las prácticas administrativas UNIX convencionales. Debe estar familiarizado con los conceptos de RBAC antes de iniciar la implementación. Para obtener más detalles, consulte el [Capítulo 10, “Control de acceso basado en roles \(referencia\)”](#).

### 2 Examine la política de seguridad.

La política de seguridad de la organización debe detallar las amenazas potenciales para el sistema, medir el riesgo de cada amenaza y tener una estrategia para contrarrestar estas amenazas. Aislar las tareas relacionadas con la seguridad a través de RBAC puede ser parte de la estrategia. Aunque puede instalar los roles recomendados y sus configuraciones como están, es posible que deba personalizar la configuración de RBAC para cumplir con la política de seguridad.

### 3 Decida qué nivel de RBAC necesita la organización.

En función de las necesidades de seguridad, puede utilizar distintos grados de RBAC, como se muestra a continuación:

- **Sin RBAC:** puede realizar todas las tareas como usuario root. En esta configuración, debe iniciar sesión con su usuario. Luego, debe escribir root como usuario cuando seleccione una herramienta de Solaris Management Console.
- **Rol único solamente:** este método agrega un rol. Se asigna al rol único el perfil de derechos de administrador principal. Este método es similar al modelo de superusuario, ya que el rol tiene capacidades de superusuario. Sin embargo, este método permite realizar un seguimiento del usuario que asumió el rol.
- **Roles recomendados:** este método crea tres roles que se basan en los siguientes perfiles de derechos: administrador principal, administrador del sistema y operador. Los roles son adecuados para las organizaciones con administradores con diferentes niveles de responsabilidad.
- **Roles personalizados:** puede crear sus propios roles para cumplir con los requisitos de seguridad de la organización. Los nuevos roles se pueden basar en perfiles de derechos existentes o personalizados. Para personalizar los perfiles de derechos que aplican la separación de tareas, consulte [“Creación de roles y usuarios en Trusted Extensions” de Guía de configuración de Oracle Solaris Trusted Extensions](#).
- **Usuario root como rol:** este método impide que cualquier usuario inicie sesión como root. En su lugar, los usuarios deben iniciar sesión como usuarios comunes antes de asumir el rol root. Para obtener detalles, consulte [“Cómo convertir el usuario root en un rol” en la página 215](#).

#### 4 Decida qué roles recomendados son adecuados para la organización.

Revise las capacidades de los roles recomendados y los perfiles de derechos predeterminados. Los perfiles de derechos predeterminados permiten a los administradores configurar un rol recomendado por medio de un único perfil.

Hay tres perfiles de derechos predeterminados disponibles para configurar los roles recomendados:

- **Perfil de derechos de administrador principal:** para configurar un rol que pueda llevar a cabo todas las tareas administrativas, pueda otorgar derechos a otros usuarios y pueda editar los derechos asociados a roles administrativos. Un usuario con este rol puede asignar este rol a otros usuarios y puede otorgar derechos a otros usuarios.
- **Perfil de derechos de administrador del sistema:** para configurar un rol que pueda realizar la mayoría de las tareas administrativas que no están relacionados con la seguridad. Por ejemplo, el administrador del sistema puede agregar nuevas cuentas de usuario, pero no puede definir contraseñas ni otorgar derechos a otros usuarios.
- **Perfil de derechos de operador:** para configurar un rol que pueda realizar tareas administrativas sencillas, como copias de seguridad de medios y mantenimiento de impresoras.

Para examinar de forma más detallada los perfiles de derechos, lea uno de los siguientes temas:

- En el directorio `/etc/security`, lea el contenido de la base de datos `prof_attr` y la base de datos `exec_attr`.
- En Solaris Management Console, utilice la herramienta Rights para mostrar el contenido de un perfil de derechos.
- En esta guía, consulte [“Contenido de los perfiles de derechos” en la página 237](#) para obtener resúmenes de algunos perfiles de derechos típicos.

## 5 Decida si otros roles o perfiles de derechos son adecuados para la organización.

Busque otras aplicaciones o familias de aplicaciones en su sitio que puedan beneficiarse del acceso restringido. Las aplicaciones que afectan la seguridad, que pueden causar problemas de denegación del servicio, o que requieren una formación de administrador especial son opciones apropiadas para RBAC. Puede personalizar roles y perfiles de derechos para gestionar los requisitos de seguridad de la organización.

### a. Determine qué comandos son necesarios para la nueva tarea.

### b. Decida qué perfil de derechos es adecuado para esta tarea.

Compruebe si un perfil de derechos existente puede gestionar esta tarea o si es necesario crear un perfil de derechos independiente.

### c. Determine qué rol es adecuado para este perfil de derechos.

Decida si el perfil de derechos para esta tarea se debe asignar a un rol existente o si es necesario crear un nuevo rol. Si utiliza un rol existente, compruebe que los demás perfiles de derechos sean adecuados para los usuarios que están asignados a este rol.

## 6 Decida qué usuarios se deben asignar a los roles disponibles.

Según el principio de privilegio mínimo, debe asignar los usuarios a roles que sean adecuados para su nivel de confianza. Al impedir el acceso de usuarios a tareas que los usuarios no necesitan realizar, se reducen los problemas potenciales.

## ▼ Cómo crear y asignar un rol con la interfaz gráfica de usuario

Para crear un nuevo rol, puede ser superusuario o puede utilizar el rol de administrador principal. En este procedimiento, el creador del nuevo rol asumió el rol de administrador principal.

**Antes de empezar**

- Ya creó usuarios que pueden asumir un rol en su sitio. Si los usuarios aún no se crearon, créelos siguiendo las instrucciones detalladas en [“Uso de las herramientas de gestión de Solaris con RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: administración básica*.
- Se le asignó el rol de administrador principal siguiendo los procedimientos descritos en [“Uso de las herramientas de gestión de Solaris con RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**1 Inicie Solaris Management Console.**

```
# /usr/sbin/smc &
```

Para obtener instrucciones relacionadas con el inicio de sesión, consulte [“Cómo asumir un rol en Solaris Management Console”](#) en la [página 222](#).

**2 Haga clic en el icono Administrative Roles.****3 Seleccione Add Administrative Role en el menú Action.****4 Para crear un nuevo rol, complete los campos de la serie de cuadros de diálogo.**

Para conocer los posibles roles, consulte del [Ejemplo 9–1](#) al [Ejemplo 9–4](#).

---

**Consejo** – Todas las herramientas de Solaris Management Console muestran información en la sección inferior de la página o en la parte izquierda de un panel de asistente. Seleccione Help en cualquier momento para buscar información adicional sobre cómo realizar tareas en esta interfaz.

---

**5 Asigne el rol a un usuario.**

---

**Consejo** – Después de completar las propiedades del rol, el último cuadro de diálogo le solicita un usuario para el rol.

---

**6 En una ventana de terminal, reinicie el daemon de antememoria de servicio de nombres.**

```
# svcadm restart system/name-service-cache
```

Para obtener más información, consulte las páginas del comando man [svcadm\(1M\)](#) y [nscd\(1M\)](#).

**Ejemplo 9–1 Creación de un rol para el perfil de derechos de administrador del sistema**

En este ejemplo, el nuevo rol puede realizar tareas de administración del sistema que no estén conectadas con la seguridad. El rol se crea siguiendo el procedimiento anterior con los siguientes parámetros:

- Nombre del rol: sysadmin
- Nombre completo del rol: System Administrator



- Descripción del rol: Performs non-security admin tasks
- Perfil de derechos: System Administrator

Este perfil de derechos está en la parte superior de la lista de perfiles incluidos en el rol.

### **Ejemplo 9-2** Creación de un rol para el perfil de derechos de operador

El perfil de derechos de operador puede gestionar impresoras y realizar copias de seguridad del sistema en medios sin conexión. Es posible que desee asignar el rol a un usuario en cada turno. Para ello, debe seleccionar la opción de lista de correo del rol en el cuadro de diálogo Step 1: Enter a Role Name. El rol se crea siguiendo el procedimiento anterior con los siguientes parámetros:

- Nombre del rol: operadm
- Nombre completo del rol: Operator
- Descripción del rol: Backup operator
- Perfil de derechos: Operator

Este perfil de derechos debe estar en la parte superior de la lista de perfiles incluidos en el rol.

### **Ejemplo 9-3** Creación de un rol para un perfil de derechos relacionados con la seguridad

De manera predeterminada, el único perfil de derechos que contiene comandos y derechos relacionados con la seguridad es el perfil de administrador principal. Si desea crear un rol que no sea tan poderoso como el administrador principal, pero que pueda gestionar algunas tareas relacionadas con la seguridad, debe crear el rol.

En el siguiente ejemplo, el rol protege dispositivos. El rol se crea siguiendo el procedimiento anterior con los siguientes parámetros:

- Nombre del rol: devicesec
- Nombre completo del rol: Device Security
- Descripción del rol: Configures Devices
- Perfil de derechos: Device Security

En el siguiente ejemplo, el rol protege los sistemas y hosts de la red. El rol se crea siguiendo el procedimiento anterior con los siguientes parámetros:

- Nombre del rol: netsec
- Nombre completo del rol: Network Security
- Descripción del rol: Handles IPsec, IKE, and SSH
- Perfil de derechos: Network Security

**Ejemplo 9–4 Creación de un rol para un perfil de derechos con ámbito limitado**

Algunos perfiles de derechos son de alcance limitado. En este ejemplo, la única tarea del rol es gestionar DHCP. El rol se crea siguiendo el procedimiento anterior con los siguientes parámetros:

- Nombre del rol: `dhcpgmt`
- Nombre completo del rol: `DHCP Management`
- Descripción del rol: `Manages Dynamic Host Config Protocol`
- Perfil de derechos: `DHCP Management`

**Ejemplo 9–5 Modificación de la asignación de rol de un usuario**

En este ejemplo, se agrega un rol a un usuario existente. Para modificar la asignación de rol del usuario, haga clic en el icono `User Accounts` en la herramienta `Users` de `Solaris Management Console`, haga doble clic en el usuario y siga la ayuda en pantalla para agregar un rol a las capacidades del usuario.

**Errores más frecuentes**

Compruebe lo siguiente si el rol no tiene las capacidades que debería tener:

- ¿Los perfiles de derechos del rol están enumerados en la interfaz gráfica de usuario del más al menos poderoso?

Por ejemplo, si el perfil de derechos `All` está en la parte superior de la lista, no se ejecuta ningún comando con atributos de seguridad. Un perfil que contiene comandos con atributos de seguridad debe preceder al perfil de derechos `All` en la lista.

- ¿Los comandos de los perfiles de derechos del rol tienen los atributos de seguridad adecuados?

Por ejemplo, cuando la política es `suser`, algunos comandos requieren `uid=0` en lugar de `euid=0`.

- ¿El perfil de derechos está definido en el ámbito de servicio de nombres adecuado? ¿El rol funciona en el ámbito de servicio de nombres donde está definido el perfil de derechos?
- ¿La antememoria de servicio de nombres, `svc:/system/name-service-cache`, se reinició?

El daemon `nscd` puede tener un intervalo de tiempo de vida prolongado. Al reiniciar el daemon, actualiza el nombre de servicios con los datos actuales.

## ▼ Cómo crear un rol desde la línea de comandos

La interfaz gráfica de usuario de `Solaris Management Console` es el método preferido para gestionar RBAC. Para usar la interfaz gráfica de usuario, consulte [“Cómo crear y asignar un rol con la interfaz gráfica de usuario” en la página 207](#). También puede utilizar las interfaces de línea de comandos, como se describe en este procedimiento.

---

**Nota** – No intente administrar RBAC con la línea de comandos y la interfaz gráfica de usuario al mismo tiempo. En ese caso, se podrían realizar cambios en la configuración que entren en conflicto y el comportamiento sería impredecible. Puede utilizar ambas herramientas para administrar RBAC, pero no puede hacerlo simultáneamente.

---

**Antes de empezar** Para crear un rol, debe asumir un rol que incluya el perfil de derechos de administrador principal, o bien cambiar al usuario root.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Seleccione uno de los siguientes comandos para crear un rol en la línea de comandos.**

- **Para los roles en el ámbito de servicio de nombres local, utilice el comando `roleadd`.**

---

**Nota** – El comando `roleadd` es más limitado que las interfaces de línea de comandos o la interfaz gráfica de usuario de Solaris Management Console. Después de ejecutar el comando `roleadd`, debe ejecutar el comando `usermod` para asignar el rol a un usuario. Y, a continuación, el usuario debe definir la contraseña para el rol, como se muestra en [“Cómo asignar un rol a un usuario local”](#) en la [página 213](#).

---

```
# roleadd -c comment \
-g group -m homedir -u UID -s shell \
-P profile rolename
```

-c <i>comentario</i>	Comentario que describe a <i>nombre_rol</i> .
-g <i>grupo</i>	Asignación de grupo para <i>nombre_rol</i> .
-m <i>dir_ppal</i>	Ruta del directorio principal para <i>nombre_rol</i> .
-u <i>UID</i>	UID para <i>nombre_rol</i> .
-s <i>shell</i>	Shell de inicio de sesión para <i>nombre_rol</i> . Este shell debe ser un shell de perfil.
-P <i>perfil</i>	Uno o varios perfiles de derechos para <i>nombre_rol</i> .
<i>nombre_rol</i>	Nombre del nuevo rol local.

■ **Utilice el comando `smrole add`.**

Este comando crea un rol en un servicio de nombres distribuido, como NIS, NIS+ o LDAP. Este comando se ejecuta como cliente del servidor de Solaris Management Console.

```
$ /usr/sadm/bin/smrole -D domain-name \  
-r admin-role -l <Type admin-role password> \  
add -- -n rolename -a rolename -d directory\  
-F full-description -p profile
```

-D <i>nombre_dominio</i>	Nombre del dominio que desea gestionar.
-r <i>rol_admin</i>	Nombre del rol administrativo que puede modificar el rol. El rol administrativo debe tener la autorización <code>solaris.role.assign</code> . Si desea modificar un rol que asumió, el rol debe tener la autorización <code>solaris.role.delegate</code> .
-l	Petición de datos para la contraseña de <i>rol_admin</i> .
--	Separador obligatorio entre las opciones de autenticación y las opciones de subcomando.
-n <i>nombre_rol</i>	Nombre del nuevo rol.
-c <i>comentario</i>	Comentario que describe las capacidades del rol.
-a <i>nombre_usuario</i>	Nombre del usuario que puede asumir <i>nombre_rol</i> .
-d <i>directorío</i>	Directorio principal para <i>nombre_rol</i> .
-F <i>descripción_completa</i>	Descripción completa para <i>nombre_rol</i> . Esta descripción se muestra en la interfaz gráfica de usuario de Solaris Management Console.
-p <i>perfil</i>	Perfil de derechos que se incluye en las capacidades de <i>nombre_rol</i> . Esta opción proporciona comandos con capacidades administrativas al rol. Puede especificar varias opciones -p <i>perfil</i> .

**3** Para aplicar los cambios, consulte [“Cómo asignar un rol a un usuario local” en la página 213](#).

**Ejemplo 9–6** Creación de un rol de operador personalizado con el comando `smrole`

El comando `smrole` especifica un nuevo rol y sus atributos en un nombre de servicios. En el siguiente ejemplo, el administrador principal crea una nueva versión del rol de copia de seguridad de medios. El rol incluye el perfil de derechos de copia de seguridad de medios estándar, así como el perfil de derechos de gestión de FTP. Tenga en cuenta que el comando solicita una contraseña para el nuevo rol.

```
% su - primaryadm  
Password: <Type primaryadm password>
```

```
$ /usr/sadm/bin/smrole add -H myHost -- -c "FTP and Backup Operator" \
-n operadm2 -a janedoe -d /export/home/operadm \
-F "Backup/FTP Operator" -p "Media Backup" -p "FTP Management"
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::      <Type primaryadm password>
```

```
Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.
```

```
Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::      <Type operadm2 password>
```

```
$ svcadm restart system/name-service-cache
```

El comando `smrole` con el subcomando `list` se utiliza para mostrar el nuevo rol:

```
$ /usr/sadm/bin/smrole list --
Authenticating as user: primaryadm

Type /? for help, pressing <enter> accepts the default denoted by [ ]
Please enter a string value for: password ::      <Type primaryadm password>

Loading Tool: com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost
Login to myHost as user primaryadm was successful.
Download of com.sun.admin.usermgr.cli.role.UserMgrRoleCli from myHost was successful.
```

root	0	Superuser
primaryadm	100	Most powerful role
sysadmin	101	Performs non-security admin tasks
operadm	102	Backup Operator
operadm2	103	Backup/FTP Operator

Tenga en cuenta que los perfiles de derechos que incluyen copia de seguridad de medios o restauración de medios proporcionan un rol con acceso a todo el sistema de archivos raíz. Por lo tanto, el administrador debe asignar esos perfiles de derechos a usuarios de confianza. El administrador también puede optar por no asignar estos perfiles de derechos. En este caso, sólo el superusuario puede realizar operaciones de copia de seguridad y restauración.

## ▼ Cómo asignar un rol a un usuario local

Este procedimiento asigna un rol local a un usuario local, reinicia el daemon de antememoria de servicio de nombres y luego muestra cómo un usuario puede asumir el rol.

Para asignar un rol a un usuario en un servicio de nombres distribuido, consulte [“Cómo crear un rol desde la línea de comandos” en la página 210](#) y [“Cómo cambiar las propiedades de un rol” en la página 226](#).

**Antes de empezar** Ha agregado un rol local, como se describe en [“Cómo crear un rol desde la línea de comandos” en la página 210](#). Debe asumir un rol que incluya el perfil de derechos de administrador principal, o bien cambiar al usuario root.

### 1 Asigne el rol a un usuario local.

Si agregó un rol local con el comando `roleadd`, este paso es necesario. Este paso es opcional cuando utiliza el comando `smrole` y Solaris Management Console para crear un rol.

```
# usermod -u UID -R rolename login-name
-u UID                                UID del usuario.
-R nombre_rol                          Rol que se asignará al usuario.
nombre_inicio_sesión                  Nombre de inicio de sesión del usuario.
```

### 2 Para aplicar los cambios, reinicie el daemon de antememoria de servicio de nombres.

```
# svcadm restart system/name-service-cache
```

Si agregó un rol con una interfaz de Solaris Management Console, vaya a [“Uso de roles \(mapa de tareas\)” en la página 219](#). De lo contrario, continúe con el paso siguiente.

### 3 (Opcional) Para desbloquear la cuenta de rol, el usuario debe crear una contraseña.

Si agregó un rol local con el comando `roleadd`, este paso es necesario.

```
% su - rolename
Password:      <Type rolename password>
Confirm Password:  <Retype rolename password>
$
```

## Ejemplo 9-7 Creación y asignación de un rol local desde la línea de comandos

En este ejemplo, se crea un rol para administrar la estructura criptográfica de Oracle Solaris. El perfil de derechos de gestión de criptografía contiene el comando `cryptoadm` para administrar los servicios criptográficos de hardware y software en un sistema local.

```
# roleadd -c "Cryptographic Services manager" \
-g 14 -m /export/home/cryptoadm -u 104 -s pfksh \
-P "Crypto Management" cryptomgt
# usermod -u 1111 -R cryptomgt
# svcadm restart system/name-service-cache
% su - cryptomgt
Password:      <Type cryptomgt password>
Confirm Password:  <Retype cryptomgt password>
```

```
$ /usr/ucb/whoami
cryptomgt
$
```

Para obtener información sobre la estructura criptográfica de Oracle Solaris, consulte el [Capítulo 13, “Estructura criptográfica de Oracle Solaris \(descripción general\)”](#). Para administrar la estructura, consulte [“Administración de la estructura criptográfica \(mapa de tareas\)”](#) en la [página 299](#).

## ▼ Cómo auditar roles

Las acciones que realiza un rol se pueden auditar. En el registro de auditoría, se incluye el nombre de inicio de sesión del usuario que asumió el rol, el nombre del rol y la acción que realizó el rol. El evento de auditoría 6180:AUE\_prof\_cmd:profile command:ua,as recopila la información. Al preseleccionar la clase as o la clase ua, puede auditar acciones de roles.

### 1 Planifique la auditoría y edite los archivos de configuración de auditoría.

Para obtener más información, consulte [“Auditoría de Oracle Solaris \(mapa de tareas\)”](#) en la [página 613](#).

### 2 Incluya la clase ua o la clase as en la línea flags del archivo audit\_control.

```
## audit_control file
flags:lo,as
naflags:lo
plugin:name=audit_binfile.so; p_dir=/var/audit
```

La clase ua y la clase as incluyen otros eventos de auditoría. Para ver los eventos de auditoría que se incluyen en una clase, lea el archivo audit\_event. También puede utilizar el comando bsmrecord, como se muestra en el [Ejemplo 30–27](#).

### 3 Finalice la configuración del servicio de auditoría y, a continuación, habilite la auditoría.

Para obtener más información, consulte [“Configuración y habilitación del servicio de auditoría \(tareas\)”](#) en la [página 625](#).

## ▼ Cómo convertir el usuario root en un rol

Este procedimiento muestra cómo cambiar root de un usuario de inicio de sesión a un rol. Al completar este procedimiento, ya no podrá iniciar sesión directamente en el sistema como root, excepto en el modo de usuario único. Debe tener asignado el rol root y usar su para convertirse en root.

Al cambiar el usuario root a un rol, impide que el inicio de sesión anónimo de root. Debido a que un usuario debe iniciar sesión y *luego* asumir el rol root, se proporciona el ID de inicio de sesión del usuario para el servicio de auditoría y se encuentra en el archivo su`log`.

En este procedimiento, crea un usuario local y asigna el rol root al usuario. Para impedir que los usuarios asuman el rol, consulte el [Ejemplo 9-8](#).

**Antes de empezar** No puede realizar este procedimiento cuando inició sesión directamente como root. Debe iniciar sesión con su usuario y, a continuación, usar su para convertirse en root.

**1 Como usuario común, inicie sesión en el sistema de destino.**

**2 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte “[Uso de las herramientas de gestión de Solaris con RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: administración básica*.

**3 Cree un usuario local que pueda asumir el rol root.**

Por motivos de seguridad, se debe asignar el rol root a un usuario local como mínimo.

```
$ useradd -c comment -u uid -d homedir username
-c comentario          Comentario que describe al usuario.
-d dir_ppal            Directorio principal del usuario. Este directorio debe estar en el sistema
                        local.
-u uid                 Número de identificación del usuario.
nombre_usuario        Nombre del nuevo usuario local.

# useradd -c "JDoe's local account" -u 123 -d /export/home1 jdoe-local
```

**4 Proporcione una contraseña para el usuario.**

```
# passwd -r files jdoe-local
New Password:          <Type password>
Re-enter new Password: <Retype password>
passwd: password successfully changed for jdoe-local
#
```

**5 Asegúrese de que no haya iniciado sesión como root.**

```
# who
jdoe    console      May 24 13:51      (:0)
jdoe    pts/5           May 24 13:51      (:0.0)
jdoe    pts/4           May 24 13:51      (:0.0)
jdoe    pts/10          May 24 13:51      (:0.0)
```



**6 Cambie el usuario root a un rol.**

```
# usermod -K type=role root
```

**7 Verifique que root sea un rol.**

La entrada root del archivo `user_attr` debe ser similar a la siguiente:

```
# grep root /etc/user_attr
root:::type=role;auths=solaris.*,solaris.grant;profiles=...
```

**8 Asigne el rol root a su cuenta local.**

```
# usermod -R root jdoe-local
```



**Precaución** – Si no asigna el rol root a un usuario, nadie podrá convertirse en superusuario, excepto en el modo de usuario único. Debe escribir una contraseña de usuario root para acceder al modo de usuario único.

**9 Configure el servicio de nombres que regresará en caso de error.****a. Abra una ventana de terminal nueva y asuma el rol root.**

```
% whoami
jdoe
% su - jdoe-local
Enter password:      <Type jdoe-local password>
% roles
root
% su - root
Enter password:      <Type root password>
#
```

**b. Edite el archivo `nsswitch.conf`.**

Por ejemplo, las siguientes entradas del archivo `nsswitch.conf` permitirán que regrese el servicio de nombres.

```
passwd: files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
group:  files nis [TRYAGAIN=0 UNAVAIL=return NOTFOUND=return]
```

**10 (Opcional) Asigne el rol root a las cuentas de usuario seleccionadas en el servicio de nombres.**

Para conocer el procedimiento, consulte [“Cómo cambiar las propiedades RBAC de un usuario” en la página 231](#).

**Ejemplo 9–8 Evitar que el rol root se utilice para configurar un sistema**

En este ejemplo, la política de seguridad del sitio requiere que varios roles discretos configuren el sistema. Estos roles discretos se han creado y probado. Para evitar que la cuenta root se utilice

para configurar el sistema, el administrador de la seguridad cambia root a un rol, pero no asigna el rol. El rol root conserva una contraseña para acceder al sistema en el modo de usuario único.

En primer lugar, el administrador verifica que root no sea un rol asignado.

```
% whoami
jdoe-local
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local:::type=normal;roles=secadmin
kdoe-local:::type=normal;roles=sysadmin
```

Aún en la cuenta root, el administrador cambia root a un rol.

```
# usermod -K type=role root
```

A continuación, el administrador verifica el cambio en la entrada root del archivo user\_attr.

```
# grep root /etc/user_attr
root:::type=role;auths=solaris.*,solaris.grant;profiles=...
```

### Ejemplo 9-9 Cambiar de nuevo el rol root al usuario root

En este ejemplo, el administrador está retirando un sistema y desea iniciar sesión en el escritorio como superusuario. El sistema se eliminó de la red.

En primer lugar, el administrador asume el rol root para eliminar todas las asignaciones de rol root.

```
% whoami
jdoe-local
% su - root
Password: a!2@3#4$5%6^7
# grep roles /etc/user_attr
jdoe-local:::type=normal;roles=root
kdoe-local:::type=normal;roles=root
# usermod -R "" jdoe-local
# usermod -R "" kdoe-local
# grep roles /etc/user_attr
#
```

Aún en el rol root, el administrador cambia root a un usuario.

```
# rolemod -K type=normal root
```

A continuación, el administrador verifica el cambio en la entrada root del archivo user\_attr.

```
# grep root /etc/user_attr
root:::type=normal;auths=solaris.*,solaris.grant;profiles=...
```

**Errores más frecuentes**

En un entorno de escritorio, no puede iniciar sesión directamente como root cuando root es un rol. Un mensaje de diagnóstico indica que root es un rol en el sistema. Si no tiene una cuenta local que pueda asumir el rol root, cree una. Como root, inicie sesión en el sistema en el modo de usuario único, cree una cuenta de usuario local y asigne el rol root a la nueva cuenta. A continuación, inicie sesión como el nuevo usuario y asuma el rol root.

Nadie se puede convertir en superusuario si cambia el usuario root a un rol y no realiza alguna de las siguientes asignaciones:

- Asigne el rol root a un usuario válido.
- Asigne un perfil de derechos que sea equivalente al perfil de derechos de root a un usuario válido. El perfil de administrador principal es un perfil de derechos equivalente para las capacidades de root.
- Cree un rol que tenga las capacidades de root y asígnelo a un usuario válido. Un rol que tiene asignado el perfil de administrador principal es equivalente al rol root.

## Uso de roles (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para usar el rol una vez que se asignaron los roles.

Tarea	Descripción	Para obtener instrucciones
Usar Solaris Management Console	Autentíquese como un rol para realizar tareas administrativas en Solaris Management Console.	<a href="#">“Cómo asumir un rol en Solaris Management Console” en la página 222</a>
Asumir un rol en una ventana de terminal	Realice tareas administrativas de línea de comandos en un shell de perfil.	<a href="#">“Cómo asumir un rol en una ventana de terminal” en la página 219</a>

## Uso de roles

Después de configurar roles con los perfiles de derechos predeterminados de Oracle Solaris y asignar los roles a los usuarios, es posible utilizar los roles. Un rol se puede asumir en la línea de comandos. En Solaris Management Console, un rol también se puede utilizar para administrar el sistema de manera local y a través de la red.

### ▼ Cómo asumir un rol en una ventana de terminal

**Antes de empezar**

Ya se debe tener asignado el rol. El servicio de nombres se debe actualizar con dicha información.

**1 En una ventana de terminal, determine los roles que puede asumir.**

```
% roles
Comma-separated list of role names is displayed
```

**2 Utilice el comando su para asumir un rol.**

```
% su - rolename
Password: <Type rolename password>
$
```

El comando `su - nombre_rol` cambia el shell a un shell de perfil para el rol. Un shell de perfil reconoce los atributos de seguridad (autorizaciones, privilegios y bits de ID de conjunto).

**3 Verifique si está ahora en un rol.**

```
$ /usr/ucb/whoami
rolename
```

Ahora puede realizar tareas del rol en esta ventana de terminal.

**4 (Opcional) Vea las capacidades de su rol.**

Para conocer el procedimiento, consulte [“Cómo determinar los comandos con privilegios que puede ejecutar un rol” en la página 267](#).

**Ejemplo 9–10 Asunción del rol de administrador principal**

En el siguiente ejemplo, el usuario asume el rol de administrador principal. En la configuración predeterminada, este rol es equivalente al superusuario. El rol luego comprueba los privilegios que están disponibles para cualquier comando que se escriba en el shell de perfil para el rol.

```
% roles
sysadmin,oper,primaryadm
% su - primaryadm
Password: <Type primaryadm password>
$ /usr/ucb/whoami      Prompt has changed to role prompt
primaryadm
$ ppriv $$
1200:  pfksh
flags = <none>
      E (Effective): all
      I (Inheritable): basic
      P (Permitted): all
      L (Limit): all
```

Para obtener información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#).

### Ejemplo 9–11 Asunción del rol root

En el siguiente ejemplo, el usuario asume el rol root. El rol se creó en [“Cómo convertir el usuario root en un rol” en la página 215](#).

```
% roles
root
% su - root
Password:      <Type root password>
# /usr/ucb/whoami      Prompt has changed to role prompt
root
$ ppriv $$
1200:   pfksh
flags = <none>
      E: all
      I: basic
      P: all
      L: all
```

Para obtener información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#).

### Ejemplo 9–12 Asunción del rol de administrador del sistema

En el siguiente ejemplo, el usuario asume el rol de administrador del sistema. A diferencia del rol de administrador principal, el administrador del sistema tiene el conjunto básico de privilegios en su conjunto vigente.

```
% roles
sysadmin,oper,primaryadm
% su - sysadmin
Password:      <Type sysadmin password>
$ /usr/ucb/whoami      Prompt has changed to role prompt
sysadmin
$ ppriv $$
1200:   pfksh
flags = <none>
      E: basic
      I: basic
      P: basic
      L: all
```

Para obtener información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#). Para obtener una breve descripción de las capacidades del rol, consulte [“Perfil de derechos de administrador del sistema” en la página 239](#).

## ▼ Cómo asumir un rol en Solaris Management Console

Para cambiar información en la interfaz gráfica de usuario de Solaris Management Console, se necesitan capacidades administrativas. Un rol proporciona capacidades administrativas. Si desea ver información, debe tener la autorización `solaris.admin.usermgr.read`. El perfil de derechos de usuario de Solaris básico incluye esta autorización.

### **Antes de empezar**

Ya debe tener asignado un rol administrativo que pueda cambiar las propiedades de usuarios o roles. Por ejemplo, el rol de administrador principal puede cambiar las propiedades de usuarios o roles.

#### **1 Inicie Solaris Management Console.**

```
% /usr/sbin/smc &
```

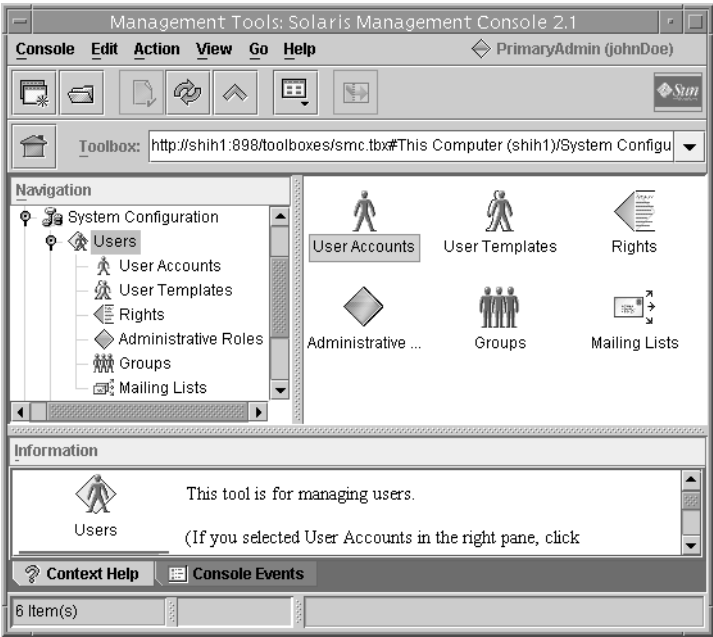
Para obtener instrucciones detalladas, consulte [“Uso de las herramientas de gestión de Solaris con RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: administración básica*.

#### **2 Seleccione la caja de herramientas para la tarea.**

Navegue hasta la caja de herramientas que contiene la herramienta o el conjunto en el ámbito de servicio de nombres adecuado, y haga clic en el icono. Los ámbitos son archivos (locales), NIS, NIS+ y LDAP. Si no se muestra la caja de herramientas adecuada en el panel de navegación, en el menú Console, seleccione Open Toolbox y cargue la caja de herramientas correspondiente.

3 Seleccione la herramienta que desea usar.

Navegue hasta la herramienta o el conjunto, y haga clic en el icono. Las herramientas para gestionar los elementos de RBAC se encuentran en la herramienta Users, como se muestra en la siguiente figura.



4 Escriba su nombre de usuario y su contraseña en el cuadro de diálogo Login: User Name.

5 Auténtiquese en el cuadro de diálogo Login: Role.

La opción de menú Role del cuadro de diálogo muestra los roles que tiene asignados. Seleccione un rol y escriba la contraseña del rol.

## Gestión de RBAC (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para personalizar el control de acceso basado en roles (RBAC) después de la implementación inicial de RBAC.

Tarea	Descripción	Para obtener instrucciones
Cambiar la contraseña del rol	Un rol o un usuario autorizado cambia la contraseña de otro rol.	<a href="#">“Cómo cambiar la contraseña de un rol” en la página 224</a>

Tarea	Descripción	Para obtener instrucciones
Modificar las propiedades de un rol	Modifica las capacidades (privilegios, comandos con privilegios, perfiles o autorizaciones) de un rol.	<a href="#">“Cómo cambiar las propiedades de un rol” en la página 226</a>
Crear o cambiar perfiles de derechos	Crea un perfil de derechos. O bien modifica autorizaciones, comandos con privilegios o perfiles de derechos complementarios en un perfil de derechos.	<a href="#">“Cómo crear o modificar un perfil de derechos” en la página 228</a>
Cambiar las capacidades administrativas de un usuario	Agrega un rol, un perfil de derechos, una autorización o privilegios a usuario común.	<a href="#">“Cómo cambiar las propiedades RBAC de un usuario” en la página 231</a>
Proteger las aplicaciones antiguas	Activa los permisos de ID de conjunto para las aplicaciones antiguas. Las secuencias de comandos pueden contener comandos con ID de conjuntos. Las aplicaciones antiguas pueden comprobar autorizaciones, si corresponde.	<a href="#">“Cómo agregar propiedades RBAC a las aplicaciones antiguas” en la página 233</a>

Estos procedimientos gestionan los elementos que se utilizan en RBAC. Para conocer los procedimientos de gestión de usuarios, consulte el [Capítulo 5, “Gestión de cuentas de usuario y grupos \(tareas\)” de \*Guía de administración del sistema: administración básica\*](#).

## Gestión de RBAC

La interfaz gráfica de usuario de Solaris Management Console es el método preferido para gestionar RBAC.

**Nota** – No intente administrar RBAC con la línea de comandos y la interfaz gráfica de usuario al mismo tiempo. En ese caso, se podrían realizar cambios en la configuración que entren en conflicto y el comportamiento sería impredecible. Ambas herramientas pueden administrar RBAC, pero no puede utilizarlas simultáneamente.

### ▼ Cómo cambiar la contraseña de un rol

**Antes de empezar** Debe haber asumido un rol que incluya el perfil de seguridad de usuarios o haber cambiado a superusuario. No puede estar en el rol cuya contraseña desea cambiar. Un rol no puede cambiar su propia contraseña.

- **Utilice uno de los siguientes métodos para cambiar la contraseña de un rol.**
  - **Ejecute el comando `passwd` como superusuario o en un rol que incluya el perfil de derechos de seguridad de usuarios.**

```
$ passwd -r naming-service target-rolename
```



-r *servicio\_nombres* Aplica el cambio de contraseña a uno de los siguientes depósitos: *files*, *nis*, *nisplus* o *ldap*. Si no se especifica ningún depósito, la contraseña se cambia en *files*.

*nombre\_rol\_destino* Nombre de un rol existente que desea modificar.

Para conocer más opciones de comandos, consulte la página del comando `man passwd(1)`.

- **Cambie la contraseña en Solaris Management Console.**

Para iniciar la consola, consulte “[Cómo asumir un rol en Solaris Management Console](#)” en la [página 222](#).

- a. **Inicie sesión en la consola como superusuario o en un rol que incluya el perfil de derechos de seguridad de usuarios.**

El rol de inicio de sesión no puede ser el rol de destino.

- b. **Elija el ámbito adecuado.**

El ámbito *Files* modifica la contraseña del rol en el sistema local. El ámbito *LDAP* modifica la contraseña del rol en el servicio de nombres LDAP.

- c. **Navegue hasta Administrative Roles y siga las instrucciones que figuran en el panel izquierdo.**

Para obtener información más exhaustiva, consulte la ayuda en pantalla.

- **Ejecute el comando `smrole` con el subcomando `modify` como superusuario o en un rol que incluya el perfil de derechos de seguridad de usuarios.**

Este comando se ejecuta como cliente del servidor de Solaris Management Console.

```
$ /usr/sadm/bin/smrole -D domain-name -r admin-role -l <Type admin-role password> \
modify -- -n target-rolename -P password
```

-D *nombre\_dominio* Nombre del dominio que desea gestionar.

-r *rol-admin* Nombre del rol administrativo que puede modificar el rol de destino. El rol administrativo debe tener la autorización `solaris.admin.usermgr.pswd`. El rol administrativo y el rol de destino no pueden ser el mismo rol.

-l Petición de datos para la contraseña de *rol\_admin*.

-- Separador obligatorio entre las opciones de autenticación y las opciones de subcomando.

-n *nombre\_rol\_destino* Nombre del rol de destino.

-P *contraseña* Nueva contraseña para *nombre\_rol\_destino*.

Para obtener la lista completa de opciones de comandos, consulte la página del comando `man smrole(1M)`.

### Ejemplo 9–13 Modificación de la contraseña de un rol local con el comando `passwd`

En este ejemplo, el superusuario cambia la contraseña del rol local `operadm`.

```
# passwd -r files operadm
New password:      Type new password
Re-enter new password:  Retype new password
```

### Ejemplo 9–14 Modificación de la contraseña de un rol en un depósito LDAP

En este ejemplo, el rol de administrador principal cambia la contraseña del rol `operadm` en el servicio de directorios LDAP.

```
$ passwd -r ldap operadm
New password:      Type new password
Re-enter new password:  Retype new password
```

### Ejemplo 9–15 Modificación de la contraseña de un rol con el comando `smrole modify`

En este ejemplo, el administrador establece contacto con el servidor de Solaris Management Console para cambiar la contraseña de `operadm` en el dominio NIS. Cuando el administrador no proporciona la contraseña antes de presionar la tecla de retorno, aparece el aviso `New Password:`.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n operadm -P      Press the Return key
New Password: a!2@3#4$5%6*7
$
```

## ▼ Cómo cambiar las propiedades de un rol

#### Antes de empezar

Debe asumir un rol que incluya el perfil de derechos de administrador principal, o bien cambiar al usuario `root` para modificar las propiedades de un rol. Las propiedades del rol incluyen la contraseña, perfiles de derechos y autorizaciones.

---

**Nota** – Para cambiar la propiedad de contraseña de un rol, consulte [“Cómo cambiar la contraseña de un rol” en la página 224](#).

---

● **Utilice uno de los siguientes métodos para cambiar las propiedades de un rol.**

■ **Utilice la herramienta Users de Solaris Management Console.**

Para iniciar la consola, consulte “[Cómo asumir un rol en Solaris Management Console](#)” en la [página 222](#). Siga las instrucciones que figuran en el panel izquierdo para modificar un rol en Administrative Roles. Para obtener información más exhaustiva, consulte la ayuda en pantalla.

■ **Utilice el comando `rolemod`.**

Este comando modifica los atributos de un rol definido en el servicio de nombres local.

```
$ rolemod -c comment -P profile-list rolename
```

-c *comentario*      Nuevo comentario que describe las capacidades del rol.

-P *lista\_perfiles*      Lista de los perfiles incluidos en el rol. Esta lista reemplaza la lista de perfiles actual.

*nombre\_rol*      Nombre de un rol local existente que desea modificar.

Para conocer más opciones de comandos, consulte la [página del comando `man rolemod\(1M\)`](#).

■ **Utilice el comando `smrole` con el subcomando `modify`.**

Este comando modifica los atributos de un rol en un servicio de nombres distribuido, como NIS, NIS+ o LDAP. Este comando se ejecuta como cliente del servidor de Solaris Management Console.

```
$ /usr/sadm/bin/smrole -D domain-name \
-r admin-role -l <Type admin-role password> \
modify -- -n rolename -r username -u username
```

-D *nombre\_dominio*      Nombre del dominio que desea gestionar.

-r *rol\_admin*      Nombre del rol administrativo que puede modificar el rol. El rol administrativo debe tener la autorización `solaris.role.assign`. Si desea modificar un rol que asumió, el rol debe tener la autorización `solaris.role.delegate`.

-l      Petición de datos para la contraseña de *rol\_admin*.

--      Separador obligatorio entre las opciones de autenticación y las opciones de subcomando.

-n *nombre\_rol*      Nombre del nuevo rol.

-r *nombre\_usuario*      Nombre del usuario que ya no puede asumir *nombre\_rol*.

-u *nombre\_usuario*      Nombre del usuario que ahora puede asumir *nombre\_rol*.

Para conocer más opciones de comandos, consulte la [página del comando `man smrole\(1M\)`](#).

**Ejemplo 9–16** Modificación de las propiedades de un rol local con el comando `rolemod`

En este ejemplo, se modifica el rol `operadm` para incluir el perfil de derechos de gestión de FTP.

```
$ rolemod -c "Handles printers, backup, and FTP" \  
-P "Operator,FTP Management,All" operadm
```

Estos perfiles de derechos se agregan a los perfiles que se otorgan por medio del archivo `policy.conf`.

**Ejemplo 9–17** Modificación de las propiedades de un rol local con el comando `smrole modify`

En el siguiente ejemplo, se modifica el rol `operadm` para agregar el perfil de derechos de gestión de FTP.

```
$ /usr/sadm/bin/smrole -r primaryadm -l <Type primaryadm password> \  
modify -- -n operadm -c "Handles printers, backup, and FTP" \  
-p "FTP Management"
```

**Ejemplo 9–18** Modificación de un rol en un dominio con el comando `smrole modify`

En el siguiente ejemplo, se modifica el rol `clockmgr`. El usuario NIS cuyo ID es 108 ya no puede asumir el rol. El usuario NIS cuyo ID es 110 puede asumir el rol `clockmgr`.

```
$ /usr/sadm/bin/smrole -D nis:/examplehost/example.domain \  
-r primaryadm -l <Type primaryadm password> \  
modify -- -n clockmgr -r 108 -u 110
```

## ▼ Cómo crear o modificar un perfil de derechos

Un perfil de derechos es una propiedad de un rol. Debe crear o modificar un perfil de derechos cuando la base de datos `prof_attr` no contiene un perfil de derechos que satisfice sus necesidades. Para obtener más información sobre los perfiles de derechos, consulte [“Perfiles de derechos de RBAC” en la página 190](#).

**Antes de empezar** Para crear o modificar un perfil de derechos, debe haber asumido el rol de administrador principal o haber cambiado a superusuario.

- **Utilice uno de los siguientes métodos para crear o modificar un perfil de derechos.**

- **Utilice la herramienta Users de Solaris Management Console.**

Para iniciar la consola, consulte “[Cómo asumir un rol en Solaris Management Console](#)” en la [página 222](#). Siga las instrucciones que figuran en el panel izquierdo para crear o modificar un perfil de derechos en Rights. Para obtener información más exhaustiva, consulte la ayuda en pantalla.

- **Utilice el comando `smprofile`.**

Este comando permite agregar, modificar, enumerar o eliminar un perfil de derechos. El comando funciona en archivos y en servicios de nombres distribuidos, como NIS, NIS+ o LDAP. El comando `smprofile` se ejecuta como cliente del servidor de Solaris Management Console.

```
$ /usr/sadm/bin/smprofile -D domain-name \
-r admin-role -l <Type admin-role password> \
add | modify -- -n profile-name \
-d description -m help-file -p supplementary-profile
```

-D <i>nombre_dominio</i>	Nombre del dominio que desea gestionar.
-r <i>rol_admin</i>	Nombre del rol administrativo que puede modificar el rol. El rol administrativo debe tener la autorización <code>solaris.role.assign</code> . Si desea modificar un rol que asumió, el rol debe tener la autorización <code>solaris.role.delegate</code> .
-l	Petición de datos para la contraseña de <i>rol_admin</i> .
--	Separador obligatorio entre las opciones de autenticación y las opciones de subcomando.
-n <i>nombre_perfil</i>	Nombre del nuevo perfil.
-d <i>descripción</i>	Descripción breve del perfil.
-m <i>archivo_ayuda</i>	Nombre del archivo de ayuda HTML que creó y guardó en el directorio <code>/usr/lib/help/profiles/locale/C</code> .
-p <i>perfil_complementario</i>	Nombre de un perfil de derechos existente que se incluye en este perfil de derechos. Puede especificar varias opciones -p <i>perfil_complementario</i> .

Para conocer más opciones de comandos, consulte la [página del comando `man smprofile\(1M\)`](#).

Ejemplo 9–19    Modificación de un perfil de derechos desde la línea de comandos

En el siguiente ejemplo, se convierte al perfil de derechos de gestión de la red en un perfil complementario del perfil de derechos de seguridad de la red. El rol que contiene el perfil de seguridad de la red ahora puede configurar la red y los hosts, además de ejecutar comandos relacionados con la seguridad.

```
$ /usr/sadm/bin/smpprofile -D nisplus:/example.host/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n "Network Security" \
-d "Manage network and host configuration and security" \
-m RtNetConfSec.html -p "Network Management"
```

El administrador creó un nuevo archivo de ayuda, RtNetConfSec.html, y lo guardó en el directorio /usr/lib/help/profiles/locale/C, antes de ejecutar este comando.

Ejemplo 9–20    Creación de un nuevo perfil de derechos con la herramienta Rights

La siguiente tabla muestra datos de ejemplo para un perfil de derechos hipotético que se denomina “Administrador de compilación”. Este perfil de derechos incluye los comandos del subdirectorio /usr/local/swctrl/bin. Estos comandos tienen un UID efectivo de 0. El perfil de derechos de creación de administrador puede resultar útil para los administradores que gestionan las compilaciones y versiones para el desarrollo de software.

Ficha	Campo	Ejemplo
General	Name	Administrador de compilación
	Descripción	Para gestionar las compilaciones y versiones del software.
	Help File Name	BuildAdmin.html
Commands	Add Directory	Haga clic en Add Directory, escriba /usr/local/swctrl/bin en el cuadro de diálogo y haga clic en OK.
	Commands Denied / Commands Permitted	Mueva /usr/local/swctrl/bin a la columna Commands Permitted.
	Set Security Attributes	Seleccione /usr/local/swctrl/bin, haga clic en Set Security Attributes y establezca UID efectivo = root.
Authorizations	Authorizations Excluded / Authorizations Included	Ninguna autorización.
Supplementary Rights	Rights Excluded / Rights Included	Ningún perfil de derechos complementario.

**Errores más frecuentes**

Compruebe lo siguiente si el perfil de derechos no proporciona el rol con las capacidades que espera:

- ¿Los perfiles de derechos del rol están enumerados en la interfaz gráfica de usuario del más al menos poderoso?

Por ejemplo, si el perfil de derechos `All` está en la parte superior de la lista, no se ejecuta ningún comando con atributos de seguridad. Un perfil que contiene comandos con atributos de seguridad debe preceder al perfil de derechos `All` en la lista.

- ¿Algún comando aparece más de una vez en los perfiles de derechos del rol? En ese caso, ¿la primera instancia del comando tiene todos los atributos de seguridad que son necesarios?

Por ejemplo, un comando puede necesitar privilegios para determinadas opciones en el comando. Para las opciones que requieren privilegios para una ejecución correcta, la primera instancia del comando que se incluye en el primer perfil de derechos de la lista debe tener los privilegios asignados.

- ¿Los comandos de los perfiles de derechos del rol tienen los atributos de seguridad adecuados?

Por ejemplo, cuando la política es `suser`, algunos comandos requieren `uid=0` en lugar de `euid=0` para ejecutarse correctamente.

- ¿La antememoria de servicio de nombres, `svc:/system/name-service-cache`, se reinició?

El daemon `nsd` puede tener un intervalo de tiempo de vida prolongado. Al reiniciar el daemon, actualiza el nombre de servicios con los datos actuales.

## ▼ **Cómo cambiar las propiedades RBAC de un usuario**

Las propiedades del usuario incluyen la contraseña, perfiles de derechos, roles y autorizaciones. El método más seguro para otorgar capacidades administrativas a un usuario es asignar un rol al usuario. Para ver una explicación, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 192](#).

**Antes de empezar**

Debe asumir un rol que incluya el perfil de derechos de administrador principal, o bien cambiar al usuario `root`.

- **Utilice uno de los siguientes métodos para cambiar las propiedades RBAC de un usuario.**

- **Utilice la herramienta `Users of Solaris Management Console`.**

Para iniciar la consola, consulte [“Cómo asumir un rol en Solaris Management Console” en la página 222](#). Siga las instrucciones que figuran en el panel izquierdo para modificar un usuario en User Accounts. Para obtener información más exhaustiva, consulte la ayuda en pantalla.

---

**Consejo** – No es recomendable asignar autorizaciones, privilegios o perfiles de derechos directamente a los usuarios. El enfoque preferido es asignar un rol a los usuarios. Los usuarios luego asumen un rol para llevar a cabo operaciones con privilegios.

---

■ **Utilice el comando `usermod`.**

Este comando modifica los atributos de un usuario definido en el servicio de nombres local.

```
$ usermod -R rolename username
```

`-R nombre_rol`      Nombre de un rol local existente.

`nombre_usuario`    Nombre de un usuario local existente que desea modificar.

Para conocer más opciones de comandos, consulte la página del comando `man usermod(1M)`.

■ **Utilice el comando `smuser` con el subcomando `modify`.**

Este comando modifica los atributos de un usuario en un servicio de nombres distribuido, como NIS, NIS+ o LDAP. Este comando se ejecuta como cliente del servidor de Solaris Management Console.

```
$ /usr/sadm/bin/smuser -D domain-name \  
-r admin-role -l <Type admin-role password> \  
modify -- -n username -a rolename
```

`-D nombre_dominio`    Nombre del dominio que desea gestionar.

`-r rol_admin`          Nombre del rol administrativo que puede modificar el rol. El rol administrativo debe tener la autorización `solaris.role.assign`. Si desea modificar un rol que asumió, el rol debe tener la autorización `solaris.role.delegate`.

`-l`                      Petición de datos para la contraseña de `rol_admin`.

`--`                      Separador obligatorio entre las opciones de autenticación y las opciones de subcomando.

`-n nombre_usuario`    Nombre del usuario al que se asigna `nombre_rol`.

`-a nombre_rol`          Nombre del rol que asigna a `nombre_usuario`. Puede especificar varias opciones `-a nombre_rol`.

Para conocer más opciones de comandos, consulte la página del comando `man smuser(1M)`.



**Ejemplo 9–21** Modificación de las propiedades RBAC de un usuario local desde la línea de comandos

En este ejemplo, el usuario `jdoe` ahora puede asumir el rol de administrador del sistema.

```
$ usermod -R sysadmin jdoe
```

A este rol se le agregan los roles que el usuario puede asumir.

**Ejemplo 9–22** Modificación de las propiedades RBAC de un usuario con el comando `smuser`

En este ejemplo, se asignan dos roles al usuario `jdoe`: administrador del sistema y operador. Como el usuario y los roles se definen de manera local, la opción `-D` no es necesaria.

```
$ /usr/sadm/bin/smuser -r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm
```

En el siguiente ejemplo, el usuario se definió en el servicio de nombres NIS. Por lo tanto, se necesita la opción `-D`. Se definieron dos roles en el servicio de nombres. Un rol, `root`, se definió de manera local.

```
$ /usr/sadm/bin/smuser -D nis:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
modify -- -n jdoe -a sysadmin -a operadm -a root
```

## ▼ Cómo agregar propiedades RBAC a las aplicaciones antiguas

Una aplicación antigua es un comando o un conjunto de comandos. Los atributos de seguridad se definen para cada comando en un perfil de derechos. El perfil de derechos se incluye luego en un rol. Un usuario que asume el rol puede ejecutar la aplicación antigua con los atributos de seguridad.

Para agregar aplicaciones antiguas en Solaris Management Console, consulte [“Cómo agregar herramientas en Solaris Management Console” de Guía de administración del sistema: administración básica](#).

**Antes de empezar** Debe haber asumido el rol de administrador principal o haber cambiado a superusuario para modificar los atributos de seguridad de un comando en un perfil de derechos.

**1 Utilice la herramienta Users de Solaris Management Console.**

Para iniciar la consola, consulte [“Cómo asumir un rol en Solaris Management Console” en la página 222](#). Siga las instrucciones que figuran en el panel izquierdo para modificar un perfil de derechos en Rights. Para obtener información más exhaustiva, consulte la ayuda en pantalla.

**2 Agregue atributos de seguridad a los comandos que implementan la aplicación antigua.**

Agregue los atributos de seguridad a una aplicación antigua del mismo modo que lo haría para cualquier comando. Debe agregar el comando con atributos de seguridad a un perfil de derechos. Para un comando antiguo, proporcione los atributos de seguridad `euid=0` o `uid=0`. Para obtener detalles del procedimiento, consulte [“Cómo crear o modificar un perfil de derechos” en la página 228](#).

**3 Después de agregar la aplicación antigua a un perfil de derechos, incluya el perfil de derechos en la lista de perfiles de un rol.**

Para agregar un perfil de derechos a un rol, consulte [“Cómo cambiar las propiedades de un rol” en la página 226](#).

**Ejemplo 9–23 Adición de atributos de seguridad a comandos de una secuencia de comandos**

Si un comando de una secuencia de comandos necesita tener el conjunto de bits `setgid` o `setuid` para ejecutarse correctamente, el archivo ejecutable de la secuencia y el comando deben tener los atributos de seguridad agregados en un perfil de derechos. Luego, el perfil de derechos se incluye en un rol, y el rol se asigna a un usuario. Cuando el usuario asume el rol y ejecuta la secuencia de comandos, el comando se ejecuta con los atributos de seguridad.

Para agregar atributos de seguridad a un comando o una secuencia de comandos de shell, consulte [“Cómo crear o modificar un perfil de derechos” en la página 228](#).

**Ejemplo 9–24 Comprobación de autorizaciones en una secuencia de comandos o un programa**

Para tener una secuencia de comandos para las autorizaciones, debe agregar una prueba basada en el comando `auths`. Para obtener información detallada sobre este comando, consulte la página del comando `man auths(1)`.

Por ejemplo, la siguiente línea verifica si el usuario tiene la autorización que se proporciona como argumento `$1`:

```
if [ '/usr/bin/auths|usr/xpg4/bin/grep $1' ]; then
    echo Auth granted
else
    echo Auth denied
fi
```

Para que la prueba sea más completa, debe incluir una lógica que compruebe otras autorizaciones que usan caracteres comodín. Por ejemplo, para verificar si el usuario tiene la autorización `solaris.admin.usermgr.write`, debe comprobar las siguientes cadenas:

- `solaris.admin.usermgr.write`
- `solaris.admin.usermgr.*`
- `solaris.admin.*`
- `solaris.*`

Si está escribiendo un programa, utilice la función `getauthattr()` para comprobar la autorización.



## Control de acceso basado en roles (referencia)

---

En este capítulo, se proporciona material de referencia sobre RBAC. A continuación, se muestra una lista de la información de referencia que se incluye en este capítulo:

- “Contenido de los perfiles de derechos” en la página 237
- “Denominación y delegación de autorizaciones” en la página 242
- “Bases de datos que admiten RBAC” en la página 243
- “Comandos de RBAC” en la página 251

Para obtener más información sobre el uso de RBAC, consulte [Capítulo 9, “Uso del control de acceso basado en roles \(tareas\)”](#). Para obtener información general, consulte “[Control de acceso basado en roles \(descripción general\)](#)” en la página 182.

### Contenido de los perfiles de derechos

En esta sección, se describen algunos perfiles de derechos típicos. Los perfiles de derechos pueden incluir autorizaciones, comandos con atributos de seguridad y perfiles de derechos complementarios. Los perfiles de derechos se enumeran del más al menos poderoso. Si obtener sugerencias sobre cómo distribuir perfiles de derechos a roles en su sitio, consulte “[Cómo planificar la implementación de RBAC](#)” en la página 205.

- **Perfil de derechos de administrador principal:** proporciona las capacidades de superusuario en un perfil.
- **Perfil de derechos de administrador del sistema:** proporciona un perfil que puede realizar la mayoría de las tareas que no están relacionadas con la seguridad. Este perfil incluye varios perfiles diferentes para crear un rol poderoso.
- **Perfil de derechos de operador:** proporciona capacidades limitadas para gestionar archivos y medios sin conexión. Este perfil incluye perfiles de derechos complementarios para crear un rol simple.

- **Perfil de derechos de gestión de impresoras:** proporciona un número limitado de comandos y autorizaciones para gestionar la impresión. Este perfil es uno de los tantos perfiles que abarcan una sola área de administración.
- **Perfil de derechos de usuario de Solaris básico:** permite a los usuarios utilizar el sistema dentro de los límites de la política de seguridad. Este perfil aparece de manera predeterminada en el archivo `policy.conf`.
- **Perfil de derechos "todos":** para los roles, proporciona acceso a los comandos que no tienen atributos de seguridad.

Cada perfil de derechos tiene un archivo de ayuda asociado. Los archivos de ayuda están en formato HTML y se pueden personalizar. Los archivos residen en el directorio `/usr/lib/help/profiles/locale/C`.

## Perfil de derechos de administrador principal

El perfil de derechos de administrador principal se asigna al rol más poderoso del sistema. El rol que incluye el perfil de derechos de administrador principal tiene capacidades de superusuario.

- La autorización `solaris.*` asigna de forma eficaz todas las autorizaciones que ofrece el software Oracle Solaris.
- La autorización `solaris.grant` permite a un rol asignar cualquier autorización a cualquier perfil de derechos, rol o usuario.
- La asignación de comando `*:uid=0;gid=0` permite ejecutar cualquier comando con `UID=0` y `GID=0`.

Puede personalizar el archivo de ayuda `RtPriAdmin.html` para su sitio, si es necesario. Los archivos de ayuda se almacenan en el directorio `/usr/lib/help/profiles/locale/C`.

Tenga en cuenta también que si el perfil de derechos de administrador principal no es coherente con la política de seguridad de un sitio, es posible modificar el perfil o no asignarlo. Sin embargo, las capacidades de seguridad del perfil de derechos de administrador principal se deberán gestionar en uno o varios perfiles de derechos diferentes. Los otros perfiles de derechos luego se deberán asignar a roles.

TABLA 10-1 Contenido del perfil de derechos de administrador principal

Finalidad	Contenido
Para llevar a cabo todas las tareas administrativas	<b>Comandos:</b> <code>*:uid=0;gid=0</code> <b>Autorizaciones:</b> <code>solaris.*</code> , <code>solaris.grant</code> <b>Archivo de ayuda:</b> <code>RtPriAdmin.html</code>

## Perfil de derechos de administrador del sistema

El perfil de derechos de administrador del sistema está diseñado para el rol de administrador del sistema. Dado que el administrador del sistema no tiene las capacidades amplias del administrador principal, no se utilizan caracteres comodín. En cambio, este perfil es un conjunto de perfiles de derechos administrativos, complementarios y discretos que no están relacionados con la seguridad. Se muestran los comandos con atributos de seguridad de uno de los perfiles de derechos complementarios.

Tenga en cuenta que el perfil de derechos "todos" se asigna al final de la lista de perfiles de derechos complementarios.

TABLA 10-2    Contenido del perfil de derechos de administrador del sistema

Finalidad	Contenido
Para realizar la mayoría de las tareas administrativas no relacionadas con la seguridad	<b>Perfiles de derechos complementarios:</b> revisión de auditoría, gestión de impresoras, gestión de cron, gestión de dispositivos, gestión de sistemas de archivos, gestión de correo, mantenimiento y reparación, gestión de servicios de nombres, gestión de la red, gestión del acceso a objetos, gestión de procesos, instalación de software, gestión de proyectos, gestión de usuarios, todos  <b>Archivo de ayuda:</b> RtSysAdmin.html
Comandos de uno de los perfiles complementarios	<b>Perfil de derechos de gestión del acceso a objetos,</b> política solaris: /usr/bin/chgrp:prvs=file_chown,/usr/bin/chmod:prvs=file_chown, /usr/bin/chown:prvs=file_chown , /usr/bin/setfacl:prvs=file_chown  política suser: /usr/bin/chgrp:euid=0,/usr/bin/chmod:euid=0, /usr/bin/chown:euid=0,/usr/bin/getfacl:euid=0, /usr/bin/setfacl:euid=0

## Perfil de derechos de operador

El perfil de derechos de operador es un perfil menos poderoso que ofrece la posibilidad de realizar copias de seguridad y mantenimiento de impresoras. La capacidad de restaurar archivos tiene consecuencias de seguridad adicionales. Por lo tanto, en este perfil, la configuración predeterminada no incluye la capacidad de restaurar archivos.

TABLA 10-3    Contenido del perfil de derechos de operador

Finalidad	Contenido
Para realizar tareas administrativas sencillas	<b>Perfiles de derechos complementarios:</b> gestión de impresoras, copia de seguridad de medios, todos  <b>Archivo de ayuda:</b> RtOperator.html

# Perfil de derechos de gestión de impresoras

La gestión de impresoras es un perfil de derechos típico que está diseñado para un área de tareas específica. Este perfil incluye autorizaciones y comandos. La siguiente tabla muestra una lista parcial de los comandos.

TABLA 10-4 Contenido del perfil de derechos de gestión de impresoras

Finalidad	Contenido
Para gestionar impresoras, daemons y trabajos en cola	<p><b>Autorizaciones:</b> <code>solaris.print.*</code>, <code>solaris.label.print</code>, <code>solaris.admin.printer.delete</code>, <code>solaris.admin.printer.modify</code>, <code>solaris.admin.printer.read</code> , <code>solaris.smf.manage.discovery.printers.*</code>, <code>solaris.smf.value.discovery.printers.*</code></p> <p><b>Comandos:</b> <code>/usr/lib/lp/local/lpadmin:uid=lp;gid=lp</code>, <code>/usr/sbin/lpfilter:euid=lp;uid=lp</code>, <code>/usr/sbin/lpforms:euid=lp</code>, <code>/usr/sbin/lpusers:euid=lp</code>, <code>/usr/sbin/ppdmgm:euid=0</code></p> <p><b>Archivo de ayuda:</b> <code>RtPrntMngmnt.html</code></p>

# Perfil de derechos de usuario de Solaris básico

De manera predeterminada, el perfil de derechos de usuario de Solaris básico se asigna automáticamente a todos los usuarios a través del archivo `policy.conf`. Este perfil proporciona autorizaciones básicas que resultan útiles en las operaciones habituales. Tenga en cuenta que la comodidad que ofrece el perfil de derechos de usuario de Solaris básico debe equilibrarse con los requisitos de seguridad del sitio. Es posible que los sitios que necesitan una seguridad más estricta prefieran eliminar este perfil del archivo `policy.conf`.



TABLA 10-5    Contenido del perfil de derechos de usuario de Solaris básico

Finalidad	Contenido
Para asignar de forma automática derechos a todos los usuarios	<b>Autorizaciones:</b> solaris.profmgr.read, solaris.jobs.user, solaris.mail.mailq, solaris.device.mount.removable, solaris.admin.usermgr.read, solaris.admin.logsvc.read, solaris.admin.fsmgr.read, solaris.admin.serialmgr.read, solaris.admin.diskmgr.read, solaris.admin.procmgr.user, solaris.compsys.read, solaris.admin.printer.read, solaris.admin.prodreg.read, solaris.admin.dcmgr.read, solaris.snmp.read, solaris.project.read, solaris.admin.patchmg.read, solaris.network.hosts.read, solaris.admin.volmgr.read  <b>Perfiles de derechos complementarios:</b> todos  <b>Archivo de ayuda:</b> RtDefault.html

## Perfil de derechos "todos"

El perfil de derechos "todos" utiliza caracteres comodín para incluir todos los comandos. Este perfil proporciona a un rol acceso a todos los comandos que no se asignaron explícitamente en otros perfiles de derechos. Sin el perfil de derechos "todos" u otros perfiles de derechos que usan caracteres comodín, un rol sólo tiene acceso a los comandos asignados de forma explícita. Un conjunto de comandos tan limitado no resulta muy práctico. No se incluyen autorizaciones en este perfil.

Si se utiliza, el perfil de derechos "todos" debe ser el último perfil que se asigna. De este modo, se garantiza la aplicación de las asignaciones de atributos de seguridad explícitas en otros perfiles de derechos.

TABLA 10-6    Contenido del perfil de derechos "todos"

Finalidad	Contenido
Para ejecutar cualquier comando como usuario o rol	<b>Comandos:</b> *  <b>Archivo de ayuda:</b> RtAll.html

## Orden de perfiles de derechos

Los comandos de perfiles de derechos se interpretan en orden. La primera instancia de un comando es la única versión del comando que se utiliza para ese rol o usuario. Diferentes perfiles de derechos pueden incluir el mismo comando. Por lo tanto, el orden de los perfiles de derechos en una lista de perfiles es importante. El perfil de derechos con más capacidades debe aparecer en primer lugar.

Los perfiles de derechos se muestran en la interfaz gráfica de usuario de Solaris Management Console y en el archivo `prof_attr`. En la interfaz gráfica de usuario de Solaris Management Console, el perfil de derechos con más capacidades debe ser el perfil ubicado en la parte superior de la lista de perfiles de derechos asignados. En el archivo `prof_attr`, el perfil de derechos con más capacidades debe ser el primero de la lista de perfiles complementarios. Esto garantiza que un comando con atributos de seguridad aparezca antes que ese mismo comando sin atributos de seguridad.

## Visualización del contenido de los perfiles de derechos

La herramienta Rights de Solaris Management Console ofrece una forma de inspeccionar el contenido de los perfiles de derechos.

Los archivos `prof_attr` y `exec_attr` proporcionan una vista más fragmentada. El archivo `prof_attr` contiene el nombre de cada perfil de derechos definido en el sistema. El archivo también incluye las autorizaciones, los privilegios y los perfiles de derechos complementarios para cada perfil. El archivo `exec_attr` contiene los nombres de los perfiles de derechos y sus comandos con atributos de seguridad.

## Denominación y delegación de autorizaciones

Una *autorización* RBAC es un derecho perfectamente definido que se puede otorgar a un rol o a un usuario. Las aplicaciones compatibles con RBAC comprueban las autorizaciones antes de que un usuario obtenga acceso a la aplicación u operaciones específicas dentro de la aplicación. Esta comprobación reemplaza las pruebas en las aplicaciones UNIX convencionales para `UID=0`.

## Convenciones de denominación de autorizaciones

Una autorización tiene un nombre que se utiliza internamente y en archivos. Por ejemplo, `solaris.admin.usermgr.pswd` es el nombre de una autorización. Una autorización tiene una descripción breve, que aparece en las interfaces gráficas de usuario (GUI). Por ejemplo, Change Passwords es la descripción de la autorización `solaris.admin.usermgr.pswd`.

Por convención, todos los nombres de autorizaciones constan del orden inverso del nombre del proveedor en Internet, el área temática, las subáreas y la función. Las partes del nombre de la autorización están separados por puntos. Un ejemplo sería `com.xyzcorp.dispositivo.acceso`. Las excepciones a esta convención son las autorizaciones de Sun Microsystems, Inc., que utilizan el prefijo `solaris` en lugar de un nombres de Internet.

La convención de denominación permite a los administradores aplicar autorizaciones de un modo jerárquico. Un carácter comodín (\*) puede representar cualquier cadena a la derecha de un punto.

## Ejemplo de granularidad de autorizaciones

Como ejemplo de la manera en que se utilizan las autorizaciones, tenga en cuenta lo siguiente:

Un usuario en el rol de operador puede estar limitado a la autorización `solaris.admin.usermgr.read`, la cual proporciona acceso de lectura, pero no de escritura en los archivos de configuración de usuario. El rol de administrador del sistema tiene lógicamente las autorizaciones `solaris.admin.usermgr.read` y `solaris.admin.usermgr.write` para efectuar cambios en archivos de usuario. Sin embargo, sin la autorización `solaris.admin.usermgr.pswd`, el administrador del sistema no puede cambiar contraseñas. El administrador principal tiene todas estas tres autorizaciones.

La autorización `solaris.admin.usermgr.pswd` se requiere para realizar cambios de contraseña en la herramienta Users de Solaris Management Console. Esta autorización también se necesita para usar las opciones de modificación de contraseñas en los comandos `smuser`, `smmultiuser` y `smrole`.

## Autoridad de delegación en autorizaciones

Una autorización que finaliza con el sufijo `grant` permite a un usuario o rol delegar a otros usuarios las autorizaciones asignadas que comienzan con el mismo prefijo.

Por ejemplo, un rol con las autorizaciones `solaris.admin.usermgr.grant` y `solaris.admin.usermgr.read` puede delegar la autorización `solaris.admin.usermgr.read` a otro usuario. Un rol con las autorizaciones `solaris.admin.usermgr.grant` y `solaris.admin.usermgr.*` puede delegar cualquiera de las autorizaciones con el prefijo `solaris.admin.usermgr` a otros usuarios.

## Bases de datos que admiten RBAC

Las siguientes cuatro bases de datos almacenan los datos de los elementos de RBAC:

- **Base de datos de atributos de usuario extendidos** (`user_attr`): asocia usuarios y los roles con autorizaciones, privilegios y perfiles de derechos.
- **Base de datos de atributos de perfil de derechos** (`prof_attr`): define perfiles de derechos, enumera autorizaciones asignadas de perfiles y palabras clave, e identifica el archivo de ayuda asociado.
- **Base de datos de atributos de autorización** (`auth_attr`): define autorizaciones y sus atributos, e identifica el archivo de ayuda asociado.

- **Base de datos de atributos de ejecución** (`exec_attr`): identifica los comandos con atributos de seguridad que están asignados a perfiles de derechos específicos.

La base de datos `policy.conf` contiene autorizaciones, privilegios y perfiles de derechos que se aplican a todos los usuarios. Para obtener más información, consulte [“Archivo `policy.conf`” en la página 250](#).

## Relaciones entre bases de datos de RBAC

Cada base de datos de RBAC utiliza la sintaxis `clave=valor` para almacenar los atributos. Este método permite ampliaciones futuras en las bases de datos. El método también permite que el funcionamiento de un sistema continúe si se encuentra una palabra clave que es desconocida para su política. El contenido de `clave=valor` enlaza los archivos. Las siguientes entradas vinculadas de la cuatro bases de datos ilustran cómo trabajan juntas las bases de datos de RBAC.

### EJEMPLO 10-1 Visualización de las conexiones de las bases de datos de RBAC

En el siguiente ejemplo, el usuario `jdoe` obtiene las capacidades del perfil de derechos de gestión de sistemas de archivos mediante la asignación del rol `filemgr`.

1. Al usuario `jdoe` se le asigna el rol `filemgr` en la entrada de usuario `jdoe` de la base de datos `user_attr`.

```
# user_attr - user definition
jdoe:::type=normal;roles=filemgr
```

2. Al rol `filemgr` se le asigna el perfil de derechos de gestión de sistemas de archivos en la entrada del rol de la base de datos `user_attr`.

```
# user_attr - role definition
filemgr:::profiles=File System Management;type=role
```

El usuario y el rol se definen de manera exclusiva en los archivos `passwd` y `shadow` del sistema local o bases de datos equivalentes en un servicio de nombres distribuido.

3. El perfil de derechos de gestión de sistemas de archivos se define en la base de datos `prof_attr`. Esta base de datos también asigna tres conjuntos de autorizaciones a la entrada de gestión de sistemas de archivos.

```
# prof_attr - rights profile definitions and assigned authorizations
File System Management::Manage, mount, share file systems:
help=RtFileSysMngmnt.html;
auths=solaris.admin.fsmgr.*,solaris.admin.diskmgr.*,solaris.admin.volmgr.*
```

4. Las autorizaciones se definen en la base de datos `auth_attr`.

```
# auth_attr - authorization definitions
solaris.admin.fsmgr:::Mounts and Shares::help=AuthFsmgrHeader.html
solaris.admin.fsmgr.read:::View Mounts and Shares::help=AuthFsmgrRead.html
solaris.admin.fsmgr.write:::Mount and Share Files::help=AuthFsmgrWrite.html
```

5. Al perfil de derechos de gestión de sistemas de archivos se le asignan comandos con atributos de seguridad en la base de datos `exec_attr`.

## EJEMPLO 10-1 Visualización de las conexiones de las bases de datos de RBAC (Continuación)

```
# exec_attr - rights profile names with secured commands
File System Management:suser:cmd:::/usr/sbin/mount:uid=0
File System Management:suser:cmd:::/usr/sbin/dfshares:euid=0
...
File System Management:solaris:cmd:::/usr/sbin/mount:privs=sys_mount
...
```

## Bases de datos de RBAC y servicios de nombres

El ámbito de servicio de nombres de las bases de datos de RBAC se puede aplicar al host local solamente. El ámbito puede incluir también todos los hosts gestionados por un servicio de nombres, como NIS, NIS+ o LDAP. En el archivo `/etc/nsswitch.conf`, se define qué servicio de nombres tiene prioridad para cada una de las bases de datos.

- **Entrada** `auth_attr`: define la prioridad de servicio de nombres para la base de datos `auth_attr`.
- **Entrada** `passwd`: define la prioridad de servicio de nombres para la base de datos `user_attr`.
- **Entrada** `prof_attr`: define la prioridad de servicio de nombres para la base de datos `prof_attr`. También define la prioridad de servicio de nombres para la base de datos `exec_attr`.

Por ejemplo, si se asigna un comando con atributos de seguridad a un perfil de derechos que existe en dos servicios de nombres, sólo se utiliza la entrada del primer servicio.

## Base de datos `user_attr`

La base de datos `user_attr` contiene información de usuarios y roles que complementa las bases de datos `passwd` y `shadow`. La base de datos `user_attr` contiene atributos de usuario extendidos, como autorizaciones, perfiles de derechos, privilegios y roles asignados. Los campos de la base de datos `user_attr` están separados por dos puntos, de la siguiente forma:

```
user:qualifier:res1:res2:attr
```

Los campos tienen los siguientes significados:

`user`

Nombre del usuario o rol como se especificó en la base de datos `passwd`.

`qualifier:res1:res2`

Estos campos están reservados para uso futuro.

`attr`

Lista opcional de pares de clave y valor separados por punto y coma (;) que describe los atributos de seguridad que se aplicarán cuando el usuario ejecute comandos. Las cuatro claves válidas son `type`, `auths`, `profiles` y `roles`.

- La palabra clave `type` se puede establecer en `normal` si esta cuenta es para un usuario común. La palabra clave `type` se define en `role` cuando esta cuenta es para un rol.
- La palabra clave `auths` especifica una lista separada por comas de nombres de autorizaciones que se eligen de los nombres definidos en la base de datos `auth_attr`. Los nombres de autorizaciones pueden incluir un asterisco (\*) como carácter comodín. Por ejemplo, `solaris.device.*` significa todas las autorizaciones de dispositivos de Oracle Solaris.
- La palabra clave `profiles` especifica una lista ordenada y separada por comas de nombres de perfiles de derechos de la base de datos `prof_attr`. El orden de los perfiles de derechos funciona de modo similar a las rutas de búsqueda UNIX. El primer perfil de la lista que contiene el comando que se ejecutará define qué atributos de seguridad (si corresponde) se aplicarán al comando.
- La palabra clave `roles` especifica una lista separada por comas de nombres de roles. Tenga en cuenta que los roles se definen en la misma base de datos `user_attr`. Los roles se indican mediante la definición del valor del tipo en `role`. No se pueden asignar roles a otros roles.

El siguiente ejemplo muestra cómo el rol de operador se define en una base de datos `user_attr` típica. El siguiente ejemplo muestra cómo se asigna el rol al usuario `jdoe`. Los roles y los usuarios se diferencian por la palabra clave `type`.

```
% grep operator /etc/user_attr
jdoe:::type=normal;roles=operator
operator:::profiles=Operator;type=role
```

## Base de datos `auth_attr`

Todas las autorizaciones se almacenan en la base de datos `auth_attr`. Las autorizaciones se pueden asignar a usuarios, roles o perfiles de derechos. El método preferido es colocar las autorizaciones en un perfil de derechos, incluir el perfil en la lista de perfiles de un rol y, a continuación, asignar el rol a un usuario.

Los campos de la base de datos `auth_attr` están separados por dos puntos, de la siguiente forma:

```
authname:res1:res2:short_desc:long_desc:attr
```

Los campos tienen los siguientes significados:

<code>authname</code>	Cadena de caracteres única que se utiliza para identificar la autorización con el formato <i>prefijo</i> . <i>[sufijo]</i> . Las autorizaciones para Oracle Solaris usan <code>solaris</code> como prefijo. Todas las demás autorizaciones deben utilizar un prefijo que comience con el orden inverso del nombre de dominio en Internet de la organización que crea la autorización (por ejemplo, <code>com.xyzcompany</code> ). El sufijo indica qué se autoriza, que suele ser el área funcional y el uso.
-----------------------	---

Cuando `authname` consta de un prefijo y un área funcional, y finaliza con un punto, `authname` funciona como encabezado para las aplicaciones en sus interfaces gráficas de usuario. Un valor `authname` con dos partes no es una autorización real. El valor `authname` de `solaris.printmgr.` es un ejemplo de encabezado.

Cuando `authname` finaliza con la palabra “grant”, `authname` funciona como autorización de concesión. Una autorización de concesión permite al usuario delegar a otros usuarios autorizaciones con el mismo prefijo y área funcional. El valor `authname` de `solaris.printmgr.grant` es un ejemplo de autorización de concesión. `solaris.printmgr.grant` otorga al usuario el derecho de delegar a otros usuarios autorizaciones como `solaris.printmgr.grant` y `solaris.printmgr.nobanner`.

<code>res1:res2</code>	Reservado para uso futuro.
<code>short_desc</code>	Nombre corto para la autorización. Este nombre corto es adecuado para su visualización en interfaces de usuario, como en una lista de desplazamiento de una interfaz gráfica de usuario.
<code>long_desc</code>	Descripción larga. Este campo identifica la finalidad de la autorización, las aplicaciones en las que se utiliza la autorización y el tipo de usuario que puede emplear la autorización. La descripción larga se puede mostrar en el texto de ayuda de una aplicación.
<code>attr</code>	Lista opcional de pares de clave y valor separados por punto y coma (;) que describen los atributos de una autorización. Es posible especificar cero claves o más.

La palabra clave `help` identifica un archivo de ayuda en HTML. Es posible acceder a los archivos de ayuda desde el archivo `index.html` del directorio `/usr/lib/help/auths/locale/C`.

El siguiente ejemplo muestra una base de datos `auth_attr` con algunos valores típicos:

```
% grep printer /etc/security/auth_attr
solaris.admin.printer.:Printer Information::help=AuthPrinterHeader.html
solaris.admin.printer.delete::Delete Printer Information::help=AuthPrinterDelete.html
solaris.admin.printer.modify::Update Printer Information::help=AuthPrinterModify.html
solaris.admin.printer.read::View Printer Information::help=AuthPrinterRead.html
```

Tenga en cuenta que `solaris.admin.printer.` se define como un encabezado, porque el nombre de la autorización finaliza con un punto (.). Los encabezados se utilizan en las interfaces gráficas de usuario para organizar las familias de autorizaciones.

# Base de datos prof\_attr

La base de datos `prof_attr` almacena el nombre, la descripción, la ubicación del archivo de ayuda, los privilegios y las autorizaciones que se asignan a los perfiles de derechos. Los comandos y los atributos de seguridad que se asignan a los perfiles de derechos se almacenan en la base de datos `exec_attr`. Para obtener más información, consulte [“Base de datos exec\\_attr” en la página 249](#). Los campos de la base de datos `prof_attr` están separados por dos puntos, de la siguiente forma:

`profname:res1:res2:desc:attr`

Los campos tienen los siguientes significados:

`profname`      Nombre del perfil de derechos. Los nombres de perfiles de derechos distinguen mayúsculas de minúsculas. Este nombre también se utiliza en la base de datos `user_attr` para indicar los perfiles asignados a roles y usuarios.

`res1:res2`      Reservado para uso futuro.

`desc`            Descripción larga. Este campo debe explicar la finalidad del perfil de derechos, incluido qué tipo de usuario estaría interesado en utilizar el perfil. La descripción larga debe ser adecuada para su visualización en el texto de ayuda de una aplicación.

`attr`            Lista opcional de pares de clave y valor separados por punto y coma (;) que describe los atributos de seguridad que se aplicarán al objeto en la ejecución. Es posible especificar cero claves o más. Las claves válidas son `help`, `profiles` y `auths`.

La palabra clave `help` identifica un archivo de ayuda en HTML. Es posible acceder a los archivos de ayuda desde el archivo `index.html` del directorio `/usr/lib/help/profiles/locale/C`.

La palabra clave `profiles` especifica una lista separada por comas de perfiles de derechos. Estos perfiles se denominan *perfiles de derechos complementarios*.

La palabra clave `auths` especifica una lista separada por comas de nombres de autorizaciones que se eligen de los nombres definidos en la base de datos `auth_attr`. Los nombres de autorizaciones se pueden especificar con un asterisco (\*) como carácter comodín.

La palabra clave `privs` especifica una lista separada por comas de privilegios. Estos privilegios están vigentes para todos los comandos en un shell de perfil.



El siguiente ejemplo muestra dos entradas típicas de la base de datos `prof_attr`. Tenga en cuenta que el perfil de derechos de gestión de impresoras es un perfil de derechos complementario del perfil de derechos de operador. El texto del ejemplo se ajustó con fines de visualización.

```
% grep 'Printer Management' /etc/security/prof_attr
Printer Management:::                               Name of rights profile
Manage printers, daemons, spooling:                 Description
help=RtPrntAdmin.html;                               Help file
auths=solaris.admin.printer.read,                    Authorizations
solaris.admin.printer.modify,solaris.admin.printer.delete
...
Operator:::                                           Name of rights profile
Can perform simple administrative tasks:             Description
profiles=Printer Management,                        Supplementary rights profiles
Media Backup,All;
help=RtOperator.html                                Help file
```

## Base de datos `exec_attr`

La base de datos `exec_attr` define los comandos que requieren atributos de seguridad para ejecutarse correctamente. Los comandos forman parte de un perfil de derechos. Un comando con sus atributos de seguridad puede ser ejecutado por los roles o usuarios a los que se asignó el perfil.

Los campos de la base de datos `exec_attr` están separados por dos puntos, de la siguiente forma:

```
name:policy:type:res1:res2:id:attr
```

Los campos tienen los siguientes significados:

profname	Nombre del perfil de derechos. Los nombres de perfiles de derechos distinguen mayúsculas de minúsculas. El nombre hace referencia a un perfil en la base de datos <code>prof_attr</code> .
policy	Política de seguridad asociada a esta entrada. Actualmente, <code>suser</code> y <code>solaris</code> son las entradas válidas. La política <code>solaris</code> reconoce privilegios. La política <code>suser</code> no.
type	Tipo de entidad que se especifica. Actualmente, el único tipo de entidad válido es <code>cmd</code> (comando).
res1:res2	Reservado para uso futuro.

**id** Cadena que identifica la entidad. Los comandos deben tener la ruta completa o una ruta con un carácter comodín (\*). Para especificar argumentos, escriba una secuencia de comandos con los argumentos y señale el **id** en la secuencia de comandos.

**attr** Lista opcional de pares de clave y valor separados por punto y coma (;) que describe los atributos de seguridad que se aplicarán a la entidad en la ejecución. Es posible especificar cero claves o más. La lista de palabras clave válidas depende de la política aplicada.

Para la política **suser**, las cuatro claves válidas son **euid**, **uid**, **egid** y **gid**.

- Las palabras clave **euid** y **uid** contienen un nombre de usuario único o un ID de usuario numérico (UID). Los comandos diseñados con **euid** se ejecutan con el UID proporcionado, un proceso similar a la definición del bit **setuid** en un archivo ejecutable. Los comandos diseñados con **uid** se ejecutan con el UID real y el UID efectivo.
- Las palabras clave **egid** y **gid** contienen un nombre de grupo único o un ID de grupo numérico (GID). Los comandos diseñados con **egid** se ejecutan con el GID proporcionado, un proceso similar a la definición del bit **setgid** en un archivo ejecutable. Los comandos diseñados con **gid** se ejecutan con el GID real y el GID efectivo.

Para la política **solaris**, la palabra clave válida es **privs**. El valor consta de una lista de privilegios separados por comas.

El siguiente ejemplo muestra algunos valores típicos de una base de datos **exec\_attr**:

```
% grep 'File System Management' /etc/security/exec_attr
File System Management:suser:cmd::/usr/sbin/ff:euid=0
File System Management:solaris:cmd::/usr/sbin/mount:privs=sys_mount
...
```

## Archivo **policy.conf**

El archivo **policy.conf** ofrece una manera de otorgar perfiles de derechos específicos, autorizaciones específicas y privilegios específicos a todos los usuarios. Las entradas pertinentes del archivo constan de pares *clave=valor*:

- **AUTHS\_GRANTED=autorizaciones**: hace referencia a una o varias autorizaciones.
- **PROFS\_GRANTED=perfiles de derechos**: hace referencia a uno o varios perfiles de derechos.
- **PRIV\_DEFAULT=privilegios**: hace referencia a uno o varios privilegios.
- **PRIV\_LIMIT=privilegios**: hace referencia a todos los privilegios.

El siguiente ejemplo muestra algunos valores típicos de una base de datos **policy.conf**:

```
# grep AUTHS /etc/security/policy
AUTHS_GRANTED=solaris.device.cdrw
```

```
# grep PROFS /etc/security/policy
PROFS_GRANTED=Basic Solaris User
```

```
# grep PRIV /etc/security/policy
```

```
#PRIV_DEFAULT=basic
```

```
#PRIV_LIMIT=all
```

Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#).

## Comandos de RBAC

Esta sección muestra los comandos que se utilizan para administrar RBAC. También se incluye una tabla de los comandos cuyo acceso se puede controlar mediante autorizaciones.

### Comandos que gestionan RBAC

Aunque es posible editar las bases de datos locales de RBAC manualmente, no se recomienda en absoluto hacerlo. Los siguientes comandos están disponibles para gestionar el acceso a tareas con RBAC.

TABLA 10-7 Comandos de administración de RBAC

Página del comando man	Descripción
<a href="#">auths(1)</a>	Muestra las autorizaciones de un usuario.
<a href="#">makedbm(1M)</a>	Genera un archivo dbm.
<a href="#">nscd(1M)</a>	Daemon de antememoria de servicio de nombres, útil para el almacenamiento en la antememoria de las bases de datos <code>user_attr</code> , <code>prof_attr</code> y <code>exec_attr</code> . Utilice el comando <code>svcadm</code> para reiniciar el daemon.
<a href="#">pam_roles(5)</a>	Módulo de gestión de cuentas de rol para PAM. Comprueba la autorización para asumir el rol.
<a href="#">pfexec(1)</a>	Utilizado por los shells de perfil para ejecutar los comandos con atributos de seguridad especificados en la base de datos <code>exec_attr</code> .
<a href="#">policy.conf(4)</a>	Archivo de configuración para la política de seguridad del sistema. Enumera las autorizaciones otorgadas, los privilegios concedidos y otra información de seguridad.
<a href="#">profiles(1)</a>	Muestra perfiles de derechos para un usuario determinado.

TABLA 10-7 Comandos de administración de RBAC (Continuación)

Página del comando man	Descripción
<a href="#">roles(1)</a>	Muestra los roles que un usuario específico puede asumir.
<a href="#">roleadd(1M)</a>	Agrega un rol a un sistema local.
<a href="#">roledel(1M)</a>	Elimina un rol de un sistema local.
<a href="#">rolemod(1M)</a>	Modifica las propiedades de un rol en un sistema local.
<a href="#">smattrpop(1M)</a>	Fusiona la base de datos de atributos de seguridad de origen en la base de datos de destino. Para utilizar en situaciones en las que las bases de datos locales se deben fusionar en un servicio de nombres. También para usar en actualizaciones donde no se proporcionan secuencias de comandos de conversión.
<a href="#">smexec(1M)</a>	Gestiona entradas en la base de datos <code>exec_attr</code> . Requiere autenticación.
<a href="#">smmultiuser(1M)</a>	Gestiona operaciones masivas en las cuentas de usuario. Requiere autenticación.
<a href="#">smprofile(1M)</a>	Gestiona perfiles de derechos en las bases de datos <code>prof_attr</code> y <code>exec_attr</code> . Requiere autenticación.
<a href="#">smrole(1M)</a>	Gestiona roles y usuarios en las cuentas de rol. Requiere autenticación.
<a href="#">smuser(1M)</a>	Gestiona entradas de usuario. Requiere autenticación.
<a href="#">useradd(1M)</a>	Agrega una cuenta de usuario al sistema. La opción <code>-R</code> asigna un rol a la cuenta de un usuario.
<a href="#">userdel(1M)</a>	Elimina el inicio de sesión de un usuario del sistema.
<a href="#">usermod(1M)</a>	Modifica las propiedades de la cuenta de un usuario en el sistema.

## Comandos que requieren autorizaciones

La siguiente tabla proporciona ejemplos acerca de cómo las autorizaciones se utilizan para limitar las opciones de comandos en un sistema Oracle Solaris. Para ver una explicación más detallada de las autorizaciones, consulte [“Denominación y delegación de autorizaciones” en la página 242](#).

TABLA 10-8 Comandos y autorizaciones asociadas

Página del comando man	Requisitos de autorización
<a href="#">at(1)</a>	<code>solaris.jobs.user</code> se requiere para todas las opciones (cuando no existen los archivos <code>at.allow</code> ni <code>at.deny</code> ).
<a href="#">atq(1)</a>	<code>solaris.jobs.admin</code> se requiere para todas las opciones.
<a href="#">cdrw(1)</a>	<code>solaris.device.cdrw</code> se requiere para todas las opciones y se otorga de manera predeterminada en el archivo <code>policy.conf</code> .

TABLA 10–8 Comandos y autorizaciones asociadas (Continuación)

Página del comando man	Requisitos de autorización
<code>crontab(1)</code>	<code>solaris.jobs.user</code> se requiere para la opción que permite ejecutar un trabajo (cuando no existen los archivos <code>crontab.allow</code> ni <code>crontab.deny</code> ).  <code>solaris.jobs.admin</code> se requiere para las opciones que permiten mostrar o modificar los archivos <code>crontab</code> de otros usuarios.
<code>allocate(1)</code>	<code>solaris.device.allocate</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code> ) se requiere para asignar un dispositivo.  <code>solaris.device.revoke</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code> ) se requiere para asignar un dispositivo a otro usuario (opción <code>-F</code> ).
<code>deallocate(1)</code>	<code>solaris.device.allocate</code> (u otra autorización, según se especifique en el archivo <code>device_allocate</code> ) se requiere para desasignar el dispositivo de otro usuario.  <code>solaris.device.revoke</code> (u otra autorización, según se especifique en <code>device_allocate</code> ) se requiere para forzar la desasignación del dispositivo especificado (opción <code>-F</code> ) o de todos los dispositivos (opción <code>-I</code> ).
<code>list_devices(1)</code>	<code>solaris.device.revoke</code> se requiere para mostrar los dispositivos de otro usuario (opción <code>-U</code> ).
<code>sendmail(1M)</code>	<code>solaris.mail</code> se requiere para acceder a las funciones del subsistema de correo; <code>solaris.mail.mailq</code> se requiere para ver la cola de correo.



# Privilegios (tareas)

Este capítulo proporciona instrucciones paso a paso para la gestión de privilegios y el uso de privilegios en el sistema. A continuación, se presenta la información que se incluye en este capítulo.

- “Gestión y uso de privilegios (mapa de tareas)” en la página 255
- “Gestión de privilegios (mapa de tareas)” en la página 256
- “Determinación de los privilegios (mapa de tareas)” en la página 264

Para obtener una descripción general de los privilegios, consulte “Privilegios (descripción general)” en la página 193. Para obtener información de referencia, consulte el Capítulo 12, “Privilegios (referencia)”.

## Gestión y uso de privilegios (mapa de tareas)

El siguiente mapa de tareas hace referencia a los mapas de tareas para la gestión de privilegios y el uso de privilegios.

Tarea	Descripción	Para obtener instrucciones
Usar privilegios en su sitio	Implica asignar, eliminar, agregar y depurar el uso de privilegios.	“Gestión de privilegios (mapa de tareas)” en la página 256
Usar privilegios al ejecutar un comando	Implica usar los privilegios que se le asignaron.	“Determinación de los privilegios (mapa de tareas)” en la página 264

# Gestión de privilegios (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para ver privilegios, asignar privilegios y ejecutar una secuencia de comandos que contiene comandos con privilegios.

Tarea	Descripción	Para obtener instrucciones
Determinar los privilegios que hay en un proceso	Muestra el conjunto vigente, heredable, permitido y límite de privilegios de un proceso.	<a href="#">“Cómo determinar los privilegios de un proceso” en la página 256</a>
Determinar los privilegios que faltan en un proceso	Muestra los privilegios que un proceso con errores necesita para ejecutarse correctamente.	<a href="#">“Cómo determinar los privilegios que necesita un programa” en la página 258</a>
Agregar privilegios a un comando	Agrega privilegios a un comando en un perfil de derechos. El perfil de derechos se puede asignar a usuarios o roles. Los usuarios luego pueden ejecutar el comando con los privilegios asignados en un shell de perfil.	<a href="#">“Cómo agregar privilegios a un comando” en la página 260</a>
Asignar privilegios a un usuario	Amplía el conjunto heredable de privilegios de un usuario o rol. Utilice este procedimiento con precaución.	<a href="#">“Cómo asignar privilegios a un usuario o rol” en la página 260</a>
Restringir los privilegios de un usuario	Limita el conjunto básico de privilegios del usuario. Utilice este procedimiento con precaución.	<a href="#">“Cómo limitar los privilegios de un usuario o rol” en la página 261</a>
Ejecutar una secuencia de comandos de shell con privilegios	Agrega privilegios a una secuencia de comandos de shell y a los comandos de la secuencia de comandos de shell. A continuación, ejecuta la secuencia de comandos en un shell de perfil.	<a href="#">“Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios” en la página 263</a>

## Gestión de privilegios

La forma más segura de gestionar privilegios para usuarios y roles es limitar el uso del privilegio a los comandos de un perfil de derechos. El perfil de derechos se incluye luego en un rol. Se asigna el rol a un usuario. Cuando el usuario asume el rol asignado, los comandos con privilegios están disponibles para su ejecución en un shell de perfil. Los siguientes procedimientos muestran cómo asignar privilegios, eliminar privilegios y depurar el uso de privilegios.

### ▼ Cómo determinar los privilegios de un proceso

Este procedimiento muestra cómo determinar los privilegios que están disponibles para los procesos. La lista no incluye privilegios que se asignaron a comandos específicos.



- **Enumere los privilegios que están disponibles para el proceso del shell.**

```
% ppriv pid
$ ppriv -v pid
```

*pid* El número de proceso. Utilice un signo de dólar doble (\$\$) para transferir el número de proceso del shell principal al comando.

-v Proporciona una lista detallada de los nombres de privilegios.

### Ejemplo 11–1 Determinación de los privilegios en el shell actual

En el siguiente ejemplo, se enumeran los privilegios del proceso principal del shell del usuario. En el segundo ejemplo, se enumeran los nombres completos de los privilegios. Las letras individuales que se visualizan hacen referencia a los siguientes conjuntos de privilegios:

E El conjunto vigente de privilegios.

I El conjunto heredable de privilegios.

P El conjunto permitido de privilegios.

L El conjunto límite de privilegios.

```
% ppriv $$
1200: -csh
flags = <none>
      E: basic
      I: basic
      P: basic
      L: all
% ppriv -v $$
1200: -csh
flags = <none>
      E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

### Ejemplo 11–2 Determinación de los privilegios de un rol que puede asumir

Los roles utilizan un shell administrativo o shell de perfil. Debe asumir un rol y utilizar el shell del rol para enumerar los privilegios que se asignaron directamente al rol. En el siguiente ejemplo, el rol sysadmin no tiene privilegios asignados directamente.

```
% su - sysadmin
Password: <Type sysadmin password>
$ /usr/ucb/whoami
sysadmin
$ ppriv -v $$
1400: pfksh
flags = <none>
```

```
E: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
I: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
P: file_link_any,net_access,proc_exec,proc_fork,proc_info,proc_session
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

## ▼ Cómo determinar los privilegios que necesita un programa

Este procedimiento determina los privilegios que necesita un comando o proceso para ejecutarse correctamente.

### Antes de empezar

El comando o proceso debe haber fallado para que este procedimiento funcione.

#### 1 Escriba el comando con errores como un argumento del comando de depuración `ppriv`.

```
% ppriv -eD touch /etc/acct/yearly
touch[11365]: missing privilege "file_dac_write"
      (euid = 130, syscall = 224) needed at ufs_direnter_cm+0x27c
touch: /etc/acct/yearly cannot create
```

#### 2 Para determinar qué llamada del sistema falla, busque el número `syscall` en el archivo `/etc/name_to_sysnum`.

```
% grep 224 /etc/name_to_sysnum
creat64          224
```

### Ejemplo 11-3 Utilización del comando `truss` para examinar el uso de privilegios

El comando `truss` puede depurar el uso de privilegios en un shell común. Por ejemplo, el siguiente comando depura el proceso con errores `touch`:

```
% truss -t creat touch /etc/acct/yearly
creat64("/etc/acct/yearly", 0666)
      Err#13 EACCES [file_dac_write]
touch: /etc/acct/yearly cannot create
```

Las interfaces ampliadas `/proc` informan el privilegio faltante después del código de error en la salida del comando `truss`.

### Ejemplo 11-4 Utilización del comando `ppriv` para examinar el uso de privilegios en un shell de perfil

El comando `ppriv` puede depurar el uso de privilegios en un shell de perfil. Si asigna un perfil de derechos a un usuario y el perfil de derechos incluye comandos con privilegios, los comandos se

deben escribir en un shell de perfil. Cuando los comandos con privilegios se escriben un shell común, los comandos no se ejecutan con privilegios.

En este ejemplo, el usuario `jdoe` puede asumir el rol `objadmin`. El rol `objadmin` incluye el perfil de derechos de gestión del acceso a objetos. Este perfil de derechos permite al rol `objadmin` cambiar permisos en archivos que no son propiedad de `objadmin`.

En el fragmento siguiente, `jdoe` no puede cambiar los permisos en el archivo `useful.script`:

```
jdoe% ls -l useful.script
-rw-r--r-- 1 aloe staff 2303 Apr 10 10:10 useful.script
jdoe% chown objadmin useful.script
chown: useful.script: Not owner
jdoe% ppriv -eD chown objadmin useful.script
chown[11444]: missing privilege "file_chown"
(euid = 130, syscall = 16) needed at ufs_setattr+0x258
chown: useful.script: Not owner
```

Cuando `jdoe` asume el rol `objadmin`, se modifican los permisos en el archivo:

```
jdoe% su - objadmin
Password: <Type objadmin password>
$ ls -l useful.script
-rw-r--r-- 1 aloe staff 2303 Apr 10 10:10 useful.script
$ chown objadmin useful.script
$ ls -l useful.script
-rw-r--r-- 1 objadmin staff 2303 Apr 10 10:10 useful.script
$ chgrp admin useful.script
$ ls -l objadmin.script
-rw-r--r-- 1 objadmin admin 2303 Apr 10 10:11 useful.script
```

### Ejemplo 11-5 Modificación de un archivo que es propiedad del usuario root

Este ejemplo ilustra la protección contra la escalada de privilegios. Para ver una explicación, consulte [“Cómo evitar la escalada de privilegios” en la página 274](#). El archivo es propiedad del usuario `root`. El rol menos poderoso, el rol `objadmin`, necesita todos los privilegios para cambiar la propiedad del archivo, por lo que la operación no se ejecuta correctamente.

```
jdoe% su - objadmin
Password: <Type objadmin password>
$ cd /etc; ls -l system
-rw-r--r-- 1 root sys 1883 Oct 10 10:20 system
$ chown objadmin system
chown: system: Not owner
$ ppriv -eD chown objadmin system
chown[11481]: missing privilege "ALL"
(euid = 101, syscall = 16) needed at ufs_setattr+0x258
chown: system: Not owner
```

## ▼ Cómo agregar privilegios a un comando

Se agregan privilegios a un comando al agregar el comando a un perfil de derechos. Los privilegios permiten al rol que incluye el perfil de derechos ejecutar el comando administrativo, sin obtener otras capacidades de superusuario.

**Antes de empezar** El comando o programa debe reconocer privilegios. Para obtener una explicación más detallada, consulte [“Cómo obtienen privilegios los procesos” en la página 198.](#)

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204.](#)

### 2 Abra la interfaz gráfica de usuario de Solaris Management Console.

Para obtener instrucciones, consulte [“Cómo asumir un rol en Solaris Management Console” en la página 222.](#)

### 3 Utilice la herramienta Rights para actualizar un perfil adecuado.

Seleccione el comando que desea incluir. Para cada comando incluido, agregue los privilegios que necesita el comando.



**Precaución** – Al incluir comandos en un perfil de derechos y agregar privilegios a los comandos, los comandos se ejecutan con esos privilegios cuando se ejecutan en un shell de perfil.

El orden de los perfiles es importante. El shell de perfil ejecuta un comando o una acción con los atributos de seguridad especificados en el primer perfil de la lista de perfiles de la cuenta. Por ejemplo, si el comando `chgrp` está en el perfil de derechos de gestión del acceso a objetos con privilegios y la gestión del acceso a objetos es el primer perfil en el que se encuentra el comando `chgrp`, el comando `chgrp` se ejecuta con los privilegios especificados en el perfil de gestión del acceso a objetos.

---

## ▼ Cómo asignar privilegios a un usuario o rol

Puede confiar un determinado privilegio a ciertos usuarios en todo momento. Los privilegios muy específicos que afectan una pequeña parte del sistema son buenos candidatos para asignar a un usuario. Para ver una explicación de las consecuencias de los privilegios asignados directamente, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 192.](#)

El siguiente procedimiento permite al usuario `j doe` usar temporizadores de alta resolución.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Agregue el privilegio que afecta los temporizadores de alta resolución al conjunto heredable inicial de privilegios del usuario.**

```
$ usermod -K defaultpriv=basic,proc_clock_highres jdoe
```

Los valores de la palabra clave `defaultpriv` reemplazan los valores existentes. Por lo tanto, para que el usuario conserve los privilegios básicos, se debe especificar el valor `basic`. En la configuración predeterminada, todos los usuarios tienen privilegios básicos.

**3 Lea la entrada `user_attr` resultante.**

```
$ grep jdoe /etc/user_attr
jdoe:::type=normal;defaultpriv=basic,proc_clock_highres
```

**Ejemplo 11–6 Creación de un rol con privilegios para configurar la hora del sistema**

En este ejemplo, se crea un rol cuya única tarea es controlar la hora del sistema.

```
$ /usr/sadm/bin/smrole -D nisplus:/examplehost/example.domain \
-r primaryadm -l <Type primaryadm password> \
add -- -n clockmgr \
-c "Role that sets system time" \
-F "Clock Manager" \
-s /bin/pfcksh \
-u 108 \
-P <Type clockmgr password> \
-K defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

El texto de la línea `-K` se ajustó con fines de visualización.

Si el rol se creó de manera local, la entrada `user_attr` del rol tendría un aspecto similar al siguiente:

```
clockmgr:::Role that sets system time:
type=role;defaultpriv=basic,proc_priocntl,sys_cpu_config,
proc_clock_highres,sys_time
```

**▼ Cómo limitar los privilegios de un usuario o rol**

Para limitar los privilegios que están disponibles para un usuario o rol, reduzca el conjunto básico o el conjunto límite. Debe tener un buen motivo para limitar los privilegios del usuario de esta manera, porque las limitaciones pueden tener efectos secundarios no deseados.



**Precaución** – Debe probar exhaustivamente las capacidades en las que el conjunto básico o el conjunto límite se han modificado para un usuario.

- Cuando el conjunto básico es inferior a la configuración predeterminada, es posible que se les impida utilizar el sistema a los usuarios.
- Cuando el conjunto límite es inferior a todos los privilegios, es posible que fallen los procesos que deben ejecutarse con un `UID=0` efectivo.

---

**1 Determine los privilegios del conjunto básico y el conjunto límite de un usuario.**

Para conocer el procedimiento, consulte “[Cómo determinar los privilegios de un proceso](#)” en la [página 256](#).

**2 (Opcional) Elimine uno de los privilegios del conjunto básico.**

```
$ usermod -K defaultpriv=basic,!priv-name username
```

Con la eliminación del privilegio `proc_session`, se impide que el usuario examine cualquier proceso que se encuentre fuera de su sesión actual. Con la eliminación del privilegio `file_link_any`, se impide que el usuario establezca enlaces físicos con archivos que no sean de su propiedad.



**Precaución** – No elimine los privilegios `proc_fork` o `proc_exec`. Sin estos privilegios, el usuario no podrá utilizar el sistema. De hecho, estos dos privilegios sólo se deben eliminar de los daemons que no necesitan ejecutar `fork()` o `exec()` para otros procesos.

---

**3 (Opcional) Elimine uno de los privilegios del conjunto límite.**

```
$ usermod -K limitpriv=all,!priv-name username
```

**4 Prueba las capacidades de *nombre\_usuario*.**

Inicie sesión como *nombre\_usuario* e intenta realizar las tareas que *nombre\_usuario* debe realizar en el sistema.

### **Ejemplo 11-7 Eliminación de privilegios del conjunto límite de un usuario**

En el siguiente ejemplo, a todas las sesiones que se originan a partir del inicio de sesión inicial de `jdoe` se les impide utilizar el privilegio `sys_linkdir`. Es decir, el usuario no puede establecer enlaces físicos a directorios ni anular el enlace a directorios, incluso después de ejecutar el comando `su`.

```
$ usermod -K limitpriv=all,!sys_linkdir jdoe
$ grep jdoe /etc/user_attr
jdoe:::type=normal;defaultpriv=basic;limitpriv=all,!sys_linkdir
```

### Ejemplo 11–8 Eliminación de privilegios del conjunto básico de un usuario

En el siguiente ejemplo, a todas las sesiones que se originan a partir del inicio de sesión inicial de `jdoe` se le impide utilizar el privilegio `proc_session`. Es decir, el usuario no puede examinar ningún proceso que se encuentre fuera de su sesión, incluso después de ejecutar el comando `su`.

```
$ usermod -K defaultpriv=basic,!proc_session jdoe

$ grep jdoe /etc/user_attr
jdoe:::type=normal;defaultpriv=basic,!proc_session;limitpriv=all
```

## ▼ Cómo ejecutar una secuencia de comandos de shell con comandos con privilegios

**Nota** – Al crear una secuencia de comandos de shell que ejecuta comandos con privilegios heredados, el perfil de derechos adecuado debe contener los comandos con privilegios asignados a ellos.

- 1 **Inicie la secuencia de comandos con `/bin/pfsh`, o cualquier otro shell de perfil, en la primera línea.**

```
#!/bin/pfsh
# Copyright (c) 2009, 2011 by Oracle Corporation
```

- 2 **Determine los privilegios que necesitan los comandos de la secuencia de comandos.**

```
% ppriv -eD script-full-path
```

- 3 **Abra la interfaz gráfica de usuario de Solaris Management Console.**

Para obtener instrucciones, consulte [“Cómo asumir un rol en Solaris Management Console” en la página 222](#). Seleccione un rol, por ejemplo, administrador principal, que pueda crear un perfil de derechos.

- 4 **Utilice la herramienta Rights para crear o actualizar un perfil adecuado.**

Seleccione la secuencia de comandos e incluya en el perfil de derechos cada uno de los comandos de la secuencia de comandos de shell que necesitan privilegios para ejecutarse. Para cada comando incluido, agregue los privilegios que necesita el comando.



**Precaución** – El orden de los perfiles de derechos es importante. El shell de perfil ejecuta la primera instancia de un comando en la lista de perfiles. Por ejemplo, si el comando `chgrp` está en el perfil de derechos de gestión del acceso a objetos y la gestión del acceso a objetos es el primer perfil en el que se encuentra el comando `chgrp`, el comando `chgrp` se ejecuta con los privilegios especificados en el perfil de gestión del acceso a objetos.

- 5 **Agregue el perfil de derechos a un rol y asigne el rol a un usuario.**
- Para ejecutar el perfil, el usuario asume el rol y ejecuta la secuencia de comandos en el shell de perfil del rol.

## Determinación de los privilegios (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para usar los privilegios que se le asignaron.

Tarea	Descripción	Para obtener instrucciones
Ver los privilegios como usuario en cualquier shell	Muestra los privilegios que se le asignaron directamente. Todos sus procesos se ejecutan con estos privilegios.	<a href="#">“Cómo determinar los privilegios que se le asignaron directamente” en la página 265</a>
Determinar qué comandos puede ejecutar con privilegios	Cuando se asignan privilegios a archivos ejecutables en un perfil de derechos, el archivo ejecutable se debe escribir en un shell de perfil.	<a href="#">“Cómo determinar los comandos con privilegios que puede ejecutar” en la página 266</a>
Determinar qué comandos un rol puede ejecutar con privilegios	Permite asumir el rol para determinar qué comandos el rol puede ejecutar con privilegios.	<a href="#">“Cómo determinar los comandos con privilegios que puede ejecutar un rol” en la página 267</a>

## Determinación de los privilegios asignados

Cuando se asignan privilegios directamente a un usuario, los privilegios están en vigor en cada shell. Cuando no se asignan privilegios directamente a un usuario, el usuario debe abrir un shell de perfil. Por ejemplo, cuando hay comandos con privilegios asignados en un perfil de derechos que está en la lista de perfiles de derechos del usuario, el usuario debe ejecutar el comando en un shell de perfil.



## ▼ Cómo determinar los privilegios que se le asignaron directamente

El siguiente procedimiento muestra cómo determinar si se le asignaron privilegios directamente.



**Precaución** – El uso inadecuado de los privilegios asignados directamente puede generar infracciones de seguridad involuntarias. Para ver una explicación, consulte [“Consideraciones de seguridad al asignar directamente atributos de seguridad” en la página 192.](#)

### 1 Enumere los privilegios que los procesos pueden utilizar.

Consulte [“Cómo determinar los privilegios de un proceso” en la página 256](#) para conocer el procedimiento.

### 2 Invoque acciones y ejecute comandos en cualquier shell.

Los privilegios que se muestran en el conjunto vigente están en vigor a lo largo de la sesión. Si se le asignaron privilegios directamente además del conjunto básico, los privilegios se muestran en el conjunto vigente.

#### Ejemplo 11–9 Determinación de los privilegios asignados directamente

Si se le asignaron privilegios directamente, su conjunto básico contiene más privilegios que el conjunto básico predeterminado. En este ejemplo, el usuario siempre tiene acceso al privilegio `proc_clock_highres`.

```
% /usr/ucb/whoami
jdoe
% ppriv -v $$
1800: pfksh
flags = <none>
      E: file_link_any,...,proc_clock_highres,proc_session
      I: file_link_any,...,proc_clock_highres,proc_session
      P: file_link_any,...,proc_clock_highres,proc_session
      L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
% ppriv -vl proc_clock_highres
      Allows a process to use high resolution timers.
```

#### Ejemplo 11–10 Determinación de los privilegios asignados directamente de un rol

Los roles utilizan un shell administrativo o shell de perfil. Los usuarios que asumen un rol pueden utilizar el shell del rol para enumerar los privilegios que se asignaron directamente al rol. En el siguiente ejemplo, al rol `realtime` se le asignaron privilegios directamente para gestionar los programas relacionados con la fecha y hora.

```
% su - realtime
Password: <Type realtime password>
$ /usr/ucb/whoami
realtime
$ ppriv -v $$
1600: pfksh
flags = <none>
E: file_link_any,...,proc_clock_highres,proc_session,sys_time
I: file_link_any,...,proc_clock_highres,proc_session,sys_time
P: file_link_any,...,proc_clock_highres,proc_session,sys_time
L: cpc_cpu,dtrace_kernel,dtrace_proc,dtrace_user,...,sys_time
```

## ▼ Cómo determinar los comandos con privilegios que puede ejecutar

Cuando no se asignan privilegios directamente a un usuario, el usuario obtiene acceso a comandos con privilegios a través de un perfil de derechos. Los comandos de un perfil de derechos se deben ejecutar en un shell de perfil.

**Antes de empezar** El usuario o el rol que se autentica en Solaris Management Console deben tener la autorización `solaris.admin.usermgr.read`. El perfil de derechos de usuario de Solaris básico incluye esta autorización.

### 1 Determine los perfiles de derechos que se le asignaron.

```
$ /usr/sadm/bin/smuser list -- -n username -l
```

```
Authenticating as user: admin
... Please enter a string value for: password ::
...
User name:      username
User ID (UID):  130
Primary group:  staff
Secondary groups:
Comment: object mgt jobs
Login Shell:    /bin/sh
Home dir server: system
Home directory: /export/home/username
AutoHome setup: True
Mail server:    system
Rights: Object Access Management
Assigned Roles:
```

### 2 Ubique la línea que comienza con “Rights:”.

La línea “Rights” muestra los nombres de los perfiles de derechos que se le asignaron directamente.

**3 Busque los nombres de los perfiles de derechos en la base de datos `exec_attr`.**

```
$ cd /etc/security
$ grep "Object Access Management" exec_attr
Object Access Management:solaris:cmd:::/usr/bin/chgrp:privs=file_chown
Object Access Management:solaris:cmd:::/usr/bin/chown:privs=file_chown
Object Access Management:suser:cmd:::/usr/bin/chgrp:euid=0
Object Access Management:suser:cmd:::/usr/bin/chmod:euid=0
...
```

Los comandos con privilegios agregados se muestran al final de las entradas de política solaris.

**4 Escriba los comandos que necesitan privilegios en un shell de perfil.**

Cuando los comandos se escriben un shell común, los comandos no se ejecutan con privilegios y no finalizan correctamente.

```
% pfsh
$
```

**Ejemplo 11–11 Ejecución de comandos con privilegios en un shell de perfil**

En el siguiente ejemplo, el usuario `jdoe` no puede cambiar los permisos de grupo en un archivo desde su shell común. Sin embargo, `jdoe` puede cambiar los permisos cuando escribe el comando en un shell de perfil.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 nodoe eng 262 Apr 2 10:52 useful.script
chgrp staff useful.script
chgrp: useful.script: Not owner
% pfksh
$ /usr/ucb/whoami
jdoe
$ chgrp staff useful.script
$ chown jdoe useful.script
$ ls -l useful.script
-rwxr-xr-- 1 jdoe staff 262 Apr 2 10:53 useful.script
```

## ▼ **Cómo determinar los comandos con privilegios que puede ejecutar un rol**

Un rol obtiene acceso a comandos con privilegios a través de un perfil de derechos que contiene comandos con privilegios asignados. La forma más segura de proporcionar a un usuario acceso a comandos con privilegios es asignarles un rol. Después de asumir el rol, el usuario puede ejecutar todos los comandos con privilegios que se incluyen en los perfiles de derechos para dicho rol.

**Antes de empezar** El usuario o el rol que se autentica en Solaris Management Console deben tener la autorización `solaris.admin.usermgr.read`. El perfil de derechos de usuario de Solaris básico incluye esta autorización.

**1 Determine los roles que puede asumir.**

```
$ /usr/sadm/bin/smuser list -- -n username -l
Authenticating as user: primadmin
...
User name:      username
User ID (UID):  110
Primary group:  staff
Secondary groups:
Comment: Has admin roles
Login Shell:    /bin/sh
...
Rights:
Assigned Roles: primadmin, admin
```

**2 Ubique la línea que comienza con “Assigned Roles:”.**

La línea “Assigned Roles” muestra los roles que puede asumir.

**3 Determine los perfiles de derechos que se incluyen en uno de sus roles.**

```
% su - devadmin
Enter password:      Type devadmin password
$ whoami
devadmin
$ profiles
Device Security

$ /usr/sadm/bin/smuser list -- -n admin -l
Authenticating as user: primadmin
...
User name:      admin
User ID (UID):  101
Primary group:  sysadmin
Secondary groups:
Comment: system administrator
Login Shell:    /bin/pfksh
...
Rights: System Administrator
Assigned Roles:
```

**4 Ubique los nombres de los perfiles de derechos para el rol en la línea “Rights:”.**

**5 Busque los perfiles de derechos en la base de datos `prof_attr`.**

Dado que el perfil de administrador del sistema representa una recopilación de perfiles, debe enumerar los perfiles en el perfil de administrador del sistema.

```
$ cd /etc/security
$ grep "System Administrator" prof_attr
System Administrator::Can perform most non-security administrative
```

```
tasks:profiles=Audit Review,Printer Management,Cron Management,
Device Management,File System Management,Mail Management,Maintenance
and Repair,Media Backup,Media Restore,Name Service Management,Network
Management,Object Access Management,Process Management,Software
Installation,User Management,All;help=RtSysAdmin.html
```

## 6 Para cada perfil de derechos, busque los perfiles de derechos en la base de datos `exec_attr`.

Por ejemplo, el perfil de gestión de la red es un perfil complementario del perfil de administrador del sistema. El perfil de gestión de la red incluye diferentes comandos con privilegios.

```
$ cd /etc/security
$ grep "Network Management" exec_attr
Network Management:solaris:cmd:::/usr/sbin/ifconfig:privs=sys_net_config
Network Management:solaris:cmd:::/usr/sbin/route:privs=sys_net_config
...
```

Los comandos y sus privilegios asignados son los dos últimos campos de las entradas de política `solaris`. Puede ejecutar estos comandos en un shell de perfil de su rol.

## Ejemplo 11–12 Ejecución de los comandos con privilegios en su rol

Cuando un usuario asume un rol, el shell se convierte en un shell de perfil. Por lo tanto, los comandos se ejecutan con los privilegios que se asignaron a los comandos. En el siguiente ejemplo, el rol `admin` puede cambiar los permisos en el archivo `useful.script`.

```
% whoami
jdoe
% ls -l useful.script
-rwxr-xr-- 1 elsee eng 262 Apr 2 10:52 useful.script
% chgrp admin useful.script
chgrp: useful.script: Not owner
% su - admin
Password: <Type admin password>
$ /usr/ucb/whoami
admin
$ chgrp admin useful.script
$ chown admin useful.script
$ ls -l useful.script
-rwxr-xr-- 1 admin admin 262 Apr 2 10:53 useful.script
```



## Privilegios (referencia)

A continuación, se muestra una lista de la información de referencia que se incluye en este capítulo:

- “Comandos administrativos para la gestión de privilegios” en la página 271
- “Archivos con información de privilegios” en la página 272
- “Privilegios y auditoría” en la página 273
- “Cómo evitar la escalada de privilegios” en la página 274
- “Aplicaciones antiguas y el modelo de privilegios” en la página 275

Para utilizar privilegios, consulte el [Capítulo 11, “Privilegios \(tareas\)”](#). Para obtener información general, consulte [“Privilegios \(descripción general\)” en la página 193](#).

## Comandos administrativos para la gestión de privilegios

La siguiente tabla muestra los comandos que están disponibles para gestionar privilegios.

TABLA 12-1 Comandos para la gestión de privilegios

Finalidad	Comando	Página del comando man
Examinar privilegios de proceso	<code>ppriv -v pid</code>	<a href="#">ppriv(1)</a>
Definir privilegios de proceso	<code>ppriv -s especificación</code>	
Enumerar los privilegios del sistema	<code>ppriv -l</code>	
Enumerar un privilegio y su descripción	<code>ppriv -lv privilegio</code>	
Depurar error en privilegio	<code>ppriv -eD operación con errores</code>	
Asignar privilegios a un usuario local nuevo	<code>useradd</code>	<a href="#">useradd(1M)</a>
Agregar privilegios a un usuario local existente	<code>usermod</code>	<a href="#">usermod(1M)</a>

TABLA 12-1 Comandos para la gestión de privilegios (Continuación)

Finalidad	Comando	Página del comando man
Asignar privilegios a un usuario en un servicio de nombres	smuser	<a href="#">smuser(1M)</a>
Asignar privilegios a un rol local nuevo	roleadd	<a href="#">roleadd(1M)</a>
Agregar privilegios a un rol local existente	rolemod	<a href="#">rolemod(1M)</a>
Asignar privilegios a un rol en un servicio de nombres	smrole	<a href="#">smrole(1M)</a>
Ver política de dispositivos	getdevpolicy	<a href="#">getdevpolicy(1M)</a>
Definir política de dispositivos	devfsadm	<a href="#">devfsadm(1M)</a>
Actualizar política de dispositivos en dispositivos abiertos	update_drv -p <i>controlador de política</i>	<a href="#">update_drv(1M)</a>
Agregar política de dispositivos a un dispositivo	add_drv -p <i>controlador de política</i>	<a href="#">add_drv(1M)</a>

La interfaz gráfica de usuario de Solaris Management Console es la herramienta preferida para asignar privilegios a comandos, usuarios y roles. Para obtener más información, consulte “[Cómo asumir un rol en Solaris Management Console](#)” en la [página 222](#).

## Archivos con información de privilegios

Los siguientes archivos contienen información sobre privilegios.

TABLA 12-2 Archivos que contienen información de privilegios

Archivo y página del comando man	Palabra clave	Descripción
<a href="#">/etc/security/policy.conf</a> <a href="#">policy.conf(4)</a>	PRIV_DEFAULT	Conjunto heredable de privilegios para el sistema
	PRIV_LIMIT	Conjunto límite de privilegios para el sistema



TABLA 12-2 Archivos que contienen información de privilegios (Continuación)

Archivo y página del comando man	Palabra clave	Descripción
/etc/user_attr <a href="#">user_attr(4)</a>	Palabra clave <code>privs</code> en entrada de usuario o de rol	Conjunto heredable de privilegios para un usuario o rol
	Palabra clave <code>defaultpriv</code> en entrada de usuario o de rol	
	El valor se suele definir en la interfaz gráfica de usuario de Solaris Management Console	Conjunto límite de privilegios para un usuario o rol
	Palabra clave <code>limitpriv</code> en entrada de usuario o de rol	
/etc/security/exec_attr <a href="#">exec_attr(4)</a>	Palabra clave <code>privs</code> en la entrada del perfil para el comando	Lista de privilegios asignados a un comando en un perfil de derechos
	La política para el comando debe ser <code>solaris</code>	
<code>syslog.conf</code> <a href="#">syslog.conf(4)</a>	Archivo de registro del sistema para mensajes de depuración	Registro de depuración de privilegios
	Ruta definida en la entrada <code>priv.debug</code>	

**Nota** – No edite las bases de datos `exec_attr` y `user_attr` directamente. Para administrar privilegios, utilice Solaris Management Console o comandos como `smuser`. Para obtener más información, consulte las páginas del comando man [smc\(1M\)](#) y [smuser\(1M\)](#). Para conocer los procedimientos, consulte “[Gestión de privilegios \(mapa de tareas\)](#)” en la página 256.

## Privilegios y auditoría

El uso de privilegios se puede auditar. Cada vez que un proceso utiliza un privilegio, el uso del privilegio se registra en la pista de auditoría, en el token de auditoría `upriv`. Cuando los nombres de privilegios forman parte del registro, se utiliza su representación textual. Los siguientes eventos de auditoría registran el uso del privilegio:

- **Evento de auditoría** `AUE_SETPPRIV`: el evento genera un registro de auditoría cuando se modifica un conjunto de privilegios. El evento de auditoría `AUE_SETPPRIV` está en la clase `pm`.
- **Evento de auditoría** `AUE_MODALLOCPRIV`: el evento de auditoría genera un registro de auditoría cuando se agrega un privilegio desde afuera del núcleo. El evento de auditoría `AUE_MODALLOCPRIV` está en la clase `ad`.
- **Evento de auditoría** `AUE_MODDEVPLCY`: el evento de auditoría genera un registro de auditoría cuando se modifica la política de dispositivos. El evento de auditoría `AUE_MODDEVPLCY` está en la clase `ad`.

- **Evento de auditoría** `AUE_prof_cmd`: el evento de auditoría genera un registro de auditoría cuando se ejecuta un comando en un shell de perfil. El evento de auditoría `AUE_prof_cmd` está en las clases de auditoría `as` y `ua`. Los nombres de los privilegios se incluyen en el registro de auditoría.

El uso correcto de privilegios que se encuentran en el conjunto básico no se audita. El intento de utilizar un privilegio básico que se eliminó del conjunto básico de un usuario se audita.

## Cómo evitar la escalada de privilegios

El núcleo de Oracle Solaris impide la *escalada de privilegios*. La escalada de privilegios se produce cuando un privilegio permite a un proceso realizar más tareas de las que debe hacer. Para evitar que un proceso obtenga más privilegios de los que debe tener, las modificaciones vulnerables del sistema requieren el conjunto completo de privilegios. Por ejemplo, un archivo o un proceso que es propiedad de `root` (`UID=0`) sólo puede ser modificado por un proceso con el conjunto completo de privilegios. La cuenta `root` no requiere privilegios para modificar un archivo que es propiedad de `root`. Sin embargo, un usuario que no es `root` debe tener todos los privilegios para modificar un archivo que es propiedad de `root`.

De modo similar, las operaciones que proporcionan acceso a dispositivos requieren todos los privilegios del conjunto vigente.

Los privilegios `file_chown_self` y `proc_owner` están sujetos a la escalada de privilegios. El privilegio `file_chown_self` permite a un proceso delegar sus archivos. El privilegio `proc_owner` permite a un proceso inspeccionar los procesos que no son de su propiedad.

El privilegio `file_chown_self` está limitado por la variable del sistema `rstchown`. Cuando la variable `rstchown` se define en cero, el privilegio `file_chown_self` se elimina del conjunto heredable inicial del sistema y de todos los usuarios. Para obtener más información sobre la variable del sistema `rstchown`, consulte la página del comando `man chown(1)`.

El privilegio `file_chown_self` se asigna de forma más segura a un comando concreto, se coloca en un perfil y se asigna a un rol para su uso en un shell de perfil.

El privilegio `proc_owner` no es suficiente para cambiar un `UID` de proceso a `0`. Para cambiar un proceso de cualquier `UID` a `UID=0`, se requieren todos los privilegios. Como el privilegio `proc_owner` otorga acceso de lectura sin restricciones a todos los archivos del sistema, el privilegio se asigna de forma más segura a un comando concreto, se coloca en un perfil y se asigna a un rol para su uso en un shell de perfil.



---

**Precaución** – La cuenta de un usuario se puede modificar para incluir el privilegio `file_chown_self` o el privilegio `proc_owner` en el conjunto heredable inicial del usuario. Debe tener un motivo de seguridad importante para colocar esos privilegios tan poderosos en el conjunto heredable de privilegios para cualquier usuario, rol o sistema.

---

Para obtener detalles sobre cómo se evita la escalada de privilegios para los dispositivos, consulte [“Privilegios y dispositivos” en la página 201](#).

## Aplicaciones antiguas y el modelo de privilegios

Para adaptarse a las aplicaciones antiguas, la implementación de privilegios funciona con el modelo de superusuario y el modelo de privilegios. El núcleo realiza automáticamente un seguimiento del indicador `PRIV_AWARE`, que señala que un programa se ha diseñado para trabajar con privilegios. Piense en un proceso secundario que no reconoce privilegios. Los privilegios que se heredaron del proceso principal están disponibles en el conjunto permitido y el conjunto vigente del proceso secundario. Si el proceso secundario define un UID en 0, es posible que el proceso secundario no tenga capacidades completas de superusuario. El conjunto vigente y el conjunto permitido del proceso están restringidos a los privilegios del conjunto límite del proceso secundario. Por lo tanto, el conjunto límite de un proceso que reconoce privilegios restringe los privilegios root de los procesos secundarios que no reconocen privilegios.



## P A R T E I V

# Servicios criptográficos

En esta sección se describen los servicios de tecnología de clave pública y criptográficos centralizados que proporciona el SO Oracle Solaris.

- Capítulo 13, “Estructura criptográfica de Oracle Solaris (descripción general)”
- Capítulo 14, “Estructura criptográfica de Oracle Solaris (tareas)”
- Capítulo 15, “Estructura de gestión de claves de Oracle Solaris”



## Estructura criptográfica de Oracle Solaris (descripción general)

---

En este capítulo se describe la estructura criptográfica de Oracle Solaris. A continuación, se presenta la información que se incluye en este capítulo.

- “Novedades de la estructura criptográfica de Oracle Solaris” en la página 279
- “Estructura criptográfica de Oracle Solaris” en la página 280
- “Terminología de la estructura criptográfica de Oracle Solaris” en la página 281
- “Ámbito de la estructura criptográfica de Oracle Solaris” en la página 282
- “Comandos administrativos de la estructura criptográfica de Oracle Solaris” en la página 283
- “Comandos de nivel de usuario de la estructura criptográfica de Oracle Solaris” en la página 283
- “Complementos de la estructura criptográfica de Oracle Solaris” en la página 284
- “Zonas y servicios criptográficos” en la página 285

Para administrar y utilizar la estructura criptográfica de Oracle Solaris, consulte el [Capítulo 14](#), “Estructura criptográfica de Oracle Solaris (tareas)”.

## Novedades de la estructura criptográfica de Oracle Solaris

**Solaris 10 1/06:** la biblioteca de estructuras, `libpkcs11.so`, contiene un componente nuevo, la *metarranura*. La *metarranura* actúa como una única ranura virtual con las capacidades combinadas de todos los identificadores y ranuras que se han instalado en la estructura. La *metarranura* permite que una aplicación se conecte eficazmente de forma transparente a cualquier servicio criptográfico disponible mediante una única ranura.

- Para obtener más información, consulte las definiciones de ranura, *metarranura* y token en [“Terminología de la estructura criptográfica de Oracle Solaris” en la página 281](#).
- Para administrar la *metarranura*, consulte la página del comando `man cryptoadm(1M)`.
- Para ver una lista completa de las nuevas funciones de Oracle Solaris y una descripción de las versiones de Oracle Solaris, consulte [Novedades de Oracle Solaris 10 8/11](#).

## Estructura criptográfica de Oracle Solaris

La estructura criptográfica de Oracle Solaris proporciona un almacén común de algoritmos y bibliotecas PKCS #11 para manejar los requisitos criptográficos. Las bibliotecas PKCS #11 se implementan según el estándar siguiente: RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki).

En el nivel de núcleo, la estructura actualmente maneja los requisitos criptográficos para Kerberos e IPsec. Los consumidores de nivel de usuario incluyen `libsasl` e IKE.

La ley de exportación de los Estados Unidos exige que el uso de interfaces criptográficas abiertas sea restringido. La estructura criptográfica de Oracle Solaris cumple con la ley actual al requerir que los proveedores criptográficos de núcleo y los proveedores criptográficos de PKCS #11 estén registrados. Para obtener más información, consulte [“Firmas binarias para software de terceros” en la página 284](#).

La estructura permite que los servicios de los *proveedores* de servicios criptográficos sean utilizados por muchos *consumidores* en el SO Oracle Solaris. Otro nombre para los proveedores es *complementos*. La estructura permite tres tipos de complementos:

- **Complementos de nivel de usuario:** objetos compartidos que prestan servicios mediante bibliotecas PKCS #11, como `pkcs11_softtoken.so.1`.
- **Complemento de nivel de núcleo:** módulos de núcleo que proporcionan implementaciones de algoritmos criptográficos en software, como [AES](#).

Muchos de los algoritmos de la estructura están optimizados para x86 con el conjunto de instrucciones SSE2 y para hardware SPARC.

- **Complementos de hardware:** controladores de dispositivos y sus aceleradores de hardware asociados. Los chips Niagara, los controladores de dispositivos `n2cp` y `ncp`, son un ejemplo. Un acelerador de hardware descarga funciones criptográficas que consumen muchos recursos del sistema operativo. La placa Crypto Accelerator 6000 de Sun es un ejemplo.

La estructura implementa una interfaz estándar, la biblioteca PKCS #11, v2.11, para proveedores de nivel de usuario. La biblioteca puede ser utilizada por aplicaciones de terceros para acceder a los proveedores. Terceros también pueden agregar bibliotecas registradas, módulos de algoritmos de núcleo registrados y controladores de dispositivos registrados a la estructura. Estos complementos se agregan cuando la utilidad `pkgadd` instala el software de terceros. Para ver un diagrama de los componentes principales de la estructura, consulte el [Capítulo 8, “Introduction to the Oracle Solaris Cryptographic Framework” de \*Developer’s Guide to Oracle Solaris Security\*](#).



# Terminología de la estructura criptográfica de Oracle Solaris

La siguiente lista de definiciones y ejemplos es útil para trabajar con la estructura criptográfica.

- **Algoritmos:** algoritmos criptográficos. Estos son procedimientos informáticos establecidos y recursivos que cifran la entrada o le aplican hash. Los algoritmos de cifrado pueden ser simétricos o asimétricos. Los algoritmos simétricos utilizan la misma clave para el cifrado y el descifrado. Los algoritmos asimétricos, que se utilizan en la criptografía de claves públicas, necesitan dos claves. Las funciones de hashing también son algoritmos.

Ejemplos de algoritmos:

- Algoritmos simétricos, como AES y ARCFOUR
- Algoritmos asimétricos, como Diffie-Hellman y RSA
- Funciones de hashing, como MD5
- **Consumidores:** usuarios de los servicios criptográficos prestados por los proveedores. Los consumidores pueden ser aplicaciones, usuarios finales u operaciones de núcleo.

Ejemplos de consumidores:

- Aplicaciones, como IKE
- Usuarios finales, como un usuario común que ejecuta el comando `encrypt`
- Operaciones de núcleo, como IPsec
- **Mecanismo:** es la aplicación de un modo de un algoritmo para un fin particular.  
Por ejemplo, un mecanismo DES que se aplica a la autenticación, como CKM\_DES\_MAC, es un mecanismo distinto de un mecanismo DES que se aplica al cifrado, CKM\_DES\_CBC\_PAD.
- **Metarranura:** es una única ranura que presenta una unión de las capacidades de otras ranuras que se cargan en la estructura. La metarranura facilita la tarea de manejar todas las capacidades de los proveedores que están disponibles mediante la estructura. Cuando una aplicación que utiliza la metarranura solicita una operación, la metarranura averigua qué ranura debe realizar la operación. Las capacidades de la metarranura son configurables, pero no se requiere configuración. La metarranura está activada de manera predeterminada. Para configurar la metarranura, consulte la página del comando `man cryptoadm(1M)`.
- **Modo:** es una versión de un algoritmo criptográfico. Por ejemplo, CBC (Cipher Block Chaining) es un modo distinto de ECB (Electronic Code Book). El algoritmo AES tiene dos modos, CKM\_AES\_ECB y CKM\_AES\_CBC.
- **Política:** es la elección, por parte de un administrador, de qué mecanismos estarán disponibles para su uso. De manera predeterminada, todos los proveedores y todos los mecanismos están disponibles para su uso. La inhabilitación de cualquier mecanismo sería una aplicación de la política. La habilitación de un mecanismo inhabilitado también sería una aplicación de la política.
- **Proveedores:** servicios criptográficos que utilizan los consumidores. Los proveedores se conectan a la estructura, por lo que también se denominan *complementos*.

Ejemplos de proveedores:

- Bibliotecas PKCS #11, como `pkcs11_softtoken.so`
- Módulos de los algoritmos criptográficos, como `aes` y `arcfour`
- Controladores de dispositivos y aceleradores de hardware asociados, como el controlador `mca` para `Crypto Accelerator 6000` de Sun
- **Ranura:** es una interfaz de uno o varios dispositivos criptográficos. Cada ranura, que corresponde a un lector físico o a otra interfaz de dispositivo, puede contener un token. Un token proporciona una vista lógica de un dispositivo criptográfico en la estructura.
- **Token:** en una ranura, un token proporciona una vista lógica de un dispositivo criptográfico en la estructura.

## Ámbito de la estructura criptográfica de Oracle Solaris

La estructura proporciona comandos para los administradores, los usuarios y los desarrolladores que suministran proveedores:

- **Comandos administrativos:** el comando `cryptoadm` proporciona un subcomando `list` para mostrar los proveedores disponibles y sus capacidades. Los usuarios comunes pueden ejecutar los comandos `cryptoadm list` y `cryptoadm --help`.

Para todos los demás subcomandos `cryptoadm` es necesario que asuma un rol que incluya el perfil de derechos de gestión de criptografía o que se convierta en superusuario. Los subcomandos como `disable`, `install` y `uninstall` están disponibles para administrar la estructura. Para obtener más información, consulte la página del comando `man cryptoadm(1M)`.

El comando `svcadm` se utiliza para gestionar el daemon `kcfd` y para actualizar la política criptográfica en el núcleo. Para obtener más información, consulte la página del comando `man svcadm(1M)`.

- **Comandos de nivel de usuario:** los comandos `digest` y `mac` proporcionan servicios de integridad de archivos. Los comandos `encrypt` y `decrypt` protegen los archivos contra intrusos. Para utilizar estos comandos, consulte [“Protección de archivos con la estructura criptográfica de Oracle Solaris \(mapa de tareas\)” en la página 288](#).
- **Firmas binarias para proveedores de terceros:** el comando `elfsign` permite a terceros registrar archivos binarios para utilizar en la estructura. Los archivos binarios que se pueden agregar a la estructura son bibliotecas PKCS #11, módulos de algoritmos de núcleo y controladores de dispositivos de hardware. Para utilizar el comando `elfsign`, consulte el [Apéndice F, “Packaging and Signing Cryptographic Providers” de \*Developer’s Guide to Oracle Solaris Security\*](#).

## Comandos administrativos de la estructura criptográfica de Oracle Solaris

El comando `cryptoadm` administra una estructura criptográfica en ejecución. El comando forma parte del perfil de derechos de gestión de criptografía. Este perfil se puede asignar a un rol para una administración segura de la estructura criptográfica. El comando `cryptoadm` gestiona lo siguiente:

- Visualización de información del proveedor de servicios criptográficos
- Inhabilitación o habilitación de mecanismos del proveedor
- Solaris 10 1/06: inhabilitación o habilitación de la metarranura

El comando `svcadm` se utiliza para habilitar, actualizar y deshabilitar el daemon de servicios criptográficos, `kcfd`. Este comando forma parte de la utilidad de gestión de servicios (SMF). `svc:/system/cryptosvcs` es la instancia de servicio para la estructura criptográfica. Para obtener más información, consulte las páginas del comando `man smf(5)` y `svcadm(1M)`.

## Comandos de nivel de usuario de la estructura criptográfica de Oracle Solaris

La estructura criptográfica de Oracle Solaris proporciona comandos de nivel de usuario para comprobar la integridad de los archivos, cifrar archivos y descifrar archivos. Un comando independiente, `elfsign`, permite a los proveedores registrar archivos binarios para utilizarlos en la estructura.

- Comando `digest` : procesa un [resumen de mensaje](#) para uno o varios archivos o para `stdin`. Un resumen es útil para verificar la integridad de un archivo. [SHA1](#) y [MD5](#) son ejemplos de funciones de resumen.
- Comando `mac` : procesa un [código de autenticación de mensajes \(MAC\)](#) para uno o varios archivos o para `stdin`. Un MAC asocia datos con un mensaje autenticado. Un MAC le permite a un receptor verificar que el mensaje provenga del remitente y no haya sido alterado. Los mecanismos `sha1_mac` y `md5_hmac` pueden procesar un MAC.
- Comando `encrypt`: cifra los archivos o `stdin` con un cifrado simétrico. El comando `encrypt -l` muestra los algoritmos que están disponibles. Los mecanismos incluidos en una biblioteca de nivel de usuario están disponibles para el comando `encrypt`. La estructura proporciona mecanismos AES, DES, 3DES (Triple-DES) y ARCFOUR para el cifrado del usuario.
- Comando `decrypt`: descifra archivos o `stdin` que se cifraron con el comando `encrypt`. El comando `decrypt` utiliza la misma clave y el mismo mecanismo que se utilizaron para cifrar el archivo original.

## Firmas binarias para software de terceros

El comando `elfsign` proporciona un medio para firmar los proveedores que se utilizarán en la estructura criptográfica de Oracle Solaris. Normalmente, este comando es ejecutado por el desarrollador de un proveedor.

El comando `elfsign` tiene subcomandos para solicitar un certificado de Sun y para registrar archivos binarios. Otro subcomando verifica la firma. Los archivos binarios no registrados no pueden ser utilizados por la estructura criptográfica de Oracle Solaris. Para registrar a uno o varios proveedores se requiere el certificado de Sun y la clave privada que se utilizó para solicitar el certificado. Para obtener más información, consulte el [Apéndice F, “Packaging and Signing Cryptographic Providers”](#) de *Developer’s Guide to Oracle Solaris Security*.

## Complementos de la estructura criptográfica de Oracle Solaris

Terceros pueden conectar sus proveedores a la estructura criptográfica de Oracle Solaris. Un proveedor de terceros puede ser uno de los siguientes objetos:

- Biblioteca compartida PKCS #11
- Módulo de software de núcleo cargable, como un algoritmo de cifrado, una función MAC o una función de resumen
- Controlador de dispositivo de núcleo para un acelerador de hardware

Los objetos de un proveedor deben estar registrados con un certificado de Sun. La solicitud de certificado se basa en una clave privada elegida por el tercero y un certificado proporcionado por Sun. La solicitud de certificado se envía a Sun, que registra al tercero y, a continuación, expide el certificado. El tercero, a continuación, registra su objeto de proveedor con el certificado de Sun.

Los módulos de software de núcleo cargable y los controladores de dispositivos de núcleo para aceleradores de hardware también se deben registrar en el núcleo. El registro se lleva a cabo mediante la interfaz del proveedor de servicios (SPI) de la estructura criptográfica de Oracle Solaris.

Para instalar al proveedor, el tercero proporciona un paquete que instala el objeto registrado y el certificado de Sun. El paquete debe incluir el certificado y debe permitir al administrador colocar el certificado en un directorio seguro. Para obtener más información, consulte el [Apéndice F, “Packaging and Signing Cryptographic Providers”](#) de *Developer’s Guide to Oracle Solaris Security*.

## Zonas y servicios criptográficos

La zona global y cada zona no global tienen su propio servicio `/system/cryptosvc`. Cuando se habilita o se actualiza el servicio criptográfico en la zona global, se inicia el daemon `kcfd` en la zona global, se define la política de nivel de usuario para la zona global y se establece la política de núcleo para el sistema. Cuando se habilita o se actualiza el servicio en una zona no global, se inicia el daemon `kcfd` en la zona y se define la política de nivel de usuario para la zona. La política de núcleo fue definida por la zona global.

Para obtener más información sobre las zonas, consulte la [Parte II, “Zonas” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#). Para obtener más información sobre la utilidad de gestión de servicios que gestiona las aplicaciones persistentes, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica](#) y la página del comando `man smf(5)`.



## Estructura criptográfica de Oracle Solaris (tareas)

---

En este capítulo se describe cómo utilizar la estructura criptográfica de Oracle Solaris. A continuación puede ver una lista de la información incluida en este capítulo.

- “Uso de la estructura criptográfica (mapa de tareas)” en la página 287
- “Protección de los archivos con la estructura criptográfica (tareas)” en la página 288
- “Administración de la estructura criptográfica (tareas)” en la página 299

### Uso de la estructura criptográfica (mapa de tareas)

En el siguiente mapa de tareas se hace referencia a las tareas para utilizar la estructura criptográfica.

Tarea	Descripción	Para obtener instrucciones
Proteger los archivos individuales o los conjuntos de archivos	Garantiza que no se haya alterado el contenido del archivo. Impide que los archivos sean leídos por intrusos. Estos procedimientos pueden ser realizados por usuarios comunes.	“Protección de archivos con la estructura criptográfica de Oracle Solaris (mapa de tareas)” en la página 288
Administrar la estructura	Agrega, configura y elimina los proveedores de software. Inhabilita y habilita los mecanismos del proveedor de hardware. Estos procedimientos son procedimientos administrativos.	“Administración de la estructura criptográfica (mapa de tareas)” en la página 299
Registrar a un proveedor	Permite agregar a un proveedor a la estructura criptográfica de Oracle Solaris. Éstos son procedimientos de desarrollador.	Apéndice F, “Packaging and Signing Cryptographic Providers” de <i>Developer’s Guide to Oracle Solaris Security</i> .

# Protección de archivos con la estructura criptográfica de Oracle Solaris (mapa de tareas)

La estructura criptográfica de Oracle Solaris puede ayudar a proteger los archivos. En el siguiente mapa de tareas se hace referencia a los procedimientos para mostrar los algoritmos disponibles y para proteger los archivos criptográficamente.

Tarea	Descripción	Para obtener instrucciones
Generar una clave simétrica	Genera una clave aleatoria para su uso con los algoritmos que especifica el usuario.	<a href="#">“Cómo generar una clave simétrica con el comando dd” en la página 288</a>
	Genera una clave de la longitud especificada por el usuario. También puede almacenar la clave en un archivo, en un almacén de claves PKCS #11 o en un almacén de claves NSS.	<a href="#">“Cómo generar una clave simétrica con el comando pkttool” en la página 290</a>
Proporcionar una suma de comprobación que garantice la integridad de un archivo	Verifica que la copia de un archivo del receptor sea idéntica al archivo que se envió.	<a href="#">“Cómo calcular un resumen de un archivo” en la página 293</a>
Proteger un archivo con un código de autenticación de mensajes (MAC)	Le comprueba al receptor del mensaje que usted era el remitente.	<a href="#">“Cómo calcular un MAC de un archivo” en la página 295</a>
Cifrar un archivo y, a continuación, descifrar el archivo cifrado	Protege el contenido de los archivos al cifrar el archivo. Proporciona los parámetros de cifrado para descifrar el archivo.	<a href="#">“Cómo cifrar y descifrar un archivo” en la página 296</a>

## Protección de los archivos con la estructura criptográfica (tareas)

En esta sección, se describe cómo generar claves simétricas, cómo crear sumas de comprobación para la integridad de archivos y cómo proteger los archivos contra intrusos. Los comandos incluidos en esta sección pueden ser ejecutados por usuarios comunes. Los desarrolladores pueden escribir secuencias de comandos que utilicen estos comandos.

### ▼ Cómo generar una clave simétrica con el comando dd

Se necesita una clave para cifrar archivos y generar el MAC de un archivo. La clave se debería obtener de una agrupación aleatoria de números.

Si su sitio cuenta con un generador de números aleatorios, utilícelo. De lo contrario, puede utilizar el comando dd con el dispositivo /dev/urandom de Oracle Solaris como entrada. Para obtener más información, consulte la página del comando man [dd\(1M\)](#).



1 Determine la longitud de clave que necesita el algoritmo.

a. Muestre los algoritmos disponibles.

```
% encrypt -l
Algorithm      Keysize:  Min   Max (bits)
-----
aes            128    128
arcfour        8      128
des            64     64
3des          192    192

% mac -l
Algorithm      Keysize:  Min   Max (bits)
-----
des_mac        64     64
sha1_hmac      8     512
md5_hmac       8     512
sha256_hmac    8     512
sha384_hmac    8    1024
sha512_hmac    8    1024
```

b. Determine la longitud de la clave en bytes para transferir al comando dd.

Divida los tamaños de clave mínimo y máximo por 8. Cuando los tamaños de clave mínimo y máximo son diferentes, es posible utilizar tamaños de clave intermedios. Por ejemplo, el valor 8, 16 o 64 pueden transferirse al comando dd para las funciones sha1\_hmac y md5\_hmac.

2 Genere la clave simétrica.

```
% dd if=/dev/urandom of=keyfile bs=n count=n

if=archivo      Es el archivo de entrada. Para una clave aleatoria, utilice el archivo
                 /dev/urandom.

of=archivo_claves  Es el archivo de salida que contiene la clave generada.

bs=n            Es el tamaño de la clave en bytes. Para obtener la longitud en bytes,
                 divida la longitud de la clave (en bytes) por 8.

count=n         Es el recuento de los bloques de entrada. El número para n debe ser 1.
```

3 Almacene su clave en un directorio protegido.

El archivo de claves sólo debe ser legible para el usuario.

```
% chmod 400 keyfile
```

Ejemplo 14–1 Creación de una clave para el algoritmo AES

En el siguiente ejemplo, se crea una clave secreta para el algoritmo AES. La clave también se almacena para el descifrado posterior. Los mecanismos AES utilizan una clave de 128 bits. La clave se expresa en 16 bytes en el comando dd.

```
% ls -al ~/keyf
drwx----- 2 jdoe staff      512 May 3 11:32 ./
% dd if=/dev/urandom of=$HOME/keyf/05.07.aes16 bs=16 count=1
% chmod 400 ~/keyf/05.07.aes16
```

#### Ejemplo 14-2 Creación de una clave para el algoritmo DES

En el siguiente ejemplo, se crea una clave secreta para el algoritmo DES. La clave también se almacena para el descifrado posterior. Los mecanismos DES utilizan una clave de 64 bits. La clave se expresa en 8 bytes en el comando dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.des8 bs=8 count=1
% chmod 400 ~/keyf/05.07.des8
```

#### Ejemplo 14-3 Creación de una clave para el algoritmo 3DES

En el siguiente ejemplo, se crea una clave secreta para el algoritmo 3DES. La clave también se almacena para el descifrado posterior. Los mecanismos 3DES utilizan una clave de 192 bits. La clave se expresa en 24 bytes en el comando dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.3des.24 bs=24 count=1
% chmod 400 ~/keyf/05.07.3des.24
```

#### Ejemplo 14-4 Creación de una clave para el algoritmo MD5

En el siguiente ejemplo, se crea una clave secreta para el algoritmo MD5. La clave también se almacena para el descifrado posterior. La clave se expresa en 64 bytes en el comando dd.

```
% dd if=/dev/urandom of=$HOME/keyf/05.07.mack64 bs=64 count=1
% chmod 400 ~/keyf/05.07.mack64
```

## ▼ Cómo generar una clave simétrica con el comando **pktool**

Algunas aplicaciones requieren una clave simétrica para el cifrado y el descifrado de las comunicaciones. En este procedimiento, se crea una clave simétrica y se la almacena.

- Si su sitio cuenta con un generador de números aleatorios, puede utilizar el generador para crear un número aleatorio para la clave. Este procedimiento no utiliza el generador de números aleatorios de su sitio.
- En su lugar, puede utilizar el comando dd con el dispositivo /dev/urandom de Oracle Solaris como entrada. El comando dd no almacena la clave. Para conocer el procedimiento, consulte [“Cómo generar una clave simétrica con el comando dd” en la página 288](#).

## 1 (Opcional) Si tiene previsto utilizar un almacén de claves, créelo.

- Para crear e inicializar un almacén de claves PKCS #11, consulte [“Cómo generar una frase de contraseña mediante el comando pktool setpin” en la página 320](#).
- Para crear e inicializar una base de datos NSS, consulte el [Ejemplo 15-5](#).

## 2 Genere un número aleatorio para usarlo como clave simétrica.

Utilice uno de los métodos siguientes.

### ■ Genere una clave y almacénela en un archivo.

La ventaja de almacenar una clave en un archivo es que se puede extraer la clave de este archivo para usarla en el archivo de claves de una aplicación, como el archivo `/etc/inet/secret/ipseckeys` o IPsec.

```
% pktool genkey keystore=file outkey=key-fn \
[keytype=symmetric-algorithm] [keylen=size-in-bits] \
[dir=directory] [print=n]
```

**keystore**

El valor `file` especifica la ubicación de almacenamiento de tipo archivo para la clave.

**outkey=nombre\_archivo\_claves**

Es el nombre de archivo cuando se especifica `keystore=file`.

**keytype=algoritmo simétrico específico**

Para un algoritmo determinado, especifique `aes`, `arcfour`, `des` o `3des`.

**keylen=tamaño en bits**

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para `des` ni `3des`.

**dir=directorio**

Es la ruta del directorio a `nombre_archivo_claves`. De manera predeterminada, el valor de `directorio` es el directorio actual.

**print=n**

Imprime la clave en la ventana de terminal. De manera predeterminada, el valor de `print` es `n`.

### ■ Genere una clave y almacénela en un almacén de claves PKCS #11.

La ventaja del almacén de claves PKCS #11 es que se puede recuperar la clave por su etiqueta. Este método es útil para las claves para cifrar y descifrar archivos. Debe completar el [Paso 1](#) antes de utilizar este método.

```
% pktool genkey label=key-label \
[keytype=symmetric-algorithm] [keylen=size-in-bits] \
[token=token] [sensitive=n] [extractable=y] [print=n]
```

`label=etiqueta_clave`

Es una etiqueta especificada por el usuario para la clave. La clave se puede recuperar del almacén de claves por su etiqueta.

`keytype=algoritmo simétrico específico`

Para un algoritmo determinado, especifique `aes`, `arcfour`, `des` o `3des`.

`keylen=tamaño en bits`

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para `des` ni `3des`.

`token=token`

Es el nombre del token. De manera predeterminada, el token es Sun Software PKCS#11 softtoken.

`sensitive=n`

Especifica la sensibilidad de la clave. Cuando el valor es `y`, la clave no se puede imprimir utilizando el argumento `print=y`. De manera predeterminada, el valor de `sensitive` es `n`.

`extractable=y`

Especifica que la clave se puede extraer del almacén de claves. Especifique `n` para evitar que se extraiga la clave.

`print=n`

Imprime la clave en la ventana de terminal. De manera predeterminada, el valor de `print` es `n`.

#### ■ Genere una clave y almacénela en un almacén de claves NSS.

Debe completar el [Paso 1](#) antes de utilizar este método.

```
% pktool keystore=nss genkey label=key-label \
[keytype=[keytype=specific-symmetric-algorithm] [keylen=size-in-bits] [token=token] \
[dir=directory-path] [prefix=database-prefix]
```

`keystore`

El valor `nss` especifica la ubicación de almacenamiento de tipo NSS para la clave.

`label=etiqueta_clave`

Es una etiqueta especificada por el usuario para la clave. La clave se puede recuperar del almacén de claves por su etiqueta.

`keytype=algoritmo simétrico específico`

Para un algoritmo determinado, especifique `aes`, `arcfour`, `des` o `3des`.

`keylen=tamaño en bits`

Es la longitud de la clave en bits. El número debe ser divisible por 8. No especificar para `des` ni `3des`.

`token=token`

Es el nombre del token. De manera predeterminada, el token es el token interno NSS.

`dir=directorio`

Es la ruta de directorio a la base de datos NSS. De manera predeterminada, el valor de *directorio* es el directorio actual.

`prefix=directorio`

Es el prefijo de la base de datos NSS. El valor predeterminado es sin prefijo.

`print=n`

Imprime la clave en la ventana de terminal. De manera predeterminada, el valor de `print` es `n`.

### 3 (Opcional) Compruebe que la clave exista.

Utilice uno de los siguientes comandos, según dónde haya guardado la clave.

- **Verifique la clave en el archivo *nombre\_archivo\_claves*.**

```
% pktool list keystore=file objtype=key infile=key-fn
Found n keys.
Key #1 - keytype:location (keylen)
```

- **Verifique la clave en el almacén de claves PKCS #11 o NSS.**

```
$ pktool list objtype=key
Enter PIN for keystore:
Found n keys.
Key #1 - keytype:location (keylen)
```

#### Ejemplo 14–5 Creación de una clave DES con el comando `pktool`

En el siguiente ejemplo, se crea una clave secreta para el algoritmo DES. La clave se almacena en un archivo local para un posterior descifrado. El comando protege el archivo con **400** permisos. Cuando se crea la clave, la opción `print=y` muestra la clave generada en la ventana de terminal.

Los mecanismos DES utilizan una clave de 64 bits. El usuario que posee el archivo de claves recupera la clave mediante el comando `od`.

```
% pktool genkey keystore=file outkey=64bit.file1 keytype=des print=y
Key Value ="a3237b2c0a8ff9b3"
% od -x 64bit.file1
00000000 a323 7b2c 0a8f f9b3
```

## ▼ Cómo calcular un resumen de un archivo

Cuando se calcula un resumen de un archivo, se puede comprobar que el archivo no haya sido alterado comparando los resultados del resumen. Un resumen no modifica el archivo original.

### 1 Muestre los algoritmos de resumen disponibles.

```
% digest -l
md5
sha1
```

```
sha256
sha384
sha512
```

## 2 Calcule el resumen del archivo y guarde la lista de resumen.

Proporcione un algoritmo con el comando `digest`.

```
% digest -v -a algorithm input-file > digest-listing
```

`-v` Muestra el resultado en el siguiente formato:

```
algorithm (input-file) = digest
```

`-a algoritmo` Es el algoritmo que se utilizará para calcular un resumen del archivo. Escriba el algoritmo tal como aparece en el resultado del [Paso 1](#).

`archivo_entrada` Es el archivo de entrada para el comando `digest`.

`lista_resumen` Es el archivo de salida para el comando `digest`.

### Ejemplo 14–6 Cálculo de un resumen con el mecanismo MD5

En el ejemplo siguiente, el comando `digest` usa el mecanismo MD5 para calcular un resumen de un anexo de correo electrónico.

```
% digest -v -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
md5 (email.attach) = 85c0a53d1a5cc71ea34d9ee7b1b28b01
```

Cuando no se utiliza la opción `-v`, el resumen se guarda sin información adicional:

```
% digest -a md5 email.attach >> $HOME/digest.emails.05.07
% cat ~/digest.emails.05.07
85c0a53d1a5cc71ea34d9ee7b1b28b01
```

### Ejemplo 14–7 Cálculo de un resumen con el mecanismo SHA1

En el ejemplo siguiente, el comando `digest` usa el mecanismo SHA1 para proporcionar una lista de directorios. Los resultados se colocarán en un archivo.

```
% digest -v -a sha1 docs/* > $HOME/digest.docs.legal.05.07
% more ~/digest.docs.legal.05.07
sha1 (docs/legal1) = 1df50e8ad219e34f0b911e097b7b588e31f9b435
sha1 (docs/legal2) = 68efa5a636291bde8f33e046eb33508c94842c38
sha1 (docs/legal3) = 085d991238d61bd0cfa2946c183be8e32cccfc6c9
sha1 (docs/legal4) = f3085eae7e2c8d008816564fdf28027d10e1d983
```

## ▼ Cómo calcular un MAC de un archivo

Un código de autenticación de mensajes, o MAC, calcula un resumen del archivo y utiliza una clave secreta para proteger aún más el resumen. Un MAC no modifica el archivo original.

### 1 Muestre los mecanismos disponibles.

```
% mac -l
Algorithm      Keysize:  Min   Max
-----
des_mac        64      64
sha1_hmac      8       512
md5_hmac       8       512
sha256_hmac    8       512
sha384_hmac    8      1024
sha512_hmac    8      1024
```

### 2 Genere una clave simétrica de la longitud adecuada.

Dispone de dos opciones. Puede proporcionar una [frase de contraseña](#) a partir de la cual se generará una clave. O bien, puede proporcionar una clave.

- Si proporciona una frase contraseña, deberá almacenarla o recordarla. Si almacena la frase de contraseña en línea, sólo usted debe poder leer el archivo de frases de contraseña.
- Si proporciona una clave, ésta debe ser del tamaño correcto para el mecanismo. Para conocer el procedimiento, consulte [“Cómo generar una clave simétrica con el comando dd” en la página 288](#).

### 3 Cree un MAC para un archivo.

Proporcione una clave y utilice un algoritmo de clave simétrico con el comando `mac`.

```
% mac -v -a algorithm [ -k keyfile ] input-file
```

`-v` Muestra el resultado en el siguiente formato:

```
algorithm (input-file) = mac
```

`-a algoritmo` Es el algoritmo que se utiliza para calcular el MAC. Escriba el algoritmo tal como aparece en el resultado del comando `mac -l`.

`-k archivo_claves` Es el archivo que contiene una clave con la longitud especificada por el algoritmo.

*archivo\_entrada* Es el archivo de entrada para el MAC.

### Ejemplo 14–8 Cálculo de un MAC con DES\_MAC y una frase de contraseña

En el ejemplo siguiente, el anexo de correo electrónico se autentica con el mecanismo DES\_MAC y una clave que se obtiene a partir de una frase de contraseña. La lista de MAC se guarda en un archivo. Si la frase de contraseña se almacena en un archivo, el usuario debe ser la única persona que pueda leer el archivo.

```
% mac -v -a des_mac email.attach
Enter passphrase: <Type passphrase>
des_mac (email.attach) = dd27870a
% echo "des_mac (email.attach) = dd27870a" >> ~/desmac.daily.05.07
```

#### Ejemplo 14–9 Cálculo de un MAC con MD5\_HMAC y un archivo de claves

En el ejemplo siguiente, el anexo de correo electrónico se autentica con el mecanismo MD5\_HMAC y una clave secreta. La lista de MAC se guarda en un archivo.

```
% mac -v -a md5_hmac -k $HOME/keyf/05.07.mack64 email.attach
md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c
% echo "md5_hmac (email.attach) = 02df6eb6c123ff25d78877eb1d55710c" \
>> ~/mac.daily.05.07
```

#### Ejemplo 14–10 Cálculo de un MAC con SHA1\_HMAC y un archivo de claves

En el ejemplo siguiente, el manifiesto de directorio se autentica con el mecanismo SHA1\_HMAC y una clave secreta. Los resultados se colocarán en un archivo.

```
% mac -v -a sha1_hmac \
-k $HOME/keyf/05.07.mack64 docs/* > $HOME/mac.docs.legal.05.07
% more ~/mac.docs.legal.05.07
sha1_hmac (docs/legal1) = 9b31536d3b3c0c6b25d653418db8e765e17fe07a
sha1_hmac (docs/legal2) = 865af61a3002f8a457462a428cdb1a88c1b51ff5
sha1_hmac (docs/legal3) = 076c944cb2528536c9aebd3b9fbe367e07b61dc7
sha1_hmac (docs/legal4) = 7aede27602ef6e4454748cbd3821e0152e45beb4
```

## ▼ Cómo cifrar y descifrar un archivo

Al cifrar un archivo, el archivo original no se elimina ni modifica. Se cifra el archivo de salida.

Para ver las soluciones a los errores comunes del comando `encrypt`, consulte sección que aparece a continuación de los ejemplos.

### 1 Cree una clave simétrica de la longitud adecuada.

Existen dos opciones. Puede proporcionar una [frase de contraseña](#) a partir de la cual se generará una clave. O bien, puede proporcionar una clave.

- Si proporciona una frase contraseña, deberá almacenarla o recordarla. Si almacena la frase de contraseña en línea, sólo usted debe poder leer el archivo de frases de contraseña.
- Si proporciona una clave, ésta debe ser del tamaño correcto para el mecanismo. Para conocer el procedimiento, consulte [“Cómo generar una clave simétrica con el comando dd” en la página 288](#).



## 2 Cifre un archivo.

Proporcione una clave y utilice un algoritmo de clave simétrico con el comando `encrypt`.

```
% encrypt -a algorithm [ -k keyfile ] -i input-file -o output-file
```

-a <i>algoritmo</i>	Es el algoritmo que se utiliza para cifrar el archivo. Escriba el algoritmo tal como aparece en el resultado del comando <code>encrypt -l</code> .
-k <i>archivo_claves</i>	Es el archivo que contiene una clave con la longitud especificada por el algoritmo. La longitud de la clave para cada algoritmo se muestra, en bits, en el resultado del comando <code>encrypt -l</code> .
-i <i>archivo_entrada</i>	Es el archivo de entrada que desea cifrar. Este archivo no es modificado por el comando.
-o <i>archivo_salida</i>	Es el archivo de salida, que es el formato cifrado del archivo de entrada.

### Ejemplo 14-11 Cifrado y descifrado con AES y una frase de contraseña

En el ejemplo siguiente, se cifra un archivo con el algoritmo AES. La clave se genera a partir de una frase de contraseña. Si la frase de contraseña se almacena en un archivo, el usuario debe ser la única persona que pueda leer el archivo.

```
% encrypt -a aes -i ticket.to.ride -o ~/enc/e.ticket.to.ride
Enter passphrase: <Type passphrase>
Re-enter passphrase: Type passphrase again
```

El archivo de entrada, `ticket.to.ride`, todavía existe en su formato original.

Para descifrar el archivo de salida, el usuario utiliza la misma frase de contraseña y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a aes -i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
Enter passphrase: <Type passphrase>
```

### Ejemplo 14-12 Cifrado y descifrado con AES y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo AES. Los mecanismos AES utilizan una clave de 128 bits o 16 bytes.

```
% encrypt -a aes -k ~/keyf/05.07.aes16 \
-i ticket.to.ride -o ~/enc/e.ticket.to.ride
```

El archivo de entrada, `ticket.to.ride`, todavía existe en su formato original.

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a aes -k ~/keyf/05.07.aes16 \
-i ~/enc/e.ticket.to.ride -o ~/d.ticket.to.ride
```

### Ejemplo 14-13 Cifrado y descifrado con ARCFOUR y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo ARCFOUR. El algoritmo ARCFOUR acepta una clave de 8 bits (1 byte), 64 bits (8 bytes) o 128 bits (16 bytes).

```
% encrypt -a arcfour -i personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/enc/e.personal.txt
```

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a arcfour -i ~/enc/e.personal.txt \
-k ~/keyf/05.07.rc4.8 -o ~/personal.txt
```

### Ejemplo 14-14 Cifrado y descifrado con 3DES y un archivo de claves

En el ejemplo siguiente, se cifra un archivo con el algoritmo 3DES. El algoritmo 3DES requiere una clave de 192 bits o 24 bytes.

```
% encrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/personal2.txt -o ~/enc/e.personal2.txt
```

Para descifrar el archivo de salida, el usuario utiliza la misma clave y el mismo mecanismo de cifrado que utilizó para cifrar el archivo.

```
% decrypt -a 3des -k ~/keyf/05.07.des24 \
-i ~/enc/e.personal2.txt -o ~/personal2.txt
```

### Errores más frecuentes

Los siguientes mensajes indican que la clave proporcionada al comando encrypt no está permitida por el algoritmo que está utilizando.

- encrypt: unable to create key for crypto operation: CKR\_ATTRIBUTE\_VALUE\_INVALID
- encrypt: failed to initialize crypto operation: CKR\_KEY\_SIZE\_RANGE

Si utiliza una clave que no cumple con los requisitos del algoritmo, debe proporcionar una clave mejor.

- Una opción es utilizar una frase de contraseña. La estructura proporciona una clave que cumple con los requisitos.
- La segunda opción es utilizar un tamaño de clave que sea aceptado por el algoritmo. Por ejemplo, el algoritmo DES requiere una clave de 64 bits. El algoritmo 3DES requiere una clave de 192 bits.

## Administración de la estructura criptográfica (mapa de tareas)

En el siguiente mapa de tareas se hace referencia a los procedimientos para administrar a los proveedores de software y hardware en la estructura criptográfica de Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Mostrar los proveedores en la estructura criptográfica de Oracle Solaris	Muestra los algoritmos, las bibliotecas y los dispositivos de hardware que están disponibles para su uso en la estructura criptográfica de Oracle Solaris.	<a href="#">“Cómo mostrar los proveedores disponibles” en la página 300</a>
Agregar un proveedor de software	Agrega una biblioteca PKCS #11 o un módulo de núcleo a la estructura criptográfica de Oracle Solaris. El proveedor debe estar registrado.	<a href="#">“Cómo agregar un proveedor de software” en la página 302</a>
Evitar el uso de un mecanismo de nivel de usuario	Elimina un mecanismo de software para que no sea utilizado. El mecanismo se puede volver a habilitar.	<a href="#">“Cómo evitar el uso de un mecanismo de nivel de usuario” en la página 304</a>
Deshabilitar temporalmente mecanismos de un módulo de núcleo	Elimina temporalmente un mecanismo para que no sea utilizado. Se suele utilizar para realizar pruebas.	<a href="#">“Cómo evitar el uso de un proveedor de software de núcleo” en la página 305</a>
Desinstalar un proveedor	Elimina un proveedor de software de núcleo para que no sea utilizado.	<a href="#">Ejemplo 14–22</a>
Mostrar los proveedores de hardware disponibles	Muestra el hardware conectado, los mecanismos que proporciona el hardware y los mecanismos que están habilitados para ser utilizados.	<a href="#">“Cómo mostrar proveedores de hardware” en la página 308</a>
Deshabilitar los mecanismos de un proveedor de hardware	Garantiza que los mecanismos seleccionados en un acelerador de hardware no sean utilizados.	<a href="#">“Cómo deshabilitar funciones y mecanismos del proveedor de hardware” en la página 308</a>
Reiniciar o actualizar los servicios criptográficos	Garantiza que los servicios criptográficos estén disponibles.	<a href="#">“Cómo actualizar o reiniciar todos los servicios criptográficos” en la página 310</a>

## Administración de la estructura criptográfica (tareas)

En esta sección se describe cómo administrar proveedores de software y hardware en la estructura criptográfica de Oracle Solaris. Los proveedores de software y hardware se pueden eliminar para no ser utilizados cuando se desee. Por ejemplo, puede deshabilitar la implementación de un algoritmo de un proveedor de software. A continuación, puede forzar al sistema a utilizar el algoritmo de otro proveedor de software.

## ▼ Cómo mostrar los proveedores disponibles

La estructura criptográfica de Oracle Solaris proporciona algoritmos para diversos tipos de consumidores:

- Los proveedores de nivel de usuario brindan una interfaz criptográfica PKCS #11 a las aplicaciones que están enlazadas a la biblioteca `libpkcs11`
- Los proveedores de software de núcleo brindan algoritmos para IPsec, Kerberos y otros componentes de núcleo de Oracle Solaris
- Los proveedores de hardware de núcleo brindan algoritmos que están disponibles para los consumidores del núcleo y para las aplicaciones por medio de la biblioteca `pkcs11_kernel`

### 1 Muestre los proveedores en un formato breve.

**Nota** – El contenido y el formato de la lista de proveedores varía para las distintas versiones de Oracle Solaris. Ejecute el comando `cryptoadm list` en el sistema, para ver los proveedores que admite el sistema.

Sólo los mecanismos de nivel de usuario están disponibles para ser utilizados por los usuarios comunes.

```
% cryptoadm list
user-level providers:
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so
```

```
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
```

```
kernel hardware providers:
    ncp/0
```

### 2 Muestre los proveedores y sus mecanismos en la estructura criptográfica de Oracle Solaris.

Todos los mecanismos se muestran en el siguiente resultado. Sin embargo, es posible que algunos de los mecanismos de la lista no estén disponibles para su uso. Para incluir en la lista sólo los mecanismos que el administrador ha aprobado para su uso, consulte el [Ejemplo 14–16](#).

El resultado se vuelve a formatear con fines de visualización.

```
% cryptoadm list -m
user-level providers:
=====
/usr/lib/security/$ISA/pkcs11_kernel.so: CKM_MD5,CKM_MD5_HMAC,
```

```

CKM_MD5_HMAC_GENERAL,CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL,
...
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
kernel software providers:
=====
des: CKM_DES_ECB,CKM_DES_CBC,CKM_DES3_ECB,CKM_DES3_CBC
aes: CKM_AES_ECB,CKM_AES_CBC
blowfish: CKM_BF_ECB,CKM_BF_CBC
arcfour: CKM_RC4
sha1: CKM_SHA_1,CKM_SHA_1_HMAC,CKM_SHA_1_HMAC_GENERAL
md5: CKM_MD5,CKM_MD5_HMAC,CKM_MD5_HMAC_GENERAL
rsa: CKM_RSA_PKCS,CKM_RSA_X_509,CKM_MD5_RSA_PKCS,CKM_SHA1_RSA_PKCS
swrand: No mechanisms presented.

kernel hardware providers:
=====
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA

```

### Ejemplo 14–15 Búsqueda de los mecanismos criptográficos existentes

En el siguiente ejemplo, se muestran todos los mecanismos que ofrece la biblioteca de nivel de usuario, `pkcs11_softtoken`.

```

% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
Mechanisms:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
CKM_SSL3_KEY_AND_MAC_DERIVE,CKM_TLS_KEY_AND_MAC_DERIVE

```

### Ejemplo 14–16 Búsqueda de los mecanismos criptográficos disponibles

La política determina qué mecanismos están disponibles para su uso. El administrador define la política. Un administrador puede elegir deshabilitar los mecanismos de un proveedor determinado. La opción `-p` muestra la lista de los mecanismos permitidos por la política que el administrador ha definido.

```

% cryptoadm list -p
user-level providers:
=====
/usr/lib/security/$ISA/pkcs11_kernel.so: all mechanisms are enabled.
random is enabled.
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.

kernel software providers:
=====
des: all mechanisms are enabled.

```

```

aes: all mechanisms are enabled.
blowfish: all mechanisms are enabled.
arcfour: all mechanisms are enabled.
sha1: all mechanisms are enabled.
md5: all mechanisms are enabled.
rsa: all mechanisms are enabled.
swrand: random is enabled.

```

```

kernel hardware providers:
=====
ncp/0: all mechanisms are enabled.

```

## ▼ Cómo agregar un proveedor de software

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Muestre los proveedores de software que están disponibles para el sistema.

```

% cryptoadm list
user-level providers:
  /usr/lib/security/$ISA/pkcs11_kernel.so
  /usr/lib/security/$ISA/pkcs11_softtoken.so

```

```

kernel software providers:
  des
  aes
  blowfish
  arcfour
  sha1
  md5
  rsa

```

```

kernel hardware providers:
  ncp/0

```

### 3 Agregue el paquete del proveedor mediante el comando pkgadd.

```
# pkgadd -d /path/to/package pkginst
```

El paquete debe incluir software que haya sido registrado mediante un certificado de Sun. Para solicitar un certificado de Sun y para registrar a un proveedor, consulte el [Apéndice F, “Packaging and Signing Cryptographic Providers”](#) de *Developer’s Guide to Oracle Solaris Security*.

El paquete debe tener secuencias de comandos que notifiquen a la estructura criptográfica que otro proveedor con un conjunto de mecanismos está disponible. Para obtener información sobre los requisitos de los paquetes, consulte el [Apéndice F, “Packaging and Signing Cryptographic Providers”](#) de *Developer’s Guide to Oracle Solaris Security*.

**4 Actualice los proveedores.**

Si agregó un proveedor de software o si agregó hardware y especificó una política para el hardware, debe actualizar los proveedores.

```
# svcadm refresh svc:/system/cryptosvc
```

**5 Ubique al nuevo proveedor en la lista.**

En este caso, se instaló un nuevo proveedor de software de núcleo.

```
# cryptoadm list
...
kernel software providers:
    des
    aes
    blowfish
    arcfour
    sha1
    md5
    rsa
    swrand
    ecc      <-- added provider
...
```

**Ejemplo 14–17 Adición de un proveedor de software de nivel de usuario**

En el ejemplo siguiente, se instala una biblioteca PKCS #11 registrada.

```
# pkgadd -d /cdrom/cdrom0/SolarisNew
  Answer the prompts
# svcadm refresh system/cryptosvc
# cryptoadm list
user-level providers:
=====
    /usr/lib/security/$ISA/pkcs11_kernel.so
    /usr/lib/security/$ISA/pkcs11_softtoken.so
    /opt/SUNWconn/lib/$ISA/libpkcs11.so.1      <-- added provider
```

Los desarrolladores que estén probando una biblioteca con la estructura criptográfica pueden instalar la biblioteca manualmente.

```
# cryptoadm install provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
```

Para obtener información sobre cómo registrar a su proveedor, consulte [“Firmas binarias para software de terceros” en la página 284](#).

## ▼ Cómo evitar el uso de un mecanismo de nivel de usuario

Si algunos de los mecanismos criptográficos de un proveedor de biblioteca no se debe utilizar, puede eliminar los mecanismos seleccionados. Este procedimiento utiliza el mecanismo DES en la biblioteca `pkcs11_softtoken` como ejemplo.

### 1 Conviértase en superusuario o asuma un rol que incluya el perfil de derechos de gestión de criptografía.

Para crear un rol que incluya el perfil de derechos de gestión de criptografía y asignar el rol a un usuario, consulte el [Ejemplo 9-7](#).

### 2 Muestre los mecanismos ofrecidos por un proveedor de software de nivel de usuario determinado.

```
% cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
CKM_AES_CBC,CKM_AES_CBC_PAD,CKM_AES_ECB,CKM_AES_KEY_GEN,
...
```

### 3 Muestre los mecanismos que están disponibles para su uso.

```
$ cryptoadm list -p
user-level providers:
=====
...
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
...
```

### 4 Deshabilite los mecanismos que no se deben utilizar.

```
$ cryptoadm disable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB
```

### 5 Muestre los mecanismos que están disponibles para su uso.

```
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

## Ejemplo 14-18 Habilitación de un mecanismo de proveedor de software de nivel de usuario

En el ejemplo siguiente, un mecanismo DES inhabilitado se vuelve a poner a disposición para su uso.

```
$ cryptoadm list -m provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so:
CKM_DES_CBC,CKM_DES_CBC_PAD,CKM_DES_ECB,CKM_DES_KEY_GEN,
```



```
CKM_DES3_CBC,CKM_DES3_CBC_PAD,CKM_DES3_ECB,CKM_DES3_KEY_GEN,
...
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_ECB,CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so \
> mechanism=CKM_DES_ECB
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled,
except CKM_DES_CBC_PAD,CKM_DES_CBC. random is enabled.
```

### Ejemplo 14–19 Habilitación de todos los mecanismos de proveedor de software de nivel de usuario

En el ejemplo siguiente, se habilitan todos mecanismos de la biblioteca de nivel de usuario.

```
$ cryptoadm enable provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so all
$ cryptoadm list -p provider=/usr/lib/security/\$ISA/pkcs11_softtoken.so
/usr/lib/security/$ISA/pkcs11_softtoken.so: all mechanisms are enabled.
random is enabled.
```

### Ejemplo 14–20 Eliminación permanente de la disponibilidad del proveedor de software de nivel de usuario

En el ejemplo siguiente, se elimina la biblioteca libpkcs11.so.1.

```
$ cryptoadm uninstall provider=/opt/SUNWconn/lib/\$ISA/libpkcs11.so.1
$ cryptoadm list
user-level providers:
  /usr/lib/security/$ISA/pkcs11_kernel.so
  /usr/lib/security/$ISA/pkcs11_softtoken.so

kernel software providers:
...
```

## ▼ Cómo evitar el uso de un proveedor de software de núcleo

Si la estructura criptográfica proporciona múltiples modos de un proveedor como AES, puede eliminar un mecanismo lento para no utilizarlo o un mecanismo dañado. Este procedimiento utiliza el algoritmo AES como ejemplo.

### 1 Conviértase en superusuario o asuma un rol que incluya el perfil de derechos de gestión de criptografía.

Para crear un rol que incluya el perfil de derechos de gestión de criptografía y asignar el rol a un usuario, consulte el [Ejemplo 9–7](#).

### 2 Muestre los mecanismos ofrecidos por un proveedor de software de núcleo determinado.

```
$ cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
```

**3 Muestre los mecanismos que están disponibles para su uso.**

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

**4 Deshabilite el mecanismo que no se debe utilizar.**

```
$ cryptoadm disable provider=aes mechanism=CKM_AES_ECB
```

**5 Muestre los mecanismos que están disponibles para su uso.**

```
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
```

**Ejemplo 14–21** Habilitación de un mecanismo de proveedor de software de núcleo

En el ejemplo siguiente, un mecanismo AES inhabilitado se vuelve a poner a disposición para su uso.

```
cryptoadm list -m provider=aes
aes: CKM_AES_ECB,CKM_AES_CBC
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled, except CKM_AES_ECB.
$ cryptoadm enable provider=aes mechanism=CKM_AES_ECB
$ cryptoadm list -p provider=aes
aes: all mechanisms are enabled.
```

**Ejemplo 14–22** Eliminación temporal de la disponibilidad de un proveedor de software de núcleo

En el siguiente ejemplo, se elimina temporalmente el proveedor AES para no utilizarlo. El subcomando `unload` es útil para evitar que un proveedor se cargue automáticamente mientras el proveedor se está desinstalando. Por ejemplo, el subcomando `unload` se utilizaría durante la instalación de un parche que afecte al proveedor.

```
$ cryptoadm unload provider=aes
```

```
$ cryptoadm list
...
kernel software providers:
  des
  aes (inactive)
  blowfish
  arcfour
  sha1
  md5
  rsa
  swrand
```

El proveedor AES no estará disponible hasta que la estructura criptográfica se haya actualizado.

```
$ svcadm refresh system/cryptosvc
```

```
$ cryptoadm list
...
kernel software providers:
  des
  aes
  blowfish
  arcfour
  sha1
  md5
  rsa
  swrand
```

Si un consumidor de núcleo está utilizando el proveedor de software de núcleo, el software no se descarga. Se muestra un mensaje de error y el proveedor sigue estando disponible para su uso.

### Ejemplo 14-23 Eliminación permanente de la disponibilidad de un proveedor de software

En el siguiente ejemplo, se elimina el proveedor AES para no utilizarlo. Una vez eliminado, el proveedor AES no aparece en la lista de la política de los proveedores de software de núcleo.

```
$ cryptoadm uninstall provider=aes

$ cryptoadm list
...
kernel software providers:
  des
  blowfish
  arcfour
  sha1
  md5
  rsa
  swrand
```

Si el consumidor de núcleo está utilizando el proveedor de software de núcleo, se muestra un mensaje de error y el proveedor sigue estando disponible para su uso.

### Ejemplo 14-24 Reinstalación de un proveedor de software de núcleo eliminado

En el siguiente ejemplo, se reinstala el proveedor de software de núcleo AES.

```
$ cryptoadm install provider=aes mechanism=CKM_AES_ECB,CKM_AES_CBC

$ cryptoadm list
...
kernel software providers:
  des
  aes
  blowfish
  arcfour
  sha1
  md5
  rsa
  swrand
```

## ▼ Cómo mostrar proveedores de hardware

Los proveedores de hardware se ubican y cargan automáticamente. Para obtener más información, consulte la página del comando `man driver.conf(4)`.

### Antes de empezar

Cuando cuanta con hardware que piensa usar dentro de la estructura criptográfica de Oracle Solaris, el hardware se registra en el SPI en el núcleo. La estructura comprueba que el controlador de hardware esté registrado. Específicamente, la estructura comprueba que el archivo de objeto del controlador esté registrado con un certificado emitido por Sun.

Por ejemplo, la placa Crypto Accelerator 6000 de Sun (`mca`), el controlador `ncp` para el acelerador criptográfico en los procesadores UltraSPARC T1 y T2 (`ncp`), y el controlador `n2cp` para los procesadores UltraSPARC T2 (`n2cp`) conectan los mecanismos de hardware a la estructura.

Para obtener información sobre cómo registrar a su proveedor, consulte “Firmas binarias para software de terceros” en la página 284.

### 1 Muestre los proveedores de hardware que están disponibles en el sistema.

```
% cryptoadm list
...
kernel hardware providers:
  ncp/0
```

### 2 Muestre los mecanismos que el chip o la placa proporcionan.

```
% cryptoadm list -m provider=ncp/0
ncp/0: CKM_DSA,CKM_RSA_X_509,CKM_RSA_PKCS,CKM_RSA_PKCS_KEY_PAIR_GEN,
CKM_DH_PKCS_KEY_PAIR_GEN,CKM_DH_PKCS_DERIVE,CKM_EC_KEY_PAIR_GEN,
CKM_ECDH1_DERIVE,CKM_ECDSA
```

### 3 Muestre los mecanismos que están disponibles para su uso en el chip o la placa.

```
% cryptoadm list -p provider=ncp/0
ncp/0: all mechanisms are enabled.
```

## ▼ Cómo deshabilitar funciones y mecanismos del proveedor de hardware

Puede deshabilitar de manera selectiva los mecanismos y la función de números aleatorios de un proveedor de hardware. Para habilitarlos nuevamente, consulte [Ejemplo 14–25](#). El hardware de este ejemplo, la placa Crypto Accelerator 1000 de Sun, proporciona un generador de números aleatorios.

## 1 Conviértase en superusuario o asuma un rol que incluya el perfil de derechos de gestión de criptografía.

Para crear un rol que incluya el perfil de derechos de gestión de criptografía y asignar el rol a un usuario, consulte el [Ejemplo 9–7](#).

## 2 Seleccione los mecanismos o la función que desea deshabilitar.

Muestre el proveedor de hardware.

```
# cryptoadm list
...
Kernel hardware providers:
  dca/0
```

### ■ Deshabilite los mecanismos seleccionados.

```
# cryptoadm list -m provider=dca/0
dca/0: CKM_RSA_PKCS, CKM_RSA_X_509, CKM_DSA, CKM_DES_CBC, CKM_DES3_CBC
random is enabled.
# cryptoadm disable provider=dca/0 mechanism=CKM_DES_CBC,CKM_DES3_CBC
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_CBC,CKM_DES3_CBC.
random is enabled.
```

### ■ Deshabilite el generador de números aleatorios.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

### ■ Deshabilite todos los mecanismos. No deshabilite el generador de números aleatorios.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is enabled.
```

### ■ Deshabilite todas las funciones y los mecanismos en el hardware.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
# cryptoadm disable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are disabled. random is disabled.
```

## Ejemplo 14–25 Habilitación de mecanismos y funciones en un proveedor de hardware

En los siguientes ejemplos, los mecanismos inhabilitados en una herramienta de hardware se habilitan de manera selectiva.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB,CKM_DES3_ECB
```

```
.
random is enabled.
# cryptoadm enable provider=dca/0 mechanism=CKM_DES3_ECB
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled except CKM_DES_ECB.
random is enabled.
```

En el ejemplo siguiente, sólo se habilita el generador aleatorio.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
# cryptoadm enable provider=dca/0 random
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is enabled.
```

En el ejemplo siguiente, sólo se habilitan los mecanismos. El generador aleatorio continúa inhabilitado.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_MD5,CKM_MD5_HMAC,...
random is disabled.
# cryptoadm enable provider=dca/0 mechanism=all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is disabled.
```

En el ejemplo siguiente, se habilitan todas las funciones y los mecanismos de la placa.

```
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled, except CKM_DES_ECB,CKM_DES3_ECB.
random is disabled.
# cryptoadm enable provider=dca/0 all
# cryptoadm list -p provider=dca/0
dca/0: all mechanisms are enabled. random is enabled.
```

## ▼ Cómo actualizar o reiniciar todos los servicios criptográficos

De manera predeterminada, la estructura criptográfica de Oracle Solaris está habilitada. Cuando el daemon `kcfd` falla por cualquier motivo, la utilidad de gestión de servicios se puede utilizar para reiniciar los servicios criptográficos. Para obtener más información, consulte las páginas del comando `man smf(5)` y `svcadm(1M)`. Para ver el efecto del reinicio de servicios criptográficos en las zonas, consulte [“Zonas y servicios criptográficos” en la página 285](#).

### 1 Compruebe el estado de los servicios criptográficos.

```
% svcs cryptosvc
STATE          STIME    FMRI
offline        Dec_09   svc:/system/cryptosvc:default
```

**2 Conviértase en superusuario o asuma un rol equivalente para habilitar servicios criptográficos.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) en la página 204.

```
# svcadm enable svc:/system/cryptosvc
```

**Ejemplo 14–26 Actualización de los servicios criptográficos**

En el siguiente ejemplo, se actualizan los servicios criptográficos en la zona global. Por lo tanto, también se actualiza la política criptográfica de nivel de núcleo de cada zona no global.

```
# svcadm refresh system/cryptosvc
```





## Estructura de gestión de claves de Oracle Solaris

---

A partir de la versión Solaris 10 8/07, la estructura de gestión de claves (KMF) proporciona herramientas e interfaces de programación para administrar objetos de clave pública. Los objetos de clave pública incluyen certificados X. 509 y pares de claves públicas o privadas. Los formatos para almacenar estos objetos pueden variar. KMF también proporciona una herramienta para administrar políticas que definan el uso de certificados X. 509 por parte de las aplicaciones.

- [“Administración de tecnologías de clave pública” en la página 313](#)
- [“Utilidades de la estructura de gestión de claves” en la página 314](#)
- [“Uso de la estructura de gestión de claves \(tareas\)” en la página 316](#)

### Administración de tecnologías de clave pública

La estructura de gestión de claves (KMF) ofrece un enfoque unificado para administrar tecnologías de clave pública (PKI). Oracle Solaris tiene varias aplicaciones que utilizan tecnologías PKI. Cada aplicación proporciona su propias interfaces de programación, mecanismos de almacenamiento de claves y utilidades administrativas. Si una aplicación proporciona un mecanismo de cumplimiento de políticas, el mecanismo se aplica sólo a esa aplicación. Con KMF, las aplicaciones utilizan un conjunto unificado de herramientas administrativas, un conjunto único de interfaces de programación y un mecanismo único de cumplimiento de políticas. Estas funciones gestionan las necesidades de PKI de todas las aplicaciones que adoptan estas interfaces.

KMF unifica la gestión de tecnologías de clave pública con las siguientes interfaces:

- **Comando `pktool`:** este comando administra objetos PKI, como certificados, en una variedad de almacenes de claves.
- **Comando `kmfcfg`:** este comando administra la base de datos de políticas PKI.

Las decisiones de políticas PKI incluyen operaciones, como el método de validación para una operación. Además, una política PKI puede limitar el ámbito de un certificado. Por ejemplo, una política PKI puede afirmar que un certificado sólo se puede utilizar para fines específicos. Una política de ese tipo puede impedir que ese certificado se utilice para otras solicitudes.

- **Biblioteca KMF:** esta biblioteca contiene interfaces de programación que abstraen el mecanismo subyacente de almacenes de claves.

Las aplicaciones no tienen que elegir un determinado mecanismo de almacenes de claves, si no que pueden migrar de un mecanismo a otro. Los almacenes de claves admitidos son PKCS #11, NSS y OpenSSL. La biblioteca incluye una estructura conectable de modo que puedan agregarse mecanismos de almacenes de claves nuevos. Por lo tanto, las aplicaciones que utilizan los mecanismos nuevos requerirían sólo pequeñas modificaciones para poder utilizar un almacén de claves nuevo.

## Utilidades de la estructura de gestión de claves

KMF proporciona métodos para administrar el almacenamiento de claves y proporciona la política global para utilizar esas claves. KMF administra la política, las claves y los certificados para tres tecnologías de clave pública:

- Tokens de los proveedores PKCS #11, es decir, de la estructura criptográfica de Oracle Solaris
- NSS, es decir, servicios de seguridad de red
- OpenSSL, un almacén de claves basado en archivos

La herramienta `kmfcfg` puede crear, modificar o eliminar entradas de políticas KMF. KMF administra almacenes de claves a través del comando `pktool`. Para obtener más información, consulte las páginas del comando `man kmfcfg(1)` y `pktool(1)`, y las secciones siguientes.

## Gestión de políticas KMF

La política KMF se almacena en una base de datos. Todas las aplicaciones que utilizan las interfaces de programación KMF acceden internamente a esta base de datos de políticas. La base de datos puede restringir el uso de las claves y los certificados administrados por la biblioteca KMF. Cuando una aplicación intenta verificar un certificado, la aplicación comprueba la base de datos de políticas. El comando `kmfcfg` modifica la base de datos de políticas.

## Gestión de almacenes de claves KMF

KMF administra los almacenes de claves para tres tecnologías de clave pública: tokens PKCS #11, NSS y OpenSSL. Para todas estas tecnologías, el comando `pktool` permite realizar las tareas siguientes:

- Generar un certificado autofirmado.
- Generar una solicitud de certificado.
- Importar objetos al almacén de claves.
- Enumerar los objetos del almacén de claves.
- Eliminar objetos del almacén de claves.
- Descargar una CRL.

Para las tecnologías PKCS #11 y NSS, el comando `pktool` también permite definir un PIN generando una frase de contraseña:

- Generar una frase de contraseña para el almacén de claves.
- Generar una frase de contraseña para un objeto del almacén de claves.

Para ver ejemplos de cómo usar la utilidad `pktool`, consulte la página del comando `man pktool(1)` y [“Uso de la estructura de gestión de claves \(mapa de tareas\)” en la página 315](#).

## Uso de la estructura de gestión de claves (mapa de tareas)

La estructura de gestión de claves (KMF) permite gestionar de manera centralizada las tecnologías de clave pública.

Tarea	Descripción	Para obtener instrucciones
Crear un certificado	Crea un certificado para uso de PKCS #11, NSS o SSL.	<a href="#">“Cómo crear un certificado mediante el comando <code>pktool gencert</code>” en la página 316</a>
Exportar un certificado	Crea un archivo con el certificado y sus claves admitidas. El archivo puede protegerse con una contraseña.	<a href="#">“Cómo exportar un certificado y una clave privada en formato PKCS #12” en la página 318</a>
Importar un certificado	Importa un certificado desde otro sistema.	<a href="#">“Cómo importar un certificado al almacén de claves” en la página 317</a>
	Importa un certificado en formato PKCS #12 desde otro sistema.	<a href="#">Ejemplo 15-2</a>
Generar una frase de contraseña	Genera una frase de contraseña para acceder a un almacén de claves PKCS #11 o a un almacén de claves NSS.	<a href="#">“Cómo generar una frase de contraseña mediante el comando <code>pktool setpin</code>” en la página 320</a>

## Uso de la estructura de gestión de claves (tareas)

En esta sección, se describe cómo utilizar el comando `pktool` para gestionar los objetos de clave pública, como contraseñas, frases de contraseña, archivos, almacenes de claves, certificados y CRL.

### ▼ Cómo crear un certificado mediante el comando `pktool gencert`

Este procedimiento crea un certificado autofirmado y almacena el certificado en el almacén de claves PKCS #11. Como parte de esta operación, también se crea un par de claves RSA públicas/privadas. La clave privada está almacenada en el almacén de claves con el certificado.

#### 1 Genere un certificado autofirmado.

```
% pktool gencert [keystore=keystore] label=label-name \
subject=subject-DN serial=hex-serial-number
```

<code>keystore=almacén de claves</code>	Especifica el almacén de claves por tipo de objeto de clave pública. El valor puede ser <code>nss</code> , <code>pkcs11</code> o <code>ssl</code> . La palabra clave es opcional.
<code>label=nombre_etiqueta</code>	Especifica un nombre único que el emisor asigna al certificado.
<code>subject=DN_asunto</code>	Especifica el nombre distintivo para el certificado.
<code>serial=número_serie_hex</code>	Especifica el número de serie en formato hexadecimal. El emisor del certificado elige el número, como <code>0x0102030405</code> .

#### 2 Verifique el contenido del almacén de claves.

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
   ID: Fingerprint that binds certificate to private key
   Subject: subject-DN
   Issuer: distinguished-name
   Serial: hex-serial-number
n. ...
```

Este comando muestra todos los certificados del almacén de claves. En el ejemplo siguiente, el almacén de claves contiene un solo certificado.

**Ejemplo 15–1 Creación de un certificado autofirmado mediante pktool**

En el ejemplo siguiente, un usuario de My Company crea un certificado autofirmado y almacena el certificado en un almacén de claves para objetos PKCS #11. El almacén de claves está vacío inicialmente. Si el almacén de claves no se inicializó, el PIN para el token de software es changeme.

```
% pktool gencert keystore=pkcs11 label="My Cert" \
subject="C=US, O=My Company, OU=Security Engineering Group, CN=MyCA" \
serial=0x00000001
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token

% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: My Cert
   ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
   Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Serial: 0x01
```

**▼ Cómo importar un certificado al almacén de claves**

Este procedimiento describe cómo importar al almacén de claves un archivo con información PKI que se codifica con PEM o con DER sin procesar. Para un procedimiento de exportación, consulte el [Ejemplo 15–4](#).

**1 Importe el certificado.**

```
% pktool import keystore=keystore infile=infile-name label=label-name
```

**2 Si va a importar objetos PKI privados, proporcione contraseñas cuando se le solicite.****a. En la petición de datos, proporcione la contraseña para el archivo.**

Si está importando información PKI que es privada, como un archivo de exportación en formato PKCS #12, el archivo requiere una contraseña. El creador del archivo que está importando proporciona la contraseña PKCS #12.

```
Enter password to use for accessing the PKCS12 file:    Type PKCS #12 password
```

**b. En la petición de datos, escriba la contraseña para el almacén de claves.**

```
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token
```

**3 Verifique el contenido del almacén de claves.**

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
```

```

ID: Fingerprint that binds certificate to private key
Subject: subject-DN
Issuer: distinguished-name
Serial: hex-serial-number
2. ...

```

### Ejemplo 15-2 Importación de un archivo PKCS #12 al almacén de claves

En el ejemplo siguiente, el usuario importa un archivo PKCS #12 de terceros. El comando `pktool import` extrae la clave privada y el certificado del archivo `gracedata.p12`, y los almacena en el almacén de claves preferido del usuario.

```

% pktool import keystore=pkcs11 infile=gracedata.p12 label=GraceCert
Enter password to use for accessing the PKCS12 file:      Type PKCS #12 password
Enter pin for Sun Software PKCS#11 softtoken:           Type PIN for token
Found 1 certificate(s) and 1 key(s) in gracedata.p12
% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: GraceCert
   ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
   Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Serial: 0x01

```

### Ejemplo 15-3 Importación de un certificado X.509 al almacén de claves

En el ejemplo siguiente, el usuario importa un certificado X.509 en formato PEM al almacén de claves preferido del usuario. Este certificado público no está protegido con una contraseña. El almacén de claves del usuario tampoco está protegido con una contraseña.

```

% pktool import keystore=pkcs11 infile=somecert.pem label="TheirCompany Root Cert"
% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: TheirCompany Root Cert
   ID: 21:ae:83:98:24:d1:1f:cb:65:5b:48:75:7d:02:47:cf:98:1f:ec:a0
   Subject: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
   Issuer: C=US, O=TheirCompany, OU=Security, CN=TheirCompany Root CA
   Serial: 0x01

```

## ▼ Cómo exportar un certificado y una clave privada en formato PKCS #12

Puede crear un archivo en formato PKCS #12 para exportar a otros sistemas las claves privadas y su certificado X.509 asociado. El acceso al archivo está protegido con una contraseña.

**1 Encuentre el certificado para exportar.**

```
% pktool list
Found number certificates.
1. (X.509 certificate)
   Label: label-name
   ID: Fingerprint that binds certificate to private key
   Subject: subject-DN
   Issuer: distinguished-name
   Serial: hex-serial-number
2. ...
```

**2 Exporte las claves y el certificado.**

Utilice el almacén de claves y la etiqueta del comando `pktool list`. Proporcione un nombre de archivo para el archivo de exportación. Si el nombre contiene un espacio, escríbalo entre comillas dobles.

```
% pktool export keystore=keystore outfile=outfile-name label=label-name
```

**3 Proteja el archivo de exportación con una contraseña.**

En la petición de datos, escriba la contraseña actual para el almacén de claves. En este punto, puede crear una contraseña para el archivo de exportación. El destinatario debe proporcionar esta contraseña al importar el archivo.

```
Enter pin for Sun Software PKCS#11 softtoken:    Type PIN for token
Enter password to use for accessing the PKCS12 file:    Create PKCS #12 password
```

---

**Consejo** – Envíe la contraseña por separado del archivo de exportación. De acuerdo con las prácticas recomendadas, es aconsejable proporcionar la contraseña fuera de banda, por ejemplo, durante una llamada telefónica.

---

**Ejemplo 15–4 Exportación de un certificado y una clave privada en formato PKCS #12**

En el ejemplo siguiente, un usuario exporta a un archivo PKCS #12 estándar las claves privadas con su certificado X.509 asociado. Este archivo se puede importar a otros almacenes de claves. La contraseña PKCS #11 protege el almacén de claves de origen. La contraseña PKCS #12 se utiliza para proteger los datos privados en el archivo PKCS #12. Esta contraseña es necesaria para importar el archivo.

```
% pktool list
Found 1 certificates.
1. (X.509 certificate)
   Label: My Cert
   ID: 12:82:17:5f:80:78:eb:44:8b:98:e3:3c:11:c0:32:5e:b6:4c:ea:eb
   Subject: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Issuer: C=US, O=My Company, OU=Security Engineering Group, CN=MyCA
   Serial: 0x01
```

```
% pktool export keystore=pkcs11 outfile=mydata.p12 label="My Cert"
Enter pin for Sun Software PKCS#11 softtoken:      Type PIN for token
Enter password to use for accessing the PKCS12 file: Create PKCS #12 password
```

A continuación, el usuario llama por teléfono al destinatario y proporciona la contraseña PKCS #12.

## ▼ Cómo generar una frase de contraseña mediante el comando `pktool setpin`

Puede generar una frase de contraseña para un objeto de un almacén de claves y para el almacén de claves en sí. La frase de contraseña es necesaria para acceder al objeto o al almacén de claves. Para ver un ejemplo de generación de una frase de contraseña para un objeto de un almacén de claves, consulte el [Ejemplo 15-4](#).

### 1 Genere una frase de contraseña para acceder a un almacén de claves.

```
% pktool setpin keystore=nss|pkcs11 dir=directory
```

### 2 Responda a las peticiones de datos.

Si el almacén de claves no tiene una contraseña definida, presione la tecla de retorno para crear la contraseña.

```
Enter current token passphrase:    Press the Return key
Create new passphrase:            Type the passphrase that you want to use
Re-enter new passphrase:          Retype the passphrase
Passphrase changed.
```

El almacén de claves está ahora protegido por la *frase de contraseña*. Si pierde la frase de contraseña, perderá el acceso a los objetos del almacén de claves.

## Ejemplo 15-5 Protección de un almacén de claves con una frase de contraseña

El ejemplo siguiente muestra cómo establecer la frase de contraseña para una base de datos NSS. Debido a que no se creó ninguna frase de contraseña, el usuario presiona la tecla de retorno en la primera petición de datos.

```
% pktool setpin keystore=nss dir=/var/nss
Enter current token passphrase:    Press the Return key
Create new passphrase:             has8n0NdaH
Re-enter new passphrase:           has8n0NdaH
Passphrase changed.
```



## P A R T E V

# Servicios de autenticación y comunicación segura

En esta sección se tratan los servicios de autenticación que se pueden configurar en un sistema que no está conectado a la red o entre dos sistemas.

- [Capítulo 16, “Uso de servicios de autenticación \(tareas\)”](#)
- [Capítulo 17, “Uso de PAM”](#)
- [Capítulo 18, “Uso de SASL”](#)
- [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#)
- [Capítulo 20, “Oracle Solaris Secure Shell \(referencia\)”](#)

Para configurar una red de usuarios autenticados y sistemas, consulte la [Parte VI](#).



## Uso de servicios de autenticación (tareas)

---

En este capítulo se proporciona información sobre cómo utilizar RPC segura para autenticar un host y un usuario en un montaje NFS. A continuación puede ver una lista de los temas de este capítulo.

- “Descripción general de RPC segura” en la página 323
- “Administración de RPC segura (mapa de tareas)” en la página 328

### Descripción general de RPC segura

La llamada de procedimiento remoto (RPC) segura protege los procedimientos remotos con un mecanismo de autenticación. El mecanismo de autenticación Diffie-Hellman autentica tanto el host como el usuario que realiza una solicitud para un servicio. El mecanismo de autenticación utiliza el cifrado Estándar de cifrado de datos (DES). Las aplicaciones que utilizan RPC segura incluyen NFS y los servicios de nombres, NIS y NIS+.

### Servicios NFS y RPC segura

NFS permite que varios hosts compartan archivos a través de la red. En el servicio NFS, un servidor contiene los datos y recursos para varios clientes. Los clientes tienen acceso a los sistemas de archivos que el servidor comparte con los clientes. Los usuarios conectados a los sistemas cliente pueden acceder a los sistemas de archivos mediante el montaje de sistemas de archivos del servidor. Para el usuario en el sistema cliente, los archivos se ven como locales para el cliente. Uno de los usos más comunes de NFS permite que los sistemas se instalen en oficinas mientras se almacenan todos los archivos de usuario en una ubicación central. Algunas de las funciones del servicio NFS, como la opción `-nosuid` para el comando `mount`, se pueden utilizar para prohibir la apertura de dispositivos y sistemas de archivos por parte de usuarios no autorizados.

El servicio NFS utiliza RPC segura para autenticar a los usuarios que realizan solicitudes a través de la red. Este proceso se conoce como *NFS seguro*. El mecanismo de autenticación Diffie-Hellman, AUTH\_DH, usa cifrado DES para garantizar el acceso autorizado. El mecanismo AUTH\_DH también se ha denominado AUTH\_DES. Para obtener más información, consulte lo siguiente:

- Para configurar y administrar NFS seguro, consulte “[Administración de sistema NFS seguro](#)” de *Guía de administración del sistema: servicios de red*.
- Para configurar las tablas NIS+ e introducir nombres en la tabla cred, consulte la *System Administration Guide: Naming and Directory Services (NIS+)*.
- Para una descripción de las transacciones implicadas en la autenticación RPC, consulte “[Implementación de autenticación Diffie-Hellman](#)” en la página 325.

## Cifrado DES con NFS seguro

Las funciones de cifrado del Estándar de cifrado de datos (DES) utiliza una clave de 56 bits para cifrar los datos. Si dos principales o usuarios de credenciales conocen la misma clave DES, pueden comunicarse en privado mediante la clave para cifrar y descifrar texto. DES es un mecanismo de cifrado relativamente rápido. Un chip DES hace que el cifrado sea incluso más rápido. Sin embargo, si el chip no está presente, se sustituye una implementación de software.

El riesgo de usar sólo la clave DES es que un intruso puede recopilar suficientes mensajes de texto cifrado que se cifraron con la misma clave para poder descubrir la clave y descifrar los mensajes. Por este motivo, los sistemas de seguridad como NFS seguro necesitan cambiar las claves con frecuencia.

## Autenticación Kerberos

Kerberos es un sistema de autenticación desarrollado en MIT. Algunos cifrados en Kerberos se basan en DES. El soporte de Kerberos V4 ya no se proporciona como parte de RPC segura. Sin embargo, una implementación por parte del cliente y por parte del servidor de Kerberos V5, que utiliza RPCSEC\_GSS, se incluye con esta versión. Para obtener más información, consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).

## Autenticación Diffie-Hellman y RPC segura

El método de autenticación de un usuario Diffie-Hellman (DH) no es trivial para un intruso que quiere ingresar. El cliente y el servidor tienen sus propias claves privadas, las cuales se utilizan con la clave pública para crear una clave común. La clave privada también se conoce como *clave secreta*. El cliente y el servidor utilizan la clave común para comunicarse entre sí. La clave común se cifra con una función de cifrado acordada, como DES.

La autenticación se basa en la capacidad del sistema emisor de utilizar la clave común para cifrar la hora actual. A continuación, el sistema receptor puede descifrar y comprobar la hora actual. La hora en el cliente y el servidor debe estar sincronizada. Para obtener más información, consulte “[Gestión del protocolo de hora de red \(tareas\)](#)” de *Guía de administración del sistema: servicios de red*.

Las claves públicas y privadas se almacenan en una base de datos NIS o NIS+. NIS almacena las claves en el mapa `publickey`. NIS+ almacena las claves en la tabla `cred`. Estos archivos contienen la clave pública y la clave privada para todos los usuarios potenciales.

El administrador del sistema es responsable de configurar mapas NIS o tablas NIS+ y de generar una clave pública y una clave privada para cada usuario. La clave privada se almacena en formato cifrado con la contraseña del usuario. Este proceso hace que sólo el usuario conozca la clave privada.

## Implementación de autenticación Diffie-Hellman

En esta sección se describe la serie de transacciones en una sesión cliente-servidor que utiliza autenticación Diffie-Hellman (AUTH\_DH).

### Generación de las claves públicas y las claves secretas para RPC segura

A veces, antes de una transacción, el administrador ejecuta el comando `newkey` o `nisaddcred` para generar una clave pública y una clave secreta. Cada usuario tiene una clave pública y una clave secreta únicas. La clave pública se almacena en una base de datos pública. La clave secreta se almacena en formato cifrado en la misma base de datos. El comando `chkey` cambia el par de claves.

### Ejecución del comando `keylogin` para RPC segura

Normalmente, la contraseña de inicio de sesión es idéntica a la contraseña de RPC segura. En este caso, el comando `keylogin` no es necesario. Sin embargo, si las contraseñas son distintas, los usuarios tienen que iniciar sesión y, a continuación, ejecutar el comando `keylogin`.

El comando `keylogin` le solicita al usuario una contraseña de RPC segura. El comando utiliza la contraseña para descifrar la clave secreta. El comando `keylogin` pasa la clave secreta descifrada al programa *servidor de claves*. El servidor de claves es un servicio RPC con una instancia local en cada equipo. El servidor de claves guarda la clave secreta descifrada y espera a que el usuario inicie una transacción RPC segura con un servidor.

Si la contraseña de inicio de sesión y la contraseña de RPC son iguales, el proceso de inicio de sesión pasa la clave secreta al servidor de claves. Si las contraseñas deben ser diferentes, el usuario debe ejecutar siempre el comando `keylogin`. Cuando el comando `keylogin` se incluye en el archivo de configuración del entorno del usuario, como el archivo `~/.login`, `~/.cshrc` o `~/.profile`, el comando `keylogin` se ejecuta automáticamente siempre que el usuario inicia sesión.

## Generación de clave de conversación para RPC segura

Cuando el usuario inicia una transacción con un servidor, ocurre lo siguiente:

1. El servidor de claves genera aleatoriamente una clave de conversación.
2. El núcleo usa la clave de conversación junto con otros materiales para cifrar la indicación de hora del cliente.
3. El servidor de claves busca la clave pública del servidor en la base de datos de claves públicas. Para obtener más información, consulte la página del comando `man publickey(4)`.
4. El servidor de claves utiliza la clave secreta del cliente y la clave pública del servidor para crear una clave común.
5. El servidor de claves cifra la clave de conversación con la clave común.

## Ponerse en contacto inicialmente con el servidor en RPC segura

La transmisión, que incluye la indicación de hora cifrada y la clave de conversación cifrada, se envía al servidor. La transmisión incluye una credencial y un verificador. La credencial contiene tres componentes:

- El nombre de red del cliente
- La clave de conversación, que se cifra con la clave común
- Una "ventana", que se cifra con la clave de conversación

La ventana es la diferencia en tiempo que el cliente afirma que se debe permitir entre el reloj del servidor y la indicación de hora del cliente. Si la diferencia entre el reloj del servidor y la indicación de hora es mayor que la ventana, el servidor rechaza la solicitud del cliente. En circunstancias normales, este rechazo no se produce porque el cliente primero se sincroniza con el servidor antes de iniciar la sesión RPC.

El verificador del cliente contiene lo siguiente:

- La indicación de hora cifrada
- Un verificador cifrado de la ventana especificada, que se reduce a 1

El verificador de ventana es necesario en caso de que alguien desee asumir la personalidad de un usuario. El imitador puede escribir un programa que, en lugar de completar los campos cifrados de la credencial y el verificador, sólo inserte bits de manera aleatoria. El servidor descifra la clave de conversación en alguna clave aleatoria. El servidor utiliza la clave para intentar descifrar la ventana y la indicación de hora. El resultado son números aleatorios. Después de miles de intentos, sin embargo, el par ventana/indicación de hora aleatorio podría pasar el sistema de autenticación. El verificador de ventana disminuye la posibilidad de que una credencial falsa se pueda autenticar.

## Descifrado de la clave de conversación en RPC segura

Cuando el servidor recibe la transmisión del cliente, se produce lo siguiente:

1. El servidor de claves local del servidor busca la clave pública del cliente en la base de datos de claves públicas.
2. El servidor de claves utiliza la clave pública del cliente y la clave secreta del servidor para deducir la clave común. La clave común es la misma clave común que el cliente procesa. Sólo el servidor y el cliente pueden calcular la clave común porque el cálculo requiere que se conozca una de las claves secretas.
3. El núcleo usa la clave común para descifrar la clave de conversación.
4. El núcleo llama al servidor de claves para descifrar la indicación de hora del cliente con la clave de conversación descifrada.

## Almacenamiento de información en el servidor en RPC segura

Después de que el servidor descifra la indicación de hora del cliente, el servidor almacena cuatro elementos de información en una tabla de credenciales:

- El nombre de equipo del cliente
- La clave de conversación
- La ventana
- La indicación de hora del cliente

El servidor almacena los primeros tres elementos para su uso futuro. El servidor almacena la indicación de hora del cliente para evitar que se realicen reproducciones. El servidor acepta sólo indicaciones de hora que son cronológicamente mayores que la última indicación de hora vista. Como resultado, cualquier transacción reproducida seguramente sea rechazada.

---

**Nota** – El nombre del emisor de llamada está implícito en las transacciones. El emisor se debe autenticar de alguna manera. El servidor de claves no puede usar la autenticación DES para autenticar el emisor de llamada porque el uso de DES por parte del servidor de claves crearía un interbloqueo. Para evitar un interbloqueo, el servidor de claves almacena las claves secretas por ID de usuario (UID) y otorga solicitudes sólo a procesos root locales.

---

## Devolución del verificador al cliente en RPC segura

El servidor devuelve un verificador al cliente, que incluye lo siguiente:

- El ID de índice, que el servidor registra en su antememoria de credenciales
- La indicación de hora del cliente menos 1, que se cifra mediante la clave de conversación

El motivo para sustraer 1 de la indicación de hora del cliente es para asegurarse de que la indicación de hora esté desactualizada. Una indicación de hora desactualizada no puede volver a utilizarse como un verificador de cliente.

### Autenticación del servidor en RPC segura

El cliente recibe el verificador y autentica el servidor. El cliente sabe que sólo el servidor pudo haber enviado el verificador ya que sólo el servidor conoce la indicación de hora que el cliente envió.

### Manejo de transacciones en RPC segura

Con cada transacción después de la primera transacción, el cliente devuelve el ID de índice al servidor en su siguiente transacción. El cliente también envía otra indicación de hora cifrada. El servidor envía de vuelta la indicación de hora del cliente menos 1, que se cifra mediante la clave de conversación.

## Administración de RPC segura (mapa de tareas)

El siguiente mapa de tareas indica los procedimientos que configuran RPC segura para NIS, NIS+ y NFS.

Tarea	Descripción	Para obtener instrucciones
1. Iniciar el servidor de claves	Asegura que se puedan crear claves para que se puedan autenticar los usuarios.	<a href="#">“Cómo reiniciar el servidor de claves RPC segura” en la página 329</a>
2. Configurar credenciales en un host NIS+	Asegura que el usuario root en un host se pueda autenticar en un entorno NIS+.	<a href="#">“Cómo configurar una clave Diffie-Hellman para un host NIS+” en la página 329</a>
3. Otorgar una clave a un usuario NIS+	Permite que se autentique un usuario en un entorno NIS+.	<a href="#">“Cómo configurar una clave Diffie-Hellman para un usuario NIS+” en la página 330</a>
4. Configurar credenciales en un host NIS	Asegura que el usuario root en un host se pueda autenticar en un entorno NIS.	<a href="#">“Cómo configurar una clave Diffie-Hellman para un host NIS” en la página 331</a>
5. Otorgar una clave a un usuario NIS	Permite que se autentique un usuario en un entorno NIS.	<a href="#">“Cómo configurar una clave Diffie-Hellman para un usuario NIS” en la página 332</a>
6. Compartir archivos NFS con autenticación	Permite a un servidor NFS proteger de manera segura los sistemas de archivos compartidos mediante la autenticación.	<a href="#">“Cómo compartir archivos NFS con autenticación Diffie-Hellman” en la página 333</a>



# Administración de autenticación con RPC segura (tareas)

Al requerir autenticación para el uso de sistemas de archivos NFS montados, aumenta la seguridad de la red.

## ▼ Cómo reiniciar el servidor de claves RPC segura

- 1 **Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Verifique que el daemon key serv esté en ejecución.**

```
# svcs \*key serv\*
STATE      STIME      FMRI
disabled Dec_14    svc:/network/rpc/key serv
```

- 3 **Habilite el servicio de servidor de claves si el servidor no está en línea.**

```
# svcadm enable network/rpc/key serv
```

## ▼ Cómo configurar una clave Diffie-Hellman para un host NIS+

Este procedimiento debe realizarse en cada host en el dominio NIS+. Después de que root haya ejecutado el comando `key login`, el servidor tiene credenciales de aceptador GSS-API para `mech_dh` y el cliente tiene credenciales de iniciador GSS-API.

Para obtener una descripción detallada de seguridad NIS+, consulte la [System Administration Guide: Naming and Directory Services \(NIS+\)](#).

- 1 **Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Habilite la tabla `publickey` en el servicio de nombres.**

Agregue la siguiente línea al archivo `/etc/nsswitch.conf`:

```
publickey: nisplus
```

- 3 **Inicialice el cliente NIS+.**

```
# nisinit -cH hostname
```

Donde *nombre de host* es el nombre de un servidor NIS+ de confianza que contiene una entrada en sus tablas para el sistema cliente.

#### 4 Agregue el cliente a la tabla cred.

Escriba los comandos siguientes:

```
# nisaddcred local
# nisaddcred des
```

#### 5 Verifique la configuración mediante el comando keylogin.

Si se le solicita una contraseña, el procedimiento se ha realizado correctamente.

```
# keylogin
Password:
```

### Ejemplo 16–1 Configuración de una nueva clave para root en un cliente NIS+

El siguiente ejemplo utiliza el host `pluto` para configurar `earth` como un cliente NIS+. Puede ignorar las advertencias. El comando `keylogin` se acepta al verificar que `earth` está correctamente configurado como un cliente NIS+ seguro.

```
# nisinit -cH pluto
NIS Server/Client setup utility.
This system is in the example.com. directory.
Setting up NIS+ client ...
All done.
# nisaddcred local
# nisaddcred des
DES principal name : unix.earth@example.com
Adding new key for unix.earth@example.com (earth.example.com.)
Network password:  <Type password>
Warning, password differs from login password.
Retype password:   <Retype password>
# keylogin
Password:          <Type password>
#
```

## ▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS+

Este procedimiento debe realizarse en cada usuario en el dominio NIS+.

#### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Agregue el usuario a la tabla cred en el servidor maestro root.**

Escriba el siguiente comando:

```
# nisaddcred -p unix.UID@domain-name -P username.domain-name. des
```

Tenga en cuenta que, en este caso, el *nombre de usuario.nombre de dominio* debe finalizar con un punto (.).

**3 Verifique la configuración mediante el inicio de sesión como cliente y mediante el comando keylogin.****Ejemplo 16–2 Configuración de una nueva clave para un usuario NIS+**

En el siguiente ejemplo, una clave para autenticación Diffie-Hellman se proporciona al usuario jdoe.

```
# nisaddcred -p unix.1234@example.com -P jdoe.example.com. des
DES principal name : unix.1234@example.com
Adding new key for unix.1234@example.com (jdoe.example.com.)
Password:          <Type password>
Retype password:   <Retype password>
# rlogin rootmaster -l jdoe
% keylogin
Password:          <Type password>
%
```

**▼ Cómo configurar una clave Diffie-Hellman para un host NIS**

Este procedimiento debe realizarse en cada host en el dominio NIS.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Habilite el mapa publickey en el servicio de nombres.**

Agregue la siguiente línea al archivo `/etc/nsswitch.conf`:

```
publickey: nis
```

**3 Cree un nuevo par de claves mediante el comando newkey.**

```
# newkey -h hostname
```

Donde *nombre de host* es el nombre del cliente.

**Ejemplo 16-3 Configuración de una nueva clave para root en un cliente NIS**

En el siguiente ejemplo, earth se configura como un cliente NIS seguro.

```
# newkey -h earth
Adding new key for unix.earth@example.com
New Password:      <Type password>
Retype password:   <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

## ▼ Cómo configurar una clave Diffie-Hellman para un usuario NIS

Este procedimiento debe realizarse para cada usuario en el dominio NIS.

**Antes de empezar** Sólo los administradores del sistema, cuando inician sesión en el servidor maestro NIS, pueden generar una nueva clave para un usuario.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 Cree una nueva clave para un usuario.**

```
# newkey -u username
```

Done *nombre de usuario* es el nombre del usuario. El sistema solicita una contraseña. Puede escribir una contraseña genérica. La clave privada se almacena en formato cifrado mediante la contraseña genérica.

**3 Indique al usuario que inicie sesión y escriba el comando chkey -p.**

Este comando permite a los usuarios volver a cifrar sus claves privadas con una contraseña que sólo ellos conozcan.

---

**Nota** – El comando chkey se puede utilizar para crear un nuevo par de claves para un usuario.

---

**Ejemplo 16-4 Configuración y cifrado de una nueva clave de usuario en NIS**

En este ejemplo, el superusuario configura la clave.

```
# newkey -u jdoe
Adding new key for unix.12345@example.com
New Password:      <Type password>
Retype password:   <Retype password>
Please wait for the database to get updated...
Your new key has been successfully stored away.
#
```

Luego el usuario jdoe vuelve a cifrar la clave con una contraseña privada.

```
% chkey -p
Updating nis publickey database.
Reencrypting key for unix.12345@example.com
Please enter the Secure-RPC password for jdoe:  <Type password>
Please enter the login password for jdoe:      <Type password>
Sending key change request to centralexample...
```

## ▼ Cómo compartir archivos NFS con autenticación Diffie-Hellman

Este procedimiento protege los sistemas de archivos compartidos en un servidor NFS mediante la solicitud de autenticación para acceso.

### Antes de empezar

La autenticación de clave pública Diffie-Hellman debe estar habilitada en la red. Para habilitar la autenticación en la red, realice una de las siguientes acciones:

- “[Cómo configurar una clave Diffie-Hellman para un host NIS+](#)” en la página 329
- “[Cómo configurar una clave Diffie-Hellman para un host NIS](#)” en la página 331

### 1 Conviértase en superusuario o asuma un rol que incluya el perfil de gestión de sistemas de archivos.

El rol de administrador del sistema incluye el perfil de gestión de sistemas de archivos. Para crear el rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” en la página 204.

### 2 En el servidor NFS, comparta un sistema de archivos con autenticación Diffie-Hellman.

```
# share -F nfs -o sec=dh /filesystem
```

Donde *sistema de archivos* es el sistema de archivos que se va a compartir.

La opción `-o sec=dh` significa que la autenticación AUTH\_DH ahora es necesaria para acceder al sistema de archivos.

### 3 En un cliente NFS, monte un sistema de archivos con autenticación Diffie-Hellman.

```
# mount -F nfs -o sec=dh server:filesystem mount-point
```

<i>servidor</i>	Es el nombre del sistema que comparte <i>sistema de archivos</i>
<i>sistema de archivos</i>	Es el nombre del sistema de archivos que se comparte, como <code>opt</code>
<i>punto_montaje</i>	Es el nombre del punto de montaje, como <code>/opt</code>
La opción <code>-o sec=dh</code> monta el sistema de archivos con autenticación <code>AUTH_DH</code> .	

## Uso de PAM

---

En este capítulo, se trata la estructura del módulo de autenticación conectable (PAM, Pluggable Authentication Module). PAM proporciona un método para “conectar” servicios de autenticación en el SO Oracle Solaris. PAM proporciona compatibilidad para varios servicios de autenticación al acceder a un sistema.

- “PAM (descripción general)” en la página 335
- “PAM (tareas)” en la página 338
- “Configuración de PAM (referencia)” en la página 341

### PAM (descripción general)

La estructura del módulo de autenticación conectable (PAM) permite “conectar” nuevos servicios de autenticación sin modificar los servicios de entrada del sistema, como login, ftp y telnet. También puede utilizar PAM para integrar el inicio de sesión de UNIX con otros mecanismos de seguridad, como Kerberos. También se pueden “conectar” mediante esta estructura mecanismos para la gestión de cuentas, credenciales, sesiones y contraseñas.

### Ventajas del uso de PAM

La estructura PAM permite configurar el uso de servicios de entrada del sistema (como, ftp, login, telnet o rsh) para la autenticación del usuario. Algunas ventajas que ofrece PAM son:

- Política de configuración flexible
  - Política de autenticación por aplicación
  - La capacidad de elegir un mecanismo de autenticación predeterminado
  - La capacidad de requerir varias autorizaciones en sistemas de seguridad elevada
- Facilidad de uso para el usuario final
  - La capacidad de no tener que volver a escribir las contraseñas si son iguales para diferentes servicios de autenticación

- La capacidad de solicitar al usuario contraseñas para varios servicios de autenticación sin necesidad de que el usuario escriba varios comandos
- La capacidad de transferir características opcionales a los servicios de autenticación de usuario
- La capacidad de implementar una política de seguridad específico del sitio sin tener que cambiar los servicios de entrada del sistema

## Introducción a la estructura PAM

La estructura PAM consta de cuatro partes:

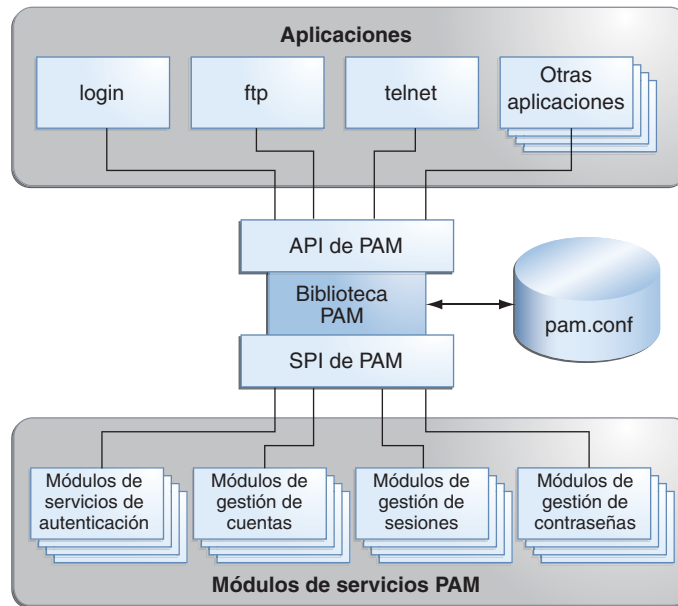
- Consumidores PAM
- Biblioteca PAM
- Archivo de configuración `pam.conf(4)`
- Módulos de servicios PAM, también denominados proveedores

La estructura proporciona un modo uniforme para llevar a cabo las actividades relacionadas con la autenticación. Este enfoque permite a los desarrolladores de aplicaciones usar los servicios PAM sin tener que conocer la semántica de la política. Los algoritmos se proporcionan de forma centralizada. Los algoritmos se pueden modificar independientemente de las aplicaciones individuales. Con PAM, los administradores pueden adaptar el proceso de autenticación a las necesidades de un determinado sistema sin tener que cambiar ninguna aplicación. Los ajustes se realizan mediante `pam.conf`, el archivo de configuración de PAM.

La siguiente figura ilustra la arquitectura PAM. Las aplicaciones se comunican con la biblioteca PAM a través de la interfaz de programación de aplicaciones (API) de PAM. Los módulos PAM se comunican con la biblioteca PAM a través de la interfaz del proveedor de servicios (SPI) de PAM. Por lo tanto, la biblioteca PAM permite a las aplicaciones y los módulos comunicarse entre sí.



FIGURA 17-1 Arquitectura PAM



## Cambios de PAM en Solaris 10

La versión Solaris 10 incluye los siguientes cambios en la estructura del módulo de autenticación conectable (PAM):

- Con el módulo `pam_authtok_check`, ahora se puede realizar una comprobación de contraseñas estricta con nuevos parámetros ajustables en el archivo `/etc/default/passwd`. Los nuevos parámetros definen:
  - Una lista de archivos de diccionario separados por comas que se usan para comprobar palabras de diccionario comunes en una contraseña.
  - Las diferencias mínimas que se requiere entre una contraseña nueva y una antigua.
  - El número mínimo de caracteres alfabéticos o no alfabéticos que se deben usar en una contraseña nueva.
  - El número mínimo de letras en mayúscula o en minúscula que se deben usar en una contraseña nueva.
  - El número permitido de caracteres repetidos consecutivos.
- El módulo `pam_unix_auth` implementa bloqueos de cuentas para los usuarios locales. Un bloqueo de cuenta se habilita con el parámetro `LOCK_AFTER_RETRIES` en `/etc/security/policy.conf` y la clave `lock_after-retries` en `/etc/user_attr`. Para obtener más información, consulte las páginas del comando `man policy.conf(4)` y `user_attr(4)`.

- Se ha definido un nuevo indicador de control `binding`. Este indicador de control se documenta en la página del comando `man pam.conf(4)` y en “[Cómo funciona el apilamiento PAM](#)” en la página 342.
- El módulo `pam_unix` se ha eliminado y se ha sustituido por un conjunto de módulos de servicios con una funcionalidad equivalente o superior. Muchos de estos módulos se introdujeron en la versión Solaris 9. A continuación, aparece la lista de los módulos de sustitución:
  - `pam_authtok_check`
  - `pam_authtok_get`
  - `pam_authtok_store`
  - `pam_dhkeys`
  - `pam_passwd_auth`
  - `pam_unix_account`
  - `pam_unix_auth`
  - `pam_unix_cred`
  - `pam_unix_session`
- Las funcionalidades del módulo `pam_unix_auth` se han dividido en dos módulos. El módulo `pam_unix_auth` se encarga ahora de verificar que la contraseña sea la correcta para el usuario, mientras que el nuevo módulo `pam_unix_cred` proporciona funciones que establecen información sobre las credenciales del usuario.
- Se han realizado adiciones al módulo `pam_krb5` para gestionar la antememoria de credenciales de Kerberos con la estructura PAM.
- Se ha agregado un nuevo módulo `pam_deny`. El módulo se puede utilizar para denegar el acceso a servicios. De manera predeterminada, el módulo `pam_deny` no se usa. Para obtener más información, consulte la página del comando `man pam_deny(5)`.

## PAM (tareas)

En esta sección, se tratan algunas tareas que pueden ser necesarias para que la estructura PAM use una determinada política de seguridad. Debe tener en cuenta algunos problemas de seguridad asociados al archivo de configuración de PAM. Para obtener información sobre los problemas de seguridad, consulte “[Planificación de la implementación de PAM](#)” en la página 339.

## PAM (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Planificar la instalación de PAM	Tenga en cuenta los problemas de configuración y tome decisiones acerca de ellos antes de iniciar el proceso de configuración de software.	<a href="#">“Planificación de la implementación de PAM” en la página 339</a>
Agregar nuevos módulos PAM	A veces, se deben escribir e instalar módulos específicos del sitio para satisfacer requisitos que no forman parte del software genérico. Este procedimiento explica cómo instalar estos nuevos módulos PAM.	<a href="#">“Cómo agregar un módulo PAM” en la página 340</a>
Bloquear el acceso a través de <code>~/ .rhosts</code>	Impida el acceso a través de <code>~/ .rhosts</code> para mejorar aún más la seguridad.	<a href="#">“Cómo evitar el acceso de tipo <code>.rhost</code> desde sistemas remotos con PAM” en la página 341</a>
Iniciar el registro de errores	Inicie el registro de mensajes de error relacionados con PAM mediante <code>syslog</code> .	<a href="#">“Cómo registrar los informes de errores de PAM” en la página 341</a>

## Planificación de la implementación de PAM

Tal como se suministra, el archivo de configuración `pam.conf` implementa la política de seguridad estándar. Esta política funciona en diversas situaciones. Si debe implementar una política de seguridad distinta, aquí se muestran los problemas en los que se debe centrar:

- Determine cuáles son sus necesidades, especialmente qué módulos de servicios PAM debe seleccionar.
- Identifique los servicios que necesitan opciones de configuración especiales. Use `other` si corresponde.
- Decida el orden en que se deben ejecutar los módulos.
- Seleccione el indicador de control para cada módulo. Consulte [“Cómo funciona el apilamiento PAM” en la página 342](#) para obtener más información sobre todos los indicadores de control.
- Seleccione las opciones que son necesarias para cada módulo. La página del comando `man` de cada módulo debe enumerar las opciones especiales.

A continuación, exponemos algunas sugerencias que se deben tener en cuenta antes de cambiar el archivo de configuración de PAM:

- Utilice entradas `other` para cada tipo de módulo para que no sea necesario incluir cada aplicación en `/etc/pam.conf`.
- Asegúrese de tener en cuenta las consecuencias para la seguridad de los indicadores de control `binding`, `sufficient` y `optional`.

- Revise las páginas del comando `man` que están asociadas a los módulos. Estas páginas del comando `man` puede ayudar a comprender cómo funciona cada módulo, qué opciones están disponibles y las interacciones entre los módulos apilados.




---

**Precaución** – Si el archivo de configuración de PAM no está configurado correctamente o se daña el archivo, es posible que ningún usuario pueda iniciar sesión. Como el comando `su` login no utiliza PAM, se necesita la contraseña de usuario `root` para iniciar el equipo en modo de usuario único y corregir el problema.

---

Después de cambiar el archivo `/etc/pam.conf`, revise el archivo lo más posible mientras sigue teniendo acceso al sistema para corregir problemas. Pruebe todos los comandos que posiblemente hayan sido afectados por los cambios. Un ejemplo es agregar un módulo nuevo al servicio `telnet`. En este ejemplo, debe utilizar el comando `telnet` y verificar que los cambios hacen que el comportamiento del servicio sea el esperado.

## ▼ Cómo agregar un módulo PAM

Este procedimiento muestra cómo agregar un nuevo módulo PAM. Es posible crear nuevos módulos para satisfacer políticas de seguridad específicas del sitio o para admitir aplicaciones de terceros.

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Determine qué indicadores de control y qué otras opciones se deben utilizar.

Consulte [“Cómo funciona el apilamiento PAM” en la página 342](#) para obtener información sobre los indicadores de control.

### 3 Asegúrese de que la propiedad y los permisos estén definidos de modo que el archivo del módulo sea propiedad de `root` y los permisos sean `555`.

### 4 Edite el archivo de configuración de PAM, `/etc/pam.conf`, y agregue este módulo a los servicios apropiados.

### 5 Verifique que el módulo se haya agregado correctamente.

Debe realizar una prueba *antes* de reiniciar el sistema en caso de que el archivo de configuración no esté configurado correctamente. Inicie sesión con un servicio directo, como `ssh`, y ejecute el comando `su` antes de reiniciar el sistema. El servicio puede ser un daemon que se reproduce sólo una vez cuando se inicia el sistema. A continuación, debe reiniciar el sistema para poder verificar que el módulo se haya agregado.

## ▼ Cómo evitar el acceso de tipo .rhost desde sistemas remotos con PAM

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Elimine todas las líneas que incluyen `rhhosts_auth.so.1` del archivo de configuración de PAM.

Este paso impide la lectura de los archivos `~/ .rhhosts` durante una sesión `rlogin`. Por lo tanto, este paso impide el acceso no autenticado al sistema local desde sistemas remotos. Cualquier acceso `rlogin` requiere una contraseña, independientemente de la presencia o el contenido de los archivos `~/ .rhhosts` o `/etc/hosts.equiv`.

### 3 Deshabilite el servicio `rsh`.

Para impedir cualquier otro acceso no autenticado a los archivos `~/ .rhhosts`, recuerde que debe deshabilitar el servicio `rsh`.

```
# svcadm disable network/shell
```

## ▼ Cómo registrar los informes de errores de PAM

### 1 Conviértase en superusuario o asuma un rol similar.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Configure el archivo `/etc/syslog.conf` para el nivel de registro que necesita.

Consulte [`syslog.conf\(4\)`](#) para obtener más información sobre los niveles de registro.

### 3 Actualice la información de configuración del daemon `syslog`.

```
# svcadm refresh system/system-log
```

## Configuración de PAM (referencia)

El archivo de configuración de PAM, [`pam.conf\(4\)`](#), se utiliza para configurar los módulos de servicios PAM para los servicios del sistema, como `login`, `rlogin`, `su` y `cron`. El administrador del sistema gestiona este archivo. Un orden incorrecto de las entradas en `pam.conf` puede provocar efectos secundarios imprevistos. Por ejemplo, un archivo `pam.conf` configurado incorrectamente puede bloquear los usuarios de manera que el modo de usuario único resulta necesario para su reparación. Para obtener una descripción acerca de cómo establecer el orden, consulte [“Cómo funciona el apilamiento PAM” en la página 342](#).

## Sintaxis de archivo de configuración de PAM

Las entradas del archivo de configuración tienen el siguiente formato:

*service-name module-type control-flag module-path module-options*

<i>nombre_servicio</i>	Nombre del servicio, por ejemplo, ftp, login o passwd. Una aplicación puede utilizar distintos nombres para los servicios que la aplicación proporciona. Por ejemplo, el daemon de shell seguro de Oracle Solaris utiliza estos nombres de servicio: sshd - none, sshd - password, sshd - kbdint, sshd - pubkey y sshd - hostbased. El nombre de servicio <i>other</i> es un nombre predefinido que se utiliza como nombre de servicio comodín. Si no se encuentra un determinado nombre de servicio en el archivo de configuración, se utiliza la configuración de <i>other</i> .
<i>tipo_módulo</i>	El tipo de servicio, es decir, auth, account, session o password.
<i>indicador_control</i>	Indica el rol del módulo en la determinación del valor de éxito o error integrado del servicio. Los indicadores de control válidos son: binding, include, optional, required, requisite y sufficient. Consulte <a href="#">“Cómo funciona el apilamiento PAM” en la página 342</a> para obtener información sobre el uso de estos indicadores.
<i>ruta_módulo</i>	La ruta del objeto de la biblioteca que implementa el servicio. Si el nombre de la ruta no es absoluto, se asume que es relativo a /usr/lib/security/\$ISA/. Utilice la macro dependiente de la arquitectura \$ISA para que libpam busque en el directorio la arquitectura específica de la aplicación.
<i>opciones_módulo</i>	Opciones que se transfieren a los módulos de servicios. La página del comando man de un módulo describe las opciones aceptadas por ese módulo. Las opciones típicas del módulo incluyen nowarn y debug.

## Cómo funciona el apilamiento PAM

Cuando una aplicación llama las siguientes funciones, libpam lee el archivo de configuración /etc/pam.conf para determinar qué módulos participan en la operación de este servicio:

- `pam_authenticate(3PAM)`
- `pam_acct_mgmt(3PAM)`
- `pam_setcred(3PAM)`
- `pam_open_session(3PAM)`
- `pam_close_session(3PAM)`
- `pam_chauthtok(3PAM)`

Si `/etc/pam.conf` contiene sólo un módulo para una operación de este servicio, como la autenticación o la gestión de cuentas, el resultado de ese módulo determina el resultado de la operación. Por ejemplo, la operación de autenticación predeterminada para la aplicación `passwd` contiene un módulo, `pam_passwd_auth.so.1`:

```
passwd auth required pam_passwd_auth.so.1
```

Por otro lado, si hay varios módulos definidos para la operación del servicio, se dice que esos módulos están *apilados* y que existe una *pila PAM* para ese servicio. Por ejemplo, analice la situación en la que `pam.conf` contiene las siguientes entradas:

```
login auth requisite pam_authok_get.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
```

Estas entradas representan un ejemplo de pila `auth` para el servicio `login`. Para determinar el resultado de esta pila, los códigos de resultado de los módulos individuales requieren un *proceso de integración*. En el proceso de integración, los módulos se ejecutan en orden, como se especifica en `/etc/pam.conf`. Cada código de éxito o error se integra en el resultado general según el indicador de control del módulo. El indicador de control puede provocar la finalización anticipada de la pila. Por ejemplo, es posible que un módulo `requisite` falle, o bien que un módulo `sufficient` o `binding` tenga éxito. Después del procesamiento de la pila, los resultados individuales se combinan en un único resultado general que se proporciona a la aplicación.

El indicador de control señala el rol que un módulo PAM tiene en la determinación del acceso al servicio. Los indicadores de control y sus efectos son:

- **Binding:** el éxito en el cumplimiento de los requisitos de un módulo `binding` devuelve inmediatamente un valor de éxito a la aplicación si no ha fallado ningún módulo `required` anterior. Si se cumplen estas condiciones, no se produce ninguna ejecución adicional de módulos. Un fallo provoca el registro de un fallo de `required` y la continuación del procesamiento de los módulos.
- **Include:** agrega líneas de un archivo de configuración de PAM independiente que se utilizará en este momento en la pila PAM. Este indicador no controla el comportamiento de éxito o error. Cuando se lee un archivo nuevo, la pila PAM incluye aumenta. Cuando finaliza la comprobación de la pila en el nuevo archivo, el valor de la pila incluye disminuye. Cuando se llega al final de un archivo y la pila PAM incluye es 0, finaliza el procesamiento de la pila. El número máximo de la pila PAM incluye es 32.
- **Optional:** el éxito en el cumplimiento de los requisitos de un módulo `optional` no es necesario para utilizar el servicio. Un fallo provoca el registro de un fallo de `optional`.

- **Required:** el éxito en el cumplimiento de los requisitos de un módulo required es necesario para utilizar el servicio. Un fallo provoca la devolución de un error tras la ejecución de los módulos restantes de este servicio. El éxito final del servicio se devuelve solamente si ningún módulo binding o required ha informado fallos.
- **Requisite:** el éxito en el cumplimiento de los requisitos de un módulo requisite es necesario para utilizar el servicio. Un fallo provoca la devolución inmediata de error sin ejecuciones adicionales de módulos. Todos los módulos requisite de un servicio deben devolver un valor de éxito para que la función pueda devolver un valor de éxito a la aplicación.
- **Sufficient:** si no se han producido fallos anteriores de required, el éxito de un módulo sufficient devuelve un valor de éxito a la aplicación inmediatamente, sin ejecuciones adicionales de módulos. Un fallo provoca el registro de un fallo de optional.

Los dos diagramas siguientes muestran cómo se determina el acceso en el proceso de integración. El primer diagrama indica cómo se registra el éxito o error para cada tipo de indicador de control. El segundo diagrama muestra cómo se determina el valor integrado.



FIGURA 17-2 Apilamiento PAM: efecto de los indicadores de control

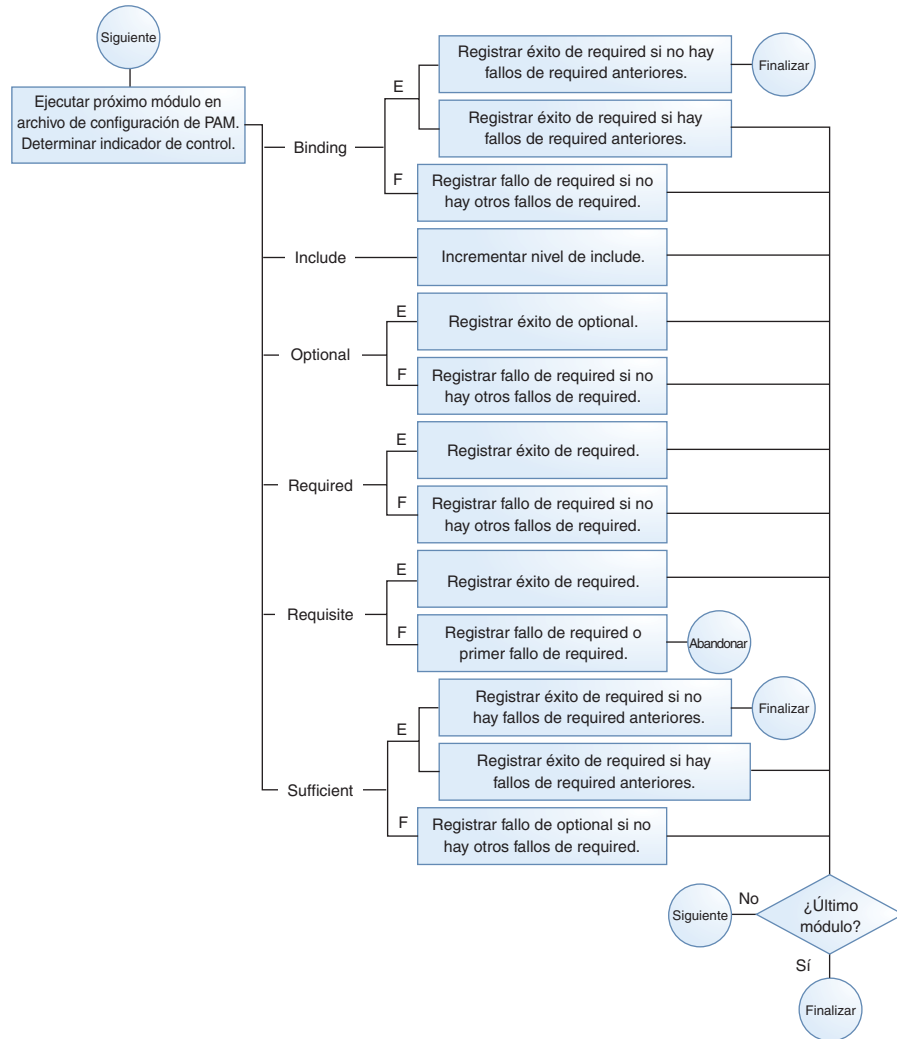
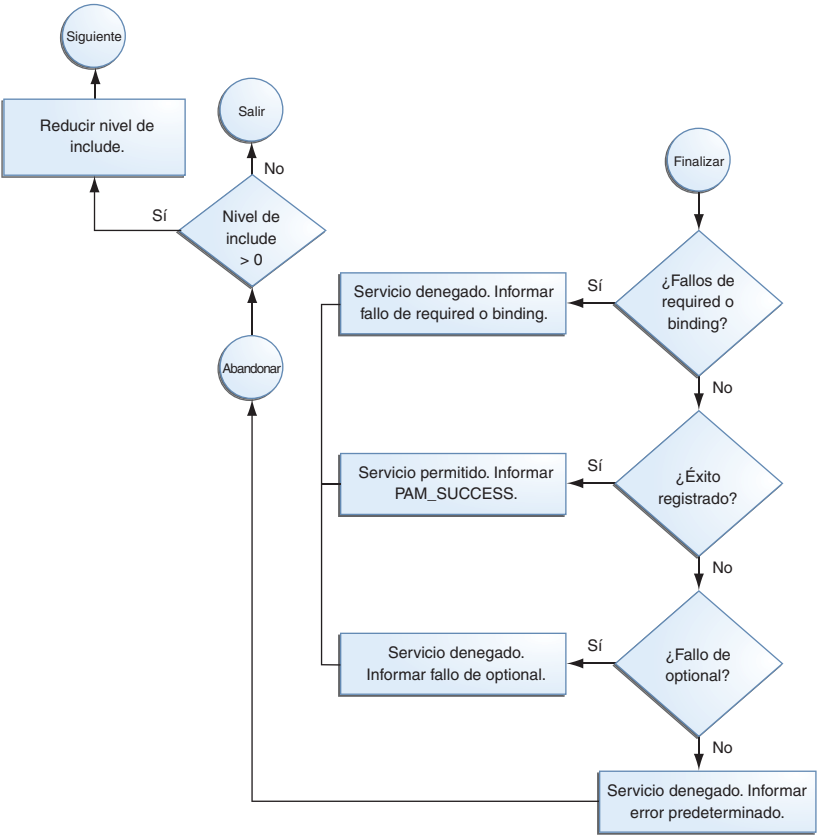


FIGURA 17-3 Apilamiento PAM: cómo se determina el valor integrado



## Ejemplo de apilamiento PAM

Tenga en cuenta el siguiente ejemplo de un servicio `rlogin` que solicita autenticación.

**EJEMPLO 17-1** Contenido parcial de un archivo de configuración de PAM típico

El archivo `pam.conf` de este ejemplo tiene el siguiente contenido para los servicios `rlogin`:

```
# Authentication management
...
# rlogin service
rlogin auth sufficient pam_rhosts_auth.so.1
rlogin auth requisite pam_authok_get.so.1
rlogin auth required pam_dhkeys.so.1
rlogin auth required pam_unix_auth.so.1
...
```

**EJEMPLO 17-1** Contenido parcial de un archivo de configuración de PAM típico *(Continuación)*

Cuando el servicio `rlogin` solicita autenticación, `libpam` primero ejecuta el módulo `pam_rhosts_auth(5)`. El indicador de control se estableció en `sufficient` para el módulo `pam_rhosts_auth`. Si el módulo `pam_rhosts_auth` puede autenticar al usuario, se detiene el procesamiento y se devuelve un valor de éxito a la aplicación.

Si el módulo `pam_rhosts_auth` no puede autenticar al usuario, se ejecuta el módulo PAM siguiente, `pam_authtok_get(5)`. El indicador de control de este módulo se estableció en `requisite`. Si `pam_authtok_get` falla, finaliza el proceso de autenticación y se devuelve un valor de error a `rlogin`.

Si `pam_authtok_get` tiene éxito, se ejecutan los dos módulos siguientes, `pam_dhkeys(5)` y `pam_unix_auth(5)`. Ambos módulos tienen los indicadores de control asociados que se establecieron en `required` para que el proceso continúe independientemente de si se devuelve un error individual. Tras la ejecución de `pam_unix_auth`, no quedan módulos para la autenticación `rlogin`. En este momento, si `pam_dhkeys` o `pam_unix_auth` han devuelto un error, se rechaza el acceso del usuario a través de `rlogin`.



## Uso de SASL

---

En este capítulo se incluye información sobre la autenticación sencilla y capa de seguridad (SASL).

- “SASL (descripción general)” en la página 349
- “SASL (referencia)” en la página 350

### SASL (descripción general)

La autenticación sencilla y capa de seguridad (SASL) es una estructura que proporciona servicios de seguridad opcionales y autenticación a los protocolos de red. Una aplicación llama a la biblioteca SASL, `/usr/lib/libsasl.so`, que proporciona una capa intermedia entre la aplicación y los distintos mecanismos de SASL. Los mecanismos se utilizan en el proceso de autenticación y para la prestación servicios de seguridad opcionales. La versión de SASL proviene de Cyrus SASL con algunos cambios.

SASL proporciona los siguientes servicios:

- Carga de cualquier complemento
- Determinación de las opciones de seguridad necesarias de la aplicación para ayudar a elegir un mecanismo de seguridad
- Listado de los complementos que están disponibles para la aplicación
- Elección del mejor mecanismo de una lista de los mecanismos disponibles para un determinado intento de autenticación
- Enrutamiento de datos de autenticación entre la aplicación y el mecanismo elegido
- Proporción de información sobre la negociación de SASL a la aplicación

## SASL (referencia)

En la siguiente sección se proporciona información sobre la implementación de SASL.

### Complementos de SASL

Los complementos de SASL admiten mecanismos de seguridad, canonización del usuario y recuperación de propiedad auxiliar. De manera predeterminada, los complementos de 32 bits cargados dinámicamente se instalan en `/usr/lib/sasl`, y los complementos de 64 bits se instalan en `/usr/lib/sasl/ $ISA`. Se proporcionan los siguientes complementos de mecanismo de seguridad:

<code>crammd5.so.1</code>	CRAM-MD5, que admite sólo autenticación, no autorización.
<code>digestmd5.so.1</code>	DIGEST-MD5, que admite autenticación, integridad, privacidad y autorización.
<code>gssapi.so.1</code>	GSSAPI, que admite autenticación, integridad, privacidad y autorización. El mecanismo de seguridad GSSAPI requiere una infraestructura Kerberos en funcionamiento.
<code>plain.so.1</code>	PLAIN, que admite autenticación y autorización.

Además, el complemento de mecanismo de seguridad EXTERNAL y el complemento de canonización de usuario INTERNAL están integrados en `libsasl.so.1`. El mecanismo EXTERNAL admite la autenticación y la autorización. El mecanismo admite integridad y privacidad, si el origen de la seguridad externa la proporciona. El complemento INTERNAL agrega el nombre de dominio al nombre de usuario, si es necesario.

La versión de Oracle Solaris no suministra ningún complemento `auxprop` en este momento. Para que los complementos de mecanismo CRAM-MD5 y DIGEST-MD5 funcionen plenamente en el servidor, el usuario debe proporcionar un complemento `auxprop` para recuperar contraseñas de texto sin cifrar. El complemento PLAIN requiere asistencia adicional para verificar la contraseña. La asistencia para la verificación de la contraseña puede ser una de las siguientes opciones: una devolución de llamada a la aplicación del servidor, un complemento `auxprop`, `saslauthd` o `pwcheck`. Los daemons `saslauthd` y `pwcheck` no se proporcionan en las versiones de Oracle Solaris. Para obtener una mejor interoperabilidad, restrinja las aplicaciones del servidor a los mecanismos que sean totalmente operativos mediante la opción de SASL `mech_list`.

### Variable de entorno de SASL

De manera predeterminada, el nombre de autenticación del cliente se establece en `getenv("LOGNAME")`. Esta variable puede ser restablecida por el cliente o por el complemento.

## Opciones de SASL

El comportamiento de `libsasl` y los complementos se pueden modificar en el servidor mediante las opciones que se pueden establecer en el archivo `/etc/sasl/app.conf`. La variable `app` es el nombre definido por el servidor para la aplicación. La documentación de la *aplicación* del servidor debe especificar el nombre de la aplicación.

Se admiten las siguientes opciones:

<code>auto_transition</code>	Pasa al usuario automáticamente a otros mecanismos cuando el usuario realiza una autenticación de texto sin formato correcta.
<code>auxprop_login</code>	Muestra el nombre de los complementos de propiedad auxiliar que se van a utilizar.
<code>canon_user_plugin</code>	Selecciona el complemento <code>canon_user</code> que se va a utilizar.
<code>mech_list</code>	Muestra los mecanismos que la aplicación del servidor tiene permitido utilizar.
<code>pwcheck_method</code>	Muestra los mecanismos utilizados para verificar las contraseñas. Actualmente, <code>auxprop</code> es el único valor permitido.
<code>reauth_timeout</code>	Ajusta el tiempo, en minutos, durante el cual la información de autenticación se almacena en la antememoria para una nueva autenticación rápida. Esta opción es utilizada por el complemento DIGEST-MD5. Al definir esta opción en 0, se inhabilita una nueva autenticación.

Las siguientes opciones no se admiten:

<code>plugin_list</code>	Muestra los mecanismos disponibles. No se utiliza porque la opción cambia el comportamiento de la carga dinámica de los complementos.
<code>saslauthd_path</code>	Define la ubicación de la puerta <code>saslauthd</code> , que se utiliza para la comunicación con el daemon <code>saslauthd</code> . El daemon <code>saslauthd</code> no se incluye en la versión de Oracle Solaris. Por lo tanto, esta opción tampoco está incluida.
<code>keytab</code>	Define la ubicación del archivo <code>keytab</code> usado por el complemento GSSAPI. Utilice la variable de entorno <code>KRB5_KTNAME</code> en su lugar para establecer la ubicación predeterminada de <code>keytab</code> .

Las siguientes son opciones que no se encuentran en Cyrus SASL. Sin embargo, se agregaron a la versión de Oracle Solaris:

<code>use_authid</code>	Adquiere las credenciales del cliente en lugar de utilizar las credenciales predeterminadas al crear el contexto de seguridad del cliente GSS. De manera predeterminada, se utiliza la identidad Kerberos del cliente por defecto.
-------------------------	--

log\_level

Establece el nivel deseado de registro para un servidor.



## Uso de Oracle Solaris Secure Shell (tareas)

---

La función Secure Shell proporciona acceso seguro a un host remoto por medio de una red no segura. El shell proporciona comandos para el inicio de sesión remoto y la transferencia de archivos remota. A continuación, se muestra una lista de los temas incluidos en este capítulo.

- “Oracle Solaris Secure Shell (descripción general)” en la página 353
- “Oracle Solaris Secure Shell y el proyecto OpenSSH” en la página 356
- “Configuración de Oracle Solaris Secure Shell (mapa de tareas)” en la página 358
- “Uso de Oracle Solaris Secure Shell (mapa de tareas)” en la página 362

Para obtener información de referencia, consulte el [Capítulo 20, “Oracle Solaris Secure Shell \(referencia\)”](#). Para obtener información sobre la relación de Oracle Solaris Secure Shell con el proyecto OpenSSH, consulte [“Oracle Solaris Secure Shell y el proyecto OpenSSH” en la página 356](#).

## Oracle Solaris Secure Shell (descripción general)

En Secure Shell, la autenticación es proporcionada por el uso de contraseñas, claves públicas, o ambas. Todo el tráfico de la red está cifrado. Por lo tanto, Secure Shell impide que un posible intruso pueda leer una comunicación interceptada. Secure Shell también impide que un adversario falsifique el sistema.

Secure Shell también puede utilizarse como una [red privada virtual \(VPN\)](#) a petición. Una VPN puede reenviar tráfico de sistemas de ventanas X o puede conectar números de puerto individuales entre los equipos locales y remotos mediante un enlace de red cifrado.

Con Secure Shell, puede realizar estas acciones:

- Iniciar sesión en otro host de forma segura por medio de una red no segura.
- Copiar archivos de forma segura entre los dos hosts.
- Ejecutar comandos de forma segura en el host remoto.

Secure Shell admite dos versiones del protocolo de shell seguro. La versión 1 es la versión original del protocolo. La versión 2 es más segura y corrige algunas brechas básicas del diseño de seguridad de la versión 1. La versión 1 sólo se proporciona para ayudar a los usuarios que migran a la versión 2. Se desaconseja a los usuarios que usen la versión 1.

**Nota** – De aquí en adelante, v1 se utiliza para representar la versión 1, y v2 se utiliza para representar la versión 2.

## Autenticación de Oracle Solaris Secure Shell

Secure Shell proporciona métodos de clave pública y contraseña para autenticar la conexión al host remoto. La autenticación de clave pública es un mecanismo de autenticación más potente que la autenticación de contraseña, porque la clave privada nunca viaja por medio de la red.

Los métodos de autenticación se prueban en el siguiente orden: cuando la configuración no satisface un método de autenticación, se prueba el siguiente método.

- **GSS-API:** utiliza credenciales para mecanismos GSS-API, como `mech_krb5` (Kerberos V) y `mech_dh` (AUTH\_DH), para autenticar clientes y servidores. Para obtener más información sobre la GSS-API, consulte [“Introduction to GSS-API” de Developer’s Guide to Oracle Solaris Security](#).
- **Autenticación basada en host:** utiliza claves de host y archivos `rhhosts`. Utiliza las claves de host públicas y privadas RSA y DSA del cliente para autenticar el cliente. Utiliza los archivos `rhhosts` para autorizar clientes a usuarios.
- **Autenticación de clave pública:** autentica a los usuarios con sus claves públicas y privadas RSA y DSA.
- **Autenticación de contraseña:** utiliza PAM para autenticar a los usuarios. El método de autenticación de teclado en v2 permite la solicitud arbitraria por PAM. Para obtener más información, consulte la sección SECURITY en la página del comando `man sshd(1M)`.

En la siguiente tabla, se muestran los requisitos para autenticar a un usuario que está intentando iniciar sesión en un host remoto. El usuario está en el host local, el cliente. El host remoto, el servidor, está ejecutando el daemon `sshd`. En la tabla, se muestran los métodos de autenticación de Secure Shell, las versiones de protocolo compatibles y los requisitos de host.

TABLA 19–1 Métodos de autenticación para Secure Shell

Método de autenticación (versión de protocolo)	Requisitos de host local (cliente)	Requisitos de host remoto (servidor)
GSS-API (v2)	Credenciales de iniciador para el mecanismo GSS.	Credenciales de aceptador para el mecanismo GSS. Para obtener más información, consulte <a href="#">“Adquisición de credenciales GSS en Secure Shell” en la página 376</a> .

TABLA 19-1 Métodos de autenticación para Secure Shell (Continuación)

Método de autenticación (versión de protocolo)	Requisitos de host local (cliente)	Requisitos de host remoto (servidor)
Basado en host (v2)	Cuenta de usuario  Clave privada de host local en /etc/ssh/ssh_host_rsa_key o /etc/ssh/ssh_host_dsa_key  HostbasedAuthentication yes en /etc/ssh/ssh_config	Cuenta de usuario  Clave pública de host local en /etc/ssh/known_hosts o ~/.ssh/known_hosts  HostbasedAuthentication yes en /etc/ssh/sshd_config  IgnoreRhosts no en /etc/ssh/sshd_config  Entrada de host local en /etc/ssh/shosts.equiv, /etc/hosts.equiv, ~/.rhosts o ~/.shosts
Clave pública RSA o DSA (v2)	Cuenta de usuario  Clave privada en ~/.ssh/id_rsa o ~/.ssh/id_dsa  Clave pública del usuario en ~/.ssh/id_rsa.pub o ~/.ssh/id_dsa.pub	Cuenta de usuario  Clave pública del usuario en ~/.ssh/authorized_keys
Clave pública RSA (v1)	Cuenta de usuario  Clave privada en ~/.ssh/identity  Clave pública del usuario en ~/.ssh/identity.pub	Cuenta de usuario  Clave pública del usuario en ~/.ssh/authorized_keys
Teclado interactivo (v2)	Cuenta de usuario	Cuenta de usuario  Admite PAM, incluidos la solicitud arbitraria y el cambio de contraseña cuando se activa la caducidad de las contraseñas
Basado en contraseña (v1 o v2)	Cuenta de usuario	Cuenta de usuario  Admite PAM
.rhosts solamente (v1)	Cuenta de usuario	Cuenta de usuario  IgnoreRhosts no en /etc/ssh/sshd_config  Entrada de host local en /etc/ssh/shosts.equiv, /etc/hosts.equiv, ~/.shosts o ~/.rhosts
.rhosts con RSA (v1) en el servidor solamente	Cuenta de usuario  Clave pública de host local en /etc/ssh/ssh_host_rsa1_key	Cuenta de usuario  Clave pública de host local en /etc/ssh/ssh_known_hosts o ~/.ssh/known_hosts  IgnoreRhosts no en /etc/ssh/sshd_config  Entrada de host local en /etc/ssh/shosts.equiv, /etc/hosts.equiv, ~/.shosts o ~/.rhosts

## Secure Shell en la empresa

Para obtener una descripción completa de Secure Shell en un sistema Oracle Solaris, consulte *Secure Shell in the Enterprise* (Shell seguro en la empresa), por Jason Reid, ISBN 0-13-142900-0, junio de 2003. El libro forma parte de Sun BluePrints Series, publicado por Sun Microsystems Press.

## Oracle Solaris Secure Shell y el proyecto OpenSSH

Oracle Solaris Secure Shell es una bifurcación del proyecto [OpenSSH \(http://www.openssh.com\)](http://www.openssh.com). Las correcciones de seguridad para las vulnerabilidades que se detectan en versiones posteriores de OpenSSH se integran en Oracle Solaris Secure Shell, ya que son funciones y correcciones de errores individuales. El desarrollo interno continúa en la bifurcación de Oracle Solaris Secure Shell.

Si bien los ingenieros de Oracle Solaris proporcionan correcciones de errores para el proyecto, también han integrado las siguientes funciones en la bifurcación de Oracle Solaris de Secure Shell:

- PAM: Oracle Solaris Secure Shell utiliza PAM. La opción de configuración UsePAM de OpenSSH no se admite.
- Separación de privilegios: Oracle Solaris Secure Shell no utiliza el código de separación de privilegios del proyecto OpenSSH. Oracle Solaris Secure Shell separa el procesamiento de auditoría, conservación de registros y restablecimiento de claves del procesamiento de protocolos de sesión.  
El código de separación de privilegios de Oracle Solaris Secure Shell siempre está activado y no se puede desactivar. La opción UsePrivilegeSeparation de OpenSSH no se admite.
- Configuración regional: Oracle Solaris Secure Shell admite completamente la negociación de idiomas, como se define en RFC 4253, *Secure Shell Transfer Protocol* (Protocolo de transferencia de shell seguro). Después de que el usuario inicia sesión, el perfil del shell de inicio de sesión del usuario puede sustituir la configuración regional negociada de Secure Shell.
- Auditoría: Oracle Solaris Secure Shell está totalmente integrado en el subsistema de auditoría de Oracle Solaris. Para obtener información sobre la auditoría, consulte [Parte VII](#).
- Compatibilidad con GSS-API: la GSS-API se puede utilizar para la autenticación de usuario y para el intercambio de claves inicial. La GSS-API se define en RFC4462, *Generic Security Service Application Program Interface* (Interfaz de programa de aplicación de servicios de seguridad genéricos).
- Comandos de proxy: Oracle Solaris Secure Shell proporciona comandos de proxy para protocolos SOCKS5 y HTTP. Para obtener un ejemplo, consulte [“Cómo configurar conexiones predeterminadas a hosts fuera de un cortafuegos” en la página 372](#).

Desde la versión Solaris 9, los siguientes cambios específicos se han introducido en Oracle Solaris Secure Shell:

- Oracle Solaris Secure Shell se bifurca de OpenSSH 3.5p1.
- El valor predeterminado de `X11Forwarding` es `yes` en el archivo `/etc/ssh/sshd_config`.
- Las palabras clave siguientes se han introducido:
  - `GSSAPIAuthentication`
  - `GSSAPIKeyExchange`
  - `GSSAPIDelegateCredentials`
  - `GSSAPIStoreDelegatedCredentials`
  - `KbdInteractiveAuthentication`

Las palabras clave `GSSAPI` permiten que Oracle Solaris Secure Shell use credenciales GSS para la autenticación. La palabra clave `KbdInteractiveAuthentication` admite la solicitud arbitraria y el cambio de contraseña en PAM. Para obtener una lista completa de palabras clave y sus valores predeterminados, consulte [“Palabras clave en Secure Shell” en la página 378](#).

- Los cifrados ARCFOUR y AES128-CTR ahora están disponibles. ARCFOUR también se conoce como RC4. El cifrado AES es AES en modo de contador.
- El daemon `sshd` usa las variables de `/etc/default/login` y del comando `login`. Las variables de `/etc/default/login` se pueden sustituir por los valores del archivo `sshd_config`. Para obtener más información, consulte [“Secure Shell y variables de entorno de inicio de sesión” en la página 382](#) y la página del comando `man sshd_config(4)`.
- Una vez que la conexión se autentica, la opción `ChrootDirectory` en el servidor permite que el servidor envíe mediante `chroot` los clientes conectados al directorio que la opción especifica. Esta opción admite un servidor SFTP dentro del proceso, es decir, un SFTP interno, cuyas configuraciones se simplifican mediante la utilización de la opción `ChrootDirectory`.

## Oracle Solaris Secure Shell (mapa de tareas)

En el siguiente mapa de tareas, se indican mapas de tareas para configurar Secure Shell y para utilizar la función Secure Shell en Oracle Solaris.

Tarea	Descripción	Para obtener instrucciones
Configurar Secure Shell	Guía a los administradores en la configuración de Secure Shell para los usuarios.	<a href="#">“Configuración de Oracle Solaris Secure Shell (mapa de tareas)” en la página 358</a>
Utilizar Secure Shell	Guía a los usuarios en el uso de Secure Shell.	<a href="#">“Uso de Oracle Solaris Secure Shell (mapa de tareas)” en la página 362</a>

# Configuración de Oracle Solaris Secure Shell (mapa de tareas)

En el siguiente mapa de tareas, se indican procedimientos para configurar Secure Shell.

Tarea	Descripción	Para obtener instrucciones
Configurar autenticación basada en host	Configura la autenticación basada en host en el cliente y el servidor.	<a href="#">“Cómo configurar la autenticación basada en host para Secure Shell” en la página 358</a>
Configurar un host para utilizar v1 y v2	Crea archivos de clave pública para hosts que utilizan protocolos v1 y v2.	<a href="#">“Cómo habilitar Secure Shell v1” en la página 361</a>
Configurar reenvío del puerto	Permite a los usuarios utilizar el reenvío del puerto.	<a href="#">“Cómo configurar el reenvío del puerto en Secure Shell” en la página 361</a>

## Configuración de Oracle Solaris Secure Shell (tareas)

De manera predeterminada, la autenticación basada en host y el uso de ambos protocolos no están habilitados en Secure Shell. El cambio de estos valores predeterminados requiere intervención administrativa. Para que el reenvío del puerto funcione, también se requiere intervención administrativa.

### ▼ Cómo configurar la autenticación basada en host para Secure Shell

El siguiente procedimiento configura un sistema de clave pública en el que la clave pública del cliente se utiliza para la autenticación en el servidor. El usuario también debe crear un par de clave pública y clave privada.

En el procedimiento, los términos *cliente* y *host local* hacen referencia al equipo en el que un usuario introduce el comando ssh. Los términos *servidor* y *host remoto* hacen referencia al equipo al que el cliente está intentando acceder.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

**2 En el cliente, habilite la autenticación basada en host.**

En el archivo de configuración del cliente, `/etc/ssh/ssh_config`, escriba la siguiente entrada:  
`HostbasedAuthentication yes`

Para ver la sintaxis del archivo, consulte la página del comando `man ssh_config(4)`.

**3 En el servidor, habilite la autenticación basada en host.**

En el archivo de configuración del servidor, `/etc/ssh/sshd_config`, escriba la misma entrada: `HostbasedAuthentication yes`

Para ver la sintaxis del archivo, consulte la página del comando `man sshd_config(4)`.

**4 En el servidor, configure un archivo que permita que el cliente se reconozca como un host de confianza.**

Para obtener más información, consulte la sección FILES de la página del comando `man sshd(1M)`.

- **Agregue el cliente como una entrada al archivo `/etc/ssh/ssh_known_hosts` del servidor.**

*client-host*

- **También puede indicar a los usuarios que agreguen una entrada para el cliente a sus archivos `~/.ssh/ssh_known_hosts` en el servidor.**

*client-host*

**5 En el servidor, asegúrese de que el daemon `sshd` pueda acceder a la lista de hosts de confianza.**

Establezca `IgnoreRhosts` en `no` en el archivo `/etc/ssh/sshd_config`.

```
## sshd_config
IgnoreRhosts no
```

**6 Asegúrese de que los usuarios de Secure Shell en su sitio tengan cuentas en ambos hosts.****7 Realice una de las siguientes acciones para colocar la clave pública del cliente en el servidor.**

- **Modifique el archivo `sshd_config` en el servidor y luego indique a sus usuarios que agreguen las claves de host públicas del cliente a sus archivos `~/.ssh/ssh_known_hosts`.**

```
## sshd_config
IgnoreUserKnownHosts no
```

Para obtener instrucciones para el usuario, consulte “[Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell](#)” en la página 363.

- **Copie la clave pública del cliente en el servidor.**

Las claves de host se almacenan en el directorio `/etc/ssh`. Las claves suelen ser generadas por el daemon `sshd` al iniciar por primera vez.

**a. Agregue la clave al archivo `/etc/ssh/ssh_known_hosts` en el servidor.**

En el cliente, escriba el comando en una línea sin barra diagonal inversa.

```
# cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> /etc/ssh/ssh_known_hosts && echo "Host key copied"'
```

**b. Cuando se le pida, proporcione la contraseña de inicio de sesión.**

Cuando el archivo se copia, se muestra el mensaje “Host key copied” (clave de host copiada).

Cada línea en el archivo `/etc/ssh/ssh_known_hosts` consta de campos que están separados por espacios:

*hostnames algorithm-name publickey comment*

**c. Edite el archivo `/etc/ssh/ssh_known_hosts` y agregue *RemoteHost* como el primer campo en la entrada copiada.**

```
## /etc/ssh/ssh_known_hosts File
RemoteHost <copied entry>
```

**Ejemplo 19-1 Configuración de autenticación basada en host**

En el siguiente ejemplo, cada host está configurado como servidor y como cliente. Un usuario en cualquiera de los hosts puede iniciar una conexión `ssh` al otro host. La siguiente configuración hace que cada host sea un servidor y un cliente:

- En cada host, los archivos de configuración de Secure Shell contienen las siguientes entradas:

```
## /etc/ssh/ssh_config
HostBasedAuthentication yes
#
## /etc/ssh/sshd_config
HostBasedAuthentication yes
IgnoreRhosts no
```

- En cada host, el archivo `shosts.equiv` contiene una entrada para el otro host:

```
## /etc/ssh/shosts.equiv on machine2
machine1

## /etc/ssh/shosts.equiv on machine1
machine2
```

- La clave pública de cada host está en el archivo `/etc/ssh/ssh_known_hosts` del otro host:

```
## /etc/ssh/ssh_known_hosts on machine2
... machine1

## /etc/ssh/ssh_known_hosts on machine1
... machine2
```

- Los usuarios tienen una cuenta en ambos hosts:

```
## /etc/passwd on machine1
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh

## /etc/passwd on machine2
jdoe:x:3111:10:J Doe:/home/jdoe:/bin/sh
```



## ▼ Cómo habilitar Secure Shell v1

Este procedimiento resulta útil cuando un host interopera con hosts que ejecutan v1 y v2.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Configure el host para que utilice ambos protocolos de Secure Shell.

Edite el archivo `/etc/ssh/sshd_config`.

```
# Protocol 2
Protocol 2,1
```

### 3 Proporcione un archivo separado para la clave de host de v1.

Agregue una entrada `HostKey` al archivo `/etc/ssh/sshd_config`.

```
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_rsa1_key
```

### 4 Genere una clave de host para v1.

```
# ssh-keygen -t rsa1 -f /etc/ssh/ssh_host_rsa1_key -N ''
```

`-t rsa1` Indica el algoritmo RSA para v1.

`-f` Indica el archivo que contiene la clave de host.

`-N ''` Indica que no se requiere ninguna frase de contraseña.

### 5 Reinicie el daemon `sshd`.

```
# svcadm restart network/ssh:default
```

También puede reiniciar el sistema.

## ▼ Cómo configurar el reenvío del puerto en Secure Shell

El reenvío del puerto permite que un puerto local sea reenviado a un host remoto.

Efectivamente, un socket se asigna para escuchar el puerto en el lado local. De forma similar, un puerto se puede especificar en el lado remoto.

---

**Nota** – El reenvío del puerto de Secure Shell debe utilizar conexiones TCP. Secure Shell no admite conexiones UDP para el reenvío del puerto.

---

- 1

Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.
- 2

Configure un valor de Secure Shell en el servidor remoto para permitir el reenvío del puerto.

Cambie el valor de `AllowTcpForwarding` a `yes` en el archivo `/etc/ssh/sshd_config`.  

```
# Port forwarding
AllowTcpForwarding yes
```
- 3

Reinicie el servicio de Secure Shell.

```
remoteHost# svcadm restart network/ssh:default
```

Para obtener información sobre la gestión de servicios persistentes, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica* y la página del comando `man svcadm(1M)`.
- 4

Verifique que el reenvío del puerto se pueda utilizar.

```
remoteHost# /usr/bin/pgrep -lf sshd
1296 ssh -L 2001:remoteHost:23 remoteHost
```

## Uso de Oracle Solaris Secure Shell (mapa de tareas)

En el siguiente mapa de tareas, se indican procedimientos de usuario para usar Secure Shell.

Tarea	Descripción	Para obtener instrucciones
Crear un par de clave pública y clave privada	Permite el acceso a Secure Shell para sitios que requieren la autenticación de clave pública.	<a href="#">“Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell” en la página 363</a>
Cambiar la frase de contraseña	Cambia la frase que autentica la clave privada.	<a href="#">“Cómo cambiar la frase de contraseña de una clave privada de Secure Shell” en la página 365</a>
Iniciar sesión con Secure Shell	Proporciona comunicación de Secure Shell cifrada cuando se inicia sesión de manera remota. El proceso es similar al uso del comando <code>rsh</code> .	<a href="#">“Cómo iniciar sesión en un host remoto con Secure Shell” en la página 366</a>
Iniciar sesión en Secure Shell sin que se le solicite una contraseña	Permite iniciar sesión mediante un agente que proporciona la contraseña a Secure Shell.	<a href="#">“Cómo reducir indicadores de contraseñas en Secure Shell” en la página 367</a>

Tarea	Descripción	Para obtener instrucciones
		<a href="#">“Cómo configurar el comando ssh-agent para que se ejecute automáticamente en el CDE” en la página 368</a>
Utilizar el reenvío del puerto en Secure Shell	Especifica un puerto local o un puerto remoto que se utilizará en una conexión de Secure Shell por TCP.	<a href="#">“Cómo utilizar el reenvío del puerto en Secure Shell” en la página 369</a>
Copiar archivos con Secure Shell	Copia archivos entre hosts de manera segura.	<a href="#">“Cómo copiar archivos con Secure Shell” en la página 371</a>
Conectarse de forma segura de un host dentro de un cortafuegos a un host fuera del cortafuegos	Utiliza comandos de Secure Shell que son compatibles con HTTP o SOCKS5 para conectar hosts que están separados por un cortafuegos.	<a href="#">“Cómo configurar conexiones predeterminadas a hosts fuera de un cortafuegos” en la página 372</a>

## Uso de Oracle Solaris Secure Shell (tareas)

Secure Shell proporciona acceso seguro entre un shell local y un shell remoto. Para obtener más información, consulte las páginas del comando `man ssh_config(4)` y `ssh(1)`.

### ▼ Cómo generar un par de clave pública y clave privada para utilizar con Secure Shell

Los usuarios deben generar un par de clave pública y clave privada cuando su sitio implementa la autenticación basada en host o la autenticación de clave pública de usuario. Para obtener opciones adicionales, consulte la página del comando `man ssh-keygen(1)`.

#### Antes de empezar

Consulte al administrador del sistema si se ha configurado la autenticación basada en host.

#### 1 Inicie el programa de generación de claves.

```
myLocalHost% ssh-keygen -t rsa
Generating public/private rsa key pair.
...
```

donde `-t` es el tipo de algoritmo, uno de `rsa`, `dsa` o `rsa1`.

#### 2 Especifique la ruta al archivo que contendrá la clave.

De manera predeterminada, el nombre de archivo `id_rsa`, que representa una clave v2 RSA, aparece entre paréntesis. Puede seleccionar este archivo presionando la tecla de retorno. O puede escribir un nombre de archivo alternativo.

```
Enter file in which to save the key (/home/jdoe/.ssh/id_rsa): <Press Return>
```

El nombre de archivo de la clave pública se crea automáticamente adjuntando la cadena `.pub` al nombre del archivo de clave privada.

**3 Escriba una frase de contraseña para usar la clave.**

Esta frase de contraseña se utiliza para cifrar la clave privada. Se *desaconseja* el uso de una entrada nula. Tenga en cuenta que la frase de contraseña no se muestra cuando la escribe.

Enter passphrase (empty for no passphrase): *<Type passphrase>*

**4 Vuelva a escribir la frase de contraseña para confirmarla.**

Enter same passphrase again: *<Type passphrase>*

Your identification has been saved in /home/jdoe/.ssh/id\_rsa.

Your public key has been saved in /home/jdoe/.ssh/id\_rsa.pub.

The key fingerprint is:

0e:fb:3d:57:71:73:bf:58:b8:eb:f3:a3:aa:df:e0:d1 jdoe@myLocalHost

**5 Compruebe los resultados.**

Compruebe que la ruta al archivo de claves sea correcta.

```
% ls ~/.ssh
id_rsa
id_rsa.pub
```

En este punto, ha creado un par de clave pública y clave privada.

**6 Elija la opción adecuada:**

- Si el administrador ha configurado la autenticación basada en host, es posible que necesite copiar la clave pública del host local en el host remoto.

Ahora puede iniciar sesión en el host remoto. Para obtener detalles, consulte [“Cómo iniciar sesión en un host remoto con Secure Shell” en la página 366](#).

**a. Escriba el comando en una línea sin barra diagonal inversa.**

```
% cat /etc/ssh/ssh_host_dsa_key.pub | ssh RemoteHost \
'cat >> ~/.ssh/known_hosts && echo "Host key copied"'
```

**b. Cuando se le pida, proporcione la contraseña de inicio de sesión.**

```
Enter password: <Type password>
Host key copied
%
```

- Si su sitio utiliza la autenticación de usuario con claves públicas, rellene el archivo `authorized_keys` en el host remoto.

**a. Copie la clave pública en el host remoto.**

Escriba el comando en una línea sin barra diagonal inversa.

```
myLocalHost% cat $HOME/.ssh/id_rsa.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

**b. Cuando se le pida, proporcione la contraseña de inicio de sesión.**

Cuando el archivo se copia, se muestra el mensaje “Key copied” (clave copiada).

```
Enter password:      Type login password
Key copied
myLocalHost%
```

**7 (Opcional) Reduzca la solicitud de frases de contraseña.**

Para obtener un procedimiento, consulte [“Cómo reducir indicadores de contraseñas en Secure Shell” en la página 367](#). Para obtener más información, consulte las páginas del comando `man ssh-agent(1)` y `ssh-add(1)`.

**Ejemplo 19–2 Establecimiento de una clave RSA v1 para un usuario**

En el siguiente ejemplo, el usuario puede ponerse en contacto con hosts que ejecutan v1 del protocolo de Secure Shell. Para ser autenticado por hosts v1, el usuario crea una clave v1 y, a continuación, copia la parte de la clave pública en el host remoto.

```
myLocalHost% ssh-keygen -t rsa1 -f /home/jdoe/.ssh/identity
Generating public/private rsa key pair.
...
Enter passphrase (empty for no passphrase):    <Type passphrase>
Enter same passphrase again:    <Type passphrase>
Your identification has been saved in /home/jdoe/.ssh/identity.
Your public key has been saved in /home/jdoe/.ssh/identity.pub.
The key fingerprint is:
...
myLocalHost% ls ~/.ssh
id_rsa
id_rsa.pub
identity
identity.pub
myLocalHost% cat $HOME/.ssh/identity.pub | ssh myRemoteHost \
'cat >> .ssh/authorized_keys && echo "Key copied"'
```

## ▼ Cómo cambiar la frase de contraseña de una clave privada de Secure Shell

El siguiente procedimiento no cambia la clave privada. El procedimiento cambia el mecanismo de autenticación para la clave privada, la frase de contraseña. Para obtener más información, consulte la página del comando `man ssh-keygen(1)`.

- **Cambie la frase de contraseña.**

Escriba el comando `ssh-keygen` con la opción `-p` y responda a las solicitudes.

```
myLocalHost% ssh-keygen -p
Enter file which contains the private key (/home/jdoe/.ssh/id_rsa):    <Press Return>
Enter passphrase (empty for no passphrase):    <Type passphrase>
Enter same passphrase again:    <Type passphrase>
```

donde `-p` solicita cambiar la frase de contraseña de un archivo de clave privada.

## ▼ **Cómo iniciar sesión en un host remoto con Secure Shell**

### 1 **Inicie una sesión de Secure Shell.**

Escriba el comando `ssh` y especifique el nombre del host remoto.

```
myLocalHost% ssh myRemoteHost
```

Una solicitud cuestiona la autenticidad del host remoto:

```
The authenticity of host 'myRemoteHost' can't be established.
RSA key fingerprint in md5 is: 04:9f:bd:fc:3d:3e:d2:e7:49:fd:6e:18:4f:9c:26
Are you sure you want to continue connecting(yes/no)?
```

Esta solicitud es normal para conexiones iniciales a hosts remotos.

### 2 **Si se le solicita, verifique la autenticidad de la clave del host remoto.**

- **Si no puede confirmar la autenticidad del host remoto, escriba `no` y póngase en contacto con el administrador del sistema.**

```
Are you sure you want to continue connecting(yes/no)? no
```

El administrador es responsable de actualizar el archivo `/etc/ssh/ssh_known_hosts` global. Un archivo `ssh_known_hosts` actualizado impide que esta solicitud aparezca.

- **Si confirma la autenticidad del host remoto, responda la solicitud y continúe con el siguiente paso.**

```
Are you sure you want to continue connecting(yes/no)? yes
```

### 3 **Auténtiquese en Secure Shell.**

- a. **Cuando se le solicite, escriba la frase de contraseña.**

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':    <Type passphrase>
```

**b. Cuando se le solicite, escriba la contraseña de su cuenta.**

```
jdoe@myRemoteHost's password:      <Type password>
Last login: Fri Jul 20 14:24:10 2001 from myLocalHost
myRemoteHost%
```

**4 Realice transacciones en el host remoto.**

Los comandos que envía están cifrados. Ninguna respuesta que recibe está cifrada.

**5 Cierre la conexión de Secure Shell.**

Cuando haya terminado, escriba salir (**exit**) o utilice el método habitual para salir de su shell.

```
myRemoteHost% exit
myRemoteHost% logout
Connection to myRemoteHost closed
myLocalHost%
```

## ▼ Cómo reducir indicadores de contraseñas en Secure Shell

Si no desea escribir la frase de contraseña ni la contraseña para utilizar Secure Shell, puede utilizar el daemon del agente. Inicie el daemon al comienzo de la sesión. A continuación, almacene las claves privadas con el daemon del agente mediante el comando `ssh-add`. Si tiene cuentas diferentes en hosts diferentes, agregue las claves que necesita para la sesión.

Puede iniciar el daemon del agente manualmente cuando sea necesario, como se describe en el siguiente procedimiento. O puede establecer que el daemon del agente se ejecute automáticamente en el inicio de cada sesión, como se describe en [“Cómo configurar el comando `ssh-agent` para que se ejecute automáticamente en el CDE” en la página 368](#).

**1 Inicie el daemon del agente.**

```
myLocalHost% eval 'ssh-agent'
Agent pid 9892
```

**2 Verifique que el daemon del agente se haya iniciado.**

```
myLocalHost% pgrep ssh-agent
9892
```

**3 Agregue la clave privada al daemon del agente.**

Escriba el comando `ssh-add`.

```
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost%
```

**4 Inicie una sesión de Secure Shell.**

```
myLocalHost% ssh myRemoteHost
```

No se le solicita una frase de contraseña.

**Ejemplo 19-3 Uso de opciones de ssh -add**

En este ejemplo, jdoe agrega dos claves al daemon del agente. La opción `-l` se utiliza para enumerar todas las claves que se almacenan en el daemon. Al final de la sesión, la opción `-D` se usa para eliminar todas las claves del daemon del agente.

```
myLocalHost% ssh-agent
myLocalHost% ssh-add
Enter passphrase for /home/jdoe/.ssh/id_rsa:      <Type passphrase>
Identity added: /home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa)
myLocalHost% ssh-add /home/jdoe/.ssh/id_dsa
Enter passphrase for /home/jdoe/.ssh/id_dsa:      <Type passphrase>
Identity added:
/home/jdoe/.ssh/id_dsa(/home/jdoe/.ssh/id_dsa)

myLocalHost% ssh-add -l
md5 1024 0e:fb:3d:53:71:77:bf:57:b8:eb:f7:a7:aa:df:e0:d1
/home/jdoe/.ssh/id_rsa(RSA)
md5 1024 c1:d3:21:5e:40:60:c5:73:d8:87:09:3a:fa:5f:32:53
/home/jdoe/.ssh/id_dsa(DSA)
```

*User conducts Oracle Solaris Secure Shell transactions*

```
myLocalHost% ssh-add -D
Identity removed:
/home/jdoe/.ssh/id_rsa(/home/jdoe/.ssh/id_rsa.pub)
/home/jdoe/.ssh/id_dsa(DSA)
```

## ▼ **Cómo configurar el comando ssh-agent para que se ejecute automáticamente en el CDE**

Si utiliza el CDE, puede evitar proporcionar la frase de contraseña y la contraseña cada vez que utiliza Secure Shell mediante el inicio automático de un daemon del agente, `ssh-agent`. Puede iniciar el daemon del agente desde la secuencia de comandos `.dtpfile`. Para agregar la frase de contraseña y la contraseña al daemon del agente, consulte el [Ejemplo 19-3](#).





**Precaución** – Si utiliza el Sun Java Desktop System (Java DS), no configure el comando `ssh-agent` para que se ejecute automáticamente. Debido a que la terminación del proceso `ssh-agent` se controla mediante una interfaz del CDE, al salir de Java DS, el daemon sigue ejecutándose. Por ejemplo, si inicia el daemon en una sesión del CDE, se desplaza hasta una sesión de Java DS y cierra sesión, el daemon se sigue ejecutando.

Un daemon en ejecución utiliza recursos del sistema. Aunque no hay ningún problema conocido asociado con dejar el daemon `ssh-agent` en ejecución, el daemon contiene una contraseña, que podría generar un riesgo de seguridad.

### 1 Inicie el daemon del agente automáticamente en una secuencia de comandos de inicio de usuario.

Agregue las siguientes líneas al final de la secuencia de comandos `$HOME/.dtprofile`:

```
if [ "$SSH_AUTH_SOCK" = "" -a -x /usr/bin/ssh-agent ]; then
    eval `/usr/bin/ssh-agent`
fi
```

### 2 Termine el daemon del agente al salir de la sesión del CDE.

Agregue las siguientes líneas a la secuencia de comandos `$HOME/.dt/sessions/sessionexit`:

```
if [ "$SSH_AGENT_PID" != "" -a -x /usr/bin/ssh-agent ]; then
    /usr/bin/ssh-agent -k
fi
```

Esta entrada garantiza que nadie pueda utilizar el agente del Secure Shell después de que una sesión del CDE se termina. Debido a que la secuencia de comandos utiliza una interfaz específica del CDE, `sessionexit`, este procedimiento no termina el daemon del agente en una sesión de Sun Java Desktop System.

## ▼ Cómo utilizar el reenvío del puerto en Secure Shell

Puede especificar que un puerto local se reenvíe a un host remoto. Efectivamente, un socket se asigna para escuchar el puerto en el lado local. La conexión desde este puerto se realiza mediante un canal seguro al host remoto. Por ejemplo, puede especificar el puerto 143 para obtener correo electrónico remotamente con IMAP4. De forma similar, un puerto se puede especificar en el lado remoto.

### Antes de empezar

Para utilizar el reenvío del puerto, el administrador debe tener habilitado el reenvío del puerto en el servidor remoto de Secure Shell. Para obtener detalles, consulte [“Cómo configurar el reenvío del puerto en Secure Shell” en la página 361](#).

- **Para usar el reenvío del puerto seguro, elija una de las siguientes opciones:**

- **Para establecer que un puerto local reciba una comunicación segura de un puerto remoto, especifique ambos puertos.**

Especifique el puerto local que escucha para la comunicación remota. Además, especifique el host remoto y el puerto remoto que reenvían la comunicación.

```
myLocalHost% ssh -L localPort:remoteHost:remotePort
```

- **Para establecer que un puerto remoto reciba una conexión segura de un puerto local, especifique ambos puertos.**

Especifique el puerto remoto que escucha para la comunicación remota. Además, especifique el host local y el puerto local que reenvían la comunicación.

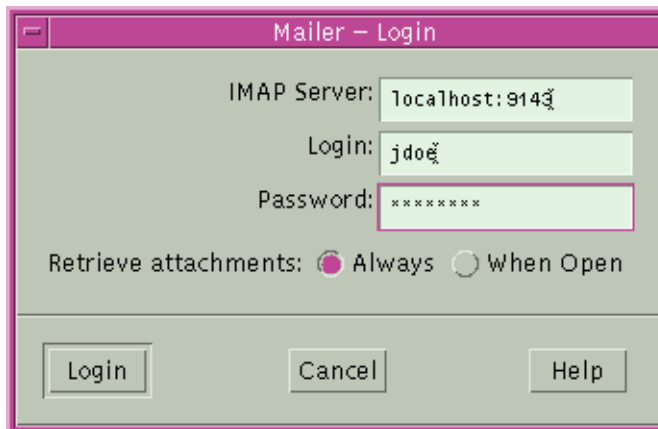
```
myLocalHost% ssh -R remotePort:localhost:localPort
```

#### **Ejemplo 19-4** Uso del reenvío del puerto local para recibir correo

El ejemplo siguiente muestra cómo puede utilizar el reenvío del puerto local para recibir correo de manera segura desde un servidor remoto.

```
myLocalHost% ssh -L 9143:myRemoteHost:143 myRemoteHost
```

Este comando reenvía conexiones del puerto 9143 en myLocalHost al puerto 143. El puerto 143 es el puerto del servidor v2 IMAP en myRemoteHost. Cuando el usuario inicia una aplicación de correo, el usuario debe especificar el número de puerto local, como se muestra en el siguiente cuadro de diálogo.



No confunda localhost en el cuadro de diálogo con myLocalHost. myLocalHost es un nombre de host hipotético. localhost es una palabra clave que identifica el sistema local.

**Ejemplo 19–5** Uso del reenvío del puerto remoto para comunicarse fuera de un cortafuegos

En el siguiente ejemplo, se muestra cómo un usuario en un entorno empresarial puede reenviar conexiones desde un host en una red externa hasta un host dentro de un cortafuegos corporativo.

```
myLocalHost% ssh -R 9022:myLocalHost:22 myOutsideHost
```

Este comando reenvía conexiones desde el puerto 9022 en myOutsideHost hasta el puerto 22, el servidor sshd, en el host local.

```
myOutsideHost% ssh -p 9022 localhost
myLocalHost%
```

▼ **Cómo copiar archivos con Secure Shell**

El siguiente procedimiento muestra cómo usar el comando `scp` para copiar archivos cifrados entre hosts. Puede copiar archivos cifrados ya sea entre un host local y un host remoto, o entre dos hosts remotos. El comando opera de forma similar al comando `rcp`, excepto que el comando `scp` solicita autenticación. Para obtener más información, consulte la página del comando [man scp\(1\)](#).

También puede utilizar `sftp`, un formato más seguro del comando `ftp`. Para obtener más información, consulte la página del comando [man sftp\(1\)](#). Si desea ver un ejemplo, consulte el [Ejemplo 19–6](#).

**1 Inicie el programa de copia segura.**

Especifique el archivo de origen, el nombre de usuario en el destino remoto y el directorio de destino.

```
myLocalHost% scp myfile.1 jdoe@myRemoteHost:~
```

**2 Indique la frase de contraseña cuando se le solicite.**

```
Enter passphrase for key '/home/jdoe/.ssh/id_rsa':      <Type passphrase>
myfile.1          25% |*****|          640 KB  0:20 ETA
myfile.1
```

Después de escribir la frase de contraseña, se muestra un indicador de progreso. Consulte la segunda línea en el resultado anterior. El indicador de progreso muestra:

- El nombre del archivo
- El porcentaje del archivo que se ha transferido
- Una serie de asteriscos que indican el porcentaje del archivo que se ha transferido
- La cantidad de datos transferidos
- El tiempo calculado de llegada, o ETA, del archivo completo (es decir, la cantidad restante de tiempo)

**Ejemplo 19-6** Especificación de un puerto cuando se utiliza el comando `sftp`

En este ejemplo, el usuario desea que el comando `sftp` utilice un puerto concreto. El usuario utiliza la opción `-o` para especificar el puerto.

```
% sftp -o port=2222 guest@RemoteFileServer
```

## ▼ Cómo configurar conexiones predeterminadas a hosts fuera de un cortafuegos

Puede utilizar Secure Shell para establecer una conexión desde un host dentro de un cortafuegos hasta un host fuera del cortafuegos. Esta tarea se realiza especificando un comando de proxy para `ssh` en un archivo de configuración o como una opción en la línea de comandos. Para la opción de línea de comandos, consulte el [Ejemplo 19-7](#).

En general, puede personalizar las interacciones de `ssh` mediante un archivo de configuración.

- Puede personalizar su propio archivo personal en `~/.ssh/config`.
- O puede utilizar los valores en el archivo de configuración administrativo, `/etc/ssh/ssh_config`.

Los archivos se pueden personalizar con dos tipos de comandos de proxy. Un comando de proxy es para conexiones HTTP. El otro comando de proxy es para conexiones SOCKS5. Para obtener más información, consulte la página del comando `man ssh_config(4)`.

### 1 Especifique los comandos de proxy y los hosts en un archivo de configuración.

Utilice la sintaxis siguiente para agregar tantas líneas como sea necesario:

```
[Host outside-host]
ProxyCommand proxy-command [-h proxy-server] \
[-p proxy-port] outside-host | %h outside-port | %p
```

Host *host\_exterior*

Limita la especificación del comando de proxy a instancias cuando un nombre de host remoto se especifica en la línea de comandos. Si utiliza un carácter comodín para *outside-host*, aplica la especificación del comando de proxy a un conjunto de hosts.

*comando\_proxy*

Especifica el comando de proxy.

El comando puede ser cualquiera de los siguientes:

- `/usr/lib/ssh/ssh-http-proxy-connect` para conexiones HTTP
- `/usr/lib/ssh/ssh-socks5-proxy-connect` para conexiones SOCKS5

`-h servidor_proxy` y `-p puerto_proxy`

Estas opciones especifican un servidor proxy y un puerto proxy, respectivamente. Si están presentes, los proxies sustituyen cualquier variable de entorno que especifica servidores

proxy y puertos proxy, como HTTPPROXY, HTTPPROXYPORT, SOCKS5\_PORT, SOCKS5\_SERVER y http\_proxy. La variable http\_proxy especifica una URL. Si las opciones no se usan, las variables de entorno relevantes se deben definir. Para obtener más información, consulte las páginas del comando man [ssh-socks5-proxy-connect\(1\)](#) y [ssh-http-proxy-connect\(1\)](#).

#### *host\_exterior*

Designa un host específico para conectarse. Utilice el argumento de sustitución %h para especificar el host en la línea de comandos.

#### *puerto\_exterior*

Designa un puerto específico para conectarse. Utilice el argumento de sustitución %p para especificar el puerto en la línea de comandos. Al especificar %h y %p sin utilizar la opción *Host outside-host*, el comando de proxy se aplica al argumento de host cada vez que se invoca el comando ssh.

## 2 Ejecute Secure Shell especificando el host externo.

Escriba, por ejemplo:

```
myLocalHost% ssh myOutsideHost
```

Este comando busca una especificación de comando de proxy para myOutsideHost en su archivo de configuración personal. Si la especificación no se ha encontrado, el comando busca en el archivo de configuración de todo el sistema, /etc/ssh/ssh\_config. El comando de proxy se sustituye por el comando ssh.

### Ejemplo 19–7 Conexión a hosts fuera de un cortafuegos desde la línea de comandos

“[Cómo configurar conexiones predeterminadas a hosts fuera de un cortafuegos](#)” en la [página 372](#) explica cómo especificar un comando de proxy en un archivo de configuración. En este ejemplo, un comando de proxy se especifica en la línea de comandos ssh.

```
% ssh -o'Proxycommand=/usr/lib/ssh/ssh-http-proxy-connect \
-h myProxyServer -p 8080 myOutsideHost 22' myOutsideHost
```

La opción -o para el comando ssh proporciona un método de línea de comandos para especificar un comando de proxy. En este ejemplo, el comando realiza lo siguiente:

- Sustituye el comando de proxy HTTP para ssh
- Utiliza el puerto 8080 y myProxyServer como el servidor proxy
- Se conecta al puerto 22 en myOutsideHost



## Oracle Solaris Secure Shell (referencia)

---

En este capítulo, se describen las opciones de configuración de la función Secure Shell de Oracle Solaris. A continuación puede ver una lista de la información de referencia que se ofrece en este capítulo:

- “Una sesión de Secure Shell típica” en la página 375
- “Configuración de cliente y servidor en Secure Shell” en la página 378
- “Palabras clave en Secure Shell” en la página 378
- “Mantenimiento de hosts conocidos en Secure Shell” en la página 383
- “Paquetes e inicialización de Secure Shell” en la página 384
- “Archivos de Secure Shell” en la página 384
- “Comandos de Secure Shell” en la página 387

Si desea obtener procedimientos para configurar Secure Shell, consulte el [Capítulo 19, “Uso de Oracle Solaris Secure Shell \(tareas\)”](#).

### Una sesión de Secure Shell típica

El daemon de Secure Shell (`sshd`) se inicia, normalmente, durante el inicio cuando los servicios de red se inician. El daemon escucha conexiones de clientes. Una sesión de Secure Shell empieza cuando el usuario ejecuta un comando `ssh`, `scp` o `sftp`. Un daemon `sshd` nuevo se bifurca para cada conexión entrante. Los daemons bifurcados manejan intercambio de claves, cifrado, autenticación, ejecución de comandos e intercambio de datos con el cliente. Estas características de la sesión son determinadas por archivos de configuración del lado del cliente y archivos de configuración del lado del servidor. Los argumentos de la línea de comandos pueden sustituir los valores de los archivos de configuración.

El cliente y el servidor deben autenticarse entre ellos. Tras una autenticación con éxito, el usuario puede ejecutar comandos de manera remota y copiar datos entre hosts.

## Características de la sesión en Secure Shell

El comportamiento del lado del servidor del daemon `sshd` se controla mediante valores de palabra clave en el archivo `/etc/ssh/sshd_config`. Por ejemplo, el archivo `sshd_config` controla los tipos de autenticación que se permiten para acceder al servidor. El comportamiento del lado del servidor también se puede controlar mediante las opciones de línea de comandos cuando el daemon `sshd` se inicia.

El comportamiento en el lado del cliente está controlado por palabras clave de Secure Shell en este orden de prioridad:

- Opciones de línea de comandos
- Archivo de configuración del usuario, `~/.ssh/config`
- Archivo de configuración de todo el sistema, `/etc/ssh/ssh_config`

Por ejemplo, un usuario puede sustituir el valor `Ciphers` de la configuración de todo el sistema, que prefiere `aes128-ctr`, especificando `-c aes256-ctr,aes128-ctr,arcfour` en la línea de comandos. Ahora se prefiere el primer cifrado, `aes256-ctr`.

## Autenticación e intercambio de claves en Secure Shell

Los protocolos de Secure Shell, v1 y v2, admiten la autenticación de host y usuario de cliente, y la autenticación de host de servidor. Ambos protocolos implican el intercambio de claves criptográficas de sesión para la protección de sesiones de Secure Shell. Cada protocolo proporciona varios métodos de autenticación e intercambio de claves. Algunos métodos son opcionales. Secure Shell admite varios mecanismos de autenticación de clientes, como se muestra en la [Tabla 19-1](#). Los servidores se autentican con claves públicas de host conocidas.

Para el protocolo v1, Secure Shell admite la autenticación de usuario con contraseñas. El protocolo también admite claves públicas y autenticación de usuario con claves públicas de host de confianza. La autenticación de servidor se realiza con una clave pública de host. Para el protocolo v1, todas las claves públicas son claves [RSA](#). Los intercambios de claves de sesión implican el uso de una clave de servidor efímera que se regenera periódicamente.

Para el protocolo v2, Secure Shell admite la autenticación de usuario y la autenticación interactiva genérica, que, por lo general, involucra contraseñas. El protocolo también admite la autenticación con claves públicas de usuario y con claves públicas de host de confianza. Las claves pueden ser RSA o [DSA](#). Los intercambios de claves de sesión constan de intercambios de claves efímeras Diffie-Hellman que se firman en el paso de autenticación de servidor. Además, Secure Shell puede usar credenciales GSS para la autenticación.

## Adquisición de credenciales GSS en Secure Shell

A fin de utilizar la GSS-API para la autenticación en Secure Shell, el servidor debe tener credenciales de aceptador GSS-API y el cliente debe tener credenciales de iniciador GSS-API. Se admiten los mecanismos `mech_dh` y `mech_krb5`.



Para `mech_dh`, el servidor tiene credenciales de aceptador GSS-API si `root` ha ejecutado el comando `keylogin`.

Para `mech_krb5`, el servidor tiene credenciales de aceptador GSS-API cuando el principal host que corresponde al servidor tiene una entrada válida en `/etc/krb5/krb5.keytab`.

El cliente tiene credenciales de iniciador para `mech_dh` si se ha realizado una de las siguientes acciones:

- El comando `keylogin` se ha ejecutado.
- El módulo `pam_dhkeys` se utiliza en el archivo `pam.conf`.

El cliente tiene credenciales de iniciador para `mech_krb5` si se ha realizado una de las siguientes acciones:

- El comando `kinit` se ha ejecutado.
- El módulo `pam_krb5` se utiliza en el archivo `pam.conf`.

Para el uso de `mech_dh` en RPC seguro, consulte el [Capítulo 16, “Uso de servicios de autenticación \(tarear\)”](#). Para el uso de `mech_krb5`, consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#). Para obtener más información sobre los mecanismos, consulte las páginas del comando `man mech(4)` y `man mech_spnego(5)`.

## Ejecución de comandos y reenvío de datos en Secure Shell

Una vez completada la autenticación, el usuario puede utilizar Secure Shell, generalmente, mediante la solicitud de un shell o la ejecución de un comando. Mediante las opciones del comando `ssh`, el usuario puede realizar solicitudes. Las solicitudes pueden incluir la asignación de un pseudo-tty, el reenvío de conexiones X11 o conexiones TCP/IP, o la habilitación de un programa de autenticación `ssh-agent` por medio de una conexión segura.

Los componentes básicos de una sesión de usuario son los siguientes:

1. El usuario solicita un shell o la ejecución de un comando, que inicia el modo de sesión.  
En este modo, los datos se envían o se reciben por medio del terminal en el lado del cliente. En el lado del servidor, los datos se envían por medio del shell o de un comando.
2. Cuando la transferencia de datos se completa, el programa de usuario finaliza.
3. Todos los reenvíos de X11 y de TCP/IP se detienen, excepto para las conexiones que ya existen. Las conexiones X11 y TCP/IP existentes permanecen abiertas.
4. El servidor envía un mensaje de estado de salida al cliente. Cuando todas las conexiones están cerradas, como los puertos reenviados que habían permanecido abiertos, el cliente cierra la conexión al servidor. A continuación, el cliente se cierra.

## Configuración de cliente y servidor en Secure Shell

Las características de una sesión de Secure Shell son controladas por los archivos de configuración. Los archivos de configuración se pueden sustituir a un cierto grado por opciones en la línea de comandos.

### Configuración de clientes en Secure Shell

En la mayoría de los casos, las características del lado del cliente de una sesión de Secure Shell son determinadas por el archivo de configuración de todo el sistema, `/etc/ssh/ssh_config`. Los valores del archivo `ssh_config` se pueden sustituir por el archivo de configuración del usuario, `~/.ssh/config`. Además, el usuario puede sustituir ambos archivos de configuración en la línea de comandos.

Los valores en el archivo `/etc/ssh/sshd_config` del servidor determinan qué solicitudes de clientes son permitidas por el servidor. Para obtener una lista de valores de configuración del servidor, consulte [“Palabras clave en Secure Shell” en la página 378](#). Para obtener información detallada, consulte la página del comando `man sshd_config(4)`.

Las palabras clave en el archivo de configuración del cliente se muestran en [“Palabras clave en Secure Shell” en la página 378](#). Si la palabra clave tiene un valor predeterminado, el valor se proporciona. Estas palabras clave se describen detalladamente en las páginas del comando `man ssh(1)`, `scp(1)`, `sftp(1)` y `ssh_config(4)`. Para obtener una lista de palabras clave en orden alfabético y sus valores de sustitución de línea de comandos equivalentes, consulte la [Tabla 20–8](#).

### Configuración de servidores en Secure Shell

Las características del lado del servidor de una sesión de Secure Shell son determinadas por el archivo `/etc/ssh/sshd_config`. Las palabras clave en el archivo de configuración del servidor se muestran en [“Palabras clave en Secure Shell” en la página 378](#). Si la palabra clave tiene un valor predeterminado, el valor se proporciona. Para obtener una descripción completa de las palabras clave, consulte la página del comando `man sshd_config(4)`.

## Palabras clave en Secure Shell

En las tablas siguientes, se enumeran las palabras clave y sus valores predeterminados (si hay). Las palabras clave están en orden alfabético. La ubicación de palabras clave en el cliente es el archivo `ssh_config`. Las palabras clave que se aplican al servidor están en el archivo `sshd_config`. Algunas palabras clave se establecen en ambos archivos. Si la palabra clave sólo se aplica a una versión de protocolo, la versión se enumera.

TABLA 20-1 Palabras clave en archivos de configuración de Secure Shell (de A a Escape)

Palabra clave	Valor predeterminado	Ubicación	Protocolo
AllowGroups	No hay valor predeterminado.	Servidor	
AllowTcpForwarding	yes	Servidor	
AllowUsers	No hay valor predeterminado.	Servidor	
AuthorizedKeysFile	~/.ssh/authorized_keys	Servidor	
Banner	/etc/issue	Servidor	
Batchmode	no	Cliente	
BindAddress	No hay valor predeterminado.	Cliente	
CheckHostIP	yes	Cliente	
ChrootDirectory	no	Servidor	v2
Cipher	blowfish, 3des	Cliente	v1
Ciphers	aes128-ctr, aes128-cbc, 3des-cbc, blowfish-cbc, arcfour	Ambos	v2
ClearAllForwardings	no	Cliente	
ClientAliveCountMax	3	Servidor	v2
ClientAliveInterval	0	Servidor	v2
Compression	no	Ambos	
CompressionLevel	No hay valor predeterminado.	Cliente	v1
ConnectionAttempts	1	Cliente	
DenyGroups	No hay valor predeterminado.	Servidor	
DenyUsers	No hay valor predeterminado.	Servidor	
DynamicForward	No hay valor predeterminado.	Cliente	
EscapeChar	~	Cliente	

TABLA 20-2 Palabras clave en archivos de configuración de Secure Shell (de Fall a Local)

Palabra clave	Valor predeterminado	Ubicación	Protocolo
FallBackToRsh	no	Cliente	
ForwardAgent	no	Cliente	
ForwardX11	no	Cliente	

TABLA 20-2 Palabras clave en archivos de configuración de Secure Shell (de Fall a Local)  
(Continuación)

Palabra clave	Valor predeterminado	Ubicación	Protocolo
GatewayPorts	no	Ambos	
GlobalKnownHostsFile	/etc/ssh/ssh_known_hosts	Cliente	
GSSAPIAuthentication	yes	Ambos	v2
GSSAPIDelegateCredentials	no	Cliente	v2
GSSAPIKeyExchange	yes	Ambos	v2
GSSAPIStoreDelegateCredentials	yes	Servidor	v2
Host	* Para obtener más información, consulte <a href="#">“Parámetros específicos de host Secure Shell” en la página 382.</a>	Cliente	
HostbasedAuthentication	no	Ambos	v2
HostbasedUsesNameFromPacketOnly	no	Servidor	v2
HostKey	/etc/ssh/ssh_host_key	Servidor	v1
HostKey	/etc/ssh/host_rsa_key, /etc/ssh/host_dsa_key	Servidor	v2
HostKeyAlgorithms	ssh-rsa, ssh-dss	Cliente	v2
HostKeyAlias	No hay valor predeterminado.	Cliente	v2
HostName	No hay valor predeterminado.	Cliente	v2
IdentityFile	~/.ssh/identity	Cliente	v1
IdentityFile	~/.ssh/id_dsa, ~/.ssh/id_rsa	Cliente	v2
IgnoreRhosts	yes	Servidor	
IgnoreUserKnownHosts	yes	Servidor	
KbdInteractiveAuthentication	yes	Ambos	
KeepAlive	yes	Ambos	
KeyRegenerationInterval	3600 (segundos)	Servidor	
ListenAddress	No hay valor predeterminado.	Servidor	
LocalForward	No hay valor predeterminado.	Cliente	

TABLA 20-3 Palabras clave en archivos de configuración de Secure Shell (de Login a R)

Palabra clave	Valor predeterminado	Ubicación	Protocolo
LoginGraceTime	600 (segundos)	Servidor	
LogLevel	info	Ambos	
LookupClientHostnames	yes	Servidor	
MACs	hmac-sha1,hmac-md5	Ambos	v2
MaxAuthTries	6	Servidor	
MaxAuthTriesLog	3	Servidor	
MaxStartups	10:30:60	Servidor	
NoHostAuthenticationForLocalHost	no	Cliente	
NumberOfPasswordPrompts	3	Cliente	
PAMAuthenticationViaKBDInt	yes	Servidor	v2
PasswordAuthentication	yes	Ambos	Ambos
PermitEmptyPasswords	no	Servidor	
PermitRootLogin	no	Servidor	
PermitUserEnvironment	no	Servidor	
PidFile	/var/run/sshd.pid	Servidor	
Port	22	Ambos	
PreferredAuthentications	hostbased,publickey,keyboard-interactive,password	Cliente	v2
PrintLastLog	yes	Servidor	v2
PrintMotd	no	Servidor	
Protocol	2,1	Ambos	
ProxyCommand	No hay valor predeterminado.	Cliente	
PubkeyAuthentication	yes	Ambos	v2
RemoteForward	No hay valor predeterminado.	Cliente	
RhostsAuthentication	no	Ambos	v1
RhostsRSAAuthentication	no	Ambos	v1
RSAAuthentication	no	Ambos	v1

TABLA 20-4 Palabras clave en archivos de configuración de Secure Shell (de S a X)

Palabra clave	Valor predeterminado	Ubicación	Protocolo
StrictHostKeyChecking	ask	Cliente	
StrictModes	yes	Servidor	
Subsystem	sftp /usr/lib/ssh/sftp-server	Servidor	
SyslogFacility	auth	Servidor	
UseLogin	no descartado e ignorado.	Servidor	
UseOpenSSLEngine	yes	Ambos	v2
UsePrivilegedPort	no	Ambos	v2
User	No hay valor predeterminado.	Cliente	
UserKnownHostsFile	~/.ssh/known_hosts	Cliente	
UseRsh	no	Cliente	
VerifyReverseMapping	no	Servidor	
X11DisplayOffset	10	Servidor	
X11Forwarding	yes	Servidor	
X11UseLocalHost	yes	Servidor	
XAuthLocation	/usr/openwin/bin/xauth	Ambos	

## Parámetros específicos de host Secure Shell

Si es útil tener diferentes características de Secure Shell para diferentes hosts locales, el administrador puede definir conjuntos separados de parámetros en el archivo `/etc/ssh/ssh_config` que se aplicarán según la expresión regular o de host. Esta tarea se realiza mediante la agrupación de entradas en el archivo por la palabra clave `Host`. Si la palabra clave `Host` no se utiliza, las entradas en el archivo de configuración del cliente se aplican a cualquier host local en el que un usuario está trabajando.

## Secure Shell y variables de entorno de inicio de sesión

Cuando las siguientes palabras clave de Secure Shell no están establecidas en el archivo `sshd_config`, obtienen el valor de entradas equivalentes en el archivo `/etc/default/login`:

Entrada en <code>/etc/default/login</code>	Palabra clave y valor en <code>sshd_config</code>
<code>CONSOLE=*</code>	<code>PermitRootLogin=without-password</code>
<code>#CONSOLE=*</code>	<code>PermitRootLogin=yes</code>
<code>PASSREQ=YES</code>	<code>PermitEmptyPasswords=no</code>
<code>PASSREQ=NO</code>	<code>PermitEmptyPasswords=yes</code>
<code>#PASSREQ</code>	<code>PermitEmptyPasswords=no</code>
<code>TIMEOUT=segundos</code>	<code>LoginGraceTime=segundos</code>
<code>#TIMEOUT</code>	<code>LoginGraceTime=300</code>
<code>RETRIES</code> y <code>SYSLOG_FAILED_LOGINS</code>	Sólo se aplican a métodos de autenticación de password y keyboard-interactive.

Cuando las siguientes variables están establecidas por las secuencias de comandos de inicialización del shell de inicio de sesión del usuario, el daemon `sshd` utiliza dichos valores. Cuando las variables no están establecidas, el daemon utiliza el valor predeterminado.

<code>TIMEZONE</code>	Controla la configuración de la variable de entorno TZ. Cuando no está establecida, el daemon <code>sshd</code> utiliza el valor de TZ cuando se inició el daemon.
<code>ALTSHELL</code>	Controla la configuración de la variable de entorno SHELL. El valor predeterminado es <code>ALTSHELL=YES</code> , donde el daemon <code>sshd</code> utiliza el valor del shell del usuario. Cuando el valor predeterminado es <code>ALTSHELL=NO</code> , el valor SHELL no está establecido.
<code>PATH</code>	Controla la configuración de la variable de entorno PATH. Cuando el valor no está establecido, la ruta predeterminada es <code>/usr/bin</code> .
<code>SUPATH</code>	Controla la configuración de la variable de entorno PATH para root. Cuando el valor no está establecido, la ruta predeterminada es <code>/usr/sbin:/usr/bin</code> .

Para obtener más información, consulte las páginas del comando `man login(1)` y `sshd(1M)`.

## Mantenimiento de hosts conocidos en Secure Shell

Cada host que necesita comunicarse de manera segura con otro host debe tener la clave pública del servidor almacenada en el archivo `/etc/ssh/ssh_known_hosts` del host local. Aunque una secuencia de comandos podría utilizarse para actualizar los archivos `/etc/ssh/ssh_known_hosts`, esta práctica es fuertemente desalentada, porque una secuencia de comandos abre una importante vulnerabilidad de seguridad.

El archivo `/etc/ssh/ssh_known_hosts` sólo debería ser distribuido por un mecanismo seguro, de la siguiente manera:

- Por medio de una conexión segura, como Secure Shell, IPsec o ftp Kerberizado de un equipo conocido y de confianza
- En el tiempo de instalación del sistema

Para evitar la posibilidad de que un intruso obtenga acceso insertando claves públicas falsas en un archivo `known_hosts`, debe utilizar un servidor JumpStart como el origen conocido y de confianza del archivo `ssh_known_hosts`. El archivo `ssh_known_hosts` se puede distribuir durante la instalación. Más tarde, las secuencias de comandos que utiliza el comando `scp` se pueden utilizar para obtener la última versión. Este enfoque es seguro, porque cada host ya tiene la clave pública del servidor JumpStart.

## Paquetes e inicialización de Secure Shell

Secure Shell depende de paquetes de Solaris centrales y de los siguientes paquetes:

- `SUNWgss`: contiene software de servicios de seguridad genéricos (GSS)
- `SUNWtcpd`: contiene envoltorios TCP
- `SUNWopenssl-libraries`: contiene bibliotecas OpenSSL
- `SUNWzlib`: contiene la biblioteca de compresión de archivos zip

Los siguientes paquetes instalan Secure Shell:

- `SUNWsshr`: contiene archivos y utilidades del cliente para el directorio `/` root
- `SUNWsshdr`: contiene archivos y utilidades del servidor para el directorio `/` root
- `SUNWsshcu`: contiene archivos de origen comunes para el directorio `/usr`
- `SUNWsshdu`: contiene archivos del servidor para el directorio `/usr`
- `SUNWsshu`: contiene archivos y utilidades del cliente para el directorio `/usr`

Al reiniciar el sistema después de la instalación, el daemon `sshd` se está ejecutando. El daemon crea claves de host en el sistema. Un sistema Oracle Solaris que ejecuta el daemon `sshd` es un servidor de Secure Shell.

## Archivos de Secure Shell

En la siguiente tabla, se muestran los principales archivos de Secure Shell y los permisos de archivo sugeridos.



TABLA 20-5 Archivos de Secure Shell

Nombre de archivo	Descripción	Permisos sugeridos y propietario
<code>/etc/ssh/sshd_config</code>	Contiene datos de configuración para <code>sshd</code> , el daemon de Secure Shell.	<code>-rw-r--r-- root</code>
<code>/etc/ssh/ssh_host_key</code>	Contiene la clave privada de host (v1).	<code>-rw----- root</code>
<code>/etc/ssh/ssh_host_dsa_key</code> o <code>/etc/ssh/ssh_host_rsa_key</code>	Contiene la clave privada de host (v2).	<code>-rw----- root</code>
<code>clave privada de host.pub</code>	Contiene la clave pública de host, por ejemplo, <code>/etc/ssh/ssh_host_rsa_key.pub</code> . Se utiliza para copiar la clave del host en el archivo <code>known_hosts</code> local.	<code>-rw-r--r-- root</code>
<code>/var/run/sshd.pid</code>	Contiene el ID de proceso del daemon de Secure Shell, <code>sshd</code> . Si hay varios daemons en ejecución, el archivo contiene el último daemon que se ha iniciado.	<code>-rw-r--r-- root</code>
<code>~/.ssh/authorized_keys</code>	Contiene las claves públicas del usuario que tiene permitido iniciar sesión en la cuenta de usuario.	<code>-rw-r--r-- nombre de usuario</code>
<code>/etc/ssh/ssh_known_hosts</code>	Contiene las claves públicas de host de todos los hosts con los que el cliente puede comunicarse de forma segura. El archivo es rellenado por el administrador.	<code>-rw-r--r-- root</code>
<code>~/.ssh/known_hosts</code>	Contiene las claves públicas de host de todos los hosts con los que el cliente puede comunicarse de forma segura. El archivo se mantiene automáticamente. Cada vez que el usuario se conecta con un host desconocido, la clave del host remoto se agrega al archivo.	<code>-rw-r--r-- nombre de usuario</code>
<code>/etc/default/login</code>	Proporciona valores predeterminados para el daemon <code>sshd</code> cuando los parámetros <code>sshd_config</code> correspondientes no están establecidos.	<code>-r--r--r-- root</code>
<code>/etc/nologin</code>	Si el archivo existe, el daemon <code>sshd</code> sólo permite que <code>root</code> inicie sesión. El contenido de este archivo se muestra a los usuarios que intentan iniciar sesión.	<code>-rw-r--r-- root</code>
<code>~/.rhosts</code>	Contiene los pares de host y nombre de usuario que especifican los hosts en los que el usuario puede iniciar sesión sin una contraseña. Este archivo también es utilizado por los daemons <code>rlogind</code> y <code>rshd</code> .	<code>-rw-r--r-- nombre de usuario</code>
<code>~/.shosts</code>	Contiene los pares de host y nombre de usuario que especifican los hosts en los que el usuario puede iniciar sesión sin una contraseña. Este archivo no es utilizado por otras utilidades. Para obtener más información, consulte la página del comando <code>man sshd(1M)</code> en la sección FILES.	<code>-rw-r--r-- nombre de usuario</code>

TABLA 20-5 Archivos de Secure Shell (Continuación)

Nombre de archivo	Descripción	Permisos sugeridos y propietario
/etc/hosts.equiv	Contiene los hosts que se utilizan en la autenticación . rhosts. Este archivo también es utilizado por los daemons rlogind y rshd.	-rw-r--r-- root
/etc/ssh/shosts.equiv	Contiene los hosts que se utilizan en la autenticación basada en host. Este archivo no es utilizado por otras utilidades.	-rw-r--r-- root
~/.ssh/environment	Contiene asignaciones iniciales en el momento del inicio de sesión. De manera predeterminada, este archivo no se lee. La palabra clave PermitUserEnvironment en el archivo sshd_config se debe establecer en yes para que este archivo se lea.	-rw-r--r-- nombre de usuario
~/.ssh/rc	Contiene las rutinas de inicialización que se ejecutan antes de que el shell del usuario se inicie. Para ver un ejemplo de rutina de inicialización, consulte la página del comando man sshd(1M).	-rw-r--r-- nombre de usuario
/etc/ssh/sshrd	Contiene rutinas de inicialización específicas de host que son especificadas por un administrador.	-rw-r--r-- root
/etc/ssh/ssh_config	Configura los valores del sistema en el sistema cliente.	-rw-r--r-- root
~/.ssh/config	Configura valores de configuración del usuario. Sustituye valores del sistema.	-rw-r--r-- nombre de usuario

En la siguiente tabla, se muestran los archivos de Secure Shell que se pueden sustituir por palabras clave u opciones de comandos.

TABLA 20-6 Valores de sustitución para la ubicación de archivos de Secure Shell

Nombre de archivo	Valor de sustitución de palabra clave	Valor de sustitución de línea de comandos
/etc/ssh/ssh_config		ssh -F archivo de configuración scp -F archivo de configuración
~/.ssh/config		ssh -F archivo de configuración
/etc/ssh/host_rsa_key	HostKey	
/etc/ssh/host_dsa_key		
~/.ssh/identity	IdentityFile	ssh -i archivo de identidad
~/.ssh/id_dsa,~/.ssh/id_rsa		scp -i archivo de identidad
~/.ssh/authorized_keys	AuthorizedKeysFile	
/etc/ssh/ssh_known_hosts	GlobalKnownHostsFile	

TABLA 20-6 Valores de sustitución para la ubicación de archivos de Secure Shell (Continuación)

Nombre de archivo	Valor de sustitución de palabra clave	Valor de sustitución de línea de comandos
~/ .ssh/known_hosts	UserKnownHostsFile	
	IgnoreUserKnownHosts	

## Comandos de Secure Shell

En la siguiente tabla, se resumen los principales comandos de Secure Shell.

TABLA 20-7 Comandos en Secure Shell

Comando	Descripción	Página del comando man
ssh	Inicia sesión de un usuario en un equipo remoto y ejecuta de manera segura comandos en un equipo remoto. Este comando es la sustitución de Secure Shell para los comandos rlogin y rsh. El comando ssh permite comunicaciones cifradas seguras entre dos hosts que no son de confianza por medio de una red no segura. Las conexiones X11 y los puertos TCP/IP arbitrarios también se pueden reenviar por medio del canal seguro.	<a href="#">ssh(1)</a>
sshd	Es el daemon para Secure Shell. El daemon escucha conexiones de clientes y permite comunicaciones cifradas seguras entre dos hosts que no son de confianza por medio de una red no segura.	<a href="#">sshd(1M)</a>
ssh-add	Agrega identidades RSA o DSA al agente de autenticación, ssh-agent. Las identidades también se denominan <i>claves</i> .	<a href="#">ssh-add(1)</a>
ssh-agent	Contiene claves privadas que se utilizan para la autenticación de clave pública. El programa ssh-agent se inicia al principio de una sesión X o de una sesión de inicio de sesión. Todas las demás ventanas y otros programas se inician como clientes del programa ssh-agent. Mediante el uso de variables de entorno, el agente se puede localizar y utilizar para la autenticación cuando los usuarios utilizan el comando ssh para iniciar sesión en otros sistemas.	<a href="#">ssh-agent(1)</a>
ssh-keygen	Genera y gestiona claves de autenticación para Secure Shell.	<a href="#">ssh-keygen(1)</a>
ssh-keyscan	Recopila las claves públicas de varios hosts de Secure Shell. Ayuda en la generación y la verificación de archivos ssh_known_hosts.	<a href="#">ssh-keyscan(1)</a>
ssh-keysign	Es utilizado por el comando ssh para acceder a las claves de host en el host local. Genera la firma digital que se requiere durante la autenticación basada en host con Secure Shell v2. El comando es invocado por el comando ssh, no por el usuario.	<a href="#">ssh-keysign(1M)</a>
scp	Copia de manera segura archivos entre hosts en una red por medio de un transporte ssh cifrado. A diferencia del comando rcp, el comando scp solicita contraseñas o frases de contraseña si la información de contraseña es necesaria para la autenticación.	<a href="#">scp(1)</a>

TABLA 20-7 Comandos en Secure Shell (Continuación)

Comando	Descripción	Página del comando man
sftp	Es un programa de transferencia de archivos interactivo similar al comando ftp. A diferencia del comando ftp, el comando sftp realiza todas las operaciones por medio de un transporte ssh cifrado. El comando se conecta, inicia sesión en el nombre de host especificado y, a continuación, introduce el modo de comando interactivo.	sftp(1)

En la siguiente tabla, se muestran las opciones de comandos que sustituyen palabras clave de Secure Shell. Las palabras clave se especifican en los archivos ssh\_config y sshd\_config.

TABLA 20-8 Equivalentes de línea de comandos para palabras clave de Secure Shell

Palabra clave	Valor de sustitución de línea de comandos ssh	Valor de sustitución de línea de comandos scp
BatchMode		scp -B
BindAddress	ssh -b <i>dirección de enlace</i>	scp -a <i>dirección de enlace</i>
Cipher	ssh -c <i>cifrado</i>	scp -c <i>cifrado</i>
Ciphers	ssh -c <i>especificación de cifrado</i>	scp -c <i>especificación de cifrado</i>
Compression	ssh -C	scp -C
DynamicForward	ssh -D <i>puerto SOCKS4</i>	
EscapeChar	ssh -e <i>carácter de escape</i>	
ForwardAgent	ssh -A para habilitar ssh -a para deshabilitar	
ForwardX11	ssh -X para habilitar ssh -x para deshabilitar	
GatewayPorts	ssh -g	
IPv4	ssh -4	scp -4
IPv6	ssh -6	scp -6
LocalForward	ssh -L <i>puerto_local:host_remoto:puerto_remoto</i>	
MACS	ssh -m <i>especificación de mac</i>	
Port	ssh -p <i>puerto</i>	scp -P <i>puerto</i>
Protocol	ssh -1 sólo para v1 ssh -2 sólo para v2	

TABLA 20-8 Equivalentes de línea de comandos para palabras clave de Secure Shell (Continuación)

Palabra clave	Valor de sustitución de línea de comandos ssh	Valor de sustitución de línea de comandos scp
RemoteForward	ssh -R <i>puerto_remoto:host_local:puerto_local</i>	



## P A R T E V I

# Servicio Kerberos

En esta sección se proporciona información acerca de la configuración, la gestión y el uso del servicio Kerberos en los siguientes capítulos:

- Capítulo 21, “Introducción al servicio Kerberos”
- Capítulo 22, “Planificación del servicio Kerberos”
- Capítulo 23, “Configuración del servicio Kerberos (tareas)”
- Capítulo 24, “Mensajes de error y resolución de problemas de Kerberos”
- Capítulo 25, “Administración de las políticas y los principales de Kerberos (tareas)”
- Capítulo 26, “Uso de aplicaciones Kerberos (tareas)”
- Capítulo 27, “El servicio Kerberos (referencia)”





## Introducción al servicio Kerberos

---

En este capítulo, se brinda una introducción al servicio Kerberos. A continuación, se presenta la información general que se incluye en este capítulo.

- “¿Qué es el servicio Kerberos?” en la página 393
- “Cómo funciona el servicio Kerberos” en la página 394
- “Servicios de seguridad de Kerberos” en la página 401
- “Componentes de las distintas versiones de Kerberos” en la página 402

### ¿Qué es el servicio Kerberos?

El *servicio Kerberos* es una arquitectura cliente-servidor que proporciona seguridad a las transacciones en las redes. El servicio ofrece una sólida autenticación de usuario y también integridad y privacidad. La *autenticación* garantiza que las identidades del remitente y del destinatario de las transacciones de la red sean verdaderas. El servicio también puede verificar la validez de los datos que se transfieren de un lugar a otro (*integridad*) y cifrar los datos durante la transmisión (*privacidad*). Con el servicio Kerberos, puede iniciar sesión en otros equipos, ejecutar comandos, intercambiar datos y transferir archivos de manera segura. Además, Kerberos proporciona servicios de *autorización*, que permiten a los administradores restringir el acceso a los servicios y los equipos. Asimismo, como usuario de Kerberos, puede regular el acceso de otras personas a su cuenta.

El servicio Kerberos es un sistema de *inicio de sesión único*. Esto significa que sólo debe autenticarse con el servicio una vez por sesión, y todas las transacciones realizadas posteriormente durante la sesión se aseguran de manera automática. Una vez que el servicio lo autenticó, no necesita volver a autenticarse cada vez que utiliza un comando basado en Kerberos, como `ftp` o `rsh`, o accede a datos en un sistema de archivos NFS. Por lo tanto, no es necesario que envíe la contraseña a través de la red, donde puede ser interceptada, cada vez que utiliza estos servicios.

El servicio Oracle Solaris Kerberos se basa en el protocolo de autenticación de red Kerberos V5, que fue desarrollado en el Instituto Tecnológico de Massachusetts (MIT, Massachusetts

Institute of Technology). A quienes hayan utilizado el producto Kerberos V5 la versión de Oracle Solaris les resultará muy familiar. Dado que el protocolo Kerberos V5 es un estándar *de facto* para la seguridad de la red en la industria, la versión de Oracle Solaris promueve la interoperabilidad con otros sistemas. En otras palabras, como el servicio Oracle Solaris Kerberos funciona con sistemas que usan el protocolo Kerberos V5, el servicio favorece las transacciones seguras incluso en redes heterogéneas. Además, el servicio proporciona autenticación y seguridad tanto entre dominios como dentro de un único dominio.

El servicio Kerberos brinda flexibilidad para la ejecución de las aplicaciones de Oracle Solaris. Puede configurar el servicio para permitir solicitudes de servicios de red que se basen o no en Kerberos, como el servicio NFS, `telnet` y `ftp`. Como resultado, las aplicaciones actuales seguirán funcionando, incluso si se ejecutan en sistemas en que el servicio Kerberos no se encuentre habilitado. Igualmente, puede configurar el servicio Kerberos para permitir únicamente solicitudes de red que se basen en Kerberos.

El servicio Kerberos ofrece un mecanismo de seguridad que permite el uso de Kerberos para la autenticación, la integridad y la privacidad cuando se utilizan aplicaciones que emplean Generic Security Service Application Programming Interface (GSS-API). Sin embargo, no es necesario que las aplicaciones permanezcan comprometidas con el servicio Kerberos si se desarrollan otros mecanismos de seguridad. Como el servicio está diseñado para integrarse en GSS-API de manera modular, las aplicaciones que utilizan GSS-API pueden emplear el mecanismo de seguridad que mejor se ajuste a sus necesidades.

## Cómo funciona el servicio Kerberos

A continuación, se ofrece una descripción general del sistema de autenticación Kerberos. Para obtener una descripción más detallada, consulte [“Cómo funciona el sistema de autenticación Kerberos” en la página 575](#).

Desde el punto de vista del usuario, una vez que se inició la sesión Kerberos, el servicio Kerberos queda invisible la mayor parte del tiempo. Los comandos como `rsh` o `ftp` trabajan de manera similar. Normalmente, para inicializar una sesión Kerberos sólo se debe iniciar sesión y proporcionar una contraseña de Kerberos.

El sistema Kerberos se basa en el concepto de *tickets*. Un ticket es un conjunto de información electrónica que identifica a un usuario o servicio, como el servicio NFS. Así como su licencia de conducir lo identifica e indica qué privilegios tiene para conducir un automóvil, el ticket lo identifica e indica qué privilegios tiene para acceder a la red. Cuando realiza una transacción que se basa en Kerberos (por ejemplo, si inicia sesión en otro equipo de manera remota), envía de manera transparente una solicitud de un ticket a un *Centro de distribución de claves* (KDC). El KDC accede a una base de datos para autenticar su identidad y devuelve un ticket que le concede permiso para acceder a otro equipo. La expresión "de manera transparente" implica que no necesita solicitar un ticket de manera explícita. La solicitud forma parte de la actividad

del comando `rlogin`. Debido a que sólo los clientes que están autenticados pueden obtener un ticket para un servicio específico, los demás clientes no pueden usar `rlogin` con una identidad asumida.

Los tickets tienen asociados algunos atributos determinados. Por ejemplo, un ticket puede ser *reenviable*, lo que significa que se puede utilizar en otro equipo sin que se realice un nuevo proceso de autenticación. Asimismo, un ticket puede ser *posfechado*, que significa que no adquiere validez hasta un momento especificado. El modo de uso de los tickets, por ejemplo, para especificar qué usuarios pueden obtener los distintos tipos de tickets, se establece mediante *políticas*. Las políticas se determinan durante la instalación o administración del servicio Kerberos.

---

**Nota** – Con frecuencia verá los términos *credencial* y *ticket*. En el ámbito de Kerberos en general, estos términos se utilizan de manera indistinta. Sin embargo, técnicamente, una credencial es un ticket con una *clave de sesión* para una sesión determinada. Esta diferencia se explica en profundidad en [“Obtención de acceso a un servicio con Kerberos” en la página 575](#).

---

Las siguientes secciones explican más detalladamente el proceso de autenticación Kerberos.

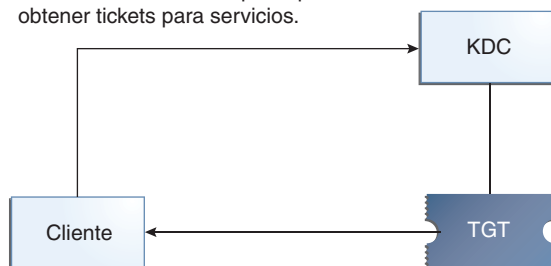
## Autenticación inicial: el ticket de otorgamiento de tickets

La autenticación de Kerberos tiene dos fases: una autenticación inicial que permite que se lleven a cabo todas las autenticaciones posteriores y las autenticaciones posteriores en sí mismas.

La siguiente figura muestra cómo se lleva a cabo la autenticación inicial.

FIGURA 21-1 Autenticación inicial para una sesión Kerberos

1. En el inicio de sesión (o con `kinit`), el cliente solicita un TGT que le permite obtener tickets para servicios.



3. El cliente usa la contraseña para descifrar, por lo tanto, proporciona la identidad. Ahora puede usar el TGT para obtener otros tickets.
2. El KDC comprueba la base de datos y envía el TGT.

TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

1. Un cliente (un usuario o un servicio como NFS) comienza una sesión Kerberos mediante la solicitud de un *ticket de otorgamiento de tickets* (TGT) desde el Centro de distribución de claves (KDC). Esta solicitud se suele llevar a cabo automáticamente en el inicio de sesión.

Se necesita un ticket de otorgamiento de tickets para obtener otros tickets de servicios específicos. El ticket de otorgamiento de tickets funciona de manera similar a un pasaporte. Como el pasaporte, el ticket de otorgamiento de tickets lo identifica y le permite obtener muchas “visas” (tickets), que en este caso no son para entrar en países extranjeros sino en equipos remotos o servicios de red. Como los pasaportes y las visas, el ticket de otorgamiento de tickets y otros tickets diversos tienen una duración limitada. La diferencia radica en que los comandos “Kerberizados” detectan que tiene un pasaporte y entonces obtienen las visas para usted. No es necesario que se encargue de efectuar las transacciones.

También puede establecerse un analogía entre el ticket de otorgamiento de tickets y un pase de esquí por tres días que sirve para acceder a cuatro centros de esquí diferentes. Puede exhibir el pase en cualquiera de los centros al que quiera acceder y así obtener un ticket de ascenso para dicho centro, siempre que el pase no esté vencido. Una vez que tenga el ticket de ascenso, puede esquiar cuanto quiera en el centro que eligió. Si el día siguiente quiere ir a otro centro, vuelve a exhibir el pase para conseguir otro ticket de ascenso para ese nuevo centro. La diferencia radica en que los comandos basados en Kerberos detectan que tiene un pase de esquí para el fin de semana y entonces obtienen un ticket de ascenso para usted. No es necesario que se encargue de efectuar las transacciones.

2. El KDC crea un ticket de otorgamiento de tickets y lo envía de vuelta al cliente en formato cifrado. El cliente descifra el ticket de otorgamiento de tickets con la contraseña del cliente.

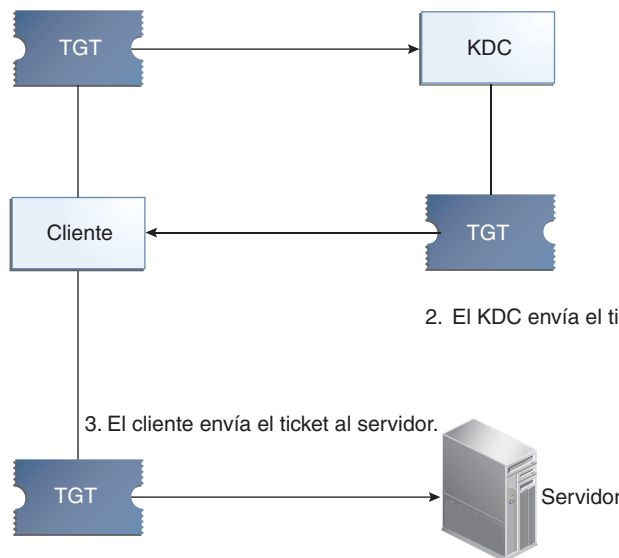
3. Con un ticket de otorgamiento de tickets válido, el cliente puede solicitar tickets para todo tipo de operaciones de red, como `rlogin` o `telnet`, durante todo el período de validez del ticket de otorgamiento de tickets. Por lo general, este ticket dura algunas horas. Cada vez que el cliente realiza una operación de red única, solicita al KDC un ticket para esa operación.

## Autenticaciones Kerberos posteriores

Una vez que el cliente ha recibido la autenticación inicial, cada autenticación posterior sigue el patrón que se muestra en la siguiente figura.

FIGURA 21-2 Obtención de acceso a un servicio con la autenticación Kerberos

1. El cliente solicita el ticket para el servidor y envía el TGT al KDC como prueba de identidad.



2. El KDC envía el ticket al cliente para el servidor.

3. El cliente envía el ticket al servidor.

4. El servidor permite el acceso del cliente.

TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

1. El cliente solicita al KDC un ticket para un servicio en particular; por ejemplo, para iniciar sesión en otro equipo de manera remota. Para ello, envía al KDC su ticket de otorgamiento de tickets como prueba de identidad.
2. El KDC envía el ticket por el servicio específico al cliente.

Por ejemplo, suponga que el usuario joe quiere acceder a un sistema de archivos NFS que se ha compartido con la autenticación krb5 requerida. Como ya se encuentra autenticado (es decir, ya tiene un ticket de otorgamiento de tickets), cuando intenta acceder a los archivos, el sistema de cliente NFS obtiene un ticket del KDC de manera automática y transparente para el servicio NFS.

Por ejemplo, suponga que el usuario joe utiliza `rlogin` en el servidor `boston`. Como ya se encuentra autenticado, (es decir, ya tiene un ticket de otorgamiento de tickets), obtiene un ticket de manera automática y transparente mediante el comando `rlogin`. Este ticket le permite iniciar sesión de manera remota en `boston` tantas veces como quiera hasta que el ticket caduque. Si joe inicia sesión de manera remota en el equipo `denver`, obtiene otro ticket, como en el paso 1.

3. El cliente envía el ticket al servidor.

Cuando se usa el servicio NFS, el cliente NFS envía el ticket de manera automática y transparente al servidor NFS para el servicio NFS.

4. El servidor permite el acceso de clientes.

Según estos pasos, parece que el servidor nunca se comunica con el KDC. Sin embargo, el servidor sí se comunica. Se registra con el KDC, como lo hace el primer cliente. A fin de simplificar el proceso, esa parte se excluye.

## Aplicaciones remotas de Kerberos

Los comandos basados en Kerberos (o “Kerberizados”) que un usuario como joe puede utilizar son los siguientes:

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Estas aplicaciones son iguales a las aplicaciones de Solaris que tienen el mismo nombre. Sin embargo, se han ampliado a fin de utilizar los principales de Kerberos para autenticar las transacciones y proporcionar así una seguridad basada en Kerberos. Consulte [“Los principales de Kerberos” en la página 399](#) para obtener información sobre los principales.

Estos comandos se analizan detalladamente en [“Comandos de usuario de Kerberos” en la página 558](#).

## Los principales de Kerberos

Un cliente en el servicio Kerberos se identifica con su *principal*. Un principal es una identidad única a la que el KDC puede asignar tickets. Un principal puede ser un usuario, como joe, o un servicio, como nfs o telnet.

Por convención, el nombre de principal consta de tres componentes: el *nombre primario*, la *instancia* y el *dominio*. Un principal de Kerberos típico sería, por ejemplo, joe/admin@ENG.EXAMPLE.COM. En este ejemplo:

- joe es el nombre primario. El nombre primario puede ser un nombre de usuario, como se muestra aquí, o un servicio, como nfs. El nombre primario también puede ser la palabra host, lo cual significa que el principal es un principal de servicio que está configurado para proporcionar distintos servicios de red, ftp, rcp, rlogin, etcétera.
- admin es la instancia. La instancia es opcional en el caso de los principales de usuario, pero es necesaria para los principales de servicio. Por ejemplo, si el usuario joe a veces actúa como administrador del sistema, puede utilizar joe/admin para distinguirse de su identidad de usuario habitual. Del mismo modo, si joe tiene cuentas en dos hosts diferentes, puede utilizar dos nombres de principal con instancias diferentes, por ejemplo, joe/denver.example.com y joe/boston.example.com. Tenga en cuenta que el servicio Kerberos trata joe y joe/admin como dos principales completamente diferentes.

En el caso de un principal de servicio, la instancia es el nombre de host completo. Un ejemplo de una instancia así es bigmachine.eng.example.com. La combinación nombre primario/instancia para esta ejemplo podría ser ftp/bigmachine.eng.example.com o host/bigmachine.eng.example.com.

- El dominio de Kerberos es ENG.EXAMPLE.COM. En [“Dominios de Kerberos” en la página 399](#) se analizan los dominios.

Todos los nombres de principal que aparecen a continuación son válidos:

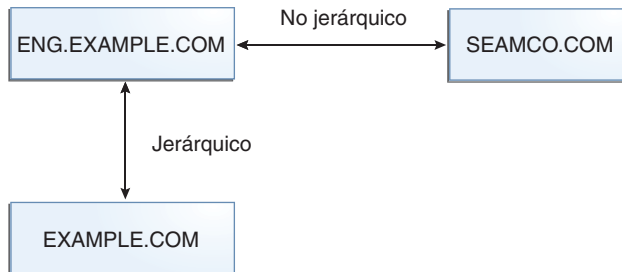
- joe
- joe/admin
- joe/admin@ENG.EXAMPLE.COM
- nfs/host.eng.example.com@ENG.EXAMPLE.COM
- host/eng.example.com@ENG.EXAMPLE.COM

## Dominios de Kerberos

Un *dominio* es una red lógica, similar a un dominio, que define un grupo de sistemas con el mismo KDC *principal*. La [Figura 21–3](#) muestra el modo en que los dominios pueden relacionarse entre sí. Algunos dominios son jerárquicos, lo que implica que un dominio es un superconjunto de los otros dominios. De lo contrario, los dominios son no jerárquicos (o “directos”), y la asignación entre los dos dominios debe definirse. Una característica del servicio

Kerberos es que permite la autenticación entre dominios. Cada dominio sólo necesita una entrada de principal para el otro dominio en su KDC. Esta función de Kerberos se denomina *autenticación entre dominios*.

FIGURA 21-3 Dominios de Kerberos



## Servidores Kerberos

Cada dominio debe incluir un servidor que mantenga la copia maestra de la base de datos del principal. Este servidor se llama *servidor KDC maestro*. Además, cada dominio debe contener por lo menos un *servidor KDC esclavo*, que contenga las copias duplicadas de la base de datos del principal. Tanto el servidor KDC maestro como el servidor KDC esclavo crean tickets que se utilizan para establecer la autenticación.

El dominio también puede incluir un *servidor de aplicaciones* Kerberos. Este servidor proporciona acceso a los servicios Kerberizados (como ftp, telnet, rsh y NFS). Si tiene instalado SEAM 1.0 o 1.0.1, puede que el dominio incluya un servidor de aplicaciones de red Kerberos, pero este software no viene incluido con estas versiones.

La siguiente figura muestra lo que un dominio hipotético puede llegar a contener.



FIGURA 21-4 Un dominio de Kerberos típico



## Servicios de seguridad de Kerberos

Además de proporcionar autenticación segura a los usuarios, el servicio Kerberos proporciona dos servicios de seguridad:

- **Integridad:** así como la autenticación garantiza que los clientes de una red sean quienes dicen ser, la integridad garantiza que los datos que estos envían sean válidos y que no se hayan alterado durante la transmisión. La integridad se lleva a cabo mediante la comprobación criptográfica de los datos. La integridad también incluye la autenticación de usuario.
- **Privacidad:** la privacidad es un paso más avanzado en torno a la seguridad. La privacidad no incluye solamente la verificación de la integridad de los datos transmitidos, sino que también cifra los datos antes de la transmisión para protegerlos de los intrusos. Además, la privacidad autentica a los usuarios.

Los desarrolladores pueden diseñar sus aplicaciones basadas en RPC para seleccionar un servicio de seguridad con la interfaz de programación RPCSEC\_GSS.

# Componentes de las distintas versiones de Kerberos

En varias de las versiones, se incluyen componentes del servicio Kerberos. Originalmente, el servicio Kerberos y los cambios realizados en el sistema operativo básico para que se admita el servicio Kerberos se lanzaron con el nombre de producto “Sun Enterprise Authentication Mechanism”, que se abrevió como SEAM. A medida que se fueron incluyendo más partes del producto SEAM en el software de Oracle Solaris, los contenidos de la versión de SEAM fueron disminuyendo. Para las versiones de Oracle Solaris se incluyen todas las partes del producto SEAM, por lo que el producto SEAM ya no es necesario. El nombre del producto SEAM existe en la documentación por razones históricas.

En la tabla siguiente, se describen los componentes que se incluyen en cada versión. Las versiones de producto se enumeran en orden cronológico. En las secciones siguientes, se describen todos los componentes.

TABLA 21–1    Contenidos de las versiones de Kerberos

Nombre de la versión	Contenido
SEAM 1.0 en Solaris Easy Access Server 3.0	Versión completa del servicio Kerberos para las versiones Solaris 2.6 y 7
Servicio Kerberos en la versión Solaris 8	Software de cliente Kerberos únicamente
SEAM 1.0.1 en Solaris 8 Admin Pack	KDC de Kerberos y aplicaciones remotas para la versión Solaris 8
Servicio Kerberos en la versión Solaris 9	KDC de Kerberos y software de cliente únicamente
SEAM 1.0.2	Aplicaciones remotas de Kerberos para la versión Solaris 9
Servicio Kerberos en la versión Solaris 10	Versión completa del servicio Kerberos con mejoras

## Componentes de Kerberos

De manera similar a la distribución del producto Kerberos V5 del MIT, el servicio Oracle Solaris Kerberos incluye lo siguiente:

- Centro de distribución de claves (KDC):
  - Daemon de administración de bases de datos de Kerberos: `kadmind`.
  - Daemon de procesamiento de tickets de Kerberos: `krb5kdc`.
  - Programas de administración de bases de datos: `kadmin` (maestro solamente), `kadmin.local` y `kdb5_util`.
  - Software de propagación de bases de datos: `kprop` (esclavo solamente) y `kpropd`.
- Programas de usuario para gestionar credenciales: `kinit`, `klist` y `kdestroy`.

- Programa de usuario para cambiar la contraseña de Kerberos: `kpasswd`.
- Aplicaciones remotas: `ftp`, `rcp`, `rdist`, `rlogin`, `rsh`, `ssh` y `telnet`.
- Daemons de aplicaciones remotas: `ftpd`, `rlogind`, `rshd`, `sshd` y `telnetd`.
- Utilidad de administración keytab: `ktutil`.
- Generic Security Service Application Programming Interface (GSS-API): permite que las aplicaciones utilicen varios mecanismos de seguridad sin solicitarle que vuelva a compilar la aplicación cada vez que se agrega un mecanismo nuevo. GSS-API utiliza interfaces estándar que permiten que las aplicaciones puedan emplearse en varios sistemas operativos. GSS-API proporciona aplicaciones que pueden incluir servicios de seguridad de la integridad y la privacidad, y también autenticación. Tanto `ftp` como `ssh` utilizan GSS-API.
- RPCSEC\_GSS Application Programming Interface (API): permite que los servicios NFS usen la autenticación Kerberos. RPCSEC\_GSS es un tipo de seguridad que proporciona servicios de seguridad que son independientes de los mecanismos que se utilizan. RPCSEC\_GSS se sitúa en la parte superior de la capa de GSS-API. Cualquier mecanismo de seguridad basado en GSS-API que sea conectable puede utilizarse mediante las aplicaciones que usan RPCSEC\_GSS.

Además, el servicio Oracle Solaris Kerberos incluye lo siguiente:

- Herramienta gráfica de administración de Kerberos (`gkadmin`): permite administrar los principales y las políticas de los principales. Esta interfaz gráfica de usuario basada en la tecnología Java es una alternativa al comando `kadmin`.
- Módulo de servicio Kerberos V5 para PAM: proporciona la autenticación y la gestión de cuentas, la gestión de sesiones y la gestión de contraseñas para el servicio Kerberos. Este módulo puede utilizarse para hacer que la autenticación Kerberos sea transparente para el usuario.
- Módulos del núcleo: proporcionan implementaciones del servicio Kerberos basadas en el núcleo para que las utilice el servicio NFS a fin de mejorar considerablemente el rendimiento.

## Adiciones de Kerberos para la versión Solaris 10 5/08

Estas mejoras se encuentran disponibles a partir de la versión Solaris 10 5/08:

- El software de Solaris Kerberos se ha sincronizado con la versión 1.4 del MIT. Específicamente, se actualizaron el software para el KDC, el comando `kinit` y el mecanismo de Kerberos.
- Se estableció la compatibilidad para acceder a registros de políticas y principales de Kerberos mediante LDAP desde un servidor de directorios. Este cambio simplifica la administración y puede proporcionar una mayor disponibilidad en función de la implementación de los KDC y los DS. Consulte [“Gestión de un KDC en un servidor de directorios LDAP” en la página 488](#) para obtener una lista de los procedimientos relacionados con LDAP.
- En esta versión, se agregó el soporte para los clientes de Solaris que no requieren configuración adicional. Se realizaron cambios en el servicio Kerberos y en algunos valores predeterminados. Los clientes de Solaris Kerberos trabajan sin configuración del lado del cliente en entornos que están adecuadamente configurados. Consulte [“Opciones de configuración de cliente” en la página 417](#) para obtener más información.

## Adiciones de Kerberos para la versión Solaris 10 8/07

La interfaz de programación de aplicaciones MIT Kerberos V5 (`krb5-api`) es compatible con la versión Solaris 10 8/07. Consulte las páginas del comando `man libkrb5(3LIB)` y `krb5-config(1)` para obtener más información. Además, consulte las páginas web del proyecto de MIT Kerberos V5 en [mit.edu](http://mit.edu) para obtener más documentación detallada a medida que esté disponible.

Aunque `krb5-api` ya se encuentra disponible, Sun promueve el uso de GSS-API para la autenticación de red y la integridad y la privacidad, ya que GSS-API es un mecanismo de seguridad independiente que es un estándar IETF. Consulte la página del comando `man libgss(3LIB)` para obtener más información.

## Adiciones de Kerberos para la versión Solaris 10 6/06

En la versión Solaris 10 6/06, el daemon `ktkt_warnd` puede renovar credenciales automáticamente, en lugar de sólo advertir al usuario cuando la credencial está a punto de caducar. El usuario debe haber iniciado sesión para que las credenciales se renueven automáticamente.

## Mejoras de Kerberos en la versión Solaris 10 3/05

Estas mejoras de Kerberos se incluyen en la versión Oracle Solaris. Varias de las mejoras se habían introducido en versiones anteriores de Software Express y actualizado en las versiones Solaris 10 Beta.

- Se proporciona compatibilidad con el protocolo Kerberos en aplicaciones remotas, como ftp, rcp, rlogin, rsh, ssh y telnet. Consulte las páginas del comando man para cada comando o daemon, y la página del comando man [krb5\\_auth\\_rules\(5\)](#) para obtener más información.
- La base de datos principal de Kerberos se puede transferir ahora mediante actualizaciones progresivas en lugar de transferir la base entera cada vez. La propagación progresiva ofrece la siguientes ventajas:
  - Mayor coherencia de la base de datos en todos los servidores
  - Menor necesidad de recursos (red, CPU, etcétera)
  - Propagación de las actualizaciones en un tiempo más reducido
  - Método de propagación automático
- Ahora se encuentra disponible una nueva secuencia de comandos para ayudar a configurar automáticamente un cliente Kerberos. La secuencia de comandos permite que un administrador pueda configurar de forma fácil y rápida un cliente Kerberos. Para conocer los procedimientos que utilizan la nueva secuencia de comandos, consulte [“Configuración de clientes Kerberos” en la página 452](#). Además, consulte la página del comando man [kclient\(1M\)](#) para obtener más información.
- Se han agregado varios tipos de cifrado al servicio Kerberos. Estos nuevos tipos de cifrado suponen un aumento de la seguridad y mejoran la compatibilidad con otras implementaciones Kerberos que admiten estos tipos de cifrado. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 579](#) para obtener más información. Entre los tipos de cifrado, se incluyen:
  - El tipo de cifrado AES puede utilizarse para establecer sesiones Kerberos con un cifrado de alta velocidad y con un nivel alto de seguridad.
  - ARCFOUR-HMAC proporciona una mejor compatibilidad con otras implementaciones de Kerberos.
  - Triple DES (3DES) con SHA1 aumenta la seguridad. Este tipo de cifrado también supone un beneficio para la interoperabilidad con otras implementaciones de Kerberos que admitan este tipo de cifrado.
- Los tipos de cifrado se habilitan mediante la estructura criptográfica. La estructura puede proporcionar criptografía acelerada por hardware para el servicio Kerberos.
- Ahora, el software KDC, los comandos de usuario y las aplicaciones de usuario admiten el uso del protocolo de red TCP. Esta mejora favorece la estabilidad del funcionamiento y la interoperabilidad con otras implementaciones de Kerberos, incluido Microsoft Active Directory. Ahora, KDC recibe los puertos UDP tradicionales y también los puertos TCP, de

manera que puede responder a las solicitudes con cualquiera de estos dos protocolos. Las aplicaciones y los comandos de usuario intentan primero enviar solicitudes a KDC con UDP y, si esto falla, intentan con TCP.

- Al software KDC se le ha agregado compatibilidad con IPv6, lo que incluye los comandos `kinit`, `klist` y `kprop`. La compatibilidad con las direcciones IPv6 se proporciona de manera predeterminada. No hay parámetros de configuración que deban cambiarse para habilitar la compatibilidad con IPv6. La compatibilidad con IPv6 no está disponible para los comandos `kadmin` y `kadminind`.
- Se ha incluido una nueva opción `-e` para varios subcomandos del comando `kadmin`. Esta nueva opción permite seleccionar el tipo de cifrado durante la creación de principales. Consulte la página del comando `man kadmin(1M)` para obtener más información.
- Se han realizado adiciones al módulo `pam_krb5` para gestionar la antememoria de credenciales de Kerberos con la estructura PAM. Consulte la página del comando `man pam_krb5(5)` para obtener más información.
- Se incorpora compatibilidad para la detección automática del KDC de Kerberos, el servidor de administración, el servidor `kpasswd` y las asignaciones de nombre de dominio para el dominio o el host mediante las búsquedas DNS. Esta mejora reduce la cantidad de pasos que son necesarios para instalar un cliente Kerberos. El cliente puede localizar un servidor KDC con DNS en lugar de tener que leer el archivo de configuración. Consulte la página del comando `man krb5.conf(4)` para obtener más información.
- Se ha incorporado un nuevo módulo PAM llamado `pam_krb5_migrate`. Este módulo ayuda a migrar usuarios de manera automática al dominio local de Kerberos en caso de que éstos no dispongan de cuentas de Kerberos. Consulte la página del comando `man pam_krb5_migrate(5)` para obtener más información.
- El archivo `~/k5login` se puede usar ahora con las aplicaciones GSS, ftp y ssh. Para obtener más información, consulte la página del comando `man gss_auth_rules(5)`.
- La utilidad `kproplog` se ha actualizado para mostrar todos los nombres de atributos por entrada de registro. Para obtener más información, consulte la página del comando `man kproplog(1M)`.
- La verificación TGT estricta puede deshabilitarse con una opción de configuración en el archivo `krb5.conf`. Consulte la página del comando `man krb5.conf(4)` para obtener más información.
- Las extensiones realizadas en las utilidades de cambio de contraseña permiten que el servidor de administración de Oracle Solaris Kerberos V5 acepte solicitudes de cambio de contraseña de los clientes que no ejecuten el software de Oracle Solaris. Consulte la página del comando `man kadmin(1M)` para obtener más información.
- La ubicación predeterminada de la antememoria de reproducción se ha cambiado de los sistemas de archivos basados en RAM al almacenamiento persistente en `/var/krb5/rcache/`. Esta nueva ubicación impide que se realicen reproducciones si se

rearranca un sistema. También se ha mejorado el rendimiento del código rcache. No obstante, el rendimiento general de la antememoria de reproducción puede ser algo inferior debido al uso del almacenamiento persistente.

- Ahora, la antememoria de reproducción se puede configurar para que use almacenamiento de archivo o de sólo memoria. Consulte la página del comando `man krb5envvar(5)` para obtener más información acerca de las variables de entorno que se pueden configurar para la tabla de claves y las ubicaciones y los tipos de antememoria de credenciales.
- La tabla de credenciales GSS ya no es necesaria para los mecanismos GSS de Kerberos. Para obtener más información, consulte “[Asignación de credenciales GSS a credenciales UNIX](#)” en la [página 416](#) o las páginas del comando `man gsscred(1M)`, `gssd(1M)` y `gsscred.conf(4)`.
- Las utilidades Kerberos, `kinit` y `ktutil`, se basan ahora en la versión 1.2.1 de MIT Kerberos. Este cambio ha supuesto la adición de nuevas opciones para el comando `kinit` y nuevos subcomandos para el comando `ktutil`. Para obtener más información, consulte las páginas del comando `man kinit(1)` y `ktutil(1)`.
- El Centro de distribución de claves (KDC) de Oracle Solaris Kerberos y `kadmind` se basa en la versión 1.2.1 de MIT Kerberos. El KDC toma como valor predeterminado una base de datos basada en `btree`, que es más confiable que la base de datos actual basada en `hash`. Para obtener más información, consulte la página del comando `man kdb5_util(1M)`.
- Los daemons `kpropd`, `kadmind`, `krb5kdc` y `ktkt_warnd` se gestionan con la utilidad de gestión de servicios. Las acciones administrativas de este servicio, como la habilitación, la deshabilitación o el reinicio, pueden llevarse a cabo con el comando `svcadm`. Utilice el comando `svcs` para consultar el estado del servicio de todos los daemons. Para ver una descripción general de la Utilidad de gestión de servicios, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*.

## Componentes de Kerberos en la versión Solaris 9

La versión Solaris 9 contiene todos los componentes incluidos en “[Componentes de Kerberos](#)” en la [página 402](#), salvo las aplicaciones remotas.

## Componentes SEAM 1.0.2

La versión SEAM 1.0.2 incluye las aplicaciones remotas. Estas aplicaciones son la única parte de SEAM 1.0 que no se ha incorporado en la versión Solaris 9. Los componentes de las aplicaciones remotas son los siguientes:

- Aplicaciones cliente: `ftp`, `rcp`, `rlogin`, `rsh` y `telnet`
- Daemons del servidor: `ftpd`, `rlogind`, `rshd` y `telnetd`

## Componentes de Kerberos en la versión Solaris 8

La versión Solaris 8 incluye solamente las partes del lado del cliente del servicio Kerberos, por lo que muchos componentes no se incluyen. Este producto permite que los sistemas en los que se ejecuta la versión Solaris 8 se conviertan en clientes Kerberos sin que tenga que instalar SEAM 1.0.1 por separado. Para utilizar estas capacidades, debe instalar un KDC que utilice Solaris Easy Access Server 3.0 o Solaris 8 Admin Pack, la distribución del MIT, o Windows 2000. Los componentes del lado del cliente no son útiles sin un KDC que esté configurado para distribuir tickets. En esta versión, se incluyen los siguientes componentes:

- Programas de usuario para obtener, visualizar y destruir tickets: `kinit`, `klist` y `kdestroy`.
- Programa de usuario para cambiar la contraseña de Kerberos: `kpasswd`.
- Utilidad de administración `keytab`: `ktutil`.
- Adiciones al módulo de autenticación conectable (PAM): permiten que las aplicaciones utilicen distintos mecanismos de autenticación. PAM puede utilizarse para hacer que los inicios y cierres de sesión sean transparentes para el usuario.
- Complementos de GSS-API: proporcionan compatibilidad de cifrado y protocolo Kerberos.
- Compatibilidad con el servidor y el cliente NFS.

## Componentes SEAM 1.0.1

La versión SEAM 1.0.1 incluye todos los componentes de la versión SEAM 1.0 que no están incluidos en la versión Solaris 8. Los componentes son los siguientes:

- Centro de distribución de claves (KDC) (maestro):
  - Daemon de administración de bases de datos de Kerberos: `kadmind`
  - Daemon de procesamiento de tickets de Kerberos: `krb5kdc`
- KDC esclavos.
- Programas de administración de bases de datos: `kadmin` y `kadmin.local`.
- Software de propagación de bases de datos: `kprop`.
- Aplicaciones remotas: `ftp`, `rcp`, `rlogin`, `rsh` y `telnet`.
- Daemons de aplicaciones remotas: `ftpd`, `rlogind`, `rshd` y `telnetd`.
- Utilidad de administración: `kdb5_util`.
- Herramienta gráfica de administración de Kerberos (`gkadmin`): permite administrar los principales y las políticas de los principales. Esta interfaz gráfica de usuario basada en la tecnología Java es una alternativa al comando `kadmin`.
- Un procedimiento de preconfiguración que permite establecer los parámetros para la instalación y la configuración de SEAM 1.0.1, lo que hace que la instalación de SEAM sea automática. Este procedimiento es especialmente útil para realizar varias instalaciones.
- Varias bibliotecas.



## Componentes SEAM 1.0

La versión SEAM 1.0 contiene todas las opciones que se incluyen en “[Componentes de Kerberos](#)” en la [página 402](#) y también las siguientes:

- Una utilidad (`gsscred`) y un daemon (`gssd`): estos programas ayudan a asignar los ID de usuarios (UID) de UNIX a los nombres de principales. Estos programas son necesarios porque los servidores NFS utilizan UID de UNIX para identificar a los usuarios y no los nombres de principales, que se almacenan en un formato distinto.
- Generic Security Service Application Programming Interface (GSS-API): permite que las aplicaciones utilicen varios mecanismos de seguridad sin solicitarle que vuelva a compilar la aplicación cada vez que se agrega un mecanismo nuevo. Dado que GSS-API es independiente del equipo, resulta conveniente para las aplicaciones de Internet. GSS-API proporciona aplicaciones que pueden incluir servicios de seguridad de la integridad y la privacidad, y también autenticación.
- RPCSEC\_GSS Application Programming Interface (API): permite que los servicios NFS usen la autenticación Kerberos. RPCSEC\_GSS es un tipo de seguridad que proporciona servicios de seguridad que son independientes de los mecanismos que se utilizan. RPCSEC\_GSS se sitúa en la parte superior de la capa de GSS-API. Cualquier mecanismo de seguridad basado en GSS-API que sea conectable puede utilizarse mediante las aplicaciones que usan RPCSEC\_GSS.
- Un procedimiento de preconfiguración: permite establecer los parámetros para la instalación y la configuración de SEAM 1.0, lo que hace que la instalación sea automática. Este procedimiento es especialmente útil para realizar varias instalaciones.



## Planificación del servicio Kerberos

---

Este capítulo debe ser estudiado por los administradores que participan en la instalación y el mantenimiento del servicio Kerberos. En el capítulo se explican diferentes opciones de instalación y configuración que los administradores deben determinar antes de instalar o configurar el servicio.

Esta es una lista de los temas que un administrador del sistema u otros profesionales de asistencia expertos deberían estudiar:

- “¿Por qué planificar implementaciones Kerberos?” en la página 411
- “Planificación de dominios Kerberos” en la página 412
- “Asignación de nombres de host en dominios” en la página 413
- “Nombres de principal de servicio y cliente” en la página 414
- “Puertos para KDC y servicios de administración” en la página 414
- “El número de KDC esclavos” en la página 415
- “Qué sistema de propagación de base de datos se debe utilizar” en la página 417
- “Sincronización de reloj dentro de un dominio” en la página 417
- “Opciones de configuración de cliente” en la página 417
- “Mejora de seguridad de inicio de sesión de cliente” en la página 418
- “Opciones de configuración de KDC” en la página 418
- “Tipos de cifrado Kerberos” en la página 419
- “URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 419

### ¿Por qué planificar implementaciones Kerberos?

Antes de instalar el servicio Kerberos, debe resolver varios problemas de configuración. Aunque el cambio de configuración después de la instalación inicial es posible, algunos cambios pueden ser difíciles de implementar. Además, algunos cambios necesitan que se reconstruya el KDC, por lo que es mejor considerar objetivos a largo plazo cuando planifique la configuración de Kerberos.

Desplegar una infraestructura Kerberos implica tareas como la instalación de KDC, la creación de claves para sus hosts y la migración de usuarios. Reconfigurar una implementación Kerberos puede ser tan complicado como realizar una implementación inicial, por lo tanto, planifique una implementación cuidadosamente para evitar tener que volver a configurarla.

## Planificación de dominios Kerberos

Un *dominio* es una red lógica, que define un grupo de sistemas que están bajo el mismo KDC maestro. Al igual que al establecer un nombre de dominio DNS, cuestiones como el nombre de dominio, el número y el tamaño de cada dominio, y la relación de un dominio con otros para autenticación entre dominios deberían resolverse antes de configurar el servicio Kerberos.

### Nombres de dominio

Los nombres de dominio pueden constar de cualquier cadena ASCII. Normalmente, el nombre de dominio es el mismo que el nombre de dominio DNS, excepto que el nombre de dominio está en mayúscula. Esta convención puede ayudar a diferenciar problemas con el servicio Kerberos de problemas con el espacio de nombres DNS al tiempo que se utiliza un nombre que es familiar. Si no utiliza DNS o decide utilizar una cadena diferente, puede utilizar cualquier cadena. Sin embargo, el proceso de configuración requiere más trabajo. Se aconseja el uso de nombres de dominio que siguen la estructura de nombres de Internet estándar.

### Número de dominios

El número de dominios que su instalación requiere depende de varios factores:

- El número de clientes que se deben admitir. Demasiados clientes en un dominio hacen que la administración sea más difícil y, finalmente, que sea necesario dividir el dominio. Los factores principales que determinan el número de clientes que se pueden admitir son los siguientes:
  - La cantidad de tráfico de Kerberos que cada cliente genera
  - El ancho de banda de la red física
  - La velocidad de los hosts

Debido a que cada instalación tendrá diferentes limitaciones, no existe ninguna regla para determinar el número máximo de clientes.

- Qué tan alejados están los clientes. La configuración de varios pequeños dominios podría tener sentido si los clientes están en diferentes regiones geográficas.
- El número de hosts disponibles para ser instalados como KDC. Cada dominio debe tener al menos dos servidores KDC, un servidor maestro y un servidor esclavo.

Se recomienda la alineación de dominios Kerberos con dominios administrativos. Tenga en cuenta que un dominio Kerberos V puede abarcar varios subdominios del dominio DNS al que corresponde el dominio.

## Jerarquía de dominios

Cuando configura varios dominios para autenticación entre dominios, debe decidir cómo relacionar los dominios. Puede establecer una relación jerárquica entre los dominios, que proporciona rutas automáticas a los dominios relacionados. Por supuesto, todos los dominios en la cadena jerárquica deben estar correctamente configurados. Las rutas automáticas pueden facilitar la carga de administración. Sin embargo, si hay muchos niveles de dominios, es posible que no desee utilizar la ruta predeterminada porque requiere demasiadas transacciones.

También puede decidir establecer la relación de confianza directamente. Una relación de confianza directa es más útil cuando existen demasiados niveles entre dos dominios jerárquicos o cuando no existe ninguna relación jerárquica. La conexión debe definirse en el archivo `/etc/krb5/krb5.conf` en todos los hosts que utilicen la conexión. Por lo tanto, se requiere trabajo adicional. La relación de confianza directa también se denomina como una relación transitiva. Para ver una introducción, consulte [“Dominios de Kerberos” en la página 399](#). Para conocer los procedimientos de configuración de varios dominios, consulte [“Configuración de autenticación entre dominios” en la página 441](#).

## Asignación de nombres de host en dominios

La asignación de nombres de host en los nombres de dominio se define en la sección `domain_realm` del archivo `krb5.conf`. Estas asignaciones se pueden definir para todo un dominio y para hosts individuales, según los requisitos.

DNS también se puede utilizar para buscar información sobre los KDC. El uso de DNS hace que sea más fácil cambiar la información porque no será necesario editar el archivo `krb5.conf` en todos los clientes cada vez que se realice un cambio. Consulte la página del comando `man krb5.conf(4)` para obtener más información.

A partir de las versiones Solaris Express Developer Edition 1/08 y Solaris 10 5/08, los clientes de Solaris Kerberos puedan interoperar mejor con servidores de Active Directory. Los servidores de Active Directory se pueden configurar para proporcionar el dominio para asignación de hosts.

## Nombres de principal de servicio y cliente

Cuando se utiliza el servicio Kerberos, DNS debe estar habilitado en todos los hosts. Con DNS, el principal debe contener el nombre de dominio completo (FQDN) de cada host. Por ejemplo, si el nombre de host es `boston`, el nombre de dominio DNS es `example.com` y el nombre de dominio es `EXAMPLE.COM`, entonces el nombre de principal para el host debe ser `host/boston.example.com@EXAMPLE.COM`. Los ejemplos de este manual requieren que DNS esté configurado y el uso de FQDN para cada host.

El servicio Kerberos pone en forma canónica nombres de alias de host a través de DNS y utiliza la forma canónica (cname) al construir el principal de servicio para el servicio asociado. Por lo tanto al crear un principal de servicio, el componente de nombre de host de nombres de principal de servicio debe ser la forma canónica del nombre de host del sistema donde se aloja el servicio.

A continuación, se muestra un ejemplo de cómo el servicio Kerberos pone en forma canónica el nombre de host. Si un usuario ejecuta el comando `"ssh alpha.example.com"` donde `alpha.example.com` es un alias de host DNS para el cname `beta.example.com`. Cuando `ssh` llama a Kerberos y solicita un ticket de servicio de host para `alpha.example.com`, el servicio Kerberos pone en forma canónica `alpha.example.com` a `beta.example.com` y solicita un ticket para el principal de servicio `"host/beta.example.com"` desde el KDC.

Para los nombres de principal que incluyen el FQDN de un host, es importante hacer coincidir la cadena que describe el nombre de dominio DNS en el archivo `/etc/resolv.conf`. El servicio Kerberos requiere que el nombre de dominio DNS esté en letras minúsculas cuando se especifica el FQDN para un principal. El nombre de dominio DNS puede incluir letras mayúsculas y minúsculas, pero sólo utilice letras minúsculas cuando cree un principal de host. Por ejemplo, no importa si el nombre de dominio DNS es `example.com`, `Example.COM` o cualquier otra variación. El nombre de principal para el host seguiría siendo `host/boston.example.com@EXAMPLE.COM`.

Además, la utilidad de gestión de servicios se ha configurado de modo que muchos de los daemons o comandos no se inicien si el servicio de cliente DNS no está en ejecución. Los daemons `kdb5_util`, `kadmind` y `kpropd`, como también el comando `kprop` están todos configurados según el servicio DNS. Para utilizar completamente las funciones disponibles mediante el servicio Kerberos y SMF, debe habilitar el servicio de cliente DNS en todos los hosts.

## Puertos para KDC y servicios de administración

De manera predeterminada, el puerto 88 y el puerto 750 se utilizan para el KDC, y el puerto 749 se utiliza para el daemon de administración KDC. Se pueden utilizar diferentes números de puerto. Sin embargo, si cambia los números de puerto, los archivos `/etc/services` y `/etc/krb5/krb5.conf` se deben cambiar en cada cliente. Además de estos archivos, se debe actualizar el archivo `/etc/krb5/kdc.conf` en cada KDC.

## El número de KDC esclavos

Los KDC esclavos generan credenciales para los clientes al igual que el KDC maestro. Los KDC esclavos proporcionan copia de seguridad si el maestro deja de estar disponible. Cada dominio debe tener al menos un KDC esclavo. Es posible que se requieran KDC esclavos adicionales según estos factores:

- El número de segmentos físicos en el dominio. Normalmente, la red debe configurarse para que cada segmento pueda funcionar, al menos mínimamente, sin el resto del dominio. Para ello, un KDC debe ser accesible desde cada segmento. El KDC en esta instancia puede ser maestro o esclavo.
- El número de clientes en el dominio. Mediante la adición de más servidores KDC, puede reducir la carga en los servidores actuales.

Es posible agregar demasiados KDC esclavos. Recuerde que la base de datos KDC se debe propagar para cada servidor, por lo tanto, cuantos más servidores KDC se instalen, mayor es el tiempo que se tarda en obtener los datos actualizados en el dominio. También, como cada esclavo retiene una copia de la base de datos KDC, una mayor cantidad de esclavos aumenta el riesgo de una infracción de seguridad.

Además, uno o más KDC esclavos pueden configurarse fácilmente para ser intercambiados con el KDC maestro. La ventaja de configurar al menos un KDC esclavo de este modo es que si el KDC maestro falla por cualquier motivo, tendrá un sistema preconfigurado que será fácil de intercambiar como KDC maestro. Para obtener instrucciones sobre cómo configurar un KDC esclavo intercambiable, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 468](#).

## Asignación de credenciales GSS a credenciales UNIX

El servicio Kerberos proporciona una asignación predeterminada de nombres de credenciales GSS a IDs de usuario UNIX (UIDs) para aplicaciones GSS que requieren esta asignación, por ejemplo NFS. Los nombres de credenciales GSS son equivalentes a los nombres de principal de Kerberos cuando se utiliza el servicio Kerberos. El algoritmo de asignación predeterminado es tomar un componente de nombre de principal de Kerberos y utilizar ese componente, que es el nombre principal del principal, para buscar el UID. La búsqueda se produce en el dominio predeterminado o en cualquier dominio permitido mediante el parámetro `auth_to_local_realm` en `/etc/krb5/krb5.conf`. Por ejemplo, el nombre de principal de usuario `bob@EXAMPLE.COM` se asigna al UID del usuario UNIX denominado `bob` con la tabla de contraseña. El nombre de principal de usuario `bob/admin@EXAMPLE.COM` no se puede asignar, porque el nombre de principal incluye un componente de la instancia de `admin`. Si las asignaciones predeterminadas para las credenciales de usuario son suficientes, no es necesario completar la tabla de credenciales GSS. En versiones anteriores, era necesario completar la tabla de credenciales GSS para que el servicio NFS funcionara. Si la asignación predeterminada no es suficiente, por ejemplo, si desea asignar un nombre de principal que contenga un componente de instancia, se deberían utilizar otros métodos. Para más información, consulte:

- [“Cómo crear una tabla de credenciales” en la página 448](#)
- [“Cómo agregar una única entrada a la tabla de credenciales” en la página 448](#)
- [“Cómo proporcionar asignación de credenciales entre dominios” en la página 449](#)
- [“Observación de asignación de credenciales GSS a credenciales UNIX” en la página 508](#)

## Migración de usuario automática a dominio Kerberos

Los usuarios UNIX que no tengan cuentas de usuario válidas en el dominio Kerberos predeterminado se pueden migrar automáticamente mediante la estructura PAM. Específicamente, el módulo `pam_krb5_migrate` se utilizaría en la pila de autenticación del servicio PAM. Los servicios se configurarían de manera que siempre que un usuario, que no tiene un principal de Kerberos, lleve a cabo un inicio de sesión correcto en un sistema utilizando su contraseña, un principal de Kerberos se crearía de manera automática para dicho usuario. La nueva contraseña de principal sería la misma que la contraseña de UNIX. Consulte [“Cómo configurar la migración automática de usuarios en un dominio Kerberos” en la página 464](#) para obtener instrucciones sobre cómo utilizar el módulo `pam_krb5_migrate`.



## Qué sistema de propagación de base de datos se debe utilizar

La base de datos que se almacena en el KDC maestro se debe propagar regularmente a los KDC esclavos. Puede configurar la propagación de la base de datos para que sea gradual. El proceso gradual propaga sólo información actualizada a los KDC esclavos, en lugar de a toda la base de datos. Para obtener más información sobre la propagación de base de datos, consulte [“Administración de la base de datos de Kerberos” en la página 473](#).

Si no utiliza propagación gradual, uno de los primeros problemas que debe resolver es la frecuencia de actualización de los KDC esclavos. La necesidad de contar con información actualizada disponible para todos los clientes se debe considerar con la cantidad de tiempo que se tarda en completar la actualización.

En las instalaciones de gran tamaño con muchos KDC en un dominio, uno o más esclavos pueden propagar los datos de forma que el proceso se realice en paralelo. Esta estrategia reduce la cantidad de tiempo que tarda la actualización, pero también aumenta el nivel de complejidad de administración del dominio. Para obtener una descripción completa de esta estrategia, consulte [“Configuración de propagación en paralelo” en la página 486](#).

## Sincronización de reloj dentro de un dominio

Todos los hosts que participan en el sistema de autenticación de Kerberos deben tener sus relojes internos sincronizados dentro un máximo de tiempo especificado. Conocida como *sesgo de reloj*, esta función proporciona otra comprobación de seguridad de Kerberos. Si el sesgo de reloj se excede entre cualquiera de los hosts participantes, las solicitudes se rechazan.

Una manera de sincronizar todos los relojes es utilizar el software de protocolo de hora de red (NTP). Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener más información. Otras maneras de sincronizar los relojes están disponibles, por lo tanto, el uso de NTP no es necesario. Sin embargo, alguna forma de sincronización se debe utilizar para evitar errores de acceso debido al sesgo de reloj.

## Opciones de configuración de cliente

Una nueva función en la versión Solaris 10 es la utilidad de configuración `kclient`. La utilidad se puede ejecutar en modo interactivo o modo no interactivo. En el modo interactivo, se le solicita al usuario valores de parámetros específicos de Kerberos, que permiten al usuario realizar cambios en la instalación existente al configurar el cliente. En el modo no interactivo, se utiliza un archivo con valores de parámetros previamente configurados. Además, las opciones de línea de comandos se pueden utilizar en el modo no interactivo. Ambos modos necesitan menos pasos que el proceso manual, lo que debería hacer que el proceso sea más rápido y menos propenso a errores.

En la versión Solaris 10 5/08, se han realizado cambios para permitir un cliente Kerberos de configuración cero. Si estas reglas se siguen en el entorno, entonces no es necesario un procedimiento de configuración explícito para un cliente Solaris Kerberos:

- DNS está configurado para devolver registros SRV para los KDC.
- El nombre de dominio coincide con el nombre de dominio DNS o KDC admite referencias.
- El cliente Kerberos no necesita una keytab.

En algunos casos, puede que sea mejor configurar explícitamente el cliente Kerberos:

- Si las referencias no se utilizan, la lógica de configuración cero depende del nombre de dominio DNS del host para determinar el dominio. Esto presenta un pequeño riesgo de seguridad, pero el riesgo es mucho menor que si se habilita `dns_lookup_realm`.
- El módulo `pam_krb5` se basa en una entrada de clave de host en la keytab. Es posible que este requisito esté deshabilitado en el archivo `krb5.conf`, sin embargo no se recomienda por razones de seguridad. Consulte la página del comando `man krb5.conf(4)`.
- El proceso de configuración cero es menos eficaz que la configuración directa y tiene una mayor dependencia de DNS. El proceso realiza más búsquedas de DNS que un cliente configurado directamente.

Consulte “[Configuración de clientes Kerberos](#)” en la [página 452](#) para obtener una descripción de todos los procesos de configuración de cliente.

## Mejora de seguridad de inicio de sesión de cliente

En la versión Solaris 10 11/06, en el inicio de sesión de un cliente, mediante el módulo `pam_krb5` se verifica que el KDC que emitió los últimos TGT sea el mismo KDC que emitió el principal de host de cliente que se almacena en `/etc/krb5/krb5.keytab`. El módulo `pam_krb5` verifica el KDC cuando el módulo está configurado en la pila de autenticación. Para algunas configuraciones, como los clientes DHCP que no almacenan un principal de host de cliente, esta verificación se debe deshabilitar. Para deshabilitar esta verificación, debe definir la opción `verify_ap_req_nofail` en el archivo `krb5.conf` como falso. Consulte “[Cómo deshabilitar la verificación del ticket de otorgamiento de tickets \(TGT\)](#)” en la [página 462](#) para obtener más información.

## Opciones de configuración de KDC

A partir de la versión Solaris 10 5/08 se ha admitido el uso de LDAP para gestionar los archivos de base de datos para Kerberos. Consulte “[Cómo configurar un KDC para utilizar un servidor de datos LDAP](#)” en la [página 429](#) para obtener instrucciones. El uso de LDAP simplifica la administración para sitios que requieren mejor coordinación entre las bases de datos Solaris Kerberos y la configuración DS existente.

## Tipos de cifrado Kerberos

Un *tipo de cifrado* es un identificador que especifica el algoritmo de cifrado, el modo de cifrado y los algoritmos hash que se usan en el servicio Kerberos. Las claves en el servicio Kerberos tienen un tipo de cifrado asociado para identificar el algoritmo criptográfico y el modo que se utilizará cuando el servicio realice operaciones criptográficas con la clave. Aquí se muestran los tipos de cifrado admitidos:

- des-cbc-md5
- des-cbc-crc
- des3-cbc-sha1-kd
- arcfour-hmac-md5
- arcfour-hmac-md5-exp
- aes128-cts-hmac-sha1-96
- aes256-cts-hmac-sha1-96

---

**Nota** – En las versiones anteriores a Solaris 10 8/07, el tipo de cifrado aes256-cts-hmac-sha1-96 puede utilizarse con el servicio Kerberos si los paquetes criptográficos complejos no desempaquetados están instalados.

---

Si desea cambiar el tipo de cifrado, debería hacerlo al crear una nueva base de datos de principal. Debido a la interacción entre el KDC, el servidor y el cliente, es difícil cambiar el tipo de cifrado en la base de datos existente. Deje estos parámetros sin configurar a menos que vuelva a crear la base de datos. Consulte “Uso de los tipos de cifrado de Kerberos” en la página 579 para obtener más información.

---

**Nota** – Si tiene un KDC maestro instalado que no ejecuta la versión Solaris 10, los KDC esclavos deben actualizarse a la versión Solaris 10 antes de actualizar el KDC maestro. Un KDC maestro Solaris 10 utilizará el nuevo tipo de cifrado, que un esclavo anterior no podrá manejar.

---

## URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos

La URL de ayuda en pantalla es utilizada por la herramienta gráfica de administración de Kerberos, `gkadmin`, por lo que la URL debe estar definida correctamente para habilitar el menú “Contenidos de ayuda” para trabajar. La versión HTML de este manual se puede instalar en cualquier servidor adecuado. También puede decidir si desea utilizar las colecciones en <http://www.oracle.com/technetwork/indexes/documentation/index.html>.

La URL se especifica en el archivo `krb5.conf` al configurar un host para utilizar el servicio Kerberos. La URL debe señalar la sección titulada “herramienta gráfica de administración de

Kerberos" en el capítulo "Administración de principales y políticas (tareas)" de este manual. Se puede seleccionar otra página HTML, si otra ubicación es más adecuada.

## Configuración del servicio Kerberos (tareas)

---

En este capítulo, se proporcionan procedimientos de configuración para servidores KDC, servidores de aplicaciones de red, servidores NFS y clientes Kerberos. Muchos de esos procedimientos necesitan acceso de superusuario, por lo que deben ser utilizados por administradores del sistema o usuarios avanzados. También se incluyen procedimientos de configuración entre dominios y otros temas relacionados con servidores KDC.

Se tratan los temas siguientes:

- “Configuración del servicio Kerberos (mapa de tareas)” en la página 421
- “Configuración de servidores KDC” en la página 423
- “Configuración de clientes Kerberos” en la página 452
- “Configuración de autenticación entre dominios” en la página 441
- “Configuración de servidores de aplicaciones de red de Kerberos” en la página 444
- “Configuración de servidores NFS con Kerberos” en la página 446
- “Sincronización de relojes entre clientes Kerberos y KDC” en la página 466
- “Intercambio de un KDC maestro y un KDC esclavo” en la página 468
- “Administración de la base de datos de Kerberos” en la página 473
- “Aumento de la seguridad en servidores Kerberos” en la página 490

## Configuración del servicio Kerberos (mapa de tareas)

Las partes del proceso de configuración dependen de otras partes y deben realizarse en un orden específico. Estos procedimientos, a menudo, establecen servicios que son necesarios para utilizar el servicio Kerberos. Otros procedimientos no dependen de ningún orden y pueden realizarse cuando corresponde. El siguiente mapa de tareas muestra un orden sugerido para una instalación de Kerberos.

Tarea	Descripción	Para obtener instrucciones
1. Planificar la instalación de Kerberos	Permite resolver problemas de configuración antes de iniciar el proceso de configuración de software. La planificación anticipada permite ahorrar tiempo y otros recursos a la larga.	<a href="#">Capítulo 22, “Planificación del servicio Kerberos”</a>
2. Instalar el NTP (opcional)	Configura el software de protocolo de hora de red (NTP) u otro protocolo de sincronización de relojes. Para que el servicio Kerberos funcione correctamente, los relojes de todos los sistemas en el dominio deben estar sincronizados.	<a href="#">“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466</a>
3. Configurar los servidores KDC	Configura y genera los servidores KDC maestros y los servidores KDC esclavos, y la base de datos KDC de un dominio.	<a href="#">“Configuración de servidores KDC” en la página 423</a>
4. Aumentar la seguridad en los servidores KDC (opcional)	Evita infracciones de seguridad en los servidores KDC.	<a href="#">“Cómo restringir el acceso a servidores KDC” en la página 490</a>
5. Configurar los servidores KDC intercambiables (opcional)	Facilita la tarea de intercambio del servidor KDC maestro y un servidor KDC esclavo.	<a href="#">“Cómo configurar un KDC esclavo intercambiable” en la página 468</a>

# Configuración de servicios Kerberos adicionales (mapa de tareas)

Una vez que se hayan completado los pasos necesarios, se podrán utilizar los procedimientos siguientes, cuando corresponda.

Tarea	Descripción	Para obtener instrucciones
Configurar la autenticación entre dominios	Permite comunicaciones de un dominio a otro dominio.	<a href="#">“Configuración de autenticación entre dominios” en la página 441</a>
Configurar los servidores de aplicaciones Kerberos	Permite que un servidor admita servicios, como ftp, telnet y rsh, utilizando la autenticación Kerberos.	<a href="#">“Configuración de servidores de aplicaciones de red de Kerberos” en la página 444</a>
Configurar los clientes Kerberos	Permite que un cliente utilice servicios Kerberos.	<a href="#">“Configuración de clientes Kerberos” en la página 452</a>
Configurar el servidor NFS con Kerberos	Permite que un servidor comparta un sistema de archivos que requiere la autenticación Kerberos.	<a href="#">“Configuración de servidores NFS con Kerberos” en la página 446</a>
Aumentar la seguridad en un servidor de aplicaciones	Aumenta la seguridad en un servidor de aplicaciones mediante la restricción del acceso a transacciones autenticadas solamente.	<a href="#">“Cómo habilitar sólo aplicaciones Kerberizadas” en la página 490</a>

## Configuración de servidores KDC

Después de instalar el software Kerberos, debe configurar los servidores KDC. La configuración de un servidor KDC maestro y de, al menos, un servidor KDC esclavo proporciona el servicio que emite credenciales. Estas credenciales son la base para el servicio Kerberos, por lo que los KDC se deben instalar antes de intentar otras tareas.

La diferencia más importante entre un KDC maestro y un KDC esclavo es que sólo el KDC maestro puede manejar solicitudes de administración de bases de datos. Por ejemplo, el cambio de una contraseña o la adición de un nuevo principal se deben realizar en el KDC maestro. Estos cambios, luego, se pueden propagar a los KDC esclavos. Tanto el KDC esclavo como el KDC maestro generan credenciales. Esta función proporciona redundancia en el caso de que el KDC maestro no pueda responder.

**TABLA 23-1** Configuración de servidores KDC (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Configurar un servidor KDC maestro	Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual, que se necesita para instalaciones más complejas.  Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual y un LDAP para el KDC.	<a href="#">“Cómo configurar manualmente un KDC maestro” en la página 423</a>  <a href="#">“Cómo configurar un KDC para utilizar un servidor de datos LDAP” en la página 429</a>
Configurar un servidor KDC esclavo	Configura y genera un servidor KDC esclavo para un dominio mediante un proceso manual, que se necesita para instalaciones más complejas.	<a href="#">“Cómo configurar manualmente un KDC esclavo” en la página 437</a>
Actualizar las claves del principal en un servidor KDC	Actualiza la clave de la sesión en un servidor KDC para utilizar nuevos tipos de cifrado.	<a href="#">“Cómo actualizar las claves del servicio de otorgamiento de tickets en un servidor maestro” en la página 440</a>

### ▼ Cómo configurar manualmente un KDC maestro

En este procedimiento, se configura la propagación incremental. Además, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- Principal admin = `kws/admin`
- URL de ayuda en pantalla =  
`http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

---

**Nota** – Ajuste la dirección URL para que enlace a la sección "Herramienta gráfica de administración de Kerberos", como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos”](#) en la página 419.

---

**Antes de empezar** Este procedimiento requiere que el host esté configurado para usar DNS. Para obtener instrucciones específicas de nomenclatura si este maestro se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo”](#) en la página 468.

**1 Conviértase en superusuario en el KDC maestro.**

**2 Edite el archivo de configuración de Kerberos (krb5.conf).**

Necesita cambiar los nombres de dominio y los nombres de los servidores. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM

#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
    kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
    }
```

En este ejemplo, se modificaron las líneas para las entradas `default_realm`, `kdc`, `admin_server` y `domain_realm`. Además, se editó la línea que define `help_url`.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_enctypes` o `default_tgs_enctypes`. Consulte [“Uso de los tipos de cifrado de Kerberos”](#) en la página 579 para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---



### 3 Edite el archivo de configuración de KDC (kdc.conf).

Necesita cambiar el nombre de dominio. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ologsize = 1000
    }
```

En este ejemplo, se modificó la definición del nombre de dominio en la sección `realms`. Además, en la sección `realms`, se agregaron líneas para permitir la propagación incremental y para seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `permitted_encetypes`, `supported_encetypes` o `master_key_type`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 579](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

### 4 Cree la base de datos KDC mediante el comando `kdb5_util`.

El comando `kdb5_util` crea la base de datos KDC. Además, cuando se utiliza con la opción `-s`, este comando crea un archivo intermedio que se utiliza para autenticar el KDC para él mismo antes de que los daemons `kadmind` y `krb5kdc` se inicien.

```
kdc1 # /usr/sbin/kdb5_util create -s
Initializing database '/var/krb5/principal' for realm 'EXAMPLE.COM'
master key name 'K/M@EXAMPLE.COM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:      <Type the key>
Re-enter KDC database master key to verify:  <Type it again>
```

### 5 Edite el archivo de la lista de control de acceso de Kerberos (kadm5.acl).

Una vez que se rellena, el archivo `/etc/krb5/kadm5.acl` debe contener todos los nombres de principales que tienen permitido administrar el KDC.

```
kws/admin@EXAMPLE.COM *
```

La entrada `da` al principal `kws/admin` en el dominio `EXAMPLE.COM` la capacidad de modificar los principales o las políticas en el KDC. La instalación predeterminada incluye un asterisco (\*) para que concuerde con todos los principales `admin`. Este valor predeterminado puede ser un

riesgo de seguridad, por lo que es más seguro incluir una lista de todos los principales admin. Consulte la página del comando `man kadm5.acl(4)` para obtener más información.

## 6 Inicie el comando `kadmin.local` y agregue principales.

Los próximos pasos secundarios crean los principales que son utilizados por el servicio Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

### a. Agregue principales de administración a la base de datos.

Puede agregar tantos principales admin como necesite. Debe agregar, al menos, un principal admin para completar el proceso de configuración del KDC. Para este ejemplo, se agrega un principal `kws/admin`. Puede sustituir un nombre de principal adecuado en lugar de “kws”.

```
kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM: <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

### b. Cree los principales `kiprop`.

El principal `kiprop` se utiliza para autorizar actualizaciones del KDC maestro.

```
kadmin.local: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin.local:
```

### c. Cree un archivo `keytab` para el servicio `kadmind`.

Esta secuencia de comandos crea un archivo `keytab` especial con entradas de principales para `kadmin/<FQDN>` y `changepw/<FQDN>`. Estos principales son necesarios para el servicio `kadmind` y para las contraseñas que se van a cambiar. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`. El principal `kadmin/changepw` se utiliza para cambiar contraseñas de clientes que no ejecutan una versión de Solaris.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
```

```

    with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:

```

#### d. Agregue el principal kiprop para el servidor KDC maestro al archivo keytab kadmind.

La adición del principal kiprop al archivo kadm5.keytab permite que el comando kadmind se autentique cuando se inicia la propagación incremental.

```

kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:

```

#### e. Salga de kadmin.local.

Ha agregado todos los principales necesarios para los pasos siguientes.

```
kadmin.local: quit
```

### 7 Inicie los daemons Kerberos.

```

kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin

```

## 8 Inicie `kadmin` y agregue más principales.

En este punto, puede agregar principales con la herramienta gráfica de administración de Kerberos. Para ello, debe iniciar sesión con uno de los nombres de principales `admin` creados anteriormente en este procedimiento. Sin embargo, el siguiente ejemplo de línea de comandos se muestra para que resulte más sencillo.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

### a. Cree el principal `host` del KDC maestro.

El principal `host` es utilizado por aplicaciones Kerberizadas, como `kprop`, para propagar los cambios a los KDC esclavos. Este principal también se utiliza para proporcionar acceso remoto seguro al servidor KDC mediante aplicaciones, como `ssh`. Tenga en cuenta que cuando la instancia de principal es un nombre de `host`, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

### b. (Opcional) Cree el principal `clnt`.

Este principal es utilizado por la utilidad `clnt` durante la instalación de un cliente Kerberos. Si no planea utilizar esta utilidad, no tiene que agregar el principal. Los usuarios de la utilidad `clnt` necesitan usar esta contraseña.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

### c. Agregue el principal `host` del KDC maestro al archivo `keytab` del KDC maestro.

La adición del principal `host` al archivo `keytab` permite que este principal sea utilizado por servidores de aplicaciones, como `sshd`, automáticamente.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**d. Salga de kadmin.**

```
kadmin: quit
```

**9 (Opcional) Sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener información sobre el NTP.

**10 Configure los KDC esclavos.**

Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 437](#) para obtener instrucciones específicas.

## ▼ **Cómo configurar un KDC para utilizar un servidor de datos LDAP**

A partir de la versión Solaris 10 5/08, se puede configurar un KDC para utilizar un servidor de datos LDAP mediante el procedimiento siguiente.

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdcl.example.com`
- Servidor de directorios = `dsserver.example.com`
- Principal admin = `kws/admin`
- FMRI para el servicio LDAP =  
`svc:/application/sun/ds:ds - var-opt - SUNWdsee-dsins1`
- URL de ayuda en pantalla =  
`http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956`

---

**Nota** – Ajuste la dirección URL para que enlace a la sección "Herramienta gráfica de administración de Kerberos", como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos” en la página 419](#).

---

**Antes de empezar**

Este procedimiento también requiere que el host esté configurado para usar DNS. Para obtener un mejor rendimiento, instale el KDC y el servicio de directorios LDAP en el mismo servidor.

Además, un servidor de directorios debe estar en ejecución. El procedimiento que se indica a continuación funciona con servidores que utilizan la versión Sun Java Directory Server Enterprise Edition.

**1 Conviértase en superusuario en el KDC.**

**2 Cree un certificado para el servidor de directorios e impórtelo.**

Siga los siguientes pasos para configurar un KDC S10 con el fin de utilizar el certificado autofirmado de Directory Server 6.1. Si el certificado ha caducado, siga las instrucciones para renovar un certificado en la sección “[To Manage Self-Signed Certificates](#)” de *Sun Java System Directory Server Enterprise Edition 6.2 Administration Guide*.

**a. Exporte el certificado autofirmado de Directory Server.**

```
# /usr/sfw/bin/certutil -L -n defaultCert -d /export/sun-ds6.1/directory/alias \
-P 'slapd-' -a > /var/tmp/ds_cert.pem
```

**b. Cree la base de datos de certificados local.**

```
# /usr/sfw/bin/certutil -N -d /var/ldap
```

**c. Agregue el certificado del servidor de directorios a la base de datos de certificados local.**

```
# /usr/sfw/bin/certutil -A -n defaultCert -i /var/tmp/ds_cert -a -t CT -d /var/ldap
```

**d. Importe el certificado de Directory Server.**

```
# pktool setpin keystore=nss dir=/var/ldap
# chmod a+r /var/ldap/*.db
# pktool import keystore=nss objtype=cert trust="CT" infile=/tmp/defaultCert.certutil.der \
label=defaultCert dir=/var/ldap
```

**3 Rellene el directorio LDAP si es necesario.**

**4 Agregue el esquema Kerberos al esquema existente.**

```
# ldapmodify -h dsserver.example.com -D "cn=directory manager" -f /usr/share/lib/ldif/kerberos.ldif
```

**5 Cree el contenedor Kerberos en el directorio LDAP.**

Agregue las entradas siguientes al archivo `krb5.conf`.

**a. Defina el tipo de base de datos.**

Agregue una entrada para definir `database_module` para la sección `realms`.

```
database_module = LDAP
```

**b. Defina el módulo de la base de datos.**

```
[dbmodules]
LDAP = {
    ldap_kerberos_container_dn = "cn=krbcontainer,dc=example,dc=com"
    db_library = kldap
```

```

ldap_kdc_dn = "cn=kdc service,ou=profile,dc=example,dc=com"
ldap_kadmin_dn = "cn=kadmin service,ou=profile,dc=example,dc=com"
ldap_cert_path = /var/ldap
ldap_servers = ldaps://dsserver.example.com
}

```

### c. Cree el KDC en el directorio LDAP.

Este comando crea krbcontainer y varios otros objetos. También crea un archivo intermedio de clave maestra /var/krb5/.k5.EXAMPLE.COM.

```
# kdb5_ldap_util -D "cn=directory manager" create -P abcd1234 -r EXAMPLE.COM -s
```

## 6 Guarde las contraseñas del nombre distintivo del vínculo (DN) del KDC.

Estas contraseñas son utilizadas por el KDC cuando se enlaza al DS. El KDC utiliza diferentes roles según el tipo de acceso que el KDC está utilizando.

```
# kdb5_ldap_util stashesrvpw "cn=kdc service,ou=profile,dc=example,dc=com"
# kdb5_ldap_util stashesrvpw "cn=kadmin service,ou=profile,dc=example,dc=com"
```

## 7 Agregue roles de servicio KDC.

### a. Cree un archivo kdc\_roles.ldif con contenido como el siguiente:

```

dn: cn=kdc service,ou=profile,dc=example,dc=com
cn: kdc service
sn: kdc service
objectclass: top
objectclass: person
userpassword: test123

dn: cn=kadmin service,ou=profile,dc=example,dc=com
cn: kadmin service
sn: kadmin service
objectclass: top
objectclass: person
userpassword: test123

```

### b. Cree las entradas de rol en el directorio LDAP.

```
# ldapmodify -a -h dsserver.example.com -D "cn=directory manager" -f kdc_roles.ldif
```

## 8 Defina las ACL para los roles relacionados con el KDC.

```

# cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
# Set kadmin ACL for everything under krbcontainer.
dn: cn=krbcontainer,dc=example,dc=com
changetype: modify
add: aci
aci: (target="ldap:///cn=krbcontainer,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
    acl kadmin ACL; allow (all)\
    userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com");)

# Set kadmin ACL for everything under the people subtree if there are
# mix-in entries for krb princis:
dn: ou=people,dc=example,dc=com
changetype: modify

```

```
add: aci
aci: (target="ldap:///ou=people,dc=example,dc=com")(targetattr="krb*")(version 3.0;\
acl kadmin ACL; allow (all)\
    userdn = "ldap:///cn=kadmin service,ou=profile,dc=example,dc=com";)
EOF
```

## 9 Edite el archivo de configuración de Kerberos (krb5.conf).

Necesita cambiar los nombres de dominio y los nombres de los servidores. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        admin_server = kdc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM
#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
    kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
    }
```

En este ejemplo, se modificaron las líneas para las entradas `default_realm`, `kdc`, `admin_server` y `domain_realm`. Además, se editó la línea que define `help_url`.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_enctypes` o `default_tgs_enctypes`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 579](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 10 Edite el archivo de configuración de KDC (kdc.conf).

Necesita cambiar el nombre de dominio. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
```



```

database_name = /var/krb5/principal
admin_keytab = /etc/krb5/kadm5.keytab
acl_file = /etc/krb5/kadm5.acl
kadmind_port = 749
max_life = 8h 0m 0s
max_renewable_life = 7d 0h 0m 0s
sunw_dbprop_enable = true
sunw_dbprop_master_uologsize = 1000
}

```

En este ejemplo, se modificó la definición del nombre de dominio en la sección `realms`. Además, en la sección `realms`, se agregaron líneas para permitir la propagación incremental y para seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro.

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `permitted_enctypes`, `supported_enctypes` o `master_key_type`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 579](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 11 Edite el archivo de la lista de control de acceso de Kerberos (`kadm5.acl`).

Una vez que se rellena, el archivo `/etc/krb5/kadm5.acl` debe contener todos los nombres de principales que tienen permitido administrar el KDC.

```
kws/admin@EXAMPLE.COM *
```

La entrada `da` al principal `kws/admin` en el dominio `EXAMPLE.COM` la capacidad de modificar los principales o las políticas en el KDC. La instalación predeterminada incluye un asterisco (\*) para que concuerde con todos los principales `admin`. Este valor predeterminado puede ser un riesgo de seguridad, por lo que es más seguro incluir una lista de todos los principales `admin`. Consulte la página del comando `man kadm5.acl(4)` para obtener más información.

## 12 Inicie el comando `kadmin.local` y agregue principales.

Los próximos pasos secundarios crean los principales que son utilizados por el servicio Kerberos.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local:
```

### a. Agregue principales de administración a la base de datos.

Puede agregar tantos principales `admin` como necesite. Debe agregar, al menos, un principal `admin` para completar el proceso de configuración del KDC. Para este ejemplo, se agrega un principal `kws/admin`. Puede sustituir un nombre de principal adecuado en lugar de “`kws`”.

```

kadmin.local: addprinc kws/admin
Enter password for principal kws/admin@EXAMPLE.COM: <Type the password>
Re-enter password for principal kws/admin@EXAMPLE.COM: <Type it again>
Principal "kws/admin@EXAMPLE.COM" created.
kadmin.local:
```

**b. Cree un archivo keytab para el servicio kadmind.**

Esta secuencia de comandos crea un archivo keytab especial con entradas de principales para kadmin y changepw. Estos principales son necesarios para el servicio kadmind. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolve.conf`.

```
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc1.example.com
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local:
```

**c. Salga de kadmin.local.**

Ha agregado todos los principales necesarios para los pasos siguientes.

```
kadmin.local: quit
```

### 13 (Opcional) Configure la dependencia LDAP para servicios Kerberos.

Si los servidores LDAP y KDC se están ejecutando en el mismo host y si el servicio LDAP está configurado con un FMRI de SMF, agregue una dependencia al servicio LDAP para los daemons Kerberos. Esto reiniciará el servicio KDC si el servicio LDAP se reinicia.

#### a. Agregue la dependencia al servicio krb5kdc.

```
# svccfg -s security/krb5kdc
svc:/network/security/krb5kdc> addpg dsins1 dependency
svc:/network/security/krb5kdc> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/krb5kdc> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/krb5kdc> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/krb5kdc> setprop dsins1/type = astring: "service"
svc:/network/security/krb5kdc> exit
```

#### b. Agregue la dependencia al servicio kadmin.

```
# svccfg -s security/kadmin
svc:/network/security/kadmin> addpg dsins1 dependency
svc:/network/security/kadmin> setprop dsins1/entities = \
    fmri: "svc:/application/sun/ds:ds--var-opt-SUNWdsee-dsins1"
svc:/network/security/kadmin> setprop dsins1/grouping = astring: "require_all"
svc:/network/security/kadmin> setprop dsins1/restart_on = astring: "restart"
svc:/network/security/kadmin> setprop dsins1/type = astring: "service"
svc:/network/security/kadmin> exit
```

### 14 Inicie los daemons Kerberos.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

### 15 Inicie kadmin y agregue más principales.

En este punto, puede agregar principales con la herramienta gráfica de administración de Kerberos. Para ello, debe iniciar sesión con uno de los nombres de principales admin creados anteriormente en este procedimiento. Sin embargo, el siguiente ejemplo de línea de comandos se muestra para que resulte más sencillo.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree el principal host del KDC maestro.

El principal host es utilizado por aplicaciones Kerberizadas, como klist y kprop. Los clientes utilizan este principal cuando montan un sistema de archivos NFS autenticado. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo /etc/resolv.conf.

```
kadmin: addprinc -randkey host/kdc1.example.com
Principal "host/kdc1.example.com@EXAMPLE.COM" created.
kadmin:
```

**b. (Opcional) Cree el principal `kcLient`.**

Este principal es utilizado por la utilidad `kcLient` durante la instalación de un cliente Kerberos. Si no planea utilizar esta utilidad, no tiene que agregar el principal. Los usuarios de la utilidad `kcLient` necesitan usar esta contraseña.

```
kadmin: addprinc clntconfig/admin
Enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type the password>
Re-enter password for principal clntconfig/admin@EXAMPLE.COM:  <Type it again>
Principal "clntconfig/admin@EXAMPLE.COM" created.
kadmin:
```

**c. Agregue el principal `host` del KDC maestro al archivo `keytab` del KDC maestro.**

La adición del principal `host` al archivo `keytab` permite que este principal se utilice automáticamente.

```
kadmin: ktadd host/kdc1.example.com
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**d. Salga de `kadmin`.**

```
kadmin: quit
```

**16 (Opcional) Sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener información sobre el NTP.

**17 Configure los KDC esclavos.**

Para proporcionar redundancia, asegúrese de instalar, al menos, un KDC esclavo. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 437](#) para obtener instrucciones específicas.

## ▼ Cómo configurar manualmente un KDC esclavo

En este procedimiento, se configura un nuevo KDC esclavo denominado `kdc2`. Además, se configura la propagación incremental. Este procedimiento utiliza los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- KDC maestro = `kdc1.example.com`
- KDC esclavo = `kdc2.example.com`
- Principal admin = `kws/admin`

### Antes de empezar

El KDC maestro debe estar configurado. Para obtener instrucciones específicas si este esclavo se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo” en la página 468](#).

#### 1 En el KDC maestro, conviértase en superusuario.

#### 2 En el KDC maestro, inicie `kadmin`.

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

##### a. En el KDC maestro, agregue principales host esclavos a la base de datos si aún no lo ha hecho.

Para que el esclavo funcione, debe tener un principal host. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc2.example.com
Principal "host/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

##### b. En el KDC maestro, cree el principal `kiprop`.

El principal `kiprop` se utiliza para autorizar la propagación incremental del KDC maestro.

```
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

##### c. Salga de `kadmin`.

```
kadmin: quit
```

**3 En el KDC maestro, edite el archivo de configuración de Kerberos (krb5.conf).**

Debe agregar una entrada para cada esclavo. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
.
.
[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
    }
```

**4 En el KDC maestro, agregue una entrada kprop a kadm5.acl.**

Esta entrada permite que el KDC maestro reciba solicitudes de propagación incremental para el servidor kdc2.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kprop/kdc2.example.com@EXAMPLE.COM p
```

**5 En el KDC maestro, reinicie kadmind para utilizar las nuevas entradas en el archivo kadm5.acl.**

```
kdc1 # svcadm restart network/security/kadmin
```

**6 En todos los KDC esclavos, copie los archivos de administración KDC del servidor KDC maestro.**

Este paso se debe realizar en todos los KDC esclavos, ya que el servidor KDC maestro ha actualizado información que cada servidor KDC necesita. Puede utilizar `ftp` o un mecanismo de transferencia similar para capturar copias de los siguientes archivos del KDC maestro:

- /etc/krb5/krb5.conf
- /etc/krb5/kdc.conf

**7 En todos los KDC esclavos, agregue una entrada para el KDC maestro y cada KDC esclavo en el archivo de configuración de propagación de bases de datos, kpropd.acl.**

Esta información se debe actualizar en todos los servidores KDC esclavos.

```
kdc2 # cat /etc/krb5/kpropd.acl
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
```

**8 En todos los KDC esclavos, asegúrese de que el archivo de la lista de control de acceso de Kerberos, kadm5.acl, no esté relleno.**

Un archivo `kadm5.acl` sin modificaciones sería de la siguiente manera:

```
kdc2 # cat /etc/krb5/kadm5.acl
*/admin@___default_realm___ *
```

Si el archivo tiene entradas `kprop`, elimínelas.

## 9 En el nuevo esclavo, cambie una entrada en `kdc.conf`.

Reemplace la entrada `sunw_dbprop_master_ologsize` por una entrada que defina `sunw_dbprop_slave_poll`. La entrada establece el tiempo de sondeo en 2 min.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_slave_poll = 2m
    }
```

## 10 En el nuevo esclavo, inicie el comando `kadmin`.

Debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

### a. Agregue el principal `host` del esclavo al archivo `keytab` del esclavo mediante `kadmin`.

Esta entrada permite que `kprop` y otras aplicaciones Kerberizadas funcionen. Tenga en cuenta que cuando la instancia de principal es un nombre de `host`, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: ktadd host/kdc2.example.com
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### b. Agregue el principal `kiprop` al archivo `keytab` del KDC esclavo.

La adición del principal `kiprop` al archivo `krb5.keytab` permite que el comando `kpropd` se autentique cuando se inicia la propagación incremental.

```
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
```

```
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
  with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
  mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
  with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
  with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### c. Salga de kadmin.

```
kadmin: quit
```

## 11 En el nuevo esclavo, inicie el daemon de propagación de Kerberos.

```
kdc2 # /usr/lib/krb5/kpropd
```

## 12 En el nuevo esclavo, cree un archivo intermedio con kdb5\_util.

```
kdc2 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key:      <Type the key>
```

## 13 Elimine el daemon de propagación de Kerberos.

```
kdc2 # pkill kpropd
```

## 14 (Opcional) En el nuevo KDC esclavo, sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección `libdefaults` del archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener información sobre el NTP.

## 15 En el nuevo esclavo, inicie el daemon del KDC (krb5kdc).

Cuando el servicio `krb5kdc` está habilitado, `kpropd` también se inicia si el sistema está configurado como esclavo.

```
kdc2 # svcadm enable network/security/krb5kdc
```

## ▼ Cómo actualizar las claves del servicio de otorgamiento de tickets en un servidor maestro

Cuando el principal Servicio de otorgamiento de tickets (TGS) sólo tiene una clave DES, que es el caso de los servidores KDC creados antes de la versión Solaris 10, la clave restringe el tipo de cifrado de la clave de la sesión Ticket de otorgamiento de tickets (TGT) a DES. Si un KDC se actualiza a una versión que admite otros tipos de cifrado más seguros, el administrador puede



esperar que un cifrado más seguro se utilice para todas las claves de sesión generadas por el KDC. Sin embargo, si al principal TGS existente no se le actualizan las claves para incluir los nuevos tipos de cifrado, la clave de la sesión TGT seguirá estando limitada a DES. El siguiente procedimiento actualiza la clave para que se puedan utilizar tipos de cifrado adicionales.

- **Actualice la clave del principal del servicio TGS.**

```
kdc1 % /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

### Ejemplo 23-1 Actualización de claves de principales de un servidor maestro

Si ha iniciado sesión en el KDC maestro como root, puede actualizar el principal del servicio TGS con el siguiente comando:

```
kdc1 # kadmin.local -q 'cpw -randkey krbtgt/EXAMPLE.COM@EXAMPLE.COM'
```

## Configuración de autenticación entre dominios

Existen varias maneras de enlazar dominios para que los usuarios de un dominio se puedan autenticar en otro dominio. La autenticación entre dominios se lleva a cabo mediante el establecimiento de una clave secreta que se comparte entre dos dominios. La relación de los dominios puede ser jerárquica o direccional (consulte [“Jerarquía de dominios” en la página 413](#)).

### ▼ Cómo establecer la autenticación entre dominios jerárquica

El ejemplo de este procedimiento utiliza dos dominios, ENG.EAST.EXAMPLE.COM y EAST.EXAMPLE.COM. La autenticación entre dominios se establecerá en ambas direcciones. Este procedimiento debe realizarse en el KDC maestro de ambos dominios.

**Antes de empezar** El KDC maestro para cada dominio debe estar configurado. Para probar completamente el proceso de autenticación, varios clientes Kerberos deben estar configurados.

- 1 **Conviértase en superusuario en el primer KDC maestro.**
- 2 **Cree principales de servicio de ticket de otorgamiento de tickets para los dos dominios.**  
Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
# /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
```

```
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM
Enter password for principal krgtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM: <Type password>
kadmin: addprinc krbtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal krgtgt/EAST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: <Type password>
kadmin: quit
```

---

**Nota** – La contraseña que se ha especificado para cada principal de servicio debe ser idéntica en ambos KDC. Por lo tanto, la contraseña para el principal de servicio `krbtgt/ENG.EAST.EXAMPLE.COM@EAST.EXAMPLE.COM` debe ser la misma en ambos dominios.

---

**3 Agregue entradas al archivo de configuración de Kerberos (`krb5.conf`) para definir nombres de dominio para cada dominio.**

```
# cat /etc/krb5/krb5.conf
[libdefaults]
.
.
[domain_realm]
    .eng.east.example.com = ENG.EAST.EXAMPLE.COM
    .east.example.com = EAST.EXAMPLE.COM
```

En este ejemplo, se definen nombres de dominio para los dominios `ENG.EAST.EXAMPLE.COM` y `EAST.EXAMPLE.COM`. Es importante incluir el subdominio en primer lugar, puesto que el archivo se busca de arriba abajo.

**4 Copie el archivo de configuración de Kerberos en todos los clientes de este dominio.**

Para que la autenticación entre dominios funcione, todos los sistemas (incluidos los KDC esclavos y otros servidores) deben tener instalada la nueva versión del archivo de configuración de Kerberos (`/etc/krb5/krb5.conf`).

**5 Repita todos estos pasos en el segundo dominio.**

## ▼ **Cómo establecer la autenticación entre dominios directa**

El ejemplo de este procedimiento utiliza dos dominios, `ENG.EAST.EXAMPLE.COM` y `SALES.WEST.EXAMPLE.COM`. La autenticación entre dominios se establecerá en ambas direcciones. Este procedimiento debe realizarse en el KDC maestro de ambos dominios.

**Antes de empezar** El KDC maestro para cada dominio debe estar configurado. Para probar completamente el proceso de autenticación, varios clientes Kerberos deben estar configurados.

**1 Conviértase en superusuario en uno de los servidores KDC maestros.**

## 2 Cree principales de servicio de ticket de otorgamiento de tickets para los dos dominios.

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
# /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM
Enter password for principal
krtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM: <Type the password>
kadmin: addprinc krbtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM
Enter password for principal
krtgt/SALES.WEST.EXAMPLE.COM@ENG.EAST.EXAMPLE.COM: <Type the password>
kadmin: quit
```

---

**Nota** – La contraseña que se ha especificado para cada principal de servicio debe ser idéntica en ambos KDC. Por lo tanto, la contraseña para el principal de servicio `krbtgt/ENG.EAST.EXAMPLE.COM@SALES.WEST.EXAMPLE.COM` debe ser la misma en ambos dominios.

---

## 3 Agregue entradas en el archivo de configuración de Kerberos para definir la ruta directa al dominio remoto.

En este ejemplo, se muestran los clientes en el dominio `ENG.EAST.EXAMPLE.COM`. Debe intercambiar los nombres de dominio para obtener las definiciones adecuadas en el dominio `SALES.WEST.EXAMPLE.COM`.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
.
.
.
[capaths]
ENG.EAST.EXAMPLE.COM = {
    SALES.WEST.EXAMPLE.COM = .
}

SALES.WEST.EXAMPLE.COM = {
    ENG.EAST.EXAMPLE.COM = .
}
```

## 4 Copie el archivo de configuración de Kerberos en todos los clientes del dominio actual.

Para que la autenticación entre dominios funcione, todos los sistemas (incluidos los KDC esclavos y otros servidores) deben tener instalada la nueva versión del archivo de configuración de Kerberos (`/etc/krb5/krb5.conf`).

## 5 Repita todos estos pasos para el segundo dominio.

# Configuración de servidores de aplicaciones de red de Kerberos

Los servidores de aplicaciones de red son hosts que proporcionan acceso mediante una o más de las siguientes aplicaciones de red: ftp, rcp, rlogin, rsh, ssh y telnet. Sólo se requieren unos pocos pasos para habilitar la versión de Kerberos de estos comandos en un servidor.

## ▼ Cómo configurar un servidor de aplicaciones de red de Kerberos

Este procedimiento utiliza los siguientes parámetros de configuración:

- Servidor de aplicaciones = boston
- Principal admin = kws/admin
- Nombre de dominio DNS = example.com
- Nombre de dominio = EXAMPLE.COM

### Antes de empezar

Este procedimiento requiere que el KDC maestro se haya configurado. Para probar completamente el proceso, varios clientes Kerberos deben estar configurados.

#### 1 (Opcional) Instale el cliente NTP u otro mecanismo de sincronización de relojes.

Consulte [“Sincronización de relojes entre clientes Kerberos y KDC”](#) en la página 466 para obtener información sobre el NTP.

#### 2 Agregue principales para el nuevo servidor y actualice el archivo keytab del servidor.

El siguiente comando informa la existencia del principal host:

```
boston # klist -k |grep host
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
4 host/boston.example.com@EXAMPLE.COM
```

Si el comando no devuelve un principal, cree nuevos principales mediante los siguientes pasos.

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos”](#) en la página 520. El ejemplo de los siguientes pasos muestra cómo agregar los principales

necesarios mediante la línea de comandos. Debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.

```
boston # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

#### a. Cree el principal host del servidor.

El principal host se utiliza:

- Para autenticar el tráfico al utilizar los comandos remotos, como `rsh` y `ssh`.
- Por `pam_krb5` para evitar ataques de falsificación de KDC mediante el principal host a fin de verificar que la credencial de Kerberos de un usuario se haya obtenido de un KDC de confianza.
- Para permitir que el usuario `root` adquiera automáticamente una credencial de Kerberos sin necesidad de que exista un principal `root`. Esto puede ser útil al realizar un montaje de NFS manual donde el recurso compartido requiere una credencial de Kerberos.

Este principal es necesario si el tráfico que utiliza la aplicación remota se va a autenticar mediante el servicio Kerberos. Si el servidor tiene varios nombres de host asociados con él, cree un principal para cada nombre de host utilizando el formato de FQDN del nombre de host.

```
kadmin: addprinc -randkey host/boston.example.com
Principal "host/boston.example.com" created.
kadmin:
```

#### b. Agregue el principal host del servidor al archivo `keytab` del servidor.

Si el comando `kadmin` no se está ejecutando, reinicielo con un comando similar al siguiente:  
`/usr/sbin/kadmin -p kws/admin`.

Si el servidor tiene varios nombres de host asociados con él, agregue un principal al archivo `keytab` para cada nombre de host.

```
kadmin: ktadd host/boston.example.com
Entry for principal host/boston.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/boston.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### c. Salga de `kadmin`.

```
kadmin: quit
```

# Configuración de servidores NFS con Kerberos

Los servicios NFS utilizan ID de usuario (UID) de UNIX para identificar a un usuario y no pueden utilizar directamente credenciales GSS. Para traducir la credencial a un UID, es posible que se deba crear una tabla de credenciales que asigne credenciales de usuario a UID de UNIX. Consulte [“Asignación de credenciales GSS a credenciales UNIX” en la página 416](#) para obtener más información sobre la asignación predeterminada de credenciales. Los procedimientos de esta sección se centran en las tareas que se necesitan para configurar un servidor NFS con Kerberos, administrar la tabla de credenciales e iniciar los modos de seguridad de Kerberos para sistemas de archivos montados en NFS. En el siguiente mapa de tareas, se describen las tareas que se tratan en esta sección.

TABLA 23–2 Configuración de servidores NFS con Kerberos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Configurar un servidor NFS con Kerberos	Permite que un servidor comparta un sistema de archivos que requiere la autenticación Kerberos.	<a href="#">“Cómo configurar servidores NFS con Kerberos” en la página 446</a>
Crear una tabla de credenciales	Genera una tabla de credenciales que se puede utilizar para proporcionar asignación de credenciales GSS a ID de usuario de UNIX si la asignación predeterminada no es suficiente.	<a href="#">“Cómo crear una tabla de credenciales” en la página 448</a>
Cambiar la tabla de credenciales que asigna credenciales de usuario a UID de UNIX	Actualiza la información en la tabla de credenciales.	<a href="#">“Cómo agregar una única entrada a la tabla de credenciales” en la página 448</a>
Crear asignaciones de credenciales entre dos dominios similares	Proporciona instrucciones sobre cómo asignar UID de un dominio a otro si los dominios comparten un archivo de contraseña.	<a href="#">“Cómo proporcionar asignación de credenciales entre dominios” en la página 449</a>
Compartir un sistema de archivos con autenticación Kerberos	Comparte un sistema de archivos con modos de seguridad, de manera que la autenticación Kerberos es necesaria.	<a href="#">“Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos” en la página 450</a>

## ▼ Cómo configurar servidores NFS con Kerberos

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- Nombre de dominio DNS = `example.com`
- Servidor NFS = `denver.example.com`
- Principal admin = `kws/admin`

### 1 Complete los requisitos para configurar un servidor NFS con Kerberos.

El KDC maestro debe estar configurado. Para probar completamente el proceso, necesita varios clientes.

## 2 (Opcional) Instale el cliente NTP u otro mecanismo de sincronización de relojes.

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar sincronizado con la hora en el servidor KDC dentro de una diferencia máxima definida por la relación `clockskew` en el archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener información sobre el NTP.

## 3 Configure el servidor NFS como un cliente Kerberos.

Siga las instrucciones en [“Configuración de clientes Kerberos” en la página 452](#).

## 4 Inicie `kadmin`.

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos” en la página 520](#). Para ello, debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

### a. Cree el principal de servicio NFS del servidor.

Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

Repita este paso para cada interfaz única en el sistema que pueda ser utilizada para acceder a datos de NFS. Si un host tiene varias interfaces con nombres únicos, cada nombre único debe tener su propio principal de servicio NFS.

```
kadmin: addprinc -randkey nfs/denver.example.com
Principal "nfs/denver.example.com" created.
kadmin:
```

### b. Agregue el principal de servicio NFS del servidor al archivo keytab del servidor.

Repita este paso para cada principal de servicio único creado en el [Paso a](#).

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

**c. Salga de kadmin.**

kadmin: **quit**

**5 (Opcional) Cree asignaciones de credenciales GSS especiales si es necesario.**

Normalmente, el servicio Kerberos genera asignaciones adecuadas entre las credenciales GSS y los UID de UNIX. La asignación predeterminada se describe en [“Asignación de credenciales GSS a credenciales UNIX” en la página 416](#). Si la asignación predeterminada no es suficiente, consulte [“Cómo crear una tabla de credenciales” en la página 448](#) para obtener más información.

**6 Comparta el sistema de archivos NFS con modos de seguridad de Kerberos.**

Consulte [“Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos” en la página 450](#) para obtener más información.

## ▼ **Cómo crear una tabla de credenciales**

La tabla de credenciales `gsscred` es utilizada por un servidor NFS para asignar credenciales Kerberos a un UID. De manera predeterminada, la parte principal del nombre del principal se compara con un nombre de inicio de sesión de UNIX. Para que los clientes NFS monten sistemas de archivos de un servidor NFS con autenticación Kerberos, esta tabla se debe crear si la asignación predeterminada no es suficiente.

**1 Edite `/etc/gss/gsscred.conf` y cambie el mecanismo de seguridad.**

Cambie el mecanismo a `files`.

**2 Cree la tabla de credenciales mediante el comando `gsscred`.**

```
# gsscred -m kerberos_v5 -a
```

El comando `gsscred` recopila información de todos los orígenes que se muestran con la entrada `passwd` en el archivo `/etc/nsswitch.conf`. Es posible que necesite eliminar temporalmente la entrada `files` si no desea las entradas de contraseñas locales incluidas en la tabla de credenciales. Consulte la página del comando `man gsscred(1M)` para obtener más información.

## ▼ **Cómo agregar una única entrada a la tabla de credenciales**

**Antes de empezar**

Este procedimiento requiere que la tabla `gsscred` ya se haya creado en el servidor NFS. Consulte [“Cómo crear una tabla de credenciales” en la página 448](#) para obtener instrucciones.

**1 Conviértase en superusuario en el servidor NFS.**



**2 Agregue una entrada a la tabla de credenciales mediante el comando `gsscred`.**

```
# gsscred -m mech [ -n name [ -u uid ] ] -a
```

*mec* Define el mecanismo de seguridad que se va a utilizar.

*nombre* Define el nombre de principal para el usuario, como se define en el KDC.

*uid* Define el UID para el usuario, como se define en la base de datos de contraseñas.

*-a* Agrega el UID a la asignación del nombre de principal.

**Ejemplo 23-2 Adición de un principal de componente múltiple a la tabla de credenciales**

En el siguiente ejemplo, se agrega una entrada para un principal denominado `sandy/admin`, que está asignado al UID 3736.

```
# gsscred -m kerberos_v5 -n sandy/admin -u 3736 -a
```

**Ejemplo 23-3 Adición de un principal de un dominio diferente en la tabla de credenciales**

En el siguiente ejemplo, se agrega una entrada para un principal denominado `sandy/admin@EXAMPLE.COM`, que está asignado al UID 3736.

```
# gsscred -m kerberos_v5 -n sandy/admin@EXAMPLE.COM -u 3736 -a
```

## ▼ Cómo proporcionar asignación de credenciales entre dominios

Este procedimiento proporciona una asignación de credenciales apropiada entre dominios que utilizan el mismo archivo de contraseña. En este ejemplo, los dominios `CORP.EXAMPLE.COM` y `SALES.EXAMPLE.COM` utilizan el mismo archivo de contraseña. Las credenciales para `bob@CORP.EXAMPLE.COM` y `bob@SALES.EXAMPLE.COM` están asignadas al mismo UID.

**1 Conviértase en superusuario.****2 En el sistema cliente, agregue entradas al archivo `krb5.conf`.**

```
# cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = CORP.EXAMPLE.COM

[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

**Ejemplo 23-4** Asignación de credenciales entre dominios mediante el mismo archivo de contraseña

Este ejemplo proporciona una asignación de credenciales apropiada entre dominios que utilizan el mismo archivo de contraseña. En este ejemplo, los dominios CORP.EXAMPLE.COM y SALES.EXAMPLE.COM utilizan el mismo archivo de contraseña. Las credenciales para bob@CORP.EXAMPLE.COM y bob@SALES.EXAMPLE.COM están asignadas al mismo UID. En el sistema cliente, agregue entradas al archivo krb5.conf.

```
# cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = CORP.EXAMPLE.COM
.
[realms]
    CORP.EXAMPLE.COM = {
        .
        auth_to_local_realm = SALES.EXAMPLE.COM
        .
    }
```

**Errores más  
frecuentes**

Consulte “[Observación de asignación de credenciales GSS a credenciales UNIX](#)” en la [página 508](#) para obtener ayuda con el proceso de resolución de problemas de asignación de credenciales.

## ▼ Cómo configurar un entorno NFS seguro con varios modos de seguridad de Kerberos

Este procedimiento permite que un servidor NFS proporcione acceso seguro al NFS mediante diferentes tipos o modos de seguridad. Cuando un cliente negocia un tipo de seguridad con el servidor NFS, se utiliza el primer tipo ofrecido por el servidor al cual el cliente tiene acceso. Este tipo se utiliza para todas las solicitudes de cliente posteriores del sistema de archivos compartidas por el servidor NFS.

- 1 **Conviértase en superusuario en el servidor NFS.**
- 2 **Verifique que exista un principal de servicio NFS en el archivo keytab.**

El comando `klist` informa si hay un archivo keytab y muestra los principales. Si los resultados muestran que no existe ningún archivo keytab o que no existe ningún principal de servicio NFS, debe verificar que se hayan completado todos los pasos en “[Cómo configurar servidores NFS con Kerberos](#)” en la [página 446](#).

```
# klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
-----
3 nfs/denver.example.com@EXAMPLE.COM
```

```
3 nfs/denver.example.com@EXAMPLE.COM
3 nfs/denver.example.com@EXAMPLE.COM
3 nfs/denver.example.com@EXAMPLE.COM
```

### 3 Habilite los modos de seguridad de Kerberos en el archivo `/etc/nfssec.conf`.

Edite el archivo `/etc/nfssec.conf` y elimine el símbolo “#” que se encuentra delante de los modos de seguridad de Kerberos.

```
# cat /etc/nfssec.conf
.
.
#
# Uncomment the following lines to use Kerberos V5 with NFS
#
krb5          390003  kerberos_v5    default -          # RPCSEC_GSS
krb5i         390004  kerberos_v5    default integrity # RPCSEC_GSS
krb5p         390005  kerberos_v5    default privacy   # RPCSEC_GSS
```

### 4 Edite el archivo `/etc/dfs/dfstab` y agregue la opción `sec=` con los modos de seguridad necesarios a las entradas adecuadas.

```
share -F nfs -o sec=mode file-system
```

*modo* Especifica los modos de seguridad que se utilizarán al compartir el sistema de archivos. Cuando se utilizan varios modos de seguridad, el primero en la lista se utiliza de manera predeterminada.

*sistema\_archivos* Define la ruta al sistema de archivos que se va a compartir.

Todos los clientes que intentan acceder a los archivos desde el sistema de archivos especificado requieren autenticación Kerberos. Para acceder a los archivos, el principal de usuario en el cliente NFS debe autenticarse.

### 5 Asegúrese de que el servicio NFS se esté ejecutando en el servidor.

Si este comando es el primer comando `share` o conjunto de comandos `share` que ha iniciado, es posible que los daemons NFS no se estén ejecutando. El siguiente comando reinicia los daemons:

```
# svcadm restart network/nfs/server
```

### 6 (Opcional) Si el montador automático se está utilizando, edite la base de datos `auto_master` para seleccionar un modo de seguridad distinto del predeterminado.

No es necesario que siga este procedimiento si no está utilizando el montador automático para acceder al sistema de archivos o si la selección predeterminada para el modo de seguridad es aceptable.

```
file-system auto_home -nosuid,sec=mode
```

- 7 (Opcional) Emita manualmente el comando `mount` para acceder al sistema de archivos mediante un modo que no esté predeterminado.

Como alternativa, puede utilizar el comando `mount` para especificar el modo de seguridad, pero esta alternativa no aprovecha el montador automático.

```
# mount -F nfs -o sec=mode file-system
```

#### Ejemplo 23-5 Uso compartido de un sistema de archivos con un modo de seguridad de Kerberos

En este ejemplo, la línea de archivo `dfstab` significa que la autenticación Kerberos debe completarse correctamente para poder acceder a los archivos mediante el servicio NFS.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5 /export/home
```

#### Ejemplo 23-6 Uso compartido de un sistema de archivos con varios modos de seguridad de Kerberos

En este ejemplo, los tres modos de seguridad de Kerberos se han seleccionado. El modo que se utiliza se negocia entre el cliente y el servidor NFS. Si falla el primer modo en el comando, se intenta con el siguiente. Consulte la página del comando `man nfssec(5)` para obtener más información.

```
# grep krb /etc/dfs/dfstab
share -F nfs -o sec=krb5:krb5i:krb5p /export/home
```

## Configuración de clientes Kerberos

Los clientes Kerberos incluyen cualquier host, que no es un servidor KDC, en la red que necesita utilizar servicios Kerberos. Esta sección proporciona procedimientos para instalar un cliente Kerberos, así como información específica sobre el uso de la autenticación de `root` para montar sistemas de archivos NFS.

## Configuración de clientes Kerberos (mapa de tareas)

El siguiente mapa de tareas incluye todos los procedimientos asociados con la configuración de clientes Kerberos. Cada fila incluye un identificador de tarea y una descripción del motivo por el que desea realizar la tarea, seguidos de un enlace a la tarea.

Tarea	Descripción	Para obtener instrucciones
Establecer un perfil de instalación de cliente Kerberos	Genera un perfil de instalación de cliente que se puede utilizar para instalar automáticamente un cliente Kerberos.	<a href="#">“Cómo crear un perfil de instalación de cliente Kerberos” en la página 453</a>
Configurar un cliente Kerberos	<p>Instala manualmente un cliente Kerberos. Utilizar este procedimiento si la instalación de cada cliente requiere parámetros de instalación únicos.</p> <p>Instala automáticamente un cliente Kerberos. Utilice este procedimiento si los parámetros de instalación para cada cliente son los mismos.</p> <p>Instala interactivamente un cliente Kerberos. Utilice este procedimiento si sólo algunos de los parámetros de instalación deben cambiarse.</p>	<p><a href="#">“Cómo configurar manualmente un cliente Kerberos” en la página 456</a></p> <p><a href="#">“Cómo configurar automáticamente un cliente Kerberos” en la página 454</a></p> <p><a href="#">“Cómo configurar interactivamente un cliente Kerberos” en la página 455</a></p>
Permitir que un cliente acceda a un sistema de archivos NFS como el usuario root	Crea un principal root en el cliente, para que el cliente pueda montar un sistema de archivos NFS compartido con el acceso root. Además, permite que el cliente configure acceso root no interactivo al sistema de archivos NFS, de modo que se puedan ejecutar trabajos cron.	<a href="#">“Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario root” en la página 462</a>
Deshabilitar la verificación del KDC que ha emitido un ticket de otorgamiento de tickets (TGT) de cliente	Permite a los clientes que no tienen un principal host almacenado en el archivo keytab local omitir la comprobación de seguridad que verifica que el KDC que ha emitido el TGT sea el mismo servidor que ha emitido el principal host.	<a href="#">“Cómo deshabilitar la verificación del ticket de otorgamiento de tickets (TGT)” en la página 462</a>

## ▼ Cómo crear un perfil de instalación de cliente Kerberos

Este procedimiento crea un perfil kclient que se puede utilizar al instalar un cliente Kerberos. Mediante el perfil kclient, se reducen las probabilidades de errores de escritura. Asimismo, el uso del perfil reduce la intervención del usuario, en comparación con el proceso interactivo.

- 1 **Conviértase en superusuario.**
- 2 **Cree un perfil de instalación kclient.**

Un ejemplo de perfil kclient podría ser similar al siguiente:

```
client# cat /net/denver.example.com/export/install/profile
REALM EXAMPLE.COM
KDC kdc1.example.com
ADMIN clntconfig
FILEPATH /net/denver.example.com/export/install/krb5.conf
NFS 1
DNSLOOKUP none
```

## ▼ Cómo configurar automáticamente un cliente Kerberos

**Antes de empezar** Este procedimiento utiliza un perfil de instalación. Consulte “[Cómo crear un perfil de instalación de cliente Kerberos](#)” en la página 453.

### 1 Conviértase en superusuario.

### 2 Ejecute la secuencia de comandos de instalación de `kclient`.

Debe proporcionar la contraseña para el principal `clntconfig` con el fin de completar el proceso.

```
client# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile
```

```
Starting client setup
```

```
-----
```

```
kdc1.example.com
```

```
Setting up /etc/krb5/krb5.conf.
```

```
Obtaining TGT for clntconfig/admin ...
```

```
Password for clntconfig/admin@EXAMPLE.COM: <Type the password>
```

```
nfs/client.example.com entry ADDED to KDC database.
```

```
nfs/client.example.com entry ADDED to keytab.
```

```
host/client.example.com entry ADDED to KDC database.
```

```
host/client.example.com entry ADDED to keytab.
```

```
Copied /net/denver.example.com/export/install/krb5.conf.
```

```
-----
```

```
Setup COMPLETE.
```

```
client#
```

### Ejemplo 23-7 Configuración automática de un cliente Kerberos con valores de sustitución de línea de comandos

El siguiente ejemplo sustituye los parámetros `DNSARG` y `KDC` que se establecen en el perfil de instalación.

```
# /usr/sbin/kclient -p /net/denver.example.com/export/install/profile\
-d dns_fallback -k kdc2.example.com
```

```
Starting client setup
```

```
-----
```

```

kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>

nfs/client.example.com entry ADDED to KDC database.
nfs/client.example.com entry ADDED to keytab.

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Copied /net/denver.example.com/export/install/krb5.conf.

-----
Setup COMPLETE.

client#

```

## ▼ Cómo configurar interactivamente un cliente Kerberos

Este procedimiento utiliza la utilidad de instalación `kclient` sin un perfil de instalación.

- 1 **Conviértase en superusuario.**
- 2 **Ejecute la secuencia de comandos de instalación de `kclient`.**  
Necesita proporcionar la siguiente información:
  - Nombre de dominio Kerberos
  - Nombre de host de KDC maestro
  - Nombre de principal administrativo
  - Contraseña para el principal administrativo

### Ejemplo 23-8 Ejecución de la utilidad de instalación `kclient`

A continuación, se muestra la salida de los resultados de la ejecución del comando `kclient`.

```

client# /usr/sbin/kclient

Starting client setup
-----

Do you want to use DNS for kerberos lookups ? [y/n]: n
      No action performed.
Enter the Kerberos realm: EXAMPLE.COM

```

```
Specify the KDC hostname for the above realm: kdc1.example.com

Setting up /etc/krb5/krb5.conf.

Enter the krb5 administrative principal to be used: clntconfig/admin
Obtaining TGT for clntconfig/admin ...
Password for clntconfig/admin@EXAMPLE.COM:      <Type the password>
Do you plan on doing Kerberized nfs ? [y/n]: n

host/client.example.com entry ADDED to KDC database.
host/client.example.com entry ADDED to keytab.

Do you want to copy over the master krb5.conf file ? [y/n]: y
Enter the pathname of the file to be copied: \
/net/denver.example.com/export/install/krb5.conf

Copied /net/denver.example.com/export/install/krb5.conf.

-----
Setup COMPLETE !
#
```

## ▼ Cómo configurar manualmente un cliente Kerberos

En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = **EXAMPLE.COM**
- Nombre de dominio DNS = **example.com**
- KDC maestro = **kdc1.example.com**
- KDC esclavo = **kdc2.example.com**
- Servidor NFS = **denver.example.com**
- Cliente = **client.example.com**
- Principal admin = **kws/admin**
- Principal de usuario = **mre**
- URL de ayuda en pantalla =  
**http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956**

---

**Nota** – Ajuste la dirección URL para que enlace a la sección "Herramienta gráfica de administración de Kerberos", como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos”](#) en la página 419.

---

### 1 Conviértase en superusuario.



## 2 Edite el archivo de configuración de Kerberos (krb5.conf).

Para cambiar el archivo de la versión predeterminada de Kerberos, debe cambiar los nombres de dominios y los nombres de servidores. También tiene que identificar la ruta a los archivos de ayuda para gkadmin.

```
kdc1 # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM

[realms]
    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        admin_server = kdc1.example.com
    }

[domain_realm]
    .example.com = EXAMPLE.COM

#
# if the domain name and realm name are equivalent,
# this entry is not needed
#
[logging]
    default = FILE:/var/krb5/kdc.log
    kdc = FILE:/var/krb5/kdc.log

[appdefaults]
    gkadmin = {
        help_url = http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956
```

---

**Nota** – Si desea restringir los tipos de cifrado, puede definir las líneas `default_tkt_enctypes` o `default_tgs_enctypes`. Consulte [“Uso de los tipos de cifrado de Kerberos” en la página 579](#) para obtener una descripción de los problemas relacionados con la restricción de los tipos de cifrado.

---

## 3 (Opcional) Cambie el proceso utilizado para localizar los KDC.

A partir de la versión Solaris 10 5/08, de manera predeterminada, el dominio Kerberos para la asignación del KDC se determina en el orden siguiente:

- La definición en la sección `realms`, en `krb5.conf`.
- Mediante la búsqueda de registros SRV en DNS.

Puede cambiar este comportamiento agregando `dns_lookup_kdc` o `dns_fallback` a la sección `libdefaults` del archivo `krb5.conf`. Consulte la página del comando `man krb5.conf(4)` para obtener más información. Tenga en cuenta que las referencias siempre se intentan en primer lugar.

## 4 (Opcional) Cambie el proceso que se utiliza para determinar el dominio para un host.

A partir de la versión Solaris 10 5/08, de manera predeterminada, el host para la asignación del dominio se determina en el orden siguiente:

- Si el KDC admite referencias, el KDC puede informar al cliente a qué dominio pertenece el host.
- Por la definición de `domain_realm` en el archivo `krb5.conf`.
- El nombre de dominio DNS del host.
- El dominio predeterminado.

Puede cambiar este comportamiento agregando `dns_lookup_kdc` o `dns_fallback` a la sección `libdefaults` del archivo `krb5.conf`. Consulte la página del comando `man krb5.conf(4)` para obtener más información. Tenga en cuenta que las referencias siempre se intentarán en primer lugar.

## 5 (Opcional) Sincronice el reloj del cliente con el reloj del KDC maestro mediante NTP u otro mecanismo de sincronización de relojes.

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar sincronizado con la hora en el servidor KDC dentro de una diferencia máxima definida por la relación `clockskew` en el archivo `krb5.conf` para que la autenticación se realice con éxito. Consulte “[Sincronización de relojes entre clientes Kerberos y KDC](#)” en la página 466 para obtener información sobre el NTP.

## 6 Inicie `kadmin`.

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte “[Cómo crear un nuevo principal de Kerberos](#)” en la página 520. Para ello, debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

### a. (Opcional) Cree un principal de usuario si aún no existe ningún principal de usuario.

Necesita crear un principal de usuario sólo si el usuario asociado con este host no tiene un principal asignado a él.

```
kadmin: addprinc mre
Enter password for principal mre@EXAMPLE.COM:      <Type the password>
Re-enter password for principal mre@EXAMPLE.COM:    <Type it again>
kadmin:
```

### b. (Opcional) Cree un principal `root` y agregue el principal al archivo `keytab` del servidor.

Este paso es necesario para que el cliente pueda tener acceso `root` a sistemas de archivos montados mediante el servicio NFS. Este paso también es necesario si se necesita acceso `root` no interactivo, por ejemplo, la ejecución de trabajos cron como `root`.

Si el cliente no requiere acceso root a un sistema de archivos remoto que está montado mediante el servicio NFS, puede omitir este paso. El principal root debe ser un principal de dos componentes, donde el segundo componente es el nombre de host del sistema cliente Kerberos, para evitar la creación de un principal root de todo el dominio. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### c. Cree un principal host y agregue el principal al archivo keytab del servidor.

El principal host es utilizado por servicios de acceso remoto para proporcionar autenticación. El principal permite que root adquiera una credencial si ya no hay una en el archivo keytab.

```
kadmin: addprinc -randkey host/denver.example.com
Principal "host/denver.example.com@EXAMPLE.COM" created.
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

#### d. (Opcional) Agregue el principal de servicio NFS del servidor al archivo keytab del servidor.

Este paso sólo es necesario si el cliente necesita acceder a sistemas de archivos NFS utilizando la autenticación Kerberos.

```
kadmin: ktadd nfs/denver.example.com
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal nfs/denver.example.com with kvno 3, encryption type ArcFour
```

```
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  
Entry for principal nfs/denver.example.com with kvno 3, encryption type DES cbc mode  
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.  
kadmin:
```

**e. Salga de kadmin.**

```
kadmin: quit
```

**7 (Opcional) Habilite Kerberos con NFS.**

**a. Habilite los modos de seguridad de Kerberos en el archivo `/etc/nfssec.conf`.**

Edite el archivo `/etc/nfssec.conf` y elimine el símbolo “#” que se encuentra delante de los modos de seguridad de Kerberos.

```
# cat /etc/nfssec.conf  
.  
#  
# Uncomment the following lines to use Kerberos V5 with NFS  
#  
krb5          390003  kerberos_v5      default -           # RPCSEC_GSS  
krb5i         390004  kerberos_v5      default integrity   # RPCSEC_GSS  
krb5p         390005  kerberos_v5      default privacy     # RPCSEC_GSS
```

**b. Habilite el DNS.**

Si el archivo `/etc/resolv.conf` aún no se ha creado, créelo, ya que la canonización del principal de servicio depende del DNS para hacerlo. Consulte la página del comando [man resolv.conf\(4\)](#) para obtener más información.

**c. Reinicie el servicio gssd.**

Después de que el archivo `/etc/resolv.conf` se ha creado o modificado, debe reiniciar el daemon `gssd` para volver a leer los cambios.

```
# svcadm restart network/rpc/gss
```

**8 Si desea que el cliente renueve automáticamente el TGT o advierta a los usuarios acerca de la caducidad del ticket Kerberos, cree una entrada en el archivo `/etc/krb5/warn.conf`.**

Consulte la página del comando [man warn.conf\(4\)](#) para obtener más información.

### **Ejemplo 23–9 Configuración de un cliente Kerberos mediante un KDC que no sea Solaris**

Un cliente Kerberos se puede configurar para trabajar con un KDC que no sea Solaris. En este caso, se debe incluir una línea en el archivo `/etc/krb5/krb5.conf`, en la sección `realms`. Esta línea cambia el protocolo que se utiliza cuando el cliente se comunica con el servidor de cambio de contraseña de Kerberos. A continuación, se indica el formato de esta línea.

```
[realms]  
    EXAMPLE.COM = {  
        kdc = kdc1.example.com
```

```
kdc = kdc2.example.com
admin_server = kdc1.example.com
kpasswd_protocol = SET_CHANGE
}
```

**Ejemplo 23–10** Registros TXT de DNS para la asignación de nombre de host y dominio al dominio Kerberos

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
    1989020501 ;serial
    10800      ;refresh
    3600       ;retry
    3600000    ;expire
    86400      ;minimum

    IN      NS      kdc1.example.com.
kdc1      IN      A      192.146.86.20
kdc2      IN      A      192.146.86.21

_kerberos.example.com.      IN      TXT      "EXAMPLE.COM"
_kerberos.kdc1.example.com.  IN      TXT      "EXAMPLE.COM"
_kerberos.kdc2.example.com.  IN      TXT      "EXAMPLE.COM"
```

**Ejemplo 23–11** Registros SRV de DNS para ubicaciones del servidor Kerberos

En este ejemplo, se definen los registros para la ubicación de los KDC, el servidor admin y servidor kpasswd, respectivamente.

```
@ IN SOA kdc1.example.com root.kdc1.example.com (
    1989020501 ;serial
    10800      ;refresh
    3600       ;retry
    3600000    ;expire
    86400      ;minimum

    IN      NS      kdc1.example.com.
kdc1      IN      A      192.146.86.20
kdc2      IN      A      192.146.86.21

_kerberos._udp.EXAMPLE.COM      IN      SRV 0 0 88 kdc2.example.com
_kerberos._tcp.EXAMPLE.COM      IN      SRV 0 0 88 kdc2.example.com
_kerberos._udp.EXAMPLE.COM      IN      SRV 1 0 88 kdc1.example.com
_kerberos._tcp.EXAMPLE.COM      IN      SRV 1 0 88 kdc1.example.com
_kerberos-adm._tcp.EXAMPLE.COM  IN      SRV 0 0 749 kdc1.example.com
_kpasswd._udp.EXAMPLE.COM       IN      SRV 0 0 749 kdc1.example.com
```

## ▼ Cómo deshabilitar la verificación del ticket de otorgamiento de tickets (TGT)

Este procedimiento deshabilita la comprobación de seguridad que comprueba que el KDC del principal host almacenado en el archivo `/etc/krb5/krb5.keytab` local sea el mismo KDC que ha emitido el ticket de otorgamiento de tickets. Esta comprobación impide ataques de falsificación de DNS. Sin embargo, para algunas configuraciones de clientes, el principal host puede no estar disponible, por lo que esta comprobación debería ser deshabilitada para permitir que el cliente funcione. Éstas son las configuraciones que requieren que esta comprobación esté deshabilitada:

- La dirección IP del cliente se asigna dinámicamente. Por ejemplo, un cliente DHCP.
- El cliente no está configurado para hospedar servicios, por lo que no se ha creado ningún principal host.
- La clave del host no se almacena en el cliente.

### 1 Conviértase en superusuario.

### 2 Cambie el archivo `krb5.conf`.

Si la opción `verify_ap_req_nofail` se establece en `false`, el proceso de verificación de TGT no está habilitado. Consulte la página del comando `man krb5.conf(4)` para obtener más información sobre esta opción.

```
client # cat /etc/krb5/krb5.conf
[libdefaults]
    default_realm = EXAMPLE.COM
    verify_ap_req_nofail = false
...
```

---

**Nota** – La opción `verify_ap_req_nofail` se puede introducir en la sección `[libdefaults]` o `[realms]` del archivo `krb5.conf`. Si la opción está en la sección `[libdefaults]`, el valor se utiliza para todos los dominios. Si la opción está en la sección `[realms]`, el valor sólo se aplica al dominio definido.

---

## ▼ Cómo acceder a un sistema de archivos NFS protegido con Kerberos como el usuario `root`

Este procedimiento permite a un cliente acceder a un sistema de archivos NFS que requiere la autenticación Kerberos con el privilegio de ID `root`. En particular, cuando el sistema de archivos NFS está compartido con opciones, como `-o sec=krb5,root=client1.sun.com`.

### 1 Conviértase en superusuario.

## 2 Inicie kadmin.

Si desea obtener información sobre cómo utilizar la herramienta gráfica de administración de Kerberos para agregar un principal, consulte [“Cómo crear un nuevo principal de Kerberos” en la página 520](#). Para ello, debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro. Sin embargo, el siguiente ejemplo muestra cómo agregar los principales necesarios mediante la línea de comandos.

```
denver # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

### a. Cree un principal root para el cliente NFS.

Este principal se utiliza para proporcionar acceso equivalente a root a sistemas de archivos montados en NFS que requieren la autenticación Kerberos. El principal root debe ser un principal de dos componentes, donde el segundo componente es el nombre de host del sistema cliente Kerberos, para evitar la creación de un principal root de todo el dominio. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo /etc/resolv.conf.

```
kadmin: addprinc -randkey root/client.example.com
Principal "root/client.example.com" created.
kadmin:
```

### b. Agregue el principal root al archivo keytab del servidor.

Este paso es necesario si ha agregado un principal root para que el cliente pueda tener acceso root a sistemas de archivos montados mediante el servicio NFS. Este paso también es necesario si se necesita acceso root no interactivo, por ejemplo, la ejecución de trabajos cron como root.

```
kadmin: ktadd root/client.example.com
Entry for principal root/client.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal root/client.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:
```

### c. Salga de kadmin.

```
kadmin: quit
```

## ▼ Cómo configurar la migración automática de usuarios en un dominio Kerberos

Los usuarios, que no tienen un principal de Kerberos, se pueden migrar automáticamente a un dominio Kerberos existente. La migración se logra utilizando la estructura PAM para el servicio en uso mediante el apilamiento del módulo `pam_krb5_migrate` en la pila de autenticación del servicio, en `/etc/pam.conf`.

En este ejemplo, los nombres de servicio PAM `dtlogin` y `other` se configuran para usar la migración automática. Se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = `EXAMPLE.COM`
- KDC maestro = `kdc1.example.com`
- Equipo que hospeda el servicio de migración = `server1.example.com`
- Principal de servicio de migración = `host/server1.example.com`

### Antes de empezar

Configure `server1` como un cliente Kerberos del dominio `EXAMPLE.COM`. Consulte [“Configuración de clientes Kerberos” en la página 452](#) para obtener más información.

#### 1 Compruebe si existe un principal de servicio de host para `server1`.

El principal de servicio de host en el archivo `keytab` de `server1` se utiliza para autenticar el servidor en el KDC maestro.

```
server1 # klist -k
Keytab name: FILE:/etc/krb5/krb5.keytab
KVNO Principal
-----
3 host/server1.example.com@EXAMPLE.COM
3 host/server1.example.com@EXAMPLE.COM
3 host/server1.example.com@EXAMPLE.COM
3 host/server1.example.com@EXAMPLE.COM
```

#### 2 Realice cambios en el archivo de configuración de PAM.

##### a. Agregue entradas para el servicio `dtlogin`.

```
# cat /etc/pam.conf
.
.
#
# dtlogin service (explicit because of pam_krb5_migrate)
#
dtlogin      auth requisite      pam_authtok_get.so.1
dtlogin      auth required       pam_dhkeys.so.1
dtlogin      auth required       pam_unix_cred.so.1
dtlogin      auth sufficient     pam_krb5.so.1
dtlogin      auth requisite      pam_unix_auth.so.1
dtlogin      auth optional       pam_krb5_migrate.so.1
```



**b. (Opcional) Fuerce un cambio inmediato de contraseña si es necesario.**

Las cuentas de Kerberos recién creadas pueden tener el tiempo de caducidad de contraseña establecido en la hora actual (ahora) para forzar un cambio inmediato de contraseña Kerberos. Para establecer el tiempo de caducidad en la hora actual, agregue la opción `expire_pw` a las líneas que utilizan el módulo `pam_krb5_migrate`. Consulte la página del comando `man pam_krb5_migrate(5)` para obtener más información.

```
# cat /etc/pam.conf
.
.
dtlogin  auth optional          pam_krb5_migrate.so.1 expire_pw
```

**c. Agregue el módulo `pam_krb5` a la pila de cuentas.**

Esta adición permite la caducidad de la contraseña en Kerberos para bloquear el acceso.

```
# cat /etc/pam.conf
.
.
#
# Default definition for Account management
# Used when service name is not explicitly mentioned for account management
#
other    account requisite      pam_roles.so.1
other    account required      pam_krb5.so.1
other    account required      pam_unix_account.so.1
```

**d. Agregue el módulo `pam_krb5` a la pila de contraseñas.**

Esta adición permite que las contraseñas se actualicen cuando la contraseña caduca.

```
# cat /etc/pam.conf
.
.
#
# Default definition for Password management
# Used when service name is not explicitly mentioned for password management
#
other    password required      pam_dhkeys.so.1
other    password requisite      pam_authtok_get.so.1
other    password requisite      pam_authtok_check.so.1
other    password sufficient     pam_krb5.so.1
other    password required      pam_authtok_store.so.1
```

**3 En el KDC maestro, actualice el archivo de control de acceso.**

Las entradas siguientes otorgan privilegios de migración y consulta al principal de servicio `host/server1.example.com` para todos los usuarios, excepto el usuario `root`. Es importante que los usuarios que no se deben migrar se enumeren en el archivo `kadm5.acl` utilizando el privilegio `U`. Estas entradas deben estar antes de la entrada `ui` o permitir todo. Consulte la página del comando `man kadm5.acl(4)` para obtener más información.

```
kdc1 # cat /etc/krb5/kadm5.acl
host/server1.example.com@EXAMPLE.COM U root
host/server1.example.com@EXAMPLE.COM ui *
*/admin@EXAMPLE.COM *
```

**4 En el KDC maestro, reinicie el daemon de administración Kerberos.**

Este paso permite al daemon `kadmind` utilizar las nuevas entradas `kadm5.ac1`.

```
kdc1 # svcadm restart network/security/kadmin
```

**5 En el KDC maestro, agregue entradas al archivo `pam.conf`.**

Las entradas siguientes permiten que el daemon `kadmind` utilice el servicio PAM `k5migrate` para validar la contraseña de usuario de UNIX para las cuentas que necesitan migración.

```
# grep k5migrate /etc/pam.conf
k5migrate      auth      required      pam_unix_auth.so.1
k5migrate      account   required      pam_unix_account.so.1
```

## Sincronización de relojes entre clientes Kerberos y KDC

Todos los hosts que participan en el sistema de autenticación Kerberos deben tener los relojes internos sincronizados dentro de una cantidad de tiempo máxima especificada (conocida como *desfase de reloj*). Este requisito proporciona otra comprobación de seguridad de Kerberos. Si el desfase del reloj se supera entre cualquiera de los hosts que participan, las solicitudes de los clientes se rechazan.

El desfase del reloj también determina el tiempo durante el cual los servidores de aplicaciones deben realizar un seguimiento de todos los mensajes del protocolo Kerberos a fin de reconocer y rechazar solicitudes reproducidas. Por lo tanto, cuanto más grande es el valor del desfase del reloj, más información tienen que recopilar los servidores de aplicaciones.

El valor predeterminado para el desfase máximo del reloj es de 300 s (5 min). Puede cambiar este valor predeterminado en la sección `libdefaults` del archivo `krb5.conf`.

---

**Nota** – Por motivos de seguridad, no aumente el desfase del reloj más allá de 300 s.

---

Debido a que mantener los relojes sincronizados entre los clientes Kerberos y los KDC es importante, debe utilizar el software de protocolo de hora de red (NTP) para sincronizarlos. El software de dominio público NTP de la Universidad de Delaware se incluye en el software Oracle Solaris.

---

**Nota** – Otra forma de sincronizar los relojes es utilizar el comando `rdate` y los trabajos `cron`, un proceso que puede ser menos involucrado que utilizar el NTP. Sin embargo, esta sección se centra en el uso del NTP. Y, si utiliza la red para sincronizar los relojes, el protocolo de sincronización de relojes debe ser seguro.

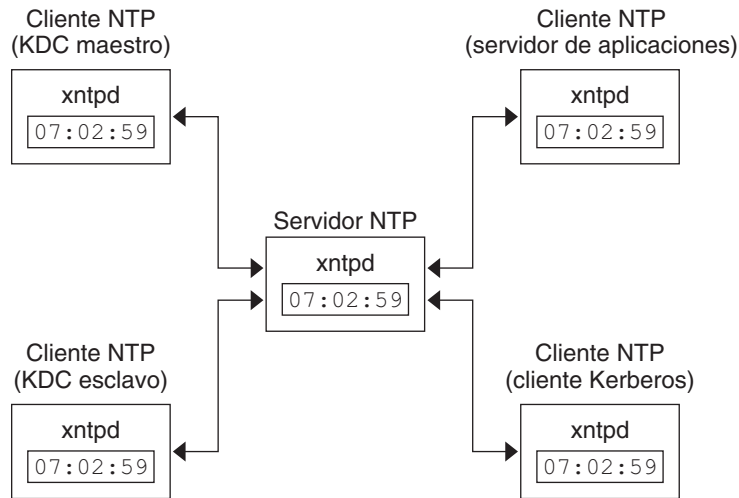
---

El NTP permite gestionar la sincronización de relojes de red o el tiempo preciso, o ambos, en un entorno de red. El NTP es, básicamente, una implementación de servidor y cliente. Elija un

sistema para que sea el reloj maestro (el servidor NTP). A continuación, configure todos los otros sistemas (los clientes NTP) para sincronizar sus relojes con el reloj principal.

Para sincronizar los relojes, el NTP utiliza el daemon `xntpd`, que establece y mantiene una hora del día del sistema UNIX de acuerdo con los servidores de hora estándar de Internet. A continuación, se muestra un ejemplo de esta implementación de NTP de servidor y cliente.

FIGURA 23-1 Sincronización de relojes mediante el NTP



Asegurarse de que los clientes Kerberos y los KDC mantengan relojes sincronizados implica la implementación de los siguientes pasos:

1. Configure un servidor NTP en la red. Este servidor puede ser cualquier sistema, excepto el KDC maestro. Consulte [“Gestión del protocolo de hora de red \(tareas\)” de Guía de administración del sistema: servicios de red](#) para buscar la tarea del servidor NTP.
2. Al realizar la configuración de los clientes Kerberos y los KDC en la red, configúrelos para que sean clientes NTP del servidor NTP. Consulte [“Gestión del protocolo de hora de red \(tareas\)” de Guía de administración del sistema: servicios de red](#) para buscar la tarea del cliente NTP.

## Intercambio de un KDC maestro y un KDC esclavo

Debe utilizar los procedimientos de esta sección para facilitar el intercambio de un KDC maestro con un KDC esclavo. Debe intercambiar el KDC maestro con un KDC esclavo sólo si el servidor KDC maestro falla por algún motivo o si el KDC maestro debe volver a instalarse (por ejemplo, porque se instaló un nuevo hardware).

### ▼ Cómo configurar un KDC esclavo intercambiable

Realice este procedimiento en el servidor KDC esclavo que desea que esté disponible para convertirse en el KDC maestro. Este procedimiento supone que utiliza la propagación incremental.

#### 1 Utilice nombres de alias para el KDC maestro y el KDC esclavo intercambiable durante la instalación del KDC.

Al definir los nombres de host para los KDC, asegúrese de que cada sistema tenga un alias incluido en DNS. Asimismo, utilice los nombres de alias al definir los hosts en el archivo `/etc/krb5/krb5.conf`.

#### 2 Siga los pasos para instalar un KDC esclavo.

Antes de realizar un intercambio, este servidor debe funcionar como cualquier otro KDC esclavo en el dominio. Consulte [“Cómo configurar manualmente un KDC esclavo” en la página 437](#) para obtener instrucciones.

#### 3 Mueva los comandos del KDC maestro.

Para evitar que los comandos del KDC maestro se ejecuten desde este KDC esclavo, mueva los comandos `kprop`, `kadmind` y `kadmin.local` a un lugar reservado.

```
kdc4 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc4 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
kdc4 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
```

### ▼ Cómo intercambiar un KDC maestro y un KDC esclavo

En este procedimiento, el servidor KDC maestro que se está intercambiando se denomina `kdc1`. El KDC esclavo que se convertirá en el nuevo KDC maestro se denomina `kdc4`. Este procedimiento supone que utiliza la propagación incremental.

#### Antes de empezar

Este procedimiento requiere que el servidor KDC esclavo se haya configurado como un esclavo intercambiable. Para obtener más información, consulte [“Cómo configurar un KDC esclavo intercambiable” en la página 468](#)).

## 1 En el nuevo KDC maestro, inicie kadmin.

```
kdc4 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

### a. Cree nuevos principales para el servicio kadmin.

El ejemplo siguiente muestra el primer comando `addprinc` en dos líneas, pero debe escribirse en una línea.

```
kadmin: addprinc -randkey -allow_tgs_req +password_changing_service -clearpolicy \
changepw/kdc4.example.com
Principal "changepw/kdc4.example.com@ENG.SUN.COM" created.
kadmin: addprinc -randkey -allow_tgs_req -clearpolicy kadmin/kdc4.example.com
Principal "kadmin/kdc4.example.com@EXAMPLE.COM" created.
kadmin:
```

### b. Cree un archivo keytab.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc4.example.com
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc4.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab changepw/kdc4.example.com
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc4.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: ktadd -k /etc/krb5/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin:
```

### c. Salga de kadmin.

```
kadmin: quit
```

**2 En el nuevo KDC maestro, fuerce la sincronización.**

Los siguientes pasos fuerzan una actualización completa del KDC en el servidor esclavo.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**3 En el nuevo KDC maestro, verifique que la actualización se haya completado.**

```
kdc4 # /usr/sbin/kproplog -h
```

**4 En el nuevo KDC maestro, reinicie el servicio KDC.**

```
kdc4 # svcadm enable -r network/security/krb5kdc
```

**5 En el nuevo KDC maestro, borre el registro de actualización.**

Estos pasos reinician el registro de actualización para el nuevo servidor KDC maestro.

```
kdc4 # svcadm disable network/security/krb5kdc
kdc4 # rm /var/krb5/principal.ulong
```

**6 En el KDC maestro antiguo, termine los procesos kadmind y krb5kdc.**

Al terminar el proceso kadmind, evita que se realicen cambios en la base de datos del KDC.

```
kdc1 # svcadm disable network/security/kadmind
kdc1 # svcadm disable network/security/krb5kdc
```

**7 En el KDC maestro antiguo, especifique el tiempo de sondeo para solicitar propagaciones.**

Elimine el comentario de la entrada `sunw_dbprop_master_ulogsize` en `/etc/krb5/kdc.conf` y agregue una entrada que defina `sunw_dbprop_slave_poll`. La entrada establece el tiempo de sondeo en 2 min.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
        sunw_dbprop_slave_poll = 2m
    }
```

**8 En el KDC maestro antiguo, mueva los comandos del KDC maestro y el archivo `kadm5.acl`.**

Para evitar que los comandos del KDC maestro se ejecuten, mueva los comandos `kprop`, `kadmind` y `kadmin.local` a un lugar reservado.

```
kdc1 # mv /usr/lib/krb5/kprop /usr/lib/krb5/kprop.save
kdc1 # mv /usr/lib/krb5/kadmind /usr/lib/krb5/kadmind.save
```

```
kdc1 # mv /usr/sbin/kadmin.local /usr/sbin/kadmin.local.save
kdc1 # mv /etc/krb5/kadm5.acl /etc/krb5/kadm5.acl.save
```

## 9 En el servidor DNS, cambie los nombres de alias del KDC maestro.

Para cambiar los servidores, edite el archivo de zona `example.com` y cambie la entrada para `masterkdc`.

```
masterkdc IN CNAME kdc4
```

## 10 En el servidor DNS, reinicie el servidor de nombres de dominio de Internet.

Ejecute el siguiente comando para volver a cargar la nueva información de alias:

```
# svcadm refresh network/dns/server
```

## 11 En el nuevo KDC maestro, mueva los comandos del KDC maestro y el archivo `kpropd.acl` esclavo.

```
kdc4 # mv /usr/lib/krb5/kprop.save /usr/lib/krb5/kprop
kdc4 # mv /usr/lib/krb5/kadmind.save /usr/lib/krb5/kadmind
kdc4 # mv /usr/sbin/kadmin.local.save /usr/sbin/kadmin.local
kdc4 # mv /etc/krb5/kpropd.acl /etc/krb5/kpropd.acl.save
```

## 12 En el nuevo KDC maestro, cree el archivo de la lista de control de acceso de Kerberos (`kadm5.acl`).

Una vez que se rellena, el archivo `/etc/krb5/kadm5.acl` debe contener todos los nombres de principales que tienen permitido administrar el KDC. El archivo también debe mostrar todos los esclavos que realizan solicitudes de propagación incremental. Consulte la página del comando `man kadm5.acl(4)` para obtener más información.

```
kdc4 # cat /etc/krb5/kadm5.acl
kws/admin@EXAMPLE.COM *
kiprop/kdc1.example.com@EXAMPLE.COM p
```

## 13 En el nuevo KDC maestro, especifique el tamaño de registro de actualización en el archivo `kdc.conf`.

Elimine el comentario de la entrada `sunw_dbprop_slave_poll` y agregue una entrada que defina `sunw_dbprop_master_ulogsize`. La entrada establece el tamaño de registro en 1000 entradas.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
```

```
#                sunw_dbprop_slave_poll = 2m
                sunw_dbprop_master_ulogsize = 1000
}
```

#### 14 En el nuevo KDC maestro, agregue el principal kiprop al archivo keytab kadmin.

```
kdc4 # kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc4.example.com
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc4.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin.local: quit
```

#### 15 En el nuevo KDC maestro, inicie kadmin y krb5kdc.

```
kdc4 # svcadm enable -r network/security/krb5kdc
kdc4 # svcadm enable -r network/security/kadmin
```

#### 16 En el KDC maestro antiguo, agregue el principal de servicio kiprop.

La adición del principal kiprop al archivo krb5.keytab permite que el daemon kpropd se autentique para el servicio de propagación incremental.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Authenticating as principal kws/admin@EXAMPLE.COM with password.
Enter password: <Type kws/admin password>
kadmin: ktadd kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

#### 17 En el KDC maestro antiguo, agregue una entrada para cada KDC que aparece en krb5.conf al archivo de configuración de propagación, kpropd.acf.

```
kdc1 # cat /etc/krb5/kpropd.acf
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
host/kdc4.example.com@EXAMPLE.COM
```



**18 En el KDC maestro antiguo, inicie kpropd y krb5kdc.**

Cuando el daemon `krb5kdc` se inicia, `kpropd` también se inicia si el sistema está configurado como esclavo.

```
kdc1 # svcadm enable network/security/krb5kdc
```

## Administración de la base de datos de Kerberos

La base de datos de Kerberos es la red principal de Kerberos y se debe mantener correctamente. En esta sección, se proporcionan algunos procedimientos sobre cómo administrar la base de datos de Kerberos, como la copia de seguridad y restauración de la base de datos, la configuración de la propagación incremental o en paralelo, y la administración del archivo intermedio. Los pasos para configurar inicialmente la base de datos se detallan en [“Cómo configurar manualmente un KDC maestro” en la página 423](#).

### Copia de seguridad y propagación de la base de datos de Kerberos

La propagación de la base de datos de Kerberos desde el KDC maestro hasta los KDC esclavos es una de las tareas de configuración más importantes. Si la propagación no ocurre con suficiente frecuencia, el KDC maestro y los KDC esclavos pierden la sincronización. Por lo tanto, si el KDC maestro deja de funcionar, los KDC esclavos no tendrán la información más reciente de la base de datos. Además, si un KDC esclavo se ha configurado como un KDC maestro con fines de equilibrio de carga, los clientes que utilicen ese KDC esclavo como KDC maestro no tendrán la información más reciente. Por lo tanto, debe asegurarse de que la propagación se produzca con suficiente frecuencia o configurar los servidores para la propagación incremental en función de la frecuencia con la que se cambia la base de datos de Kerberos. La propagación incremental se prefiere frente a la propagación manual porque hay más sobrecarga administrativa cuando se propaga manualmente la base de datos. También hay ineficacias cuando se realiza la propagación completa de la base de datos.

Al configurar el KDC maestro, se configura el comando `kprop_script` en un trabajo `cron` para realizar automáticamente una copia de seguridad de la base de datos de Kerberos en el archivo de volcado `/var/krb5/slave_datatrans` y propagarlo a los KDC esclavos. No obstante, como con cualquier archivo, la base de datos de Kerberos puede dañarse. Si se dañan los datos en un KDC esclavo, es posible que nunca lo note, porque la próxima propagación automática de la base de datos instala una copia nueva. Sin embargo, si se dañan los datos en el KDC maestro, la base de datos dañada se propaga a todos los KDC esclavos durante la siguiente propagación. Por lo tanto, la copia de seguridad dañada sobrescribe el archivo de copia de seguridad anterior que no está dañado en el KDC maestro.

Debido a que no hay ninguna copia de seguridad “segura” en este escenario, también debe configurar un trabajo `cron` para copiar periódicamente el archivo de volcado `slave_datatrans`.

en otra ubicación o para crear otra copia de seguridad separada mediante el comando `dump de kdb5_util`. De este modo, si se daña su base de datos, puede restaurar la copia de seguridad más reciente en el KDC maestro mediante el comando `load de kdb5_util`.

Otra nota importante: debido a que el archivo de volcado de la base de datos contiene claves de principales, necesita proteger el archivo contra el acceso de usuarios no autorizados. De manera predeterminada, el archivo de volcado de la base de datos tiene permisos de lectura y escritura sólo como `root`. Para protegerlo contra el acceso no autorizado, utilice sólo el comando `kprop` para propagar el archivo de volcado de la base de datos, que cifra los datos que se transfieren. Además, `kprop` propaga los datos sólo a los KDC esclavos, lo cual minimiza la posibilidad de enviar accidentalmente el archivo de volcado de la base de datos a hosts no autorizados.



---

**Precaución** – Si la base de datos de Kerberos se actualiza después de ser propagada y si la base se daña posteriormente antes de la siguiente propagación, los KDC esclavos no contendrán las actualizaciones. Las actualizaciones se perderán. Por este motivo, si agrega actualizaciones importantes a la base de datos de Kerberos antes de una propagación programada con regularidad, debe propagar manualmente la base de datos para evitar pérdidas de datos.

---

## El archivo `kpropd.acf`

El archivo `kpropd.acf` en un KDC esclavo proporciona una lista de nombres de principales `host`, un nombre por línea, que especifica los sistemas desde los cuales el KDC puede recibir una base de datos actualizada mediante la propagación. Si el KDC maestro se utiliza para propagar todos los KDC esclavos, el archivo `kpropd.acf` de cada esclavo necesita contener sólo el nombre del principal `host` del KDC maestro.

Sin embargo, la instalación de Kerberos y los pasos de configuración posteriores en este manual le indican que agregue el mismo archivo `kpropd.acf` al KDC maestro y a los KDC esclavos. Este archivo contiene todos los nombres de principales `host` del KDC. Esta configuración permite propagar desde cualquier KDC, en caso de que los KDC que se propagan no estén disponibles temporalmente. De este modo, al conservar una copia idéntica en todos los KDC, hace que la configuración sea fácil de mantener.

## El comando `kprop_script`

El comando `kprop_script` usa el comando `kprop` para propagar la base de datos de Kerberos a otros KDC. Si el comando `kprop_script` se ejecuta en un KDC esclavo, propaga la copia del KDC esclavo de la base de datos de Kerberos a otros KDC. El comando `kprop_script` acepta una lista de nombres de `host` para argumentos, separados por espacios, que indican los KDC para propagar.

Cuando `kprop_script` se ejecuta, crea una copia de seguridad de la base de datos de Kerberos en el archivo `/var/krb5/slave_data/atrans` y copia el archivo en los KDC especificados. La base de datos de Kerberos se bloquea hasta que la propagación se termina.

## ▼ Cómo realizar copias de seguridad de la base de datos de Kerberos

- 1 Conviértase en superusuario en el KDC maestro.
- 2 Realice una copia de seguridad de la base de datos de Kerberos mediante el comando `dump` del comando `kdb5_util`.

```
# /usr/sbin/kdb5_util dump [-verbose] [-d dbname] [filename [principals...]]
```

`-verbose` Imprime el nombre de cada principal y política a los que se está realizando una copia de seguridad.

`nombre_base_datos` Define el nombre de la base de datos para realizar copia de seguridad. Tenga en cuenta que puede especificar una ruta absoluta para el archivo. Si la opción `-d` no está especificada, el nombre de la base de datos predeterminado es `/var/krb5/principal`.

`nombre_archivo` Define el archivo que se utiliza para realizar la copia de seguridad de la base de datos. Puede especificar una ruta absoluta para el archivo. Si no especifica un archivo, la base de datos se vuelca a una salida estándar.

`principales` Define una lista de uno o más principales (separados por un espacio) para realizar copia de seguridad. Debe utilizar nombres completos de principales. Si no especifica ningún principal, se realiza una copia de seguridad de la base de datos completa.

### Ejemplo 23-12 Copia de seguridad de la base de datos de Kerberos

En el siguiente ejemplo, se realiza una copia de seguridad de la base de datos de Kerberos en un archivo denominado `dumpfile`. Debido a que la opción `-verbose` está especificada, cada principal se imprime a medida que se le realiza una copia de seguridad.

```
# kdb5_util dump -verbose dumpfile
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/ENG.EXAMPLE.COM@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

En el ejemplo siguiente, se realiza una copia de seguridad de los principales `pak` y `pak/admin` de la base de datos de Kerberos.

```
# kdb5_util dump -verbose dumpfile pak/admin@ENG.EXAMPLE.COM pak@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
```

## ▼ Cómo restaurar la base de datos de Kerberos

- 1 Conviértase en superusuario en el KDC maestro.

- 2 En el maestro, detenga los daemons del KDC.

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

- 3 Restaure la base de datos de Kerberos mediante el comando `load` del comando `kdb_util`.

```
# /usr/sbin/kdb5_util load [-verbose] [-d dbname] [-update] [filename]
```

`-verbose` Imprime el nombre de cada principal y política que se están restaurando.

`nombre_base_datos` Define el nombre de la base de datos para restaurar. Tenga en cuenta que puede especificar una ruta absoluta para el archivo. Si la opción `-d` no está especificada, el nombre de la base de datos predeterminado es `/var/krb5/principal`.

`-update` Actualiza la base de datos existente. De lo contrario, se crea una base de datos nueva o la base de datos existente se sobrescribe.

`nombre_archivo` Define el archivo desde el cual se va a restaurar la base de datos. Puede especificar una ruta absoluta para el archivo.

- 4 Inicie los daemons del KDC.

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

### Ejemplo 23-13 Restauración de la base de datos de Kerberos

En el ejemplo siguiente, la base de datos denominada `database1` se restaura en el directorio actual del archivo `dumpfile`. Debido a que la opción `-update` no está especificada, se crea una base de datos nueva con la restauración.

```
# kdb5_util load -d database1 dumpfile
```

## ▼ Cómo convertir una base de datos de Kerberos después de una actualización de servidor

Si la base de datos del KDC se ha creado en un servidor que ejecuta la versión Solaris 8 o Solaris 9, la conversión de la base de datos permite aprovechar un mejor formato de base de datos.

**Antes de empezar** Asegúrese de que la base de datos esté utilizando un formato antiguo.

**1 En el maestro, detenga los daemons del KDC.**

```
kdc1 # svcadm disable network/security/krb5kdc
kdc1 # svcadm disable network/security/kadmin
```

**2 Cree un directorio para almacenar una copia temporal de la base de datos.**

```
kdc1 # mkdir /var/krb5/tmp
kdc1 # chmod 700 /var/krb5/tmp
```

**3 Vuelque la base de datos del KDC.**

```
kdc1 # kdb5_util dump /var/krb5/tmp/prdb.txt
```

**4 Guarde copias de los archivos de la base de datos actual.**

```
kdc1 # cd /var/krb5
kdc1 # mv princ* tmp/
```

**5 Cargue la base de datos.**

```
kdc1 # kdb5_util load /var/krb5/tmp/prdb.txt
```

**6 Inicie los daemons del KDC.**

```
kdc1 # svcadm enable -r network/security/krb5kdc
kdc1 # svcadm enable -r network/security/kadmin
```

## ▼ Cómo reconfigurar un KDC maestro para utilizar la propagación incremental

Los pasos de este procedimiento se pueden utilizar para volver a configurar un KDC maestro existente a fin de utilizar la propagación incremental. En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Nombre de dominio = EXAMPLE.COM
- Nombre de dominio DNS = example.com
- KDC maestro = kdc1.example.com
- KDC esclavo = kdc2.example.com
- Principal admin = kws/admin

**1 Agregue entradas a `kdc.conf`.**

Necesita habilitar la propagación incremental y seleccionar el número de actualizaciones que el KDC maestro mantiene en el registro. Consulte la página del comando `man kdc.conf(4)` para obtener más información.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
```

```
kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
    }
```

## 2 Cree el principal kiprop.

El principal kiprop se utiliza para autenticar el servidor KDC maestro y para autorizar las actualizaciones del KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: addprinc -randkey kiprop/kdc1.example.com
Principal "kiprop/kdc1.example.com@EXAMPLE.COM" created.
kadmin: addprinc -randkey kiprop/kdc2.example.com
Principal "kiprop/kdc2.example.com@EXAMPLE.COM" created.
kadmin:
```

## 3 Agregue el principal kiprop al archivo keytab kadmind.

La adición del principal kiprop al archivo kadm5.keytab permite que el comando kadmind se autentique cuando se inicia.

```
kadmin: ktadd -k /etc/krb5/kadm5.keytab kiprop/kdc1.example.com
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kiprop/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
kadmin: quit
```

## 4 En el KDC maestro, agregue una entrada kiprop a kadm5.acl.

Esta entrada permite que el KDC maestro reciba solicitudes de propagación incremental del servidor kdc2.

```
kdc1 # cat /etc/krb5/kadm5.acl
*/admin@EXAMPLE.COM *
kiprop/kdc2.example.com@EXAMPLE.COM p
```

**5 Elimine el comentario de la línea kprop en el archivo crontab root.**

Este paso impide que el KDC maestro propague su copia de la base de datos del KDC.

```
kdc1 # crontab -e
#ident "@(#)root      1.20      01/11/06 SMI"
#
# The root crontab should be used to perform accounting data collection.
#
# The rtc command is run to adjust the real time clock if and when
# daylight savings time changes.
#
10 3 * * * /usr/sbin/logadm
15 3 * * 0 /usr/lib/fs/nfs/nfsfind
1 2 * * * [ -x /usr/sbin/rtc ] && /usr/sbin/rtc -c > /dev/null 2>&1
30 3 * * * [ -x /usr/lib/gss/gsscred_clean ] && /usr/lib/gss/gsscred_clean
#10 3 * * * /usr/lib/krb5kprop_script kdc2.example.sun.com #SUNWkr5ma
```

**6 Reinicie kadmind.**

```
kdc1 # svcadm restart network/security/kadmin
```

**7 Reconfigure todos los servidores KDC esclavos que utilicen la propagación incremental.**

Consulte [“Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental” en la página 479](#) para obtener instrucciones completas.

## ▼ Cómo reconfigurar un KDC esclavo para utilizar la propagación incremental

**1 Agregue entradas a krb5.conf.**

Las nuevas entradas habilitan la propagación incremental y definen el tiempo de sondeo en 2 min.

```
kdc2 # cat /etc/krb5/krb5.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM= {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_slave_poll = 2m
    }
```

## 2 Agregue el principal kiprop al archivo krb5.keytab.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin: ktadd kiprop/kdc2.example.com
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal kiprop/kdc2.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## 3 Deshabilite kpropd.

```
kdc2 # svcadm disable network/security/krb5_prop
```

## 4 Reinicie el servidor KDC.

```
kdc2 # svcadm restart network/security/krb5kdc
```

# ▼ Cómo configurar un KDC esclavo para utilizar la propagación completa

Este procedimiento muestra cómo reconfigurar un servidor KDC esclavo que ejecuta la versión Solaris 10 para utilizar la propagación completa. Normalmente, el procedimiento sólo se debe utilizar si el servidor KDC maestro está ejecutando la versión Solaris 9 o una versión anterior. En este caso, el servidor KDC maestro no puede admitir la propagación incremental, por lo que el esclavo debe estar configurado para que la propagación funcione.

En este procedimiento, se configura un KDC esclavo denominado kdc3. Este procedimiento utiliza los siguientes parámetros de configuración:

- Nombre de dominio = EXAMPLE.COM
- Nombre de dominio DNS = example.com
- KDC maestro = kdc1.example.com
- KDC esclavo = kdc2.example.com y kdc3.example.com
- Principal admin = kws/admin
- URL de ayuda en pantalla =  
<http://denver:8888/ab2/coll.384.1/SEAM/@AB2PageView/6956>



---

**Nota** – Ajuste la dirección URL para que enlace a la sección "Herramienta gráfica de administración de Kerberos", como se describe en [“URL de ayuda en pantalla en la herramienta gráfica de administración de Kerberos”](#) en la página 419.

---

**Antes de empezar** El KDC maestro debe estar configurado. Para obtener instrucciones específicas si este esclavo se va a intercambiar, consulte [“Intercambio de un KDC maestro y un KDC esclavo”](#) en la página 468.

**1 En el KDC maestro, conviértase en superusuario.**

**2 En el KDC maestro, inicie kadmin.**

Debe iniciar sesión con uno de los nombres de principales admin que creó cuando configuró el KDC maestro.

```
kdc1 # /usr/sbin/kadmin -p kws/admin
Enter password:      <Type kws/admin password>
kadmin:
```

**a. En el KDC maestro, agregue principales host esclavos a la base de datos si aún no lo ha hecho.**

Para que el esclavo funcione, debe tener un principal host. Tenga en cuenta que cuando la instancia de principal es un nombre de host, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: addprinc -randkey host/kdc3.example.com
Principal "host/kdc3@EXAMPLE.COM" created.
kadmin:
```

**b. Salga de kadmin.**

```
kadmin: quit
```

**3 En el KDC maestro, edite el archivo de configuración de Kerberos (krb5.conf).**

Debe agregar una entrada para cada esclavo. Consulte la página del comando `man krb5.conf(4)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/krb5.conf
:
[realms]

    EXAMPLE.COM = {
        kdc = kdc1.example.com
        kdc = kdc2.example.com
        kdc = kdc3.example.com
        admin_server = kdc1.example.com
    }
```

**4 En el KDC maestro, agregue una entrada para el KDC maestro y cada KDC esclavo en el archivo `kpropd.ac1`.**

Consulte la página del comando `man kprop(1M)` para obtener una descripción completa de este archivo.

```
kdc1 # cat /etc/krb5/kpropd.ac1
host/kdc1.example.com@EXAMPLE.COM
host/kdc2.example.com@EXAMPLE.COM
host/kdc3.example.com@EXAMPLE.COM
```

**5 En todos los KDC esclavos, copie los archivos de administración KDC del servidor KDC maestro.**

Este paso se debe realizar en todos los KDC esclavos, ya que el servidor KDC maestro ha actualizado información que cada servidor KDC necesita. Puede utilizar `ftp` o un mecanismo de transferencia similar para capturar copias de los siguientes archivos del KDC maestro:

- `/etc/krb5/krb5.conf`
- `/etc/krb5/kdc.conf`
- `/etc/krb5/kpropd.ac1`

**6 En todos los KDC esclavos, asegúrese de que el archivo de la lista de control de acceso de Kerberos, `kadm5.ac1`, no esté relleno.**

Un archivo `kadm5.ac1` sin modificaciones sería de la siguiente manera:

```
kdc2 # cat /etc/krb5/kadm5.ac1
*/admin@__default_realm__ *
```

Si el archivo tiene entradas `kprop`, elimínelas.

**7 En el nuevo esclavo, inicie el comando `kadmin`.**

Debe iniciar sesión con uno de los nombres de principales `admin` que creó cuando configuró el KDC maestro.

```
kdc2 # /usr/sbin/kadmin -p kws/admin
Enter password: <Type kws/admin password>
kadmin:
```

**a. Agregue el principal `host` del esclavo al archivo `keytab` del esclavo mediante `kadmin`.**

Esta entrada permite que `kprop` y otras aplicaciones Kerberizadas funcionen. Tenga en cuenta que cuando la instancia de principal es un nombre de `host`, el FQDN se debe especificar en letras minúsculas, independientemente de si el nombre de dominio está en mayúsculas o minúsculas, en el archivo `/etc/resolv.conf`.

```
kadmin: ktadd host/kdc3.example.com
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type ArcFour
```

```

with HMAC/md5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
Entry for principal host/kdc3.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin:

```

## b. Salga de kadmin.

```
kadmin: quit
```

- 8 En el KDC maestro, agregue el nombre del KDC esclavo al trabajo cron, que ejecuta de forma automática las copias de seguridad, ejecutando crontab -e.**

Agregue el nombre de cada servidor KDC esclavo al final de la línea kprop\_script.

```
10 3 * * * /usr/lib/krb5/kprop_script kdc2.example.com kdc3.example.com
```

Es posible que también desee cambiar la hora de las copias de seguridad. Esta entrada inicia el proceso de copia de seguridad cada día a las 3:10 a. m.

- 9 En el nuevo esclavo, inicie el daemon de propagación de Kerberos.**

```
kdc3 # svcadm enable network/security/krb5_prop
```

- 10 En el KDC maestro, realice una copia de seguridad de la base de datos y propáguela mediante kprop\_script.**

Si ya hay disponible una copia de seguridad de la base de datos, no es necesario completar otra copia de seguridad. Consulte [“Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos” en la página 485](#) para obtener más instrucciones.

```
kdc1 # /usr/lib/krb5/kprop_script kdc3.example.com
Database propagation to kdc3.example.com: SUCCEEDED
```

- 11 En el nuevo esclavo, cree un archivo intermedio con kdb5\_util.**

```
kdc3 # /usr/sbin/kdb5_util stash
kdb5_util: Cannot find/read stored master key while reading master key
kdb5_util: Warning: proceeding without master key
```

```
Enter KDC database master key: <Type the key>
```

- 12 (Opcional) En el nuevo KDC esclavo, sincronice el reloj de los KDC maestros mediante NTP u otro mecanismo de sincronización de relojes.**

No es necesario instalar ni utilizar el protocolo de hora de red (NTP). Sin embargo, cada reloj debe estar dentro de la hora predeterminada que está definida en la sección libdefaults del archivo krb5.conf para que la autenticación se realice con éxito. Consulte [“Sincronización de relojes entre clientes Kerberos y KDC” en la página 466](#) para obtener información sobre el NTP.

- 13 En el nuevo esclavo, inicie el daemon del KDC (krb5kdc).**

```
kdc3 # svcadm enable network/security/krb5kdc
```

## ▼ Cómo verificar que los servidores KDC estén sincronizados

Si la propagación incremental se ha configurado, este procedimiento garantiza que la información en el KDC esclavo se ha actualizado.

- 1 En el servidor KDC maestro, ejecute el comando `kproplog`.

```
kdc1 # /usr/sbin/kproplog -h
```

- 2 En un servidor KDC esclavo, ejecute el comando `kproplog`.

```
kdc2 # /usr/sbin/kproplog -h
```

- 3 Compruebe que el último número de serie y los últimos valores de indicación de hora coincidan.

### Ejemplo 23-14 Verificación de que los servidores KDC estén sincronizados

A continuación, se muestra un ejemplo de resultados de la ejecución del comando `kproplog` en el servidor KDC maestro.

```
kdc1 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
  Log version #: 1
  Log state: Stable
  Entry block size: 2048
  Number of entries: 2500
  First serial #: 137966
  Last serial #: 140465
  First time stamp: Fri Nov 28 00:59:27 2004
  Last time stamp: Fri Nov 28 01:06:13 2004
```

A continuación, se muestra un ejemplo de resultados de la ejecución del comando `kproplog` en un servidor KDC esclavo.

```
kdc2 # /usr/sbin/kproplog -h

Kerberos update log (/var/krb5/principal.ulong)
Update log dump:
  Log version #: 1
  Log state: Stable
  Entry block size: 2048
  Number of entries: 0
  First serial #: None
  Last serial #: 140465
  First time stamp: None
  Last time stamp: Fri Nov 28 01:06:13 2004
```

Tenga en cuenta que los valores para el último número de serie y la última indicación de hora son idénticos, lo que indica que el esclavo está sincronizado con el servidor KDC maestro.

En la salida del servidor KDC esclavo, observe que no existen entradas de actualización en el registro de actualización del servidor KDC esclavo. No existen entradas porque el servidor KDC esclavo no conserva un conjunto de actualizaciones, a diferencia del servidor KDC maestro. Además, el servidor KDC esclavo no incluye información sobre el primer número de serie ni la primera indicación de hora porque no es información relevante.

## ▼ **Cómo propagar manualmente la base de datos de Kerberos a los KDC esclavos**

Este procedimiento muestra cómo propagar la base de datos de Kerberos mediante el comando `kprop`. Utilice este procedimiento si necesita sincronizar un KDC esclavo con el KDC maestro fuera del trabajo `cron` periódico. A diferencia de `kprop_script`, puede utilizar `kprop` para propagar sólo la copia de seguridad de la base de datos actual sin realizar primero una nueva copia de seguridad de la base de datos de Kerberos.

---

**Nota** – No utilice este procedimiento si está usando la propagación incremental.

---

- 1 **Conviértase en superusuario en el KDC maestro.**
- 2 **(Opcional) Cree una copia de seguridad de la base de datos mediante el comando `kdb5_util`.**  
`# /usr/sbin/kdb5_util dump /var/krb5/slave_datatrans`
- 3 **Propague la base de datos a un KDC esclavo mediante el comando `kprop`.**  
`# /usr/lib/krb5/kprop -f /var/krb5/slave_datatrans slave-KDC`

### **Ejemplo 23–15** Propagación manual de la base de datos de Kerberos a los KDC esclavos mediante `kprop_script`

Si desea realizar una copia de seguridad de la base de datos y propagarla a un KDC esclavo fuera del trabajo `cron` periódico, también puede utilizar el comando `kprop_script`, como se indica a continuación:

```
# /usr/lib/krb5/kprop_script slave-KDC
```

## Configuración de propagación en paralelo

En la mayoría de los casos, el KDC maestro se utiliza, exclusivamente, para propagar su base de datos de Kerberos a los KDC esclavos. Sin embargo, si su sitio tiene muchos KDC esclavos, es posible que deba considerar el uso compartido de carga del proceso de propagación, conocido como *propagación en paralelo*.

---

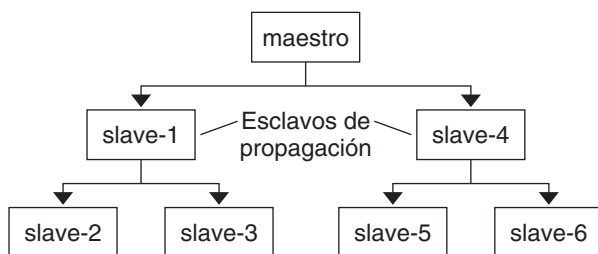
**Nota** – No utilice este procedimiento si está usando la propagación incremental.

---

La propagación en paralelo permite que KDC esclavos específicos compartan las tareas de propagación con el KDC maestro. Este uso compartido de tareas permite que la propagación se realice más rápido y alivie el trabajo para el KDC maestro.

Por ejemplo, suponga que su sitio tiene un KDC maestro y seis KDC esclavos (que se muestran en la [Figura 23-2](#)), donde del `slave-1` al `slave-3` constan de una agrupación lógica y del `slave-4` al `slave-6` constan de otra agrupación lógica. Para configurar la propagación en paralelo, puede hacer que el KDC maestro propague la base de datos al `slave-1` y al `slave-4`. A su vez, los KDC esclavos pueden propagar la base de datos a los KDC esclavos de su grupo.

FIGURA 23-2 Ejemplo de configuración de propagación en paralelo



## Pasos de configuración para la propagación en paralelo

A continuación, no se muestra un procedimiento detallado paso a paso, sino una lista de nivel superior con pasos de configuración para habilitar la propagación en paralelo. Estos pasos implican lo siguiente:

1. En el KDC maestro, cambie la entrada `kprop_script` en su trabajo `cron` a fin de incluir argumentos sólo para los KDC esclavos que realizarán la propagación subsiguiente (los *esclavos de propagación*).

2. En cada esclavo de propagación, agregue una entrada `kprop_script` a su trabajo `cron`, que debe incluir argumentos para que los esclavos se propaguen. Para propagar en paralelo correctamente, el trabajo `cron` se debe configurar para que se ejecute después de que el esclavo de propagación se propaga con la nueva base de datos de Kerberos.

---

**Nota** – El tiempo que tomará que un esclavo de propagación se propague depende de factores, como el ancho de banda de la red y el tamaño de la base de datos de Kerberos.

---

3. En cada KDC esclavo, configure los permisos adecuados que se van a propagar. Este paso se realiza mediante la adición del nombre del principal `host` del KDC de propagación al archivo `kpropd.acl`.

#### EJEMPLO 23–16 Configuración de propagación en paralelo

Mediante el ejemplo de la [Figura 23–2](#), la entrada `kprop_script` de los KDC maestros sería similar a la siguiente:

```
0 3 * * * /usr/lib/krb5/kprop_script slave-1.example.com slave-4.example.com
```

La entrada `kprop_script` de `slave-1` sería similar a la siguiente:

```
0 4 * * * /usr/lib/krb5/kprop_script slave-2.example.com slave-3.example.com
```

Tenga en cuenta que la propagación en el esclavo comienza una hora después de que es propagado por el maestro.

El archivo `kpropd.acl` en los esclavos de propagación contendría la siguiente entrada:

```
host/master.example.com@EXAMPLE.COM
```

El archivo `kpropd.acl` en los KDC esclavos que están siendo propagados por `slave-1` contendría la siguiente entrada:

```
host/slave-1.example.com@EXAMPLE.COM
```

## Administración del archivo intermedio

El *archivo intermedio* contiene la clave maestra para la base de datos de Kerberos, que se crea automáticamente al crear una base de datos de Kerberos. Si el archivo intermedio se daña, puede utilizar el comando `stash` de la utilidad `kdb5_util` para sustituir el archivo dañado. La única vez que debe eliminar un archivo intermedio es después de eliminar la base de datos de Kerberos con el comando `destroy` de `kdb5_util`. Debido a que el archivo intermedio no se elimina automáticamente con la base de datos, tiene que eliminarlo para finalizar la limpieza.

## ▼ Cómo eliminar un archivo intermedio

1 Conviértase en superusuario en el KDC que contiene el archivo intermedio.

2 Elimine el archivo intermedio.

```
# rm stash-file
```

Donde *stash-file* es la ruta al archivo intermedio. De manera predeterminada, el archivo intermedio se encuentra en `/var/krb5/.k5.dominio`.

---

**Nota** – Si necesita volver a crear el archivo intermedio, puede utilizar la opción `-f` del comando `kdb5_util`.

---

# Gestión de un KDC en un servidor de directorios LDAP

La mayoría de las tareas de administración del KDC que usan un servidor de directorios LDAP son las mismas que las tareas para el servidor DB2. Hay algunas tareas nuevas que son específicas para trabajar con LDAP.

TABLA 23–3 Configuración de servidores KDC para utilizar LDAP (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Configurar un KDC maestro	Configura y genera el servidor KDC maestro y la base de datos para un dominio mediante un proceso manual y un LDAP para el KDC.	<a href="#">“Cómo configurar un KDC para utilizar un servidor de datos LDAP” en la página 429</a>
Mezclar atributos de principales de Kerberos con tipos de clases de objeto que no son de Kerberos	Permite que la información almacenada con los registros de Kerberos se comparta con otras bases de datos LDAP.	<a href="#">“Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos” en la página 488</a>
Destruir un dominio	Elimina todos los datos asociados con un dominio.	<a href="#">“Cómo destruir un dominio en un servidor de directorios LDAP” en la página 489</a>

## ▼ Cómo mezclar atributos de principales de Kerberos en un tipo de clase de objeto que no es de Kerberos

Este procedimiento permite que los atributos de principales de Kerberos se asocien con tipos de clases de objeto que no son de Kerberos. En este procedimiento, los atributos `krbprincipalaux`, `krbTicketPolicyAux` y `krbPrincipalName` están asociados con la clase de objeto de personas.



En este procedimiento, se utilizan los siguientes parámetros de configuración:

- Servidor de directorios = `dsserver.example.com`
- Principal de usuario = `willf@EXAMPLE.COM`

### 1 Conviértase en superusuario.

### 2 Prepare cada entrada en la clase de objeto de personas.

Repita este paso para cada entrada.

```
cat << EOF | ldapmodify -h dsserver.example.com -D "cn=directory manager"
dn: uid=willf,ou=people,dc=example,dc=com
changetype: modify
objectClass: krbprincipalAux
objectClass: krbTicketPolicyAux
krbPrincipalName: willf@EXAMPLE.COM
EOF
```

### 3 Agregue un atributo de subárbol al contenedor del dominio.

Este paso permite buscar entradas de principales en el contenedor `ou=people,dc=example,dc=com`, así como en el contenedor `EXAMPLE.COM` predeterminado.

```
# kdb5_ldap_util -D "cn=directory manager" modify \
    -subtrees 'ou=people,dc=example,dc=com' -r EXAMPLE.COM
```

### 4 (Opcional) Si los registros del KDC están almacenados en DB2, migre las entradas de DB2.

#### a. Vuelque las entradas de DB2.

```
# kdb5_util dump > dumpfile
```

#### b. Cargue la base de datos en el servidor LDAP.

```
# kdb5_util load -update dumpfile
```

### 5 (Opcional) Agregue los atributos de los principales al KDC.

```
# kadmin.local -q 'addprinc willf'
```

## ▼ Cómo destruir un dominio en un servidor de directorios LDAP

Este procedimiento se puede utilizar si un servidor de directorios LDAP distinto se ha configurado para manejar un dominio.

### 1 Conviértase en superusuario.

### 2 Destruya el dominio.

```
# kdb5_ldap_util -D "cn=directory manager" destroy
```

# Aumento de la seguridad en servidores Kerberos

Siga estos pasos para aumentar la seguridad en servidores de aplicaciones Kerberos y en servidores KDC.

TABLA 23–4 Aumento de la seguridad en servidores Kerberos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Habilitar el acceso mediante la autenticación Kerberos	Restringe el acceso a la red a un servidor para permitir sólo la autenticación Kerberos.	<a href="#">“Cómo habilitar sólo aplicaciones Kerberizadas” en la página 490</a>
Restringir el acceso a los servidores KDC	Aumenta la seguridad de los servidores KDC y sus datos.	<a href="#">“Cómo restringir el acceso a servidores KDC” en la página 490</a>
Aumentar la seguridad de contraseñas utilizando un archivo de diccionario	Aumenta la seguridad de cualquier contraseña nueva comprobando la nueva contraseña con un diccionario.	<a href="#">“Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas” en la página 491</a>

## ▼ Cómo habilitar sólo aplicaciones Kerberizadas

Este procedimiento restringe el acceso a la red al servidor que está ejecutando telnet, ftp, rcp, rsh y rlogin para usar sólo las transacciones autenticadas de Kerberos.

**1 Cambie la propiedad exec para el servicio telnet.**

Agregue la opción -a user a la propiedad exec para telnet a fin de restringir el acceso a aquellos usuarios que pueden proporcionar información de autenticación válida.

```
# inetadm -m svc:/network/telnet:default exec="/usr/sbin/in.telnetd -a user"
```

**2 (Opcional) Si aún no está configurada, cambie la propiedad exec para el servicio telnet.**

Agregue la opción -a a la propiedad exec para ftp a fin de permitir sólo conexiones autenticadas de Kerberos.

```
# inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a"
```

**3 Deshabilite otros servicios.**

El daemon in.rshd y el daemon in.rlogind deben estar deshabilitados.

```
# svcadm disable network/shell
# svcadm disable network/login:rlogin
```

## ▼ Cómo restringir el acceso a servidores KDC

Tanto los servidores KDC maestros como los servidores KDC esclavos tienen copias de la base de datos del KDC almacenadas localmente. La restricción del acceso a estos servidores para que las bases de datos sean seguras es importante para la seguridad general de la instalación de Kerberos.

## 1 Deshabilite servicios remotos, según sea necesario.

Para proporcionar un servidor KDC seguro, todos los servicios de red que no son esenciales se deben deshabilitar. En función de la configuración, es posible que algunos de estos servicios ya estén deshabilitados. Compruebe el estado del servicio con el comando `svcs`. En la mayoría de los casos, los únicos servicios que se deberían ejecutar son `krb5kdc` y `kadmin` si el KDC es un maestro. Además, los servicios que utilizan el bucle de retorno `tli` (`ticlts`, `ticotsord` y `ticots`) pueden dejarse habilitados.

```
# svcadm disable network/comsat
# svcadm disable network/dtspc/tcp
# svcadm disable network/finger
# svcadm disable network/login:rlogin
# svcadm disable network/rexec
# svcadm disable network/shell
# svcadm disable network/talk
# svcadm disable network/tname
# svcadm disable network/uucp
# svcadm disable network/rpc_100068_2-5/rpc_udp
```

## 2 Restrinja el acceso al hardware que admite el KDC.

Para restringir el acceso físico, asegúrese de que el servidor KDC y su monitor se encuentren en una instalación segura. Los usuarios no deben poder acceder a este servidor de ninguna forma.

## 3 Almacene las copias de seguridad de la base de datos del KDC en discos locales o en los KDC esclavos.

Realice copias de seguridad en cinta del KDC sólo si las cintas están almacenadas de manera segura. Siga la misma práctica para las copias de los archivos `keytab`. Sería mejor almacenar estos archivos en un sistema de archivos local que no esté compartido con otros sistemas. El sistema de archivos de almacenamiento puede estar en el servidor KDC maestro o en cualquier KDC esclavo.

# ▼ Cómo utilizar un archivo de diccionario para aumentar la seguridad de contraseñas

Un archivo de diccionario puede ser utilizado por el servicio Kerberos para evitar que las palabras del diccionario se usen como contraseñas al crear nuevas credenciales. Impedir el uso de términos del diccionario como contraseñas hace que sea más difícil adivinar las contraseñas. De manera predeterminada, se utiliza el archivo `/var/krb5/kadm5.dict`, pero está vacío.

## 1 Conviértase en superusuario en el KDC maestro.

## 2 Edite el archivo de configuración del KDC (`kdc.conf`).

Necesita agregar una línea para indicar al servicio que utilice un archivo de diccionario. En este ejemplo, se utiliza el diccionario que se incluye con la utilidad `spell`. Consulte la página del comando `man kdc.conf(4)` para obtener una descripción completa del archivo de configuración.

```
kdc1 # cat /etc/krb5/kdc.conf
[kdcdefaults]
    kdc_ports = 88,750

[realms]
    EXAMPLE.COM = {
        profile = /etc/krb5/krb5.conf
        database_name = /var/krb5/principal
        admin_keytab = /etc/krb5/kadm5.keytab
        acl_file = /etc/krb5/kadm5.acl
        kadmind_port = 749
        max_life = 8h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        sunw_dbprop_enable = true
        sunw_dbprop_master_ulogsize = 1000
        dict_file = /usr/share/lib/dict/words
    }
```

## 3 Reinicie los daemons Kerberos.

```
kdc1 # svcadm restart -r network/security/krb5kdc
kdc1 # svcadm restart -r network/security/kadmin
```

## Mensajes de error y resolución de problemas de Kerberos

---

En este capítulo se proporcionan soluciones para mensajes de error que puede llegar a recibir cuando utiliza el servicio Kerberos. En este capítulo se brindan además algunos consejos sobre la resolución de diversos problemas. Esta es una lista de mensajes de error e información sobre resolución de problemas de este capítulo.

- “Mensajes de error de la herramienta SEAM” en la página 493
- “Mensajes de error comunes de Kerberos (A-M)” en la página 494
- “Mensajes de error comunes de Kerberos (N-Z)” en la página 502
- “Problemas con el formato del archivo `krb5.conf`” en la página 506
- “Problemas al propagar la base de datos de Kerberos” en la página 506
- “Problemas al montar un sistema de archivos NFS Kerberizado” en la página 507
- “Problemas de autenticación como `root`” en la página 507
- “Observación de asignación de credenciales GSS a credenciales UNIX” en la página 508

## Mensajes de error de Kerberos

En esta sección se proporciona información acerca de los mensajes de error de Kerberos, incluido el motivo por el cual se produce cada error y una forma de solucionarlo.

### Mensajes de error de la herramienta SEAM

No se puede ver la lista de principales o políticas; utilice el campo Nombre.

**Causa:** El principal `admin` con el que inició sesión no tiene el privilegio de lista (`l`) en el archivo ACL de Kerberos (`kadm5.acl`). Por lo tanto, no puede ver la lista de principales o la lista de políticas.

**Solución:** Debe escribir los nombres de políticas y principales en el campo Nombre para trabajar con ellos o debe iniciar sesión con un principal con los privilegios apropiados.

JNI: creación de matriz Java no satisfactoria

JNI: búsqueda de clase Java no satisfactoria

JNI: búsqueda de campo Java no satisfactoria

JNI: búsqueda de método Java no satisfactoria

JNI: búsqueda de objeto Java no satisfactoria

JNI: búsqueda de campo de objeto Java no satisfactoria

JNI: acceso a cadena Java no satisfactorio

JNI: creación de cadena Java no satisfactoria

**Causa:** Existe un problema grave con la interfaz nativa de Java que utiliza la herramienta SEAM (gkadmin).

**Solución:** Salga de gkadmin y vuelva a iniciarlo. Si el problema persiste, informe acerca del error.

## Mensajes de error comunes de Kerberos (A-M)

En esta sección se proporciona una lista en orden alfabético (A-M) de mensajes de error comunes de los comandos Kerberos, los daemons Kerberos, la estructura PAM, la interfaz GSS, el servicio NFS y la biblioteca Kerberos.

Todos los sistemas de autenticación están deshabilitados; se ha rechazado la conexión

**Causa:** Esta versión de rlogind no admite ningún mecanismo de autenticación.

**Solución:** Asegúrese de que rlogind se invoque con la opción -k.

Otro mecanismo de autenticación se debe utilizar para acceder a este host

**Causa:** La autenticación no se pudo llevar a cabo.

**Solución:** Asegúrese de que el cliente use el mecanismo Kerberos V5 para la autenticación.

Error en la negociación de autenticación, que es necesaria para el cifrado.

Adiós.

**Causa:** No se pudo negociar la autenticación con el servidor.

**Solución:** Inicie la depuración de autenticación mediante la invocación del comando telnet con el comando toggle authdebug y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

Nombre de host de servidor de administración krb5 incorrecto al inicializar la interfaz kadmind

**Causa:** Un nombre de host no válido está configurado para admin\_server en el archivo krb5.conf.

**Solución:** Asegúrese de que el nombre de host correcto para el KDC maestro se especifique en la línea `admin_server` en el archivo `krb5.conf`.

Valor de vigencia incorrecto

**Causa:** El valor de vigencia especificado no es válido o su formato es incorrecto.

**Solución:** Asegúrese de que el valor proporcionado sea consistente con la sección de formatos de hora en la página del comando `man kinit(1)`.

Valor de hora de inicio incorrecto

**Causa:** El valor de hora de inicio especificado no es válido o su formato es incorrecto.

**Solución:** Asegúrese de que el valor proporcionado sea consistente con la sección de formatos de hora en la página del comando `man kinit(1)`.

No es posible contactar con ningún KDC para el dominio solicitado

**Causa:** Ningún KDC respondió en el dominio solicitado.

**Solución:** Asegúrese de que al menos se pueda acceder a un KDC (maestro o esclavo) o que el daemon `krb5kdc` se ejecute en los KDC. Compruebe el archivo `/etc/krb5/krb5.conf` para la lista de KDC configurados (`kdc = kdc-name`).

No es posible determinar el dominio para el host

**Causa:** Kerberos no puede determinar el nombre de dominio para el host.

**Solución:** Asegúrese de que haya un nombre de dominio predeterminado o que las asignaciones de nombre de dominio estén configuradas en el archivo de configuración de Kerberos (`krb5.conf`).

No es posible encontrar el KDC para el dominio solicitado

**Causa:** No se encontró ningún KDC en el dominio solicitado.

**Solución:** Asegúrese de que el archivo de configuración de Kerberos (`krb5.conf`) especifique un KDC en la sección `realm`.

No se puede inicializar el dominio *nombre de dominio*

**Causa:** El KDC podría no tener un archivo intermedio.

**Solución:** Asegúrese de que el KDC tenga un archivo intermedio. En caso contrario, cree un archivo intermedio mediante el comando `kdb5_util` e intente reiniciar el comando `krb5kdc`.

No es posible resolver el KDC para el dominio solicitado

**Causa:** Kerberos no puede determinar ningún KDC para el dominio.

**Solución:** Asegúrese de que el archivo de configuración de Kerberos (`krb5.conf`) especifique un KDC en la sección `realms`.

No es posible volver a utilizar la contraseña

**Causa:** Este principal ya ha utilizado la contraseña que especificó.

**Solución:** Seleccione una contraseña que no se haya elegido antes, al menos no dentro del número de contraseñas que se mantiene en la base de datos de KDC para cada principal. La política del principal aplica esta política.

No se pueden obtener credenciales reenviadas

**Causa:** No se pudo establecer el reenvío de credenciales.

**Solución:** Asegúrese de que el principal tenga credenciales que se puedan reenviar.

No se puede abrir/encontrar el archivo de configuración de Kerberos

**Causa:** El archivo de configuración de Kerberos (`krb5.conf`) no estaba disponible.

**Solución:** Asegúrese de que el archivo `krb5.conf` esté disponible en la ubicación correcta y tenga los permisos correctos. `root` debería poder escribir en este archivo y el resto debería poder leerlo.

El cliente no proporcionó la suma de comprobación requerida--se rechazó la conexión

**Causa:** No se negoció la autenticación con suma de comprobación con el cliente. Es posible que el cliente use un protocolo Kerberos V5 obsoleto que no admite conexión inicial.

**Solución:** Asegúrese de que el cliente use un protocolo Kerberos V5 que admita conexión inicial.

Discrepancia de dominios de cliente/servidor en solicitud de ticket inicial

**Causa:** Se produjo una discrepancia de dominios entre el cliente y el servidor en la solicitud de ticket inicial.

**Solución:** Asegúrese de que el servidor con el que se comunica esté en el mismo dominio que el cliente o que las configuraciones de dominios sean correctas.

El cliente o el servidor tienen una clave nula

**Causa:** El principal tiene una clave nula.

**Solución:** Modifique el principal para que tenga una clave no nula mediante el comando `cpw` de `kadmin`.

Error de comunicación con el servidor al inicializar la interfaz `kadmin`

**Causa:** El host que se especificó para el servidor de administración, también denominado KDC maestro, no tiene los daemons `kadmin` en ejecución.



**Solución:** Asegúrese de que ha especificado el nombre de host correcto para el KDC maestro. Si especificó el nombre de host correcto, asegúrese de que `kadmind` esté en ejecución en el KDC maestro que especificó.

#### Permisos del archivo de antememoria de credenciales incorrectos

**Causa:** No tiene los permisos de lectura o escritura apropiados en la antememoria de credenciales (`/tmp/krb5cc_uid`).

**Solución:** Asegúrese de tener los permisos de lectura y escritura en la antememoria de credenciales.

#### Operación de E/S de antememoria de credenciales no satisfactoria XXX

**Causa:** Kerberos tuvo un problema al escribir en la antememoria de credenciales del sistema (`/tmp/krb5cc_uid`).

**Solución:** Asegúrese de que la antememoria de credenciales no se haya eliminado y de que haya espacio libre en el dispositivo mediante el comando `df`.

#### Comprobación de integridad de la desencriptación no satisfactoria

**Causa:** Es posible que tenga un ticket no válido.

**Solución:** Verifique estas condiciones:

- Asegúrese de que las credenciales sean válidas. Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.
- Asegúrese de que el host de destino tenga un archivo keytab con la versión correcta de la clave del servicio. Use `kadmin` para ver el número de versión de clave del principal de servicio (por ejemplo, `host/FQDN-nombre de host`) en la base de datos de Kerberos. Asimismo, utilice `klist -k` en el host de destino para asegurarse de que tenga el mismo número de versión de clave.

No se pudo habilitar el cifrado. Adiós.

**Causa:** No se pudo negociar el cifrado con el servidor.

**Solución:** Inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle encdebug` y observe los mensajes de depuración para obtener más pistas.

#### Error en la obtención de la antememoria de credenciales

**Causa:** Durante la inicialización de `kadmin`, se produjo un error cuando `kadmin` intentó obtener credenciales para el principal `admin`.

**Solución:** Asegúrese de haber utilizado el principal y la contraseña correctos cuando ejecutó `kadmin`.

Campo demasiado largo para esta implementación

**Causa:** El tamaño del mensaje que enviaba una aplicación Kerberizada era demasiado largo. Este error se puede generar si el protocolo de transporte es UDP. Que tiene un tamaño máximo de mensaje de 65535 bytes de manera predeterminada. Además, hay límites en los campos individuales dentro de un mensaje de protocolo que se envía por el servicio Kerberos.

**Solución:** Verifique que no ha restringido el transporte a UDP en el archivo `/etc/krb5/kdc.conf` del servidor KDC.

Error de GSS-API (o Kerberos)

**Causa:** Este mensaje es un mensaje de error genérico de GSS-API o Kerberos y puede ser causado por diversos problemas.

**Solución:** Compruebe el archivo `/var/krb5/kdc.log` para encontrar el mensaje de error más específico que se registró cuando se produjo este error.

No es posible poner en forma canónica el nombre de host

**Causa:** El cliente Kerberos no puede encontrar el nombre de host completo para el servidor.

**Solución:** Asegúrese de que el nombre de host del servidor esté definido en DNS y que las asignaciones de nombre de host a dirección y de dirección a nombre de host sean consistentes.

Ticket entre dominios no permitido

**Causa:** El ticket enviado no tenía los dominios cruzados correctos. Es posible que los dominios no tengan configuradas las relaciones de confianza correctas.

**Solución:** Asegúrese de que los dominios que utilice tengan las relaciones de confianza correctas.

Formato no adecuado del archivo de configuración de Kerberos

**Causa:** El archivo de configuración de Kerberos tiene entradas no válidas.

**Solución:** Asegúrese de que todas las relaciones en el archivo `krb5.conf` estén seguidas del signo "=" y un valor. Asimismo, verifique que los paréntesis estén presentes en pares para cada subsección.

Tipo de suma de comprobación en mensaje inadecuado

**Causa:** El mensaje contenía un tipo de suma de comprobación no válido.

**Solución:** Compruebe qué tipos de suma de comprobación se especifican en los archivos `krb5.conf` y `kdc.conf`.

**Dirección de red incorrecta**

**Causa:** Existe una discrepancia en la dirección de red. La dirección de red en el ticket que se reenviaba era distinta de la dirección de red donde se procesó el ticket. Este mensaje puede aparecer cuando los tickets se reenvían.

**Solución:** Asegúrese de que las direcciones de red sean correctas. Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

**Se ha proporcionado una credencial no válida****Clave de servicio no disponible**

**Causa:** Es posible que el ticket de servicio en la antememoria de credenciales sea incorrecto.

**Solución:** Destruya la antememoria de credenciales actual y vuelva a ejecutar `kinit` antes de intentar utilizar este servicio.

**Indicador no válido para la modalidad de bloqueo de archivo**

**Causa:** Se produjo un error de Kerberos interno.

**Solución:** Informe acerca del error.

**Tipo de mensaje especificado para la codificación no válido**

**Causa:** Kerberos no pudo reconocer el tipo de mensaje que se envió mediante la aplicación Kerberizada.

**Solución:** Si utiliza una aplicación Kerberizada desarrollada por su sitio o un vendedor, asegúrese de que la aplicación utilice Kerberos correctamente.

**Número de clases de caracteres no válido**

**Causa:** La contraseña que especificó para el principal no contiene suficientes clases de contraseñas, como si se aplica mediante la política del principal.

**Solución:** Asegúrese de especificar una contraseña con el número mínimo de clases de contraseñas que la política necesita.

**Error de KADM: Asignación de memoria no satisfactoria**

**Causa:** No hay suficiente memoria para ejecutar `kadmin`.

**Solución:** Libere memoria e intente ejecutar `kadmin` nuevamente.

**Kadmin: Tipo de cifrado incorrecto al cambiar la clave de host/<FQDN>**

**Causa:** Se incluyen más tipos de cifrado de manera predeterminada en la versión base de Solaris 10 8/07. Los clientes pueden solicitar tipos de cifrado que posiblemente no sean admitidos por un KDC que ejecuta una versión anterior del software.

**Solución:** Existen varias soluciones para este problema. La más fácil de implementar es la que se enumera primero:

1. Agregar los paquetes SUNWcry y SUNWcryr al servidor KDC. Esto aumenta el número de tipos de cifrado admitidos por KDC.
2. Establecer `permitted_encetypes` en `krb5.conf` en el cliente si no desea incluir el tipo de cifrado `aes256`. Será necesario realizar este paso en cada nuevo cliente.

KDC no puede realizar la opción solicitada

**Causa:** KDC no permite la opción solicitada. Un posible problema podría ser que las opciones de posfechado o reenvío se hayan solicitado y KDC no las haya permitido. Otro problema podría ser que usted solicitó la renovación de un TGT, pero no disponía de un TGT renovable.

**Solución:** Determine si solicita una opción que KDC no permite o un tipo de ticket que no se encuentra disponible.

La política de KDC rechaza la solicitud

**Causa:** La política de KDC no permite la solicitud. Por ejemplo, la solicitud al KDC no tenía una dirección IP en su solicitud. O se solicitó el reenvío pero el KDC no lo permitía.

**Solución:** Asegúrese de utilizar `kinit` con las opciones correctas. Si es necesario, modifique la política que está asociada con el principal o cambie los atributos del principal para permitir la solicitud. Puede modificar la política o el principal mediante `kadmin`.

La respuesta de KDC no coincidió con lo que se esperaba

**Causa:** La respuesta de KDC no contenía el nombre de principal esperado u otros valores en la respuesta eran incorrectos.

**Solución:** Asegúrese de que el KDC con el que se comunica cumpla con RFC4120, que la solicitud que envía sea una solicitud Kerberos V5 o que el KDC esté disponible.

`kdestroy`: No ha sido posible obtener el nombre de principal de la antememoria

**Causa:** La antememoria de credenciales no se encuentra o está dañada.

**Solución:** Compruebe que la ubicación de la antememoria proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante `kinit`, si es necesario.

`kdestroy`: No se ha encontrado un archivo de antememoria de credenciales al destruir la antememoria

**Causa:** La antememoria de credenciales (`/tmp/krb5c_uid`) no se encuentra o está dañada.

**Solución:** Compruebe que la ubicación de la antememoria proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante `kinit`, si es necesario.

`kdestroy`: No se ha borrado el aviso de caducidad de TGT

**Causa:** La antememoria de credenciales no se encuentra o está dañada.

**Solución:** Compruebe que la ubicación de la antememoria proporcionada sea correcta. Elimine y obtenga un nuevo TGT mediante `kinit`, si es necesario.

#### Error de autenticación de Kerberos

**Causa:** La contraseña de Kerberos es incorrecta o es posible que la contraseña no esté sincronizada con la contraseña de UNIX.

**Solución:** Si la contraseña no está sincronizada, debe especificar una contraseña diferente para completar la autenticación Kerberos. Es posible que el usuario haya olvidado su contraseña original.

#### Kerberos V5 rechaza la autenticación

**Causa:** No se pudo negociar la autenticación con el servidor.

**Solución:** Inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle authdebug` y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

#### Entrada de tabla de claves no encontrada

**Causa:** No existe ninguna entrada para el principal de servicio en el archivo `keytab` del servidor de aplicación de red.

**Solución:** Agregue el principal de servicio apropiado al archivo `keytab` del servidor para que pueda proporcionar el servicio Kerberizado.

#### El número de versión de clave para el principal en la tabla de claves es incorrecto

**Causa:** Una versión de clave del principal en el archivo `keytab` es diferente de la versión en la base de datos de Kerberos. Es posible que una clave del servicio haya cambiado o que utilice un ticket de servicio antiguo.

**Solución:** Si la clave del servicio ha cambiado (por ejemplo, mediante el uso de `kadmin`), deberá extraer la nueva clave y almacenarla en el archivo `keytab` del host donde se ejecuta el servicio.

Asimismo, es posible que utilice un ticket de servicio antiguo que tiene una clave anterior. Es posible que desee ejecutar el comando `kdestroy` y luego el comando `kinit` nuevamente.

#### Kinit: Error de obtención de nombre de host

**Causa:** Un error en la configuración de red local provoca el fallo de `kinit`.

**Solución:** Asegúrese de que el host esté configurado correctamente.

#### Inicio de sesión: `load_modules`: no se puede abrir el módulo `/usr/lib/security/pam_krb5.so.1`

**Causa:** No se encuentra el módulo PAM de Kerberos o no es un binario ejecutable válido.

**Solución:** Asegúrese de que el módulo PAM de Kerberos esté en el directorio `/usr/lib/security` y que sea un binario ejecutable válido. Además, asegúrese de que el archivo `/etc/pam.conf` contenga la ruta correcta a `pam_krb5.so.1`.

Detectado bucle dentro de `krb5_get_in_tkt`

**Causa:** Kerberos realizó varios intentos de obtener los tickets iniciales pero no tuvo éxito.

**Solución:** Asegúrese de que al menos un KDC responda a las solicitudes de autenticación.

La clave maestra no coincide con la base de datos

**Causa:** El volcado de base de datos cargado no se creó a partir de una base de datos que contiene la clave maestra. La clave maestra se encuentra en `/var/krb5/.k5.REALM`.

**Solución:** Asegúrese de que la clave maestra en el volcado de base de datos cargado coincida con la clave maestra ubicada en `/var/krb5/.k5.REALM`.

Credencial concordante no encontrada

**Causa:** La credencial concordante para su solicitud no se ha encontrado. Su solicitud necesita credenciales que no están disponibles en la antememoria de credenciales.

**Solución:** Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

Mensaje fuera de orden

**Causa:** Mensajes que se enviaron utilizando privacidad de orden secuencial llegaron fuera de orden. Es posible que algunos mensajes se hayan perdido en el tránsito.

**Solución:** Debe reinicializar la sesión de Kerberos.

Canal de mensajes modificado

**Causa:** Existe una discrepancia entre la suma de comprobación calculada y la suma de comprobación de mensaje. Es posible que el mensaje se haya modificado durante el tránsito, lo que puede indicar una infracción de seguridad.

**Solución:** Asegúrese de que los mensajes se envíen a través de la red correctamente. Debido a que este mensaje también puede indicar la posible alteración de mensajes durante el envío, destruya los tickets mediante `kdestroy` y reinicialice los servicios Kerberos que utiliza.

## Mensajes de error comunes de Kerberos (N-Z)

En esta sección se proporciona una lista en orden alfabético (N-Z) de mensajes de error comunes de los comandos Kerberos, los daemons Kerberos, la estructura PAM, la interfaz GSS, el servicio NFS y la biblioteca Kerberos.

No se ha encontrado un archivo de antememoria de credenciales

**Causa:** Kerberos no pudo encontrar la antememoria de credenciales (`/tmp/krb5cc_uid`).

**Solución:** Asegúrese de que el archivo de credenciales exista y se pueda leer. En caso contrario, intente ejecutar `kinit` nuevamente.

No se han proporcionado credenciales, no estaban disponibles o eran inaccesibles

No se encontró la antememoria de credenciales

**Causa:** La antememoria de credenciales del usuario es incorrecta o no existe.

**Solución:** El usuario debe ejecutar `kinit` antes de intentar iniciar el servicio.

No se han proporcionado credenciales, no estaban disponibles o eran inaccesibles

Ningún principal en keytab coincide con el nombre deseado

**Causa:** Se ha producido un error al intentar autenticar el servidor.

**Solución:** Asegúrese de que el host o principal de servicio estén en el archivo keytab del servidor.

La operación requiere el privilegio "*privilegio*"

**Causa:** El principal `admin` que estaba en uso no tenía el privilegio adecuado configurado en el archivo `kadm5.acl`.

**Solución:** Utilice un principal que tenga los privilegios adecuados. O bien, configure el principal que estaba en uso para que tenga los privilegios adecuados mediante la modificación del archivo `kadm5.acl`. Normalmente, un principal con `/admin` como parte de su nombre tiene los privilegios adecuados.

PAM-KRB5 (auth): `krb5_verify_init_creds` no satisfactorio: Entrada de tabla de claves no encontrada

**Causa:** La aplicación remota intentó leer el principal de servicio del host en el archivo local `/etc/krb5/krb5.keytab`, pero no existe.

**Solución:** Agregue el principal de servicio del host al archivo keytab del host.

La contraseña está en el diccionario de contraseñas

**Causa:** La contraseña que especificó está en un diccionario de contraseñas que está en uso. La contraseña no es una buena elección para una contraseña.

**Solución:** Seleccione una contraseña que tenga una mezcla de clases de contraseñas.

Permiso denegado en código de antememoria de reproducción

**Causa:** No se pudo abrir la antememoria de reproducción del sistema. Es posible que el servidor se haya ejecutado por primera vez con un ID de usuario diferente del ID de usuario actual.

**Solución:** Asegúrese de que la antememoria de reproducción tenga los permisos adecuados. La antememoria de reproducción se almacena en el host donde la aplicación de servidor Kerberizada está en ejecución. El archivo de antememoria de reproducción se denomina

`/var/krb5/rcache/rc_nombre_servicio_uid` para usuarios no root. Para los usuarios root, el archivo de antememoria de reproducción se denomina `/var/krb5/rcache/root/rc_nombre_servicio`.

#### Discrepancia de versión de los protocolos

**Causa:** Lo más probable es que una solicitud de Kerberos V4 se haya enviado al KDC. El servicio Kerberos sólo admite el protocolo Kerberos V5.

**Solución:** Asegúrese de que las aplicaciones utilicen el protocolo Kerberos V5.

#### La solicitud es una reproducción

**Causa:** La solicitud ya se ha enviado a este servidor y ya se ha procesado. Es posible que los tickets hayan sido robados y alguien esté intentando volver a utilizar los tickets.

**Solución:** Espere unos minutos y vuelva a emitir la solicitud.

#### El principal y el ticket solicitados no concuerdan

**Causa:** El principal de servicio al que se conecta y el ticket de servicio que posee no concuerdan.

**Solución:** Asegúrese de que DNS funcione correctamente. Si utiliza el software de otro proveedor, asegúrese de que el software utilice los nombres de principal correctamente.

#### Versión de protocolo solicitada no admitida

**Causa:** Lo más probable es que una solicitud de Kerberos V4 se haya enviado al KDC. El servicio Kerberos sólo admite el protocolo Kerberos V5.

**Solución:** Asegúrese de que las aplicaciones utilicen el protocolo Kerberos V5.

#### El servidor rechazó negociar la autenticación, que es necesaria para el cifrado. Adiós.

**Causa:** La aplicación remota no es capaz o se ha configurado para no aceptar la autenticación Kerberos del cliente.

**Solución:** Proporcione una aplicación remota que puede negociar la autenticación o configurar la aplicación para que utilice los indicadores adecuados para activar la autenticación.

#### El servidor rechazó negociar el cifrado. Adiós.

**Causa:** No se pudo negociar el cifrado con el servidor.

**Solución:** Inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle encdebug` y observe los mensajes de depuración para obtener más pistas.



El servidor ha rechazado la autenticación (durante el intercambio de sendauth)

**Causa:** El servidor con el que intenta comunicarse rechazó la autenticación. La mayoría de las veces, este error se produce durante la propagación de la base de datos de Kerberos. Algunas de las causas comunes podrían ser problemas con el archivo `kpropd.acl`, DNS o el archivo `keytab`.

**Solución:** Si recibe este error cuando ejecuta aplicaciones que no sean `kprop`, investigue si el archivo `keytab` del servidor es correcto.

El ticket no es para nosotros

El ticket y el autenticador no concuerdan

**Causa:** Existe una discrepancia entre el ticket y el autenticador. Es posible que el nombre del principal en la solicitud no haya coincidido con el nombre del principal de servicio. Ya sea porque el ticket se enviaba con un nombre FQDN del principal mientras que el servicio esperaba un nombre no FQDN, o se envió un nombre no FQDN cuando el servicio esperaba un nombre FQDN.

**Solución:** Si recibe este error cuando ejecuta aplicaciones que no sean `kprop`, investigue si el archivo `keytab` del servidor es correcto.

Ticket caducado

**Causa:** El tiempo del ticket ha caducado.

**Solución:** Destruya los tickets con `kdestroy` y cree nuevos tickets con `kinit`.

El ticket no posee las condiciones exigidas para poder ser posfechado

**Causa:** El principal no permite que los tickets sean posfechados.

**Solución:** Modifique el principal con `kadmin` para permitir que sea posfechado.

Ticket no válido todavía

**Causa:** El ticket posfechado no es válido todavía.

**Solución:** Cree un nuevo ticket con la fecha correcta o espere hasta que el ticket actual sea válido.

Detectado archivo de entrada truncado

**Causa:** El archivo de volcado de base de datos que se utilizaba en la operación no era un archivo de volcado completo.

**Solución:** Cree el archivo de volcado de nuevo o utilice un archivo de volcado de base de datos diferente.

No se puede autenticar al usuario de manera segura ... salir

**Causa:** No se pudo negociar la autenticación con el servidor.

**Solución:** Inicie la depuración de autenticación mediante la invocación del comando `telnet` con el comando `toggle authdebug` y observe los mensajes de depuración para obtener más pistas. Además, asegúrese de tener credenciales válidas.

Principal incorrecto en solicitud

**Causa:** Había un nombre de principal no válido en el ticket. Este error puede indicar que hay un problema de DNS o FQDN.

**Solución:** Asegúrese de que el principal del servicio coincida con el principal en el ticket.

## Resolución de problemas de Kerberos

En esta sección se proporciona información acerca de la resolución de problemas del software Kerberos.

### Problemas con el formato del archivo `krb5.conf`

Si el archivo `krb5.conf` no tiene el formato correcto, es posible que se muestre el siguiente mensaje de error en la terminal o el archivo de registro:

```
Improper format of Kerberos configuration file while initializing krb5 library
```

Si hay un problema con el formato del archivo `krb5.conf`, los servicios asociados podrían quedar vulnerables a ataques. Debe solucionar el problema antes de permitir que se utilicen funciones de Kerberos.

### Problemas al propagar la base de datos de Kerberos

Si la propagación de la base de datos de Kerberos falla, pruebe `/usr/bin/rlogin -x` entre el KDC esclavo y KDC maestro, y del KDC maestro al servidor KDC esclavo.

Si los KDC se han configurado para restringir el acceso, `rlogin` está deshabilitado y no se puede utilizar para solucionar este problema. Para habilitar `rlogin` en un KDC, debe habilitar el servicio `eklogin`.

```
# svcadm enable svc:/network/login:eklogin
```

Una vez solucionado el problema, necesita deshabilitar el servicio `eklogin`.

Si `rlogin` no funciona, es posible que los problemas se deban a los archivos `keytab` en los KDC. Si `rlogin` funciona, el problema no se encuentra en el archivo `keytab` o el servicio de nombres, porque `rlogin` y el software de propagación utilizan el mismo principal `host/nombre de host`. En este caso, asegúrese de que el archivo `krb5.conf` sea correcto.

## Problemas al montar un sistema de archivos NFS Kerberizado

- Si el montaje de un sistema de archivos NFS Kerberizado falla, asegúrese de que el archivo `/var/ncache/root` exista en el servidor NFS. Si el sistema de archivos no es propiedad de `root`, elimínelo e intente el montaje nuevamente.
- Si tiene un problema al acceder a un sistema de archivos NFS Kerberizado, asegúrese de que el servicio `gssd` esté habilitado en el sistema y el servidor NFS.
- Si ve el mensaje de error `invalid argument` o `bad directory` cuando intenta acceder a un sistema de archivos NFS Kerberizado, posiblemente el problema sea que no utiliza un nombre DNS completo cuando intenta montar el sistema de archivos NFS. El `host` que se monta no es el mismo que el nombre de `host` parte del principal de servicio en el archivo `keytab` del servidor.

Este problema también puede ocurrir si el servidor tiene varias interfaces Ethernet y ha configurado DNS para que utilice un esquema "nombre por interfaz" en lugar de un esquema "varios registros de dirección por host". Para el servicio Kerberos, debe configurar varios registros de dirección por host como se indica a continuación<sup>1</sup>:

```
my.host.name.      A      1.2.3.4
                  A      1.2.4.4
                  A      1.2.5.4

my-en0.host.name.  A      1.2.3.4
my-en1.host.name.  A      1.2.4.4
my-en2.host.name.  A      1.2.5.4

4.3.2.1           PTR    my.host.name.
4.4.2.1           PTR    my.host.name.
4.5.2.1           PTR    my.host.name.
```

En este ejemplo, la configuración permite una referencia a las diferentes interfaces y a un único principal de servicio en lugar de tres principales de servicio en el archivo `keytab` del servidor.

## Problemas de autenticación como root

Si falla la autenticación cuando intenta convertirse en superusuario en el sistema y ya ha agregado el principal `root` al archivo `keytab` del `host`, hay dos posibles problemas que debe comprobar. En primer lugar, asegúrese de que el principal `root` en el archivo `keytab` tenga un nombre de `host` completo como su instancia. Si es así, compruebe el archivo `/etc/resolv.conf` para asegurarse de que el sistema esté correctamente configurado como un cliente DNS.

<sup>1</sup> Ken Hornstein, "Kerberos FAQ" [<http://www.cmf.nrl.navy.mil/CCS/people/kenh/kerberos-faq.html#kerbdns>], se accedió el 10 de marzo de 2010.

## Observación de asignación de credenciales GSS a credenciales UNIX

Para poder supervisar las asignaciones de credenciales, primero elimine el comentario de esta línea del archivo `/etc/gss/gsscred.conf`.

```
SYSLOG_UID_MAPPING=yes
```

Luego, indique al servicio `gssd` que obtenga información del archivo `/etc/gss/gsscred.conf`.

```
# pkill -HUP gssd
```

Ahora debería poder controlar las asignaciones de credenciales como `gssd` las solicita. Las asignaciones son registradas por `syslogd` si el archivo `syslog.conf` está configurado para la utilidad de sistema `auth` con el nivel de seguridad `debug`.

## Administración de las políticas y los principales de Kerberos (tareas)

---

En este capítulo se brindan los procedimientos para administrar los principales y las políticas que están relacionadas con ellos. En este capítulo también muestra cómo administrar un archivo keytab del host.

Este capítulo debe ser utilizado por cualquier persona que necesite administrar principales y políticas. Antes de utilizar este capítulo, debe estar familiarizado con los principales y las políticas, incluida cualquier consideración sobre la planificación. Consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#) y el [Capítulo 22, “Planificación del servicio Kerberos”](#), respectivamente.

A continuación se indica la información contenida en este capítulo:

- “[Maneras de administrar las políticas y los principales de Kerberos](#)” en la página 509
- “[Herramienta SEAM](#)” en la página 510
- “[Administración de los principales de Kerberos](#)” en la página 514
- “[Administración de las políticas de Kerberos](#)” en la página 528
- “[Referencia de la herramienta SEAM](#)” en la página 537
- “[Administración de los archivos keytab](#)” en la página 542

## Maneras de administrar las políticas y los principales de Kerberos

La base de datos de Kerberos en el KDC maestro contiene todos los principales de Kerberos del dominio, sus contraseñas, sus políticas y otra información administrativa. Para crear y eliminar los principales, y modificar sus atributos, puede utilizar el comando `kadmin` o `gkadmin`.

El comando `kadmin` proporciona una interfaz de línea de comandos interactiva que le permite mantener los principales, las políticas y los archivos `keytab` de Kerberos. Hay dos versiones del comando `kadmin`:

- `kadmin`: utiliza la autenticación de Kerberos para funcionar de manera segura desde cualquier parte de la red
- `kadmin.local`: se debe ejecutar directamente en el KDC maestro

Además de que `kadmin` usa Kerberos para autenticar el usuario, las capacidades de las dos versiones son idénticas. La versión local es necesaria para que usted pueda configurar una parte suficiente de la base de datos para poder utilizar la versión remota.

Asimismo, la versión de Oracle Solaris proporciona la herramienta SEAM, `gkadmin`, que es una interfaz gráfica de usuario (GUI) interactiva que proporciona, básicamente, las mismas capacidades que el comando `kadmin`. Para obtener más información, consulte [“Herramienta SEAM” en la página 510](#).

## Herramienta SEAM

La herramienta SEAM (`gkadmin`) es una interfaz gráfica de usuario (GUI) interactiva que permite mantener los principales y las políticas de Kerberos. Esta herramienta proporciona en gran parte las mismas funciones que el comando `kadmin`. Sin embargo, la herramienta no admite la gestión de los archivos `keytab`. Debe utilizar el comando `kadmin` para administrar los archivos `keytab`, lo cual se describe en [“Administración de los archivos `keytab`” en la página 542](#).

De manera similar al comando `kadmin`, la herramienta SEAM utiliza la RPC cifrada y la autenticación de Kerberos para trabajar de manera segura en cualquier parte de la red. La herramienta SEAM le permite realizar las siguientes acciones:

- Crear nuevos principales basados en los valores predeterminados o en los principales existentes.
- Crear nuevas políticas basadas en políticas existentes.
- Agregar comentarios para los principales.
- Configurar valores predeterminados para la creación de principales nuevos.
- Iniciar sesión como otro principal sin salir de la herramienta.
- Imprimir o guardar listas de principales y listas de políticas.
- Consultar y buscar listas de principales y listas de políticas.

La herramienta SEAM también proporciona ayuda contextual y ayuda general en pantalla.

Los siguientes mapas de tareas ofrecen consejos sobre las distintas tareas que puede realizar con la herramienta SEAM:

- [“Administración de los principales de Kerberos \(mapa de tareas\)” en la página 514](#)
- [“Administración de las políticas de Kerberos \(mapa de tareas\)” en la página 528](#)

También, puede ir a [“Descripción de los paneles de la herramienta SEAM” en la página 537](#) para obtener descripciones de todos los atributos de principales y atributos de políticas que puede especificar o ver en la herramienta SEAM.

## Equivalentes de línea de comandos de la herramienta SEAM

En esta sección se muestran los comandos `kadmin` que proporcionan las mismas capacidades que la herramienta SEAM. Estos comandos se puede utilizar sin ejecutar un sistema de ventana X. Aunque la mayoría de los procedimientos de este capítulo utilizan la herramienta SEAM, muchos procedimientos también proporcionan ejemplos correspondientes que utilizan equivalentes de línea de comandos.

TABLA 25-1 Equivalentes de línea de comandos de la herramienta SEAM

Procedimiento de la herramienta SEAM	Comando <code>kadmin</code> equivalente
Ver lista de principales	<code>list_principals</code> o <code>get_principals</code>
Ver atributos de un principal	<code>get_principal</code>
Crear un principal nuevo	<code>add_principal</code>
Duplicar un principal	No hay equivalente de línea de comandos
Modificar un principal	<code>modify_principal</code> o <code>change_password</code>
Suprimir un principal	<code>delete_principal</code>
Configurar valores predeterminados para crear principales nuevos	No hay equivalente de línea de comandos
Ver lista de políticas	<code>list_policies</code> o <code>get_policies</code>
Ver atributos de una política	<code>get_policy</code>
Crear una política nueva	<code>add_policy</code>
Duplicar una política	No hay equivalente de línea de comandos
Modificar una política	<code>modify_policy</code>
Suprimir una política	<code>delete_policy</code>

## El único archivo modificado por la herramienta SEAM

El único archivo que modifica la herramienta SEAM es el archivo `$HOME/.gkadmin`. Este archivo contiene los valores predeterminados para la creación de principales nuevos. Puede actualizar este archivo seleccionando Properties en el menú Edit.

## Funciones de impresión y ayuda en pantalla de la herramienta SEAM

La herramienta SEAM proporciona funciones de impresión y de ayuda en pantalla. Desde el menú Print, puede enviar lo siguiente a una impresora o un archivo:

- Lista de los principales disponibles en el KDC maestro especificado
- Lista de políticas disponibles en el KDC maestro especificado
- El principal seleccionado actualmente o el principal cargado
- La política seleccionada actualmente o la política cargada

Desde el menú Help puede acceder a la ayuda contextual y a la ayuda general. Al seleccionar la opción Context-Sensitive Help del menú Help, aparece la ventana Context-Sensitive Help y la herramienta cambia al modo de ayuda. En el modo de ayuda, al hacer clic en cualquier campo, etiqueta o botón de la ventana, aparece ayuda sobre esa opción en la ventana Help. Para volver al modo normal de la herramienta, haga clic en Dismiss en la ventana Help.

También puede seleccionar Help Contents, que abre un explorador HTML que proporciona referencias a la descripción general y a la información sobre las tareas que se proporciona en este capítulo.

## Trabajo con listas extensas en la herramienta SEAM

A medida que su sitio comience a acumular un gran número de principales y políticas, la herramienta SEAM tardará cada vez más tiempo en cargar y mostrar las listas de principales y políticas. Por lo tanto, su productividad con la herramienta se reducirá. Existen varias maneras de solucionar este problema.

Primero, puede eliminar totalmente las tiempo de carga de las listas al no hacer que la herramienta SEAM cargue las listas. Puede establecer esta opción seleccionando Properties en el menú Edit, y desactivando el campo Show Lists. Por supuesto, si la herramienta no carga las listas, no podrá mostrar las listas, y usted ya no podrá utilizar los paneles de lista para seleccionar los principales o las políticas. En cambio, deberá escribir el nombre de un principal o una política en el nuevo campo Name proporcionado y, a continuación, seleccionar la operación que desee realizar. De hecho, escribir un nombre equivale a seleccionar un elemento de la lista.



Otra manera de trabajar con listas extensas es almacenarlas en la antememoria. De hecho, el almacenamiento de las listas en la antememoria por un tiempo limitado se define como el comportamiento predeterminado para la herramienta SEAM. La herramienta SEAM aún debe cargar inicialmente las listas en la antememoria. Pero después la herramienta puede utilizar la antememoria en lugar de recuperar las listas de nuevo. Esta opción elimina la necesidad de cargar las listas del servidor una y otra vez, que es lo que lleva mucho tiempo.

Puede establecer el almacenamiento de listas en la antememoria seleccionando Properties en el menú Edit. Existen dos opciones de configuración de antememoria. Puede elegir almacenar la lista en la antememoria para siempre, o puede especificar un límite de tiempo en el cual la herramienta debe volver a cargar las listas de servidor en la antememoria.

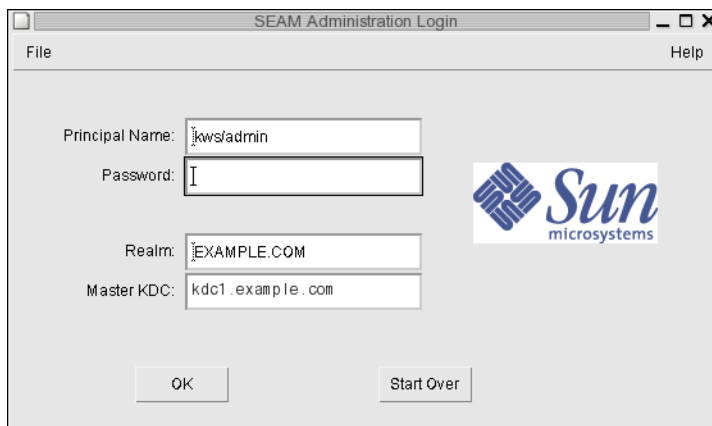
El almacenamiento de las listas en la antememoria permite utilizar los paneles de lista para seleccionar principales y políticas, por lo que no afecta la manera en que se puede utilizar la herramienta SEAM como lo hace la primera opción. Además, aunque el almacenamiento en la antememoria no le permite ver los cambios de otros usuarios, puede ver la información más reciente de la de lista según sus cambios, ya que sus cambios actualizan las listas tanto en el servidor como en la antememoria. Y, si desea actualizar la antememoria para ver otros cambios y obtener la última copia de las listas, puede utilizar el menú Refresh para actualizar la antememoria desde el servidor.

## ▼ Cómo iniciar la herramienta SEAM

- 1 Para iniciar la herramienta SEAM utilice el comando `gkadmin`.

```
$ /usr/sbin/gkadmin
```

Aparece la ventana SEAM Administration Login.



**2 Si no desea utilizar los valores predeterminados, especifique nuevos valores predeterminados.**

La ventana automáticamente se rellena con los valores predeterminados. El nombre de principal predeterminado se determina tomando su identidad actual de la variable de entorno USER y anexándole /admin a ella (*nombre\_usuario/admin*). Los valores predeterminados de los campos Realm y Master KDC se seleccionan del archivo */etc/krb5/krb5.conf*. Si alguna vez desea recuperar los valores predeterminados, haga clic en Start Over.

**Nota** – La operaciones de administración que puede realizar cada nombre de principal se rigen por el archivo ACL de Kerberos */etc/krb5/kadm5.acl*. Para obtener más información sobre privilegios limitados, consulte [“Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados” en la página 540](#).

**3 Escriba la contraseña del nombre de principal especificado.**

**4 Haga clic en OK.**

Aparece una ventana en la que se muestran todos los principales.

# Administración de los principales de Kerberos

En esta sección se proporcionan instrucciones detalladas que se deben utilizar para administrar principales con la herramienta SEAM. En esta sección también se proporcionan ejemplos de equivalentes de línea de comandos, si están disponibles.

## Administración de los principales de Kerberos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Ver lista de principales	Para ver la lista de principales, haga clic en la ficha Principals.	<a href="#">“Cómo ver la lista de los principales de Kerberos” en la página 516</a>
Ver atributos de un principal	Para ver los atributos de un principal, seleccione el principal en la lista de principales y, a continuación, haga clic en el botón Modify.	<a href="#">“Cómo ver los atributos de un principal de Kerberos” en la página 518</a>
Crear un principal nuevo	Para crear un principal nuevo, haga clic en el botón Create New en el panel Principal List.	<a href="#">“Cómo crear un nuevo principal de Kerberos” en la página 520</a>
Duplicar un principal	Para duplicar un principal, seleccione el principal que desea duplicar en la lista de principales y, a continuación, haga clic en el botón Duplicate.	<a href="#">“Cómo duplicar un principal de Kerberos” en la página 523</a>

Tarea	Descripción	Para obtener instrucciones
Modificar un principal	Para modificar un principal, seleccione el principal que desea modificar en la lista de principales y, a continuación, haga clic en el botón Modify.  Tenga en cuenta que no puede modificar el nombre de un principal. Para cambiar el nombre de un principal, debe duplicar el principal, especificar un nombre nuevo para él, guardarlo y, a continuación, suprimir el antiguo principal.	<a href="#">“Cómo modificar un principal de Kerberos” en la página 523</a>
Suprimir un principal	Para suprimir un principal, seleccione el principal que desea suprimir en la lista de principales y, a continuación, haga clic en el botón Delete.	<a href="#">“Cómo suprimir un principal de Kerberos” en la página 525</a>
Configurar valores predeterminados para crear principales nuevos	Para configurar valores predeterminado para crear principales nuevos, seleccione Properties en el menú Edit.	<a href="#">“Cómo configurar valores predeterminados para crear nuevos principales de Kerberos” en la página 525</a>
Modificar los privilegios de administración de Kerberos (archivo <code>kadm5.acl</code> ).	<i>Sólo línea de comandos.</i> Los privilegios de administración de Kerberos determinan qué operaciones puede realizar un principal en la base de datos de Kerberos, por ejemplo, agregar y modificar.  Debe editar el archivo <code>/etc/krb5/kadm5.acl</code> para modificar los privilegios de administración de Kerberos para cada principal.	<a href="#">“Cómo modificar los privilegios de administración de Kerberos” en la página 526</a>

## Automatización de la creación de nuevos principales de Kerberos

Si bien la herramienta SEAM es fácil de usar, no ofrece una manera de automatizar la creación de nuevos principales. La automatización es especialmente útil si necesita agregar 10 o, incluso, 100 nuevos principales en un breve periodo. Sin embargo, puede utilizar el comando `kadmin.local` en una secuencia de comandos de shell Bourne para hacer exactamente eso.

La siguiente secuencia de comandos de shell es un ejemplo de cómo automatizar la creación de nuevos principales:

```
awk '{ print "ank +needchange -pw", $2, $1 }' < /tmp/princnames |
time /usr/sbin/kadmin.local> /dev/null
```

Este ejemplo está dividido en dos líneas para su legibilidad. La secuencia de comandos lee un archivo llamado `princnames` que contiene los nombres de principales y sus contraseñas, y los agrega a la base de datos de Kerberos. Usted debería crear el archivo `princnames`, que contiene un nombre de principal y su contraseña en cada línea, separados por un espacio o varios. La

opción `+needchange` configura el principal para que se le pida al usuario que introduzca una nueva contraseña la primera vez que inicia sesión con el principal. Esta práctica ayuda a garantizar que las contraseñas del archivo `princnames` no sean un riesgo de seguridad.

Puede crear secuencias de comandos más elaboradas. Por ejemplo, la secuencia de comandos podría utilizar la información del servicio de nombres para obtener la lista de nombres de usuario para los nombres de principales. Lo que usted hace y cómo lo hace está determinado por las necesidades del sitio y su experiencia en secuencias de comandos.

## ▼ **Cómo ver la lista de los principales de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

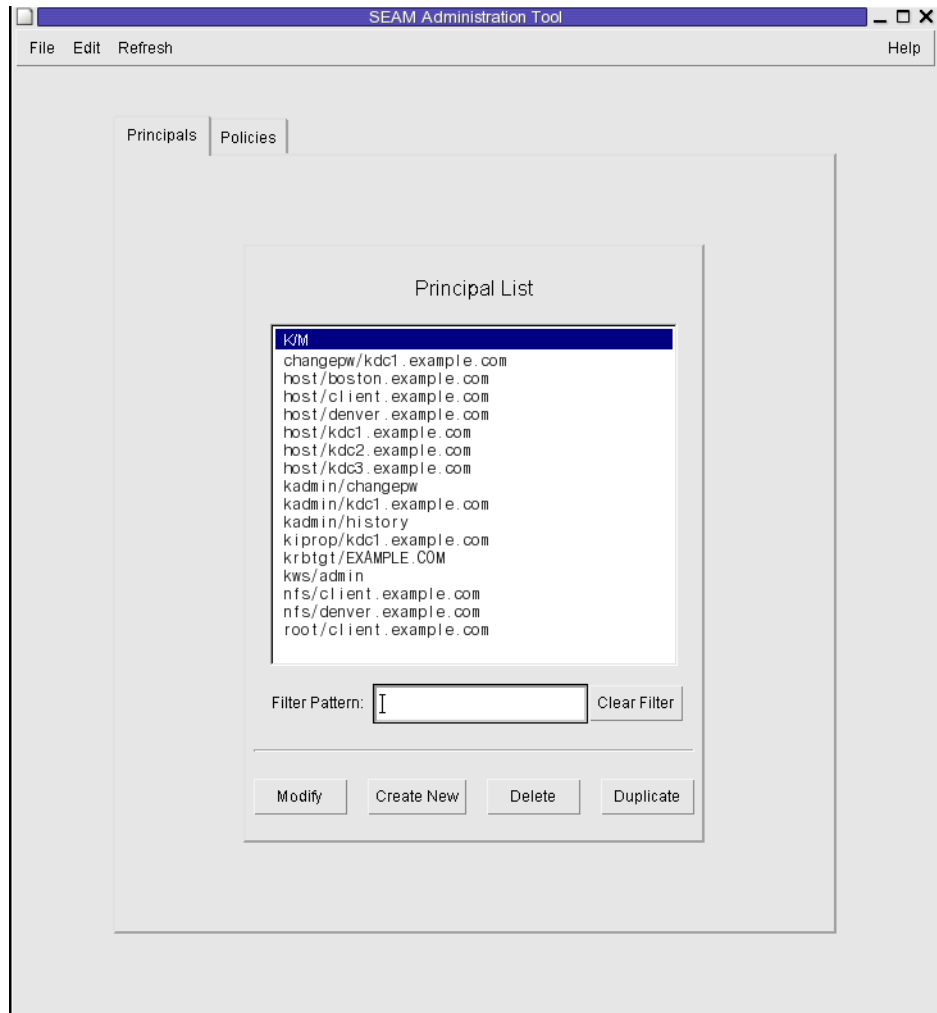
### **1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

```
$ /usr/sbin/gkadmin
```

## 2 Haga clic en la ficha Principals.

Aparecerá la lista de principales.



## 3 Muestre un principal específico o una sublista de principales.

Escriba una cadena de filtro en el campo Filter y, a continuación, presione la tecla de retorno. Si el filtro se realiza correctamente, se muestra la lista de principales que coinciden con el filtro.

La cadena de filtro debe estar compuesta por uno o varios caracteres. Debido a que el mecanismo de filtro distingue mayúsculas de minúsculas, deberá utilizar las letras mayúsculas y minúsculas correspondientes para el filtro. Por ejemplo, si escribe la cadena de filtro ge, el mecanismo de filtro mostrará sólo los principales que contengan la cadena ge (por ejemplo, george o edge).

Si desea que aparezca la lista completa de principales, haga clic en Clear Filter.

### **Ejemplo 25–1** Visualización de la lista de los principales de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `list_principals` de `kadmin` se utiliza para mostrar todos los principales que coinciden con `kadmin*`. Se pueden utilizar comodines con el comando `list_principals`.

```
kadmin: list_principals kadmin*
kadmin/changepw@EXAMPLE.COM
kadmin/kdc1.example.con@EXAMPLE.COM
kadmin/history@EXAMPLE.COM
kadmin: quit
```

## ▼ **Cómo ver los atributos de un principal de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### **1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513.](#)

```
$ /usr/sbin/gkadmin
```

### **2 Haga clic en la ficha Principals.**

### **3 Seleccione el principal que desea ver en la lista y, a continuación, haga clic en Modify.**

Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal.

### **4 A continuación, haga clic en Next para ver todos los atributos del principal.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 537.](#)

### **5 Cuando haya terminado, haga clic en Cancel.**

### **Ejemplo 25–2** Visualización de los atributos de un principal de Kerberos

En el ejemplo siguiente se muestra la primera ventana que se verá al visualizar el principal `jdb/admin`.

The screenshot shows the 'SEAM Administration Tool' window with a menu bar (File, Edit, Refresh, Help) and two tabs: 'Principals' and 'Policies'. The 'Principals' tab is active, displaying a 'Principal Basics' configuration form for the principal 'jdb/admin'.

**Principal Basics**

*General*

Principal Name:

Password:

Encryption Key Types:

Policy:

Account Expires:

*Admin History*

Last Principal Change: Sep 28, 2009 1:32:23 PM

Last Changed By: host/admin@EXAMPLE.COM

Comments:

Modify Principal

### Ejemplo 25-3 Visualización de los atributos de un principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `get_principal` de `kadmin` se utiliza para ver los atributos del principal `jdb/admin`.

```
kadmin: getprinc jdb/admin
Principal: jdb/admin@EXAMPLE.COM
```

```
Expiration date: [never]
Last password change: [never]
```

```
Password expiration date: Wed Apr 14 11:53:10 PDT 2011
Maximum ticket life: 1 day 16:00:00
Maximum renewable life: 1 day 16:00:00
```

```
Last modified: Mon Sep 28 13:32:23 PST 2009 (host/admin@EXAMPLE.COM)
Last successful authentication: [never]
Last failed authentication: [never]
Failed password attempts: 0
Number of keys: 1
Key: vno 1, AES-256 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, AES-128 CTS mode with 96-bit SHA-1 HMAC, no salt
Key: vno 1, Triple DES with HMAC/sha1, no salt
Key: vno 1, ArcFour with HMAC/md5, no salt
Key: vno 1, DES cbc mode with RSA-MD5, no salt
Attributes: REQUIRES_HW_AUTH
Policy: [none]
kadmin: quit
```

## ▼ Cómo crear un nuevo principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

---

**Nota** – Si va a crear un nuevo principal que pueda necesitar una nueva política, debe crear la nueva política antes de crear el nuevo principal. Vaya a [“Cómo crear una nueva política de Kerberos” en la página 533](#).

---

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Principals.

### 3 Haga clic en New.

Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal que se está visualizando.

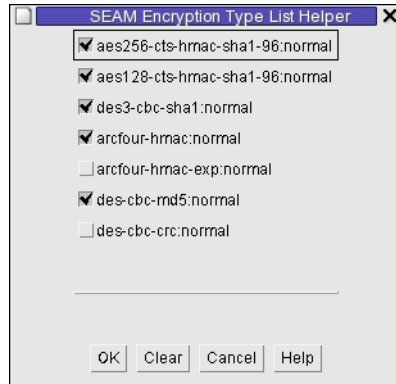
### 4 Especifique un nombre de principal y una contraseña.

Tanto el nombre de principal como la contraseña son obligatorios.



**5 Especifique los tipos de cifrado para el principal.**

Haga clic en el cuadro ubicado a la derecha del campo de tipos de clave de cifrado para abrir una nueva ventana que muestre todos los tipos de clave de cifrado disponibles. Después de seleccionar los tipos de cifrado necesarios, haga clic en OK.



**6 Especifique la política para el principal.**

**7 Especifique los valores para los atributos del principal y, a continuación, haga clic en Next para especificar más atributos.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 537.](#)

**8 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.**

**9 Si es necesario, configure los privilegios de administración de Kerberos para el nuevo principal en el archivo `/etc/krb5/kadm5.acL`.**

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 526.](#)

### **Ejemplo 25-4 Creación de un nuevo principal de Kerberos**

En el siguiente ejemplo se muestra el panel Principal Basics cuando se crea un nuevo principal denominado pak. La política se establece en testuser.

The screenshot shows the SEAM Administration Tool window. The 'Principals' tab is selected. The 'Principal Basics' form is displayed with the following fields and values:

- Principal Name:** pak
- Password:** (masked with asterisks)
- Generate Random Password:** (button)
- Encryption Key Types:** aes256-cts-hmac-sha1-96:no (dropdown menu)
- Policy:** testuser (dropdown menu)
- Account Expires:** Oct 8, 2010 10:49:40 AM (calendar icon)
- Admin History:**
  - Last Principal Change: Oct 8, 2009 11:35:10 AM
  - Last Changed By: kathys
  - Comments: (text area)

At the bottom of the form are buttons for 'Save', 'Previous', 'Next', and 'Cancel'. Below the form, the text 'Create New Principal- \*CHANGES\*' is visible.

### Ejemplo 25-5 Creación de un nuevo principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `add_principal` de `kadmin` se utiliza para crear un nuevo principal denominado `pak`. La política del principal se establece en `testuser`.

```
kadmin: add_principal -policy testuser pak
Enter password for principal "pak@EXAMPLE.COM": <Type the password>
Re-enter password for principal "pak@EXAMPLE.COM": <Type the password again>
Principal "pak@EXAMPLE.COM" created.
kadmin: quit
```

## ▼ Cómo duplicar un principal de Kerberos

En este procedimiento se explica cómo utilizar todos los atributos de un principal existente, o algunos de ellos, para crear un nuevo principal. No hay equivalente de línea de comandos para este procedimiento.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Principals.

### 3 Seleccione el principal que desea duplicar en la lista y, a continuación, haga clic en Duplicate.

Aparecerá el panel Principal Basics. Todos los atributos del principal seleccionado se duplican, excepto los campos Principal Name y Password, que están vacíos.

### 4 Especifique un nombre de principal y una contraseña.

Tanto el nombre de principal como la contraseña son obligatorios. Para realizar un duplicado exacto del principal que ha seleccionado, haga clic en Save y vaya al [Paso 7](#).

### 5 Especifique diferentes valores para los atributos del principal y, a continuación, haga clic en Next para especificar más atributos.

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 537](#).

### 6 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.

### 7 Si es necesario, configure los privilegios de administración de Kerberos para el principal en el archivo `/etc/krb5/kadm5.ac1`.

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 526](#).

## ▼ Cómo modificar un principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Principals.****3 Seleccione el principal que desea modificar en la lista y, a continuación, haga clic en Modify.**

Aparecerá el panel Principal Basics que contiene algunos de los atributos del principal que se está visualizando.

**4 Modifique los atributos del principal y, a continuación, haga clic en Next para modificar más atributos.**

Tres ventanas contienen información de atributos. Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help. O, para ver las descripciones de todos los atributos de los principales, vaya a [“Descripción de los paneles de la herramienta SEAM” en la página 537](#).

---

**Nota** – No puede modificar el nombre de un principal. Para cambiar el nombre de un principal, debe duplicar el principal, especificar un nombre nuevo para él, guardarlo y, a continuación, suprimir el antiguo principal.

---

**5 Haga clic en Save para guardar el principal, o bien, haga clic en Done en el último panel.****6 Modifique los privilegios de administración de Kerberos para el principal en el archivo `/etc/krb5/kadm5.ac1`.**

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 526](#).

**Ejemplo 25–6 Modificación de la contraseña de un principal de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `change_password` de `kadmin` se utiliza para modificar la contraseña para el principal `jdb`. El comando `change_password` no le permitirá cambiar la contraseña por una contraseña que ya esté en el historial de contraseñas del principal.

```
kadmin: change_password jdb
Enter password for principal "jdb": <Type the new password>
Re-enter password for principal "jdb": <Type the password again>
Password for "jdb@EXAMPLE.COM" changed.
kadmin: quit
```

Para modificar otros atributos de un principal, debe utilizar el comando `modify_principal` de `kadmin`.

## ▼ Cómo suprimir un principal de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513.](#)

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Principals.

### 3 Seleccione el principal que desea suprimir en la lista y, a continuación, haga clic en Delete.

Una vez que confirme la supresión, el principal se suprimirá.

### 4 Elimine el principal del archivo de la lista de control de acceso (ACL) de Kerberos, /etc/krb5/kadm5.acl.

Para obtener más información, consulte [“Cómo modificar los privilegios de administración de Kerberos” en la página 526.](#)

## Ejemplo 25–7 Supresión de un principal de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `delete_principal` de `kadmin` se utiliza para suprimir el principal `jdb`.

```
kadmin: delete_principal pak
Are you sure you want to delete the principal "pak@EXAMPLE.COM"? (yes/no): yes
Principal "pak@EXAMPLE.COM" deleted.
Make sure that you have removed this principal from all ACLs before reusing.
kadmin: quit
```

## ▼ Cómo configurar valores predeterminados para crear nuevos principales de Kerberos

No hay equivalente de línea de comandos para este procedimiento.

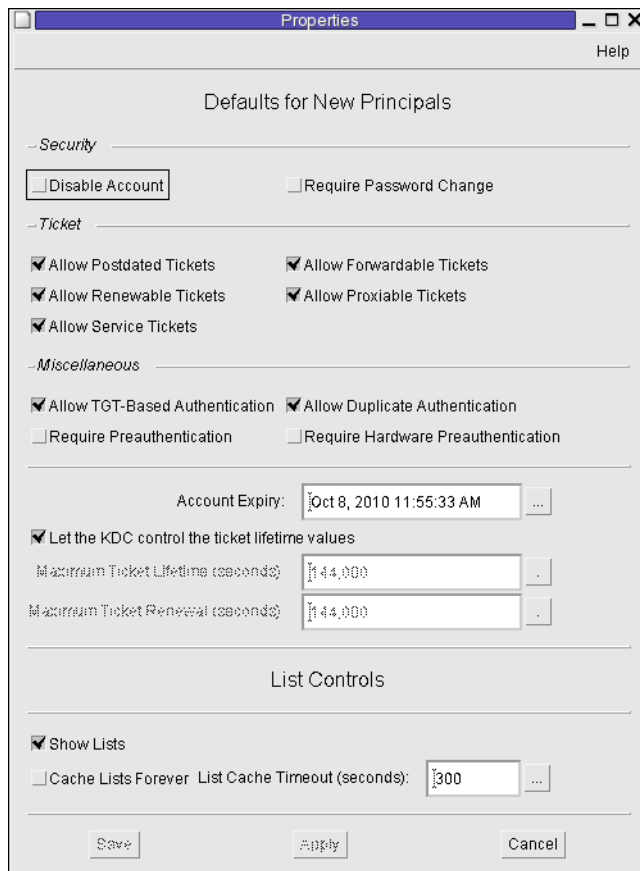
### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513.](#)

```
$ /usr/sbin/gkadmin
```

## 2 Elija Properties en el menú Edit.

Aparecerá la ventana Properties.



## 3 Seleccione los valores predeterminados que desea utilizar para crear nuevos principales.

Para obtener información sobre los diferentes atributos de cada ventana, seleccione Context-Sensitive Help desde el menú Help.

## 4 Haga clic en Save.

## ▼ Cómo modificar los privilegios de administración de Kerberos

Aunque su sitio probablemente tenga muchos principales de usuario, en general, se prefiere que sólo unos pocos usuarios puedan administrar la base de datos de Kerberos. Los privilegios para

administrar la base de datos de Kerberos se determinan mediante el archivo de la lista de control de acceso (ACL) de Kerberos, `kadm5.acl`. Mediante el archivo `kadm5.acl` se pueden permitir o prohibir privilegios para cada principal. También puede utilizar el comodín `*` en el nombre del principal para especificar privilegios para grupos de principales.

**1 Conviértase en superusuario en el KDC maestro.**

**2 Edite el archivo `/etc/krb5/kadm5.acl`.**

Las entradas del archivo `kadm5.acl` deben tener el siguiente formato:

*principal privileges [principal-target]*

<i>principal</i>	<p>Especifica el principal al que se le otorgan los privilegios. Cualquier parte del nombre del principal puede incluir el comodín <code>*</code>, que es útil para proporcionar los mismos privilegios para un grupo de principales. Por ejemplo, si desea especificar todos los principales con la instancia <code>admin</code>, debe utilizar <code>*/admin@dominio</code>.</p> <p>Tenga en cuenta que un uso común de una instancia <code>admin</code> es conceder privilegios independientes (por ejemplo, acceso de administración a la base de datos de Kerberos) a un principal de Kerberos individual. Por ejemplo, el usuario <code>jdb</code> puede tener un principal para su uso administrativo, denominado <code>jdb/admin</code>. De esta manera, el usuario <code>jdb</code> obtiene los tickets de <code>jdb/admin</code> sólo cuando realmente necesita utilizar esos privilegios.</p>														
<i>privilegios</i>	<p>Especifica qué operaciones puede, o no puede, realizar el principal. Este campo consta de una cadena compuesta por uno o varios caracteres de la siguiente lista, o por sus equivalentes en mayúscula. Si el carácter está en mayúscula (o no se ha especificado), la operación está prohibida. Si el carácter está en minúscula, la operación está permitida.</p> <table><tr><td><code>a</code></td><td>Permite o prohíbe la adición de principales o políticas.</td></tr><tr><td><code>d</code></td><td>Permite o prohíbe la supresión de principales o políticas.</td></tr><tr><td><code>m</code></td><td>Permite o prohíbe la modificación de principales o políticas.</td></tr><tr><td><code>c</code></td><td>Permite o prohíbe la modificación de contraseñas de principales.</td></tr><tr><td><code>i</code></td><td>Permite o prohíbe realizar consultas a la base de datos de Kerberos.</td></tr><tr><td><code>l</code></td><td>Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos.</td></tr><tr><td><code>x</code> o <code>*</code></td><td>Permite todos los privilegios (<code>admcil</code>).</td></tr></table>	<code>a</code>	Permite o prohíbe la adición de principales o políticas.	<code>d</code>	Permite o prohíbe la supresión de principales o políticas.	<code>m</code>	Permite o prohíbe la modificación de principales o políticas.	<code>c</code>	Permite o prohíbe la modificación de contraseñas de principales.	<code>i</code>	Permite o prohíbe realizar consultas a la base de datos de Kerberos.	<code>l</code>	Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos.	<code>x</code> o <code>*</code>	Permite todos los privilegios ( <code>admcil</code> ).
<code>a</code>	Permite o prohíbe la adición de principales o políticas.														
<code>d</code>	Permite o prohíbe la supresión de principales o políticas.														
<code>m</code>	Permite o prohíbe la modificación de principales o políticas.														
<code>c</code>	Permite o prohíbe la modificación de contraseñas de principales.														
<code>i</code>	Permite o prohíbe realizar consultas a la base de datos de Kerberos.														
<code>l</code>	Permite o prohíbe mostrar principales o políticas en la base de datos de Kerberos.														
<code>x</code> o <code>*</code>	Permite todos los privilegios ( <code>admcil</code> ).														
<i>destino_principal</i>	<p>Cuando se especifica un principal en este campo, los <i>privilegios</i> se aplican al <i>principal</i> sólo cuando el <i>principal</i> opera en el <i>destino_principal</i>. Cualquier parte del nombre del principal puede incluir el comodín <code>*</code>, que es útil para agrupar principales.</p>														

**Ejemplo 25–8**    Modificación de los privilegios de administración de Kerberos

La siguiente entrada en el archivo `kadm5.ac1` otorga a cualquier principal del dominio `EXAMPLE.COM` con la instancia `admin` todos los privilegios de la base de datos de Kerberos:

```
*/admin@EXAMPLE.COM *
```

La siguiente entrada del archivo `kadm5.ac1` le otorga al principal `jdb@EXAMPLE.COM` los privilegios para agregar, mostrar y consultar cualquier principal que tenga la instancia `root`.

```
jdb@EXAMPLE.COM ali */root@EXAMPLE.COM
```

# Administración de las políticas de Kerberos

En esta sección se proporcionan instrucciones detalladas que se deben utilizar para administrar políticas con la herramienta SEAM. En esta sección también se proporcionan ejemplos de equivalentes de línea de comandos, si están disponibles.

## Administración de las políticas de Kerberos (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Ver lista de políticas	Para ver la lista de políticas, haga clic en la ficha Policies.	<a href="#">“Cómo ver la lista de políticas de Kerberos” en la página 529</a>
Ver atributos de una política	Para ver los atributos de una política, seleccione la política en la lista de políticas y, a continuación, haga clic en el botón Modify.	<a href="#">“Cómo ver los atributos de una política de Kerberos” en la página 531</a>
Crear una política nueva	Para crear una política nueva, haga clic en el botón Create New en el panel Policy List.	<a href="#">“Cómo crear una nueva política de Kerberos” en la página 533</a>
Duplicar una política	Para duplicar una política, seleccione la política que desea duplicar en la lista de políticas y, a continuación, haga clic en el botón Duplicate.	<a href="#">“Cómo duplicar una política de Kerberos” en la página 535</a>
Modificar una política	<p>Para modificar una política, seleccione la política que desea modificar en la lista de políticas y, a continuación, haga clic en el botón Modify.</p> <p>Tenga en cuenta que no puede modificar el nombre de una política. Para cambiar el nombre de una política, debe duplicar la política, especificar un nombre nuevo para ella, guardarla y, a continuación, suprimir la antigua política.</p>	<a href="#">“Cómo modificar una política de Kerberos” en la página 535</a>



Tarea	Descripción	Para obtener instrucciones
Suprimir una política	Para suprimir una política, seleccione la política que desea suprimir en la lista de políticas y, a continuación, haga clic en el botón Delete.	<a href="#">“Cómo suprimir una política de Kerberos” en la página 536</a>

## ▼ Cómo ver la lista de políticas de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

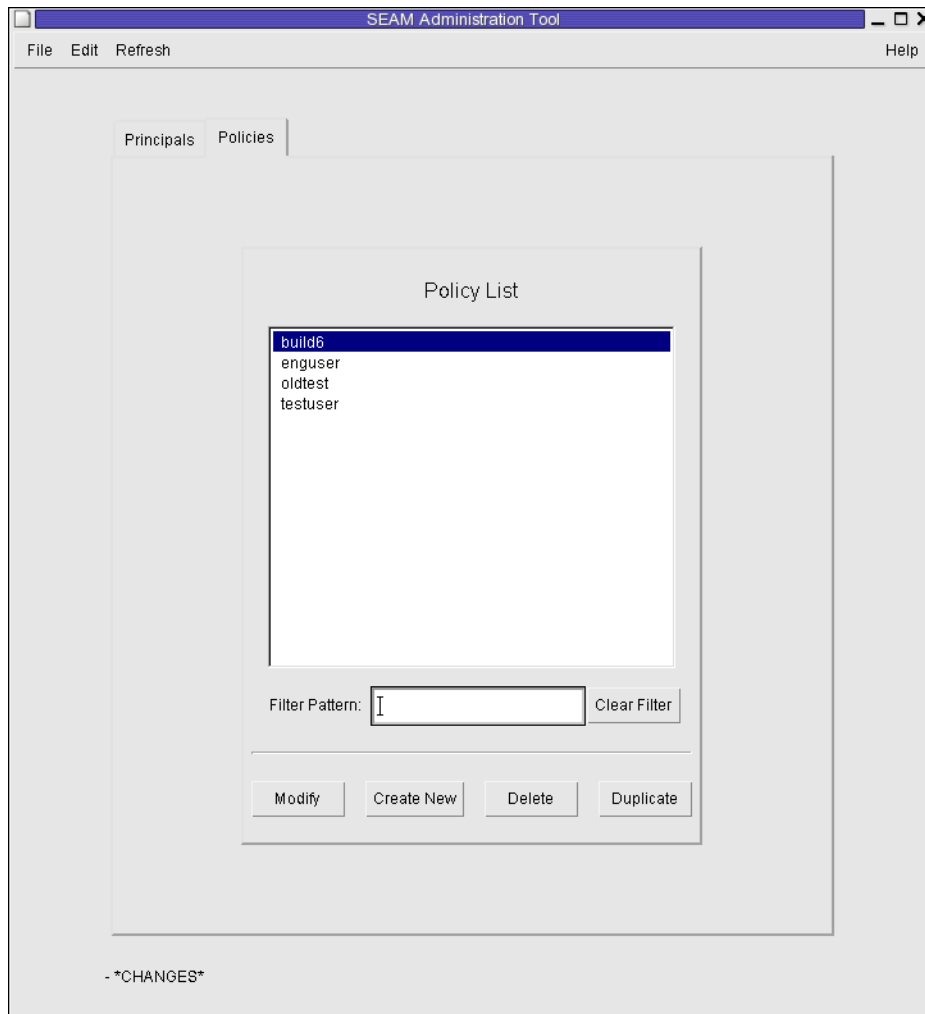
### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

```
$ /usr/sbin/gkadmin
```

## 2 Haga clic en la ficha Políticas.

Aparecerá la lista de políticas.



## 3 Muestre una política específica o una sublista de políticas.

Escriba una cadena de filtro en el campo de filtro y, a continuación, presione la tecla e retorno. Si el filtro se realiza correctamente, se muestra la lista de políticas que coinciden con el filtro.

La cadena de filtro debe estar compuesta por uno o varios caracteres. Debido a que el mecanismo de filtro distingue mayúsculas de minúsculas, deberá utilizar las letras mayúsculas y minúsculas correspondientes para el filtro. Por ejemplo, si escribe la cadena de filtro ge, el mecanismo de filtro mostrará sólo las políticas que contengan la cadena ge (por ejemplo, george o edge).

Si desea que aparezca la lista completa de políticas, haga clic en Clear Filter.

### **Ejemplo 25–9** Visualización de la lista de las políticas de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `list_policies` de `kadmin` se utiliza para mostrar todas las políticas que coinciden con `*user*`. Se pueden utilizar comodines con el comando `list_policies`.

```
kadmin: list_policies *user*
testuser
enguser
kadmin: quit
```

## ▼ **Cómo ver los atributos de una política de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### **1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513](#).

```
$ /usr/sbin/gkadmin
```

### **2 Haga clic en la ficha Policies.**

### **3 Seleccione la política que desea ver en la lista y, a continuación, haga clic en Modify.**

Aparecerá el panel Policy Details.

### **4 Cuando haya terminado, haga clic en Cancel.**

### **Ejemplo 25–10** Visualización de los atributos de una política de Kerberos

En el ejemplo siguiente se muestra el panel Policy Details que se verá al visualizar la política `test`.



### Ejemplo 25-11 Visualización de los atributos de una política de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `get_policy` de `kadmin` se utiliza para ver los atributos de la política `enguser`.

```
kadmin: get_policy enguser
Policy: enguser
Maximum password life: 2592000
Minimum password life: 0
Minimum password length: 8
Minimum number of password character classes: 2
Number of old keys kept: 3
Reference count: 0
kadmin: quit
```

El recuento de referencia (Reference count) es el número de los principales que utilizan esta política.

## ▼ **Cómo crear una nueva política de Kerberos**

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM”](#) en la página 513.

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Políticas.**

**3 Haga clic en New.**

Aparecerá el panel Policy Details.

**4 Especifique un nombre para la política en el campo Policy Name.**

El nombre de la política es obligatorio.

**5 Especifique valores para los atributos de la política.**

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 25–5](#) para ver la descripción de todos los atributos de políticas.

**6 Haga clic en Save para guardar la política, o haga clic en Done.**

### **Ejemplo 25–12 Creación de una nueva política de Kerberos**

En el siguiente ejemplo, se crea una nueva política denominada `build11`. El valor de clases mínimas para contraseña, Minimum Password Classes, se establece en 3.



### Ejemplo 25-13 Creación de una nueva política de Kerberos (línea de comandos)

En el ejemplo siguiente, el comando `add_policy` de `kadmin` se utiliza para crear la política `build11`. Esta política requiere al menos 3 clases de caracteres en una contraseña.

```
$ kadmin
kadmin: add_policy -minclasses 3 build11
kadmin: quit
```

## ▼ Cómo duplicar una política de Kerberos

En este procedimiento se explica cómo utilizar todos los atributos de una política existente, o algunos de ellos, para crear una nueva política. No hay equivalente de línea de comandos para este procedimiento.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener más información, consulte [“Cómo iniciar la herramienta SEAM” en la página 513.](#)

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Políticas.

### 3 Seleccione la política que desea duplicar en la lista y, a continuación, haga clic en Duplicate.

Aparecerá el panel Policy Details. Todos los atributos de la política seleccionada se duplican, excepto el campo Policy Name, que está vacío.

### 4 Especifique un nombre para la política duplicada en el campo Policy Name.

El nombre de la política es obligatorio. Para realizar un duplicado exacto de la política que ha seleccionado, vaya al [Paso 6](#).

### 5 Especifique valores diferentes para los atributos de la política.

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 25–5](#) para ver la descripción de todos los atributos de políticas.

### 6 Haga clic en Save para guardar la política, o haga clic en Done.

## ▼ Cómo modificar una política de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

### 1 Si es necesario, inicie la herramienta SEAM.

Para obtener detalles, consulte [“Cómo iniciar la herramienta SEAM” en la página 513.](#)

```
$ /usr/sbin/gkadmin
```

### 2 Haga clic en la ficha Políticas.

### 3 Seleccione la política que desea modificar en la lista y, a continuación, haga clic en Modify.

Aparecerá el panel Policy Details.

**4 Modifique los atributos de la política.**

Para obtener información sobre los diferentes atributos de esta ventana, seleccione Context-Sensitive Help desde el menú Help. También puede ir a la [Tabla 25-5](#) para ver la descripción de todos los atributos de políticas.

---

**Nota** – No puede modificar el nombre de una política. Para cambiar el nombre de una política, debe duplicar la política, especificar un nombre nuevo para ella, guardarla y, a continuación, suprimir la antigua política.

---

**5 Haga clic en Save para guardar la política, o haga clic en Done.****Ejemplo 25-14 Modificación de una política de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `modify_policy` de `kadmin` se utiliza para cambiar la longitud mínima de una contraseña por cinco caracteres para la política `build11`.

```
$ kadmin
kadmin: modify_policy -minlength 5 build11
kadmin: quit
```

## ▼ Cómo suprimir una política de Kerberos

Después de este procedimiento se muestra un ejemplo del equivalente de línea de comandos.

---

**Nota** – Antes de suprimir una política, debe cancelarla en todos los principales que la estén utilizando. Para ello, debe modificar el atributo de política de los principales correspondientes. La política no se puede suprimir si algún principal la está utilizando.

---

**1 Si es necesario, inicie la herramienta SEAM.**

Para obtener más información, consulte “[Cómo iniciar la herramienta SEAM](#)” en la [página 513](#).

```
$ /usr/sbin/gkadmin
```

**2 Haga clic en la ficha Políticas.****3 Seleccione la política que desea suprimir en la lista y, a continuación, haga clic en Delete.**

Una vez que confirme la supresión, la política se suprimirá.

**Ejemplo 25-15 Supresión de una política de Kerberos (línea de comandos)**

En el ejemplo siguiente, el comando `delete_policy` de `kadmin` se utiliza para suprimir la política `build11`.



```
kadmin: delete_policy build11
Are you sure you want to delete the policy "build11"? (yes/no): yes
kadmin: quit
```

Antes de suprimir una política, debe cancelarla en todos los principales que la estén utilizando. Para ello, debe utilizar el comando `modify_principal -policy` de `kadmin` en los principales correspondientes. El comando `delete_policy` fallará, si la política está siendo utilizada por un principal.

## Referencia de la herramienta SEAM

En esta sección, se proporcionan descripciones de cada panel de la herramienta SEAM. Asimismo, se proporciona información sobre el uso de privilegios limitados en la herramienta SEAM.

### Descripción de los paneles de la herramienta SEAM

En esta sección se ofrece la descripción de todos los atributos de los principales y las políticas que se pueden especificar o ver en la herramienta SEAM. Los atributos están organizados según el panel en el que aparecen.

**TABLA 25-2** Atributos del panel Principal Basics de la herramienta SEAM

Atributo	Descripción
Principal Name	El nombre del principal (que es la parte <i>principal/de instancia</i> de un nombre de principal completo). Un principal es una identidad única a la que el KDC puede asignar tickets.  Si modifica un principal, no puede editar su nombre.
Password	La contraseña para el principal. Puede utilizar el botón Generate Random Password para crear una contraseña aleatoria para el principal.
Policy	Un menú de las políticas disponibles para el principal.
Account Expires	La fecha y hora en que caduca la cuenta del principal. Cuando la cuenta caduque, el principal ya no podrá obtener un ticket de otorgamiento de tickets (TGT) y quizá no pueda iniciar sesión.
Last Principal Change	La fecha en la que se modificó por última vez la información del principal. (Sólo lectura)
Last Changed By	El nombre del principal que modificó por última vez la cuenta de este principal. (Sólo lectura)
Comments	Comentarios relacionados con el principal (por ejemplo, “Cuenta temporal”).

**TABLA 25-3** Atributos del panel de detalles del principal de la herramienta SEAM

Atributo	Descripción
Last Success	La fecha y hora en que el principal inició sesión correctamente por última vez. (Sólo lectura)

TABLA 25-3 Atributos del panel de detalles del principal de la herramienta SEAM (Continuación)

Atributo	Descripción
Last Failure	La fecha y hora en que se produjo un fallo en el inicio de sesión del principal por última vez. (Sólo lectura)
Failure Count	El número de veces que se produjeron fallos en el inicio de sesión del principal. (Sólo lectura)
Last Password Change	La fecha y la hora en que se modificó por última vez la contraseña del principal. (Sólo lectura)
Password Expires	La fecha y hora en que caduca la contraseña actual del principal.
Key Version	El número de versión de clave del principal. En general, este atributo sólo se cambia cuando una contraseña está en peligro.
Maximum Lifetime (seconds)	El período máximo durante el cual un ticket se puede otorgar al principal (sin renovación).
Maximum Renewal (seconds)	El período máximo durante el cual un ticket existente se puede renovar para el principal.

TABLA 25-4 Atributos del panel de indicadores de principal de la herramienta SEAM

Atributo (botones de radio)	Descripción
Disable Account	Cuando está activado, impide que el principal inicie sesión. Este atributo proporciona una manera sencilla de congelar temporalmente una cuenta de principal.
Require Password Change	Cuando está activado, hace que caduque la contraseña actual del principal, lo cual fuerza al usuario a utilizar el comando <code>kpasswd</code> para crear una contraseña nueva. Este atributo es útil si se produce una infracción de seguridad y, como consecuencia, es necesario asegurarse de que se sustituyan las contraseñas antiguas.
Allow Postdated Tickets	Cuando está activado, permite al principal obtener tickets posfechados.  Por ejemplo, es posible que necesite utilizar tickets posfechados para trabajos cron que se deben ejecutar fuera del horario comercial, pero no pueda obtener los tickets anticipadamente debido a la corta duración de los tickets.
Allow Forwardable Tickets	Cuando está activado, permite al principal obtener tickets reenviables.  Los tickets reenviables son aquellos que se reenvían al host remoto para proporcionar una sesión de inicio único. Por ejemplo, si está utilizando tickets reenviables y se autentica a usted mismo mediante <code>ftp</code> o <code>rsh</code> , otros servicios, como los servicios NFS, estarán disponibles sin que se le solicite otra contraseña.
Allow Renewable Tickets	Cuando está activado, permite al principal obtener tickets renovables.  Un principal puede ampliar automáticamente la fecha o la hora de caducidad de un ticket renovable (en lugar de tener que obtener un nuevo ticket una vez que caduca el primero). Actualmente, el servicio NFS es el servicio de tickets que puede renovar tickets.

TABLA 25-4 Atributos del panel de indicadores de principal de la herramienta SEAM (Continuación)

Atributo (botones de radio)	Descripción
Allow Proxiable Tickets	<p>Cuando está activado, permite al principal obtener tickets que admiten proxy.</p> <p>Un ticket que admite proxy es un ticket que puede ser utilizado por un servicio en nombre de un cliente para realizar una operación para el cliente. Con un ticket que admite proxy, un servicio puede adoptar la identidad de un cliente y obtener un ticket para otro servicio. Sin embargo, el servicio no puede obtener un ticket de otorgamiento de tickets (TGT).</p>
Allow Service Tickets	<p>Cuando está activado, permite que se emitan tickets de servicio al principal.</p> <p>No debería permitir que se emitan tickets de servicio para los principales <code>kadmin/nombre_host</code> ni <code>changepw/nombre_host</code>. Esta práctica garantiza que sólo estos principales puedan actualizar la base de datos KDC.</p>
Allow TGT-Based Authentication	<p>Cuando está activado, permite al principal de servicio proporcionar servicios a otro principal. Más concretamente, este atributo permite al KDC emitir un ticket de servicio para el principal de servicio.</p> <p>Este atributo sólo es válido para los principales de servicio. Cuando no está activado, los tickets de servicio no se pueden emitir para el principal de servicio.</p>
Allow Duplicate Authentication	<p>Cuando está activado, permite al principal de usuario obtener tickets de servicio para otros principales de usuario.</p> <p>Este atributo sólo es válido para los principales de usuario. Cuando no está activado, el principal de usuario aún puede obtener tickets de servicio para los principales de servicio, pero no para otros principales de usuario.</p>
Required Preauthentication	<p>Cuando está activado, el KDC sólo enviará un ticket de otorgamiento de tickets (TGT) solicitado al principal una vez que haya autenticado (mediante el software) que el principal es realmente el principal que está solicitando el TGT. Esta autenticación previa generalmente se realiza mediante una contraseña adicional, por ejemplo, de una tarjeta DES.</p> <p>Cuando no está activado, el KDC no necesita realizar una autenticación previa del principal antes de enviar un TGT solicitado al principal.</p>
Required Hardware Authentication	<p>Cuando está activado, el KDC sólo enviará un ticket de otorgamiento de tickets (TGT) solicitado al principal una vez que haya autenticado (mediante el hardware) que el principal es realmente el principal que está solicitando el TGT. La autenticación previa del hardware se puede llevar a cabo, por ejemplo, en un lector de anillos Java.</p> <p>Cuando no está activado, el KDC no necesita realizar una autenticación previa del principal antes de enviar un TGT solicitado al principal.</p>

TABLA 25-5 Atributos del panel de características básicas de la política de la herramienta SEAM

Atributo	Descripción
Policy Name	<p>El nombre de la política. Una política es un conjunto de reglas que rigen la contraseña y los tickets de un principal.</p> <p>Si modifica una política, no puede editar su nombre.</p>

TABLA 25-5 Atributos del panel de características básicas de la política de la herramienta SEAM (Continuación)

Atributo	Descripción
Minimum Password Length	La longitud mínima de la contraseña del principal.
Minimum Password Classes	<p>El número mínimo de tipos de caracteres diferentes que se deben utilizar en la contraseña del principal.</p> <p>Por ejemplo, un valor de clases mínimo de 2 significa que la contraseña debe tener al menos dos tipos de caracteres diferentes, como letras y números (hi2mom). Un valor de 3 significa que la contraseña debe tener al menos tres tipos de caracteres diferentes, como letras, números y signos de puntuación (hi2mom!). Y así sucesivamente.</p> <p>Un valor de 1 no establece ninguna restricción para el número tipos de caracteres de la contraseña.</p>
Saved Password History	El número de contraseñas anteriores utilizadas por el principal, y una lista de las contraseñas anteriores que no se pueden volver a utilizar.
Minimum Password Lifetime (seconds)	El período mínimo durante el cual se debe utilizar una contraseña antes de poder modificarla.
Maximum Password Lifetime (seconds)	El período máximo durante el cual se puede utilizar una contraseña antes de tener que modificarla.
Principals Using This Policy	El número de principales a los que se aplica actualmente esta política. (Sólo lectura)

## Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados

Todas las funciones de la herramienta SEAM están disponibles si su principal admin tiene todos los privilegios para administrar la base de datos de Kerberos. Sin embargo, es posible que tenga privilegios limitados, por ejemplo, que sólo pueda ver la lista de principales o cambiar la contraseña de un principal. Con privilegios de administración de Kerberos limitados, aún puede utilizar la herramienta SEAM. Sin embargo, varias partes de la herramienta SEAM cambian según los privilegios de administración de Kerberos que no se tienen. En la [Tabla 25-6](#) se muestra cómo cambia la herramienta SEAM según los privilegios de administración de Kerberos que se tengan.

El cambio más visual de la herramienta SEAM se produce cuando no se tiene el privilegio de lista. Sin el privilegio de lista, los paneles de lista no muestran la lista de principales ni la de políticas para poder manipularlas. En cambio, debe utilizar el campo Name de los paneles de lista para especificar el principal o la política que desea manipular.

Si inicia sesión en la herramienta SEAM y no tiene suficientes privilegios para realizar tareas en ella, se muestra el siguiente mensaje y se vuelve a la ventana SEAM Administration Login:

Insufficient privileges to use gkadmin: ADMCIL. Please try using another principal.

Para cambiar los privilegios de un principal para que pueda administrar la base de datos de Kerberos, vaya a [“Cómo modificar los privilegios de administración de Kerberos” en la página 526](#).

**TABLA 25–6** Uso de la herramienta SEAM con privilegios de administración de Kerberos limitados

Privilegio no permitido	Cómo cambia la herramienta SEAM
a (agregar)	Los botones Create New y Duplicate no están disponibles en los paneles Principal List y Policy List. Si no tiene el privilegio para agregar, no puede crear principales ni políticas nuevos, ni duplicarlos.
d (suprimir)	El botón Delete no está disponible en los paneles Principal List ni Policy List. Si no tiene el privilegio para suprimir, no puede suprimir principales ni políticas.
m (modificar)	El botón Modify no está disponible en los paneles Principal List ni Policy List. Si no tiene el privilegio para modificar, no puede modificar principales ni políticas.  Además, si el botón Modify no está disponible, no puede modificar ninguna contraseña de principal, aunque tenga el privilegio para cambiar contraseñas.
c (cambiar contraseña)	El campo Password del panel Principal Basics es de sólo lectura y no se puede cambiar. Si no tiene el privilegio para cambiar contraseñas, no puede modificar ninguna contraseña de principal.  Tenga en cuenta que aunque tenga el privilegio para cambiar contraseñas, para poder cambiar la contraseña de un principal también debe tener el privilegio para modificar.
i (consultar la base de datos)	Los botones Modify y Duplicate no están disponibles en los paneles Principal List y Policy List. Si no tiene el privilegio para consultar, no puede modificar ni duplicar principales ni políticas.  Además, si el botón Modify no está disponible, no puede modificar ninguna contraseña de principal, aunque tenga el privilegio para cambiar contraseñas.
l (lista)	Las listas de principales y políticas de los paneles de lista no están disponibles. Si no tiene el privilegio de lista, debe utilizar el campo Name de los paneles de lista para especificar el principal o la política que desea manipular.

## Administración de los archivos keytab

Cada host que proporciona un servicio debe tener un archivo local, denominado *keytab* (la abreviatura en inglés de “tabla de claves”). El archivo keytab contiene el principal para el servicio adecuado, denominado *clave de servicio*. La clave de servicio es utilizada por un servicio para autenticarse a sí misma en el KDC, y sólo es conocida por Kerberos y el servicio. Por ejemplo, si tiene un servidor NFS Kerberizado, ese servidor debe tener un archivo keytab que contenga su principal de servicio `nfs`.

Para agregar una clave de servicio a un archivo keytab, agregue el principal de servicio correspondiente al archivo keytab de un host mediante el comando `ktadd` de `kadmin`. Como está agregando un principal de servicio a un archivo keytab, el principal ya debe existir en la base de datos de Kerberos para que `kadmin` pueda verificar su existencia. En el KDC maestro, el archivo keytab es ubica en `/etc/krb5/kadm5.keytab`, de manera predeterminada. En los servidores de aplicaciones que proporcionan servicios Kerberizados, el archivo keytab se encuentra en `/etc/krb5/krb5.keytab`, de manera predeterminada.

Un archivo keytab es análogo a la contraseña de un usuario. De la misma manera que es importante que los usuarios protejan sus contraseñas, es importante que los servidores de aplicaciones protejan sus archivos keytab. Siempre debe guardar los archivos keytab en un disco local y permitir su lectura sólo al usuario `root`. Asimismo, nunca debe enviar un archivo keytab a través una red no segura.

También hay una instancia especial en la que se debe agregar un principal `root` al archivo keytab de un host. Si desea que un usuario del cliente Kerberos monte sistemas de archivos NFS Kerberizados que requieren acceso equivalente a `root`, debe agregar el principal `root` del cliente al archivo keytab del cliente. De lo contrario, los usuarios deberán utilizar el comando `kinit` como `root` para obtener credenciales para el principal `root` del cliente cuando deseen montar un sistema de archivos NFS Kerberizado con acceso `root`, incluso cuando estén utilizando el montador automático.

---

**Nota** – Al configurar un KDC maestro, deberá agregar los principales `kadmin` y `changepw` al archivo `kadm5.keytab`.

---

Otro comando que puede utilizar para administrar los archivos keytab es el comando `ktutil`. Este comando interactivo le permite gestionar el archivo keytab de un host local sin tener privilegios de administración de Kerberos, porque `ktutil` no interactúa con la base de datos de Kerberos como lo hace `kadmin`. Por lo tanto, después de agregar un principal a un archivo keytab, puede usar `ktutil` para ver la lista de claves en un archivo keytab o para deshabilitar temporalmente la autenticación de un servicio.

**Nota** – Al cambiar un principal en un archivo keytab mediante el comando `ktadd` en `kadmin`, se genera una clave nueva y ésta se agrega al archivo keytab.

## Administración de archivos keytab (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Agregar un principal de servicio a un archivo keytab	Utilice el comando <code>ktadd</code> de <code>kadmin</code> para agregar un principal de servicio a un archivo keytab.	<a href="#">“Cómo agregar un principal de servicio de Kerberos a un archivo keytab” en la página 543</a>
Eliminar un principal de servicio de un archivo keytab	Utilice el comando <code>ktremove</code> de <code>kadmin</code> para eliminar un servicio de un archivo keytab.	<a href="#">“Cómo eliminar un principal de servicio de un archivo keytab” en la página 545</a>
Mostrar la lista de claves (lista de principales) en un archivo keytab	Utilice el comando <code>ktutil</code> para mostrar la lista de claves en un archivo keytab.	<a href="#">“Cómo visualizar la lista de claves (principales) en un archivo keytab” en la página 546</a>
Deshabilitar temporalmente la autenticación de un servicio en un host	<p>Este procedimiento es una manera rápida de deshabilitar temporalmente la autenticación de un servicio en un host sin la necesidad de contar con privilegios <code>kadmin</code>.</p> <p>Antes de utilizar <code>ktutil</code> para suprimir el principal de servicio del archivo keytab del servidor, copie el archivo keytab original en una ubicación temporal. Cuando desee habilitar el servicio nuevamente, vuelva a copiar el archivo keytab original en la ubicación correcta.</p>	<a href="#">“Cómo deshabilitar temporalmente la autenticación de un servicio en un host” en la página 547</a>

### ▼ Cómo agregar un principal de servicio de Kerberos a un archivo keytab

- 1 Asegúrese de que el principal ya exista en la base de datos de Kerberos.

Para obtener más información, consulte [“Cómo ver la lista de los principales de Kerberos” en la página 516](#).

- 2 Conviértase en superusuario en el host en el que necesita agregar un principal al archivo keytab.

- 3 Inicie el comando `kadmin`.

```
# /usr/sbin/kadmin
```

#### 4 Agregue un principal a un archivo keytab mediante el comando `ktadd`.

kadmin: `ktadd [-e enctype] [-k keytab] [-q] [principal | -glob principal-exp]`

`-e tipo_cifrado` Sustituye la lista de tipos de cifrado definida en el archivo `krb5.conf`.

`-k keytab` Especifica el archivo keytab. De manera predeterminada, se utiliza `/etc/krb5/krb5.keytab`.

`-q` Muestra menos información detallada.

`principal` Especifica el principal que se va a agregar al archivo keytab. Se pueden agregar los siguientes principales de servicio: `host`, `root`, `nfs` y `ftp`.

`-glob expresiones_principal` Especifica las expresiones de principal. Todos los principales que coinciden con las *expresiones\_principal* se agregan al archivo keytab. Las reglas de expresión de principal son las mismas que para el comando `list_principals` de kadmin.

#### 5 Salga del comando kadmin.

kadmin: `quit`

### Ejemplo 25–16 Adición de un principal de servicio a un archivo keytab

En el ejemplo siguiente, se agregan los principales `kadmin/kdc1.example.com` y `changepw/kdc1.example.com` al archivo keytab de un KDC maestro. En este ejemplo, el archivo keytab debe ser el archivo que se especifica en el archivo `kdc.conf`.

```
kdc1 # /usr/sbin/kadmin.local
kadmin.local: ktadd -k /etc/krb5/kadm5.keytab kadmin/kdc1.example.com changepw/kdc1.example.com
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-256 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal kadmin/kdc1.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-256 CTS
mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type AES-128 CTS
mode with 96-bit SHA-1 HMAC added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type Triple DES cbc
mode with HMAC/sha1 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILE:/etc/krb5/kadm5.keytab.
Entry for principal changepw/kdc1.example.com with kvno 3, encryption type DES cbc mode
```



with RSA-MD5 added to keytab WRFILe:/etc/krb5/kadm5.keytab.  
 kadmin.local: **quit**

En el siguiente ejemplo, el principal del host de denver se agrega al archivo keytab de denver para que el KDC pueda autenticar los servicios de red de denver.

```
denver # /usr/sbin/kadmin
kadmin: ktadd host/denver.example.com
Entry for principal host/denver.example.com with kvno 3, encryption type AES-256 CTS
mode with 96-bit SHA-1 HMAC added to keytab WRFILe:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type AES-128 CTS mode
with 96-bit SHA-1 HMAC added to keytab WRFILe:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type Triple DES cbc mode
with HMAC/sha1 added to keytab WRFILe:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type ArcFour
with HMAC/md5 added to keytab WRFILe:/etc/krb5/krb5.keytab.
Entry for principal host/denver.example.com with kvno 3, encryption type DES cbc mode
with RSA-MD5 added to keytab WRFILe:/etc/krb5/krb5.keytab.
kadmin: quit
```

## ▼ Cómo eliminar un principal de servicio de un archivo keytab

- 1 Conviértase en superusuario en el host con un principal de servicio que se debe eliminar de su archivo keytab.

- 2 Inicie el comando **kadmin**.

```
# /usr/sbin/kadmin
```

- 3 (Opcional) Para mostrar la lista actual de principales (claves) del archivo keytab, utilice el comando **ktutil**.

Para obtener instrucciones detalladas, consulte [“Cómo visualizar la lista de claves \(principales\) en un archivo keytab” en la página 546](#).

- 4 Elimine un principal del archivo keytab con el comando **ktremove**.

```
kadmin: ktrremove [-k keytab] [-q] principal [kvno | all | old ]
```

**-k keytab** Especifica el archivo keytab. De manera predeterminada, se utiliza /etc/krb5/krb5.keytab.

**-q** Muestra menos información detallada.

**principal** Especifica el principal que se va a eliminar del archivo keytab.

**kvno** Elimina todas las entradas del principal especificado cuyo número de versión de clave coincida con **kvno**.

**all** Elimina todas las entradas del principal especificado.

**old** Elimina todas las entradas del principal especificado, excepto las de los principales con el número de versión más alto.

**5 Salga del comando kadmin.**

kadmin: **quit**

**Ejemplo 25–17 Eliminación de un principal de servicio de un archivo keytab**

En el siguiente ejemplo, el principal del host `denver` se elimina del archivo keytab de `denver`.

```
denver # /usr/sbin/kadmin
kadmin: ktremove host/denver.example.com@EXAMPLE.COM
kadmin: Entry for principal host/denver.example.com@EXAMPLE.COM with kvno 3
        removed from keytab WRFILE:/etc/krb5/krb5.keytab.
kadmin: quit
```

## ▼ **Cómo visualizar la lista de claves (principales) en un archivo keytab**

**1 Conviértase en superusuario en el host con el archivo keytab.**

---

**Nota** – Si bien puede crear archivos keytab que son propiedad de otros usuarios, para usar la ubicación predeterminada para el archivo keytab se requiere la propiedad de `root`.

---

**2 Inicie el comando ktutil.**

# **/usr/bin/ktutil**

**3 Lea el archivo keytab en la memoria intermedia de la lista de claves con el comando read\_kt.**

ktutil: **read\_kt keytab**

**4 Visualice la memoria intermedia de lista de claves con el comando list.**

ktutil: **list**

Aparece la memoria intermedia de lista de claves actual.

**5 Salga del comando ktutil.**

ktutil: **quit**

**Ejemplo 25–18 Visualización de la lista de claves (principales) en un archivo keytab**

En el siguiente ejemplo, se muestra la lista de claves en el archivo `/etc/krb5/krb5.keytab` en el host `denver`.

```
denver # /usr/bin/ktutil
ktutil: read_kt /etc/krb5/krb5.keytab
ktutil: list
slot KVNO Principal
-----
1      5 host/denver@EXAMPLE.COM
ktutil: quit
```

## ▼ Cómo deshabilitar temporalmente la autenticación de un servicio en un host

En algunas ocasiones, es posible que necesite deshabilitar temporalmente el mecanismo de autenticación de un servicio, como `rlogin` o `ftp`, en un servidor de aplicaciones de red. Por ejemplo, es posible que desee impedir que los usuarios inicien sesión en un sistema mientras usted está realizando tareas de mantenimiento. El comando `ktutil` le permite realizar esta tarea mediante la eliminación del principal de servicio del archivo keytab del servidor, sin necesidad de privilegios `kadmin`. Para volver a habilitar la autenticación, sólo necesita copiar el archivo keytab original que guardó nuevamente en su ubicación original.

---

**Nota** – De manera predeterminada, la mayoría de los servicios están configurados para requerir autenticación. Si un servicio no está configurado para requerir autenticación, el servicio sigue funcionando, aunque deshabilite la autenticación del servicio.

---

### 1 Conviértase en superusuario en el host con el archivo keytab.

---

**Nota** – Si bien puede crear archivos keytab que son propiedad de otros usuarios, para usar la ubicación predeterminada para el archivo keytab se requiere la propiedad de `root`.

---

### 2 Guarde el archivo keytab actual en un archivo temporal.

### 3 Inicie el comando `ktutil`.

```
# /usr/bin/ktutil
```

### 4 Lea el archivo keytab en la memoria intermedia de la lista de claves con el comando `read_kt`.

```
ktutil: read_kt keytab
```

### 5 Visualice la memoria intermedia de lista de claves con el comando `list`.

```
ktutil: list
```

Aparece la memoria intermedia de lista de claves actual. Anote el número de ranura para el servicio que desea deshabilitar.

- 6 Para deshabilitar temporalmente un servicio de host, elimine el principal de servicio específico de la memoria intermedia de lista de claves con el comando `delete_entry`.

```
ktutil: delete_entry slot-number
```

Donde *número\_ranura* especifica el número de ranura del principal de servicio que se va a suprimir, el cual se muestra mediante el comando `list`.

- 7 Escriba la memoria intermedia de lista de claves en un nuevo archivo keytab mediante el comando `write_kt`.

```
ktutil: write_kt new-keytab
```

- 8 Salga del comando `ktutil`.

```
ktutil: quit
```

- 9 Mueva el nuevo archivo keytab.

```
# mv new-keytab keytab
```

- 10 Cuando desee volver a habilitar el servicio, copie el archivo keytab (original) temporal nuevamente en su ubicación original.

### Ejemplo 25–19 Inhabilitación temporal de un servicio en un host

En el ejemplo siguiente, el servicio de host en el host `denver` está inhabilitado temporalmente. Para volver a habilitar el servicio de host en `denver`, copie el archivo `krb5.keytab.temp` en el archivo `/etc/krb5/krb5.keytab`.

```
denver # cp /etc/krb5/krb5.keytab /etc/krb5/krb5.keytab.temp
denver # /usr/bin/ktutil
      ktutil:read_kt /etc/krb5/krb5.keytab
      ktutil:list
slot KVNO Principal
-----
1      8 root/denver@EXAMPLE.COM
2      5 host/denver@EXAMPLE.COM
      ktutil:delete_entry 2
      ktutil:list
slot KVNO Principal
-----
1      8 root/denver@EXAMPLE.COM
      ktutil:write_kt /etc/krb5/new.krb5.keytab
      ktutil: quit
denver # cp /etc/krb5/new.krb5.keytab /etc/krb5/krb5.keytab
```

## Uso de aplicaciones Kerberos (tareas)

---

Este capítulo está destinado para cualquiera que utiliza un sistema con el servicio Kerberos configurado. En este capítulo, se explica cómo utilizar los servicios y comandos “Kerberizados” que se proporcionan. Ya debe estar familiarizado con estos comandos (en sus versiones no Kerberizadas) antes de leer sobre ellos aquí.

Debido a que este capítulo está destinado para el lector general, se incluye información sobre cómo obtener, visualizar y destruir los tickets. Este capítulo también incluye información sobre cómo elegir o cambiar una contraseña de Kerberos.

A continuación, se indica la información contenida en este capítulo:

- “Gestión de tickets de Kerberos” en la página 549
- “Gestión de contraseñas de Kerberos” en la página 553
- “Comandos de usuario de Kerberos” en la página 558

Para obtener una descripción general del producto Kerberos de Oracle Solaris, consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#).

### Gestión de tickets de Kerberos

En esta sección, se explica cómo obtener, visualizar y destruir tickets. Para obtener una introducción a los tickets, consulte [“Cómo funciona el servicio Kerberos” en la página 394](#).

### ¿Debe preocuparse por los tickets?

Con cualquiera de las versiones de SEAM o las versiones de Oracle Solaris instaladas, Kerberos está integrado en el comando `login`, de modo que usted obtendrá los tickets automáticamente al iniciar sesión. Los comandos Kerberizados `rsh`, `rcp`, `rdist`, `telnet` y `rlogin`, por lo general, están configurados para reenviar copias de los tickets a otros equipos, de modo que no es necesario solicitar explícitamente los tickets para obtener acceso a esos equipos. Es posible que

la configuración no incluya este reenvío automático, pero es el comportamiento predeterminado. Consulte [“Descripción general de comandos Kerberizados” en la página 558](#) y [“Reenvío de tickets de Kerberos” en la página 561](#) para obtener más información sobre el reenvío de tickets.

Para obtener información sobre las duraciones de los tickets, consulte [“Duración de los tickets” en la página 572](#).

## Creación de un ticket de Kerberos

Normalmente, si el PAM se ha configurado correctamente, un ticket se crea automáticamente cuando inicia sesión, de modo que no tiene que hacer nada especial para obtener un ticket. Sin embargo, puede que necesite crear un ticket si su ticket caduca. Además, puede que necesite utilizar un principal diferente aparte del principal predeterminado, por ejemplo, si usa `rlogin -l` para iniciar sesión en un equipo como otro usuario.

Para crear un ticket, utilice el comando `kinit`.

```
% /usr/bin/kinit
```

El comando `kinit` le solicita la contraseña. Para conocer la sintaxis completa del comando `kinit`, consulte la página del comando `man kinit(1)`.

### EJEMPLO 26-1 Creación de un ticket de Kerberos

En este ejemplo, se muestra a un usuario, `jennifer`, que crea un ticket en su propio sistema.

```
% kinit
Password for jennifer@ENG.EXAMPLE.COM: <Type password>
```

Aquí, el usuario `david` crea un ticket que tiene una validez de tres horas, con la opción `-l`.

```
% kinit -l 3h david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

En este ejemplo, se muestra al usuario `david`, que crea un ticket reenviable (con la opción `-f`) para él. Con este ticket reenviable, puede, por ejemplo, iniciar sesión en un segundo sistema y, a continuación, ejecutar el comando `telnet` para iniciar sesión en un tercer sistema.

```
% kinit -f david@EXAMPLE.ORG
Password for david@EXAMPLE.ORG: <Type password>
```

Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 561](#) y [“Tipos de tickets” en la página 570](#).

## Visualización de tickets de Kerberos

No todos los tickets son similares. Por ejemplo, un ticket puede ser *reenviable*. Otro ticket puede ser *posfechado*. Mientras que un tercer ticket puede ser reenviable y posfechado. Puede ver los tickets que tiene y sus atributos utilizando el comando `klist` con la opción `-f`:

```
% /usr/bin/klist -f
```

Los siguientes símbolos indican los atributos asociados con cada ticket, como se muestra por `klist`:

A	Preautenticado
D	Posfechable
d	Posfechado
F	Reenviable
f	Reenviado
I	Inicial
i	No válido
P	Que admite proxy
p	Proxy
R	Renovable

En la sección “[Tipos de tickets](#)” en la [página 570](#), se describen los diferentes atributos que un ticket puede tener.

### EJEMPLO 26-2 Visualización de tickets de Kerberos

En este ejemplo, se muestra que el usuario `jennifer` tiene un ticket *inicial*, que es *reenviable* (F) y *posfechado* (d), pero que aún no está validado (i).

```
% /usr/bin/klist -f
Ticket cache: /tmp/krb5cc_74287
Default principal: jennifer@EXAMPLE.COM

Valid starting          Expires              Service principal
09 Mar 04 15:09:51      09 Mar 04 21:09:51  nfs/EXAMPLE.COM@EXAMPLE.COM
                    renew until 10 Mar 04 15:12:51, Flags: Fdi
```

El siguiente ejemplo muestra que el usuario `david` tiene dos tickets que fueron *reenviados* (f) al host desde otro host. Los tickets también son *reenviables* (F).

```
% klist -f
Ticket cache: /tmp/krb5cc_74287
```

**EJEMPLO 26-2** Visualización de tickets de Kerberos (Continuación)

Default principal: david@EXAMPLE.COM

```
Valid starting          Expires          Service principal
07 Mar 04 06:09:51    09 Mar 04 23:33:51  host/EXAMPLE.COM@EXAMPLE.COM
    renew until 10 Mar 04 17:09:51, Flags: fF
```

```
Valid starting          Expires          Service principal
08 Mar 04 08:09:51    09 Mar 04 12:54:51  nfs/EXAMPLE.COM@EXAMPLE.COM
    renew until 10 Mar 04 15:22:51, Flags: fF
```

El ejemplo siguiente muestra cómo visualizar los tipos de cifrado de la clave de sesión y el ticket mediante la opción `-e`. La opción `-a` se utiliza para asignar la dirección de host a un nombre de host si el servicio de nombres puede realizar la conversión.

% **klist -fea**

Ticket cache: /tmp/krb5cc\_74287

Default principal: david@EXAMPLE.COM

```
Valid starting          Expires          Service principal
07 Mar 04 06:09:51    09 Mar 04 23:33:51  krbtgt/EXAMPLE.COM@EXAMPLE.COM
    renew until 10 Mar 04 17:09:51, Flags: FRIA
    Etype(skey, tkt): DES cbc mode with RSA-MD5, DES cbc mode with CRC-32
    Addresses: client.example.com
```

## Destrucción de tickets de Kerberos

Si desea destruir todos los tickets de Kerberos adquiridos durante la sesión actual, utilice el comando `kdestroy`. El comando destruye la antememoria de credenciales, que destruye todas las credenciales y los tickets. Si bien esto no suele ser necesario, la ejecución de `kdestroy` reduce las posibilidades de que la antememoria de credenciales esté en riesgo en los momentos en los que no tiene ninguna sesión iniciada.

Para destruir los tickets, utilice el comando `kdestroy`.

% **/usr/bin/kdestroy**

El comando `kdestroy` destruye *todos* los tickets. No puede utilizar este comando para destruir de manera selectiva un determinado ticket.

Si no va a utilizar el sistema y le preocupa que un intruso use sus permisos, debe utilizar `kdestroy` o un protector de pantalla que bloquea la pantalla.



# Gestión de contraseñas de Kerberos

Con el servicio Kerberos configurado, ahora tiene dos contraseñas: la contraseña regular de Solaris y una contraseña de Kerberos. Ambas contraseñas pueden ser iguales o pueden ser diferentes.

## Consejos para elegir una contraseña

La contraseña puede incluir casi cualquier carácter que se pueda escribir. Las principales excepciones son las teclas Ctrl y la tecla de retorno. Una buena contraseña es una contraseña que se puede recordar con rapidez, pero que ningún otro usuario puede adivinar fácilmente. Ejemplos de contraseñas incorrectas:

- Palabras que se pueden encontrar en un diccionario
- Cualquier nombre común o popular
- El nombre de una persona famosa o un personaje
- El nombre o nombre de usuario en cualquier forma (por ejemplo: el nombre escrito hacia atrás, repetido dos veces, etc.)
- El nombre de un cónyuge, de un hijo o de una mascota
- La fecha de nacimiento o la fecha de nacimiento de un familiar
- El número de seguridad social, el número de licencia de conducir, el número de pasaporte u otro número de identificación similar
- Cualquier contraseña de ejemplo que aparece en este manual o en cualquier otro manual

Una contraseña correcta tiene, al menos, ocho caracteres de longitud. Además, una contraseña debe incluir una combinación de caracteres, como letras en mayúscula y minúscula, números y signos de puntuación. Ejemplos de contraseñas que serían correctas si no aparecieran en este manual:

- Acrónimos, como “I2LMHinSF” (que se recuerda como “I too left my heart in San Francisco”)
- Palabras sin sentido fáciles de pronunciar, como “WumpaBun” o “WangDangdoodle!”
- Frases escritas de manera incorrecta deliberadamente, como “6o'cluck” o “RrriotGrrrlsRrrule!”



**Precaución** – No utilice estos ejemplos. Las contraseñas que aparecen en los manuales son las primeras contraseñas que un intruso probará.

---

## Cambio de la contraseña

Si el PAM se ha configurado correctamente, puede cambiar la contraseña de Kerberos de dos maneras:

- Con el comando `passwd` de UNIX usual. Con el servicio Kerberos configurado, el comando `passwd` también solicita automáticamente una nueva contraseña de Kerberos.

La ventaja de utilizar `passwd` en lugar de `kpasswd` es que puede establecer las contraseñas de UNIX y Kerberos al mismo tiempo. Sin embargo, normalmente, *no tiene* que cambiar ambas contraseñas con `passwd`. A menudo, sólo puede cambiar su contraseña de UNIX y dejar la contraseña de Kerberos intacta, o viceversa.

---

**Nota** – El comportamiento de `passwd` depende de cómo el módulo PAM está configurado. Es posible que se le requiera que cambie las dos contraseñas en algunas configuraciones. Algunos sitios requieren que se cambie la contraseña de UNIX, mientras que otros sitios requieren que se cambie la contraseña de Kerberos.

---

- Con el comando `kpasswd`. `kpasswd` es muy similar a `passwd`. Una diferencia es que `kpasswd` sólo cambia contraseñas de Kerberos. Debe utilizar `passwd` si desea cambiar la contraseña de UNIX.

Otra diferencia es que `kpasswd` puede cambiar una contraseña para un principal de Kerberos que no es un usuario de UNIX válido. Por ejemplo, `david/admin` es un principal de Kerberos, pero no es un usuario de UNIX real, por lo que debe utilizar `kpasswd` en lugar de `passwd`.

Después de cambiar la contraseña, el cambio tarda un tiempo en propagarse por un sistema (especialmente, en una red grande). En función de cómo está configurado el sistema, este tiempo puede ser de unos pocos minutos a una hora o más. Si necesita obtener nuevos tickets de Kerberos poco tiempo después de cambiar la contraseña, pruebe la nueva contraseña primero. Si la contraseña nueva no funciona, vuelva a intentarlo utilizando la contraseña antigua.

El protocolo Kerberos V5 permite a los administradores del sistema establecer criterios sobre contraseñas permitidas para cada usuario. Esos criterios son definidos por la *política* establecida para cada usuario (o por una política predeterminada). Consulte [“Administración de las políticas de Kerberos” en la página 528](#) para obtener más información sobre las políticas.

Por ejemplo, suponga que la política del usuario `jennifer` (denomínela `jenpol`) exige que las contraseñas deben tener, como mínimo, ocho caracteres y deben incluir una combinación de, al menos, dos tipos de caracteres. `kpasswd`, por lo tanto, rechazará un intento de utilizar “sloth” como contraseña.

% **kpasswd**

kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.

```

Old password:      <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'sloth'>
New password (again): <Jennifer re-types 'sloth'>
kpasswd: New password is too short.
Please choose a password which is at least 4 characters long.

```

Aquí, jennifer utiliza “slothrop49” como contraseña. La contraseña “slothrop49” cumple los criterios porque tiene más de ocho letras y contiene dos tipos diferentes de caracteres (números y letras minúsculas).

```

% kpasswd
kpasswd: Changing password for jennifer@ENG.EXAMPLE.COM.
Old password:      <Jennifer types her existing password>
kpasswd: jennifer@ENG.EXAMPLE.COM's password is controlled by
the policy jenpol
which requires a minimum of 8 characters from at least 2 classes
(the five classes are lowercase, uppercase, numbers, punctuation,
and all other characters).
New password:      <Jennifer types 'slothrop49'>
New password (again): <Jennifer re-types 'slothrop49'>
Kerberos password changed.

```

#### EJEMPLO 26-3 Cambio de la contraseña

En el ejemplo siguiente, el usuario david cambia tanto la contraseña de UNIX como la contraseña de Kerberos con passwd.

```

% passwd
passwd: Changing password for david
Enter login (NIS+) password:                <Type the current UNIX password>
New password:                               <Type the new UNIX password>
Re-enter password:                           <Confirm the new UNIX password>
Old KRB5 password:                           <Type the current Kerberos password>
New KRB5 password:                           <Type the new Kerberos password>
Re-enter new KRB5 password:                   <Confirm the new Kerberos password>

```

Tenga en cuenta que passwd solicita tanto la contraseña de UNIX como la contraseña de Kerberos. Este comportamiento es establecido por la configuración predeterminada. En ese caso, el usuario david debe usar kpasswd para establecer la contraseña de Kerberos como otra cosa, como se muestra a continuación.

En este ejemplo, se muestra al usuario david, que cambia sólo la contraseña de Kerberos con kpasswd.

**EJEMPLO 26-3** Cambio de la contraseña (Continuación)

```
% kpasswd
kpasswd: Changing password for david@ENG.EXAMPLE.COM.
Old password:          <Type the current Kerberos password>
New password:          <Type the new Kerberos password>
New password (again):  <Confirm the new Kerberos password>
Kerberos password changed.
```

En este ejemplo, el usuario david cambia la contraseña del principal de Kerberos david/admin (que no es un usuario de UNIX válido). Debe utilizar kpasswd.

```
% kpasswd david/admin
kpasswd: Changing password for david/admin.
Old password:          <Type the current Kerberos password>
New password:          <Type the new Kerberos password>
New password (again):  <Type the new Kerberos password>
Kerberos password changed.
```

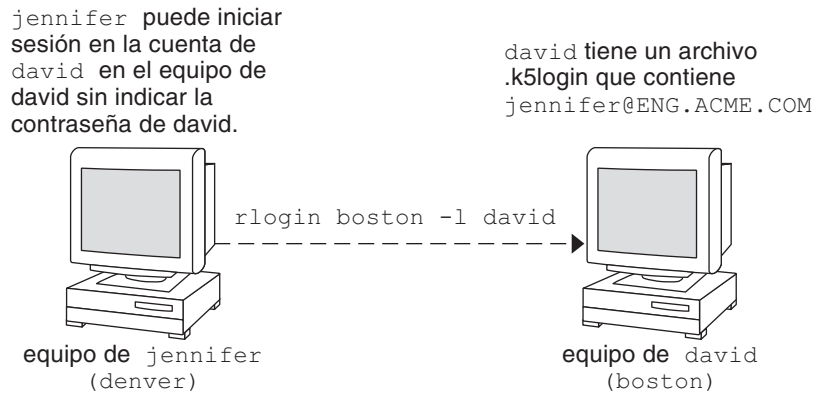
## Otorgamiento de acceso a su cuenta

Si tiene que otorgarle a alguien acceso para que inicie sesión en su cuenta (como usted), puede hacerlo mediante Kerberos, sin revelar su contraseña, colocando un archivo .k5login en el directorio principal. Un archivo .k5login es una lista de uno o más principales de Kerberos correspondientes a cada persona a la que desea otorgar acceso. Cada principal debe estar en una línea diferente.

Suponga que el usuario david tiene un archivo .k5login en el directorio principal, como el siguiente:

```
jennifer@ENG.EXAMPLE.COM
joe@EXAMPLE.ORG
```

Este archivo permite a los usuarios jennifer y joe asumir la identidad de david, siempre y cuando ya tengan tickets de Kerberos en sus respectivos dominios. Por ejemplo, jennifer puede iniciar sesión de manera remota en el equipo de david (boston), como si fuera él, sin tener que indicar la contraseña de david.

**FIGURA 26-1** Uso del archivo `.k5login` para otorgar acceso a su cuenta

En el caso donde el directorio principal de david está montado en NFS, mediante protocolos Kerberos V5, desde otro equipo (un tercer equipo), jennifer debe tener un ticket reenviable para acceder al directorio principal de david. Consulte [“Creación de un ticket de Kerberos” en la página 550](#) para obtener un ejemplo del uso de un ticket reenviable.

Si va a iniciar sesión en otros equipos de una red, es posible que desee incluir su propio principal de Kerberos en los archivos `.k5login` de esos equipos.

Usar un archivo `.k5login` es mucho más seguro que dar la contraseña, debido a los siguientes motivos:

- Puede quitar el acceso en cualquier momento eliminando el principal del archivo `.k5login`.
- Aunque los principales de usuarios nombrados en el archivo `.k5login` del directorio principal tengan acceso completo a su cuenta en ese equipo (o conjuntos de equipos si el archivo `.k5login` se comparte, por ejemplo, por medio de NFS). Sin embargo, cualquier servicio Kerberizado autorizará el acceso según la identidad del usuario, no la suya. Por lo tanto, jennifer puede iniciar sesión en el equipo de joe y realizar tareas allí. No obstante, si utiliza un programa Kerberizado, como `ftp` o `rlogin`, lo hace como ella misma.
- Kerberos mantiene un registro de quién obtiene tickets, por lo que un administrador del sistema puede detectar, si es necesario, quién puede utilizar su identidad de usuario en un momento concreto.

Una manera común de utilizar el archivo `.k5login` es colocarlo en el directorio principal de root, con lo cual se otorga a root acceso para ese equipo a los principales de Kerberos enumerados. Esta configuración permite que los administradores del sistema se conviertan en root localmente o inicien sesión de manera remota como root sin tener que proporcionar la contraseña de root y sin requerir que ningún usuario escriba la contraseña de root por medio de la red.

**EJEMPLO 26-4** Uso del archivo `.k5login` para otorgar acceso a su cuenta

Suponga que `jennifer` decide iniciar sesión en el equipo `boston.example.com` como `root`. Debido a que tiene una entrada para el nombre de principal en el archivo `.k5login` del directorio principal de `root` en `boston.example.com`, tampoco tiene que escribir su contraseña.

```
% rlogin boston.example.com -l root -x
This rlogin session is using DES encryption for all data transmissions.
Last login: Thu Jun 20 16:20:50 from daffodil
SunOS Release 5.7 (GENERIC) #2: Tue Nov 14 18:09:31 EST 1998
boston[root]%
```

## Comandos de usuario de Kerberos

El producto Kerberos V5 es un sistema de *inicio de sesión único*, lo que significa que sólo tiene que escribir la contraseña una vez. Los programas Kerberos V5 realizan la autenticación (y el cifrado opcional) porque Kerberos se ha integrado en cada paquete de programas de red familiares existentes. Las aplicaciones Kerberos V5 son versiones de programas de red UNIX existentes con las funciones de Kerberos agregadas.

Por ejemplo, cuando utiliza un programa Kerberizado para conectarse a un host remoto, el programa, el KDC y el host remoto realizan un conjunto de negociaciones rápidas. Cuando estas negociaciones están completas, el programa ha aprobado su identidad en su nombre para el host remoto, y el host remoto le ha otorgado acceso.

Tenga en cuenta que los comandos Kerberizados primero intentan autenticarse con Kerberos. Si la autenticación Kerberos falla, se produce un error o se intenta la autenticación UNIX, según las opciones que se utilizaron con el comando. Consulte la sección *Kerberos Security* en cada página del comando `man` del comando Kerberos para obtener información más detallada.

## Descripción general de comandos Kerberizados

Los servicios de red Kerberizados son programas que se conectan a otro equipo en algún lugar de Internet. Estos programas son los siguientes:

- `ftp`
- `rcp`
- `rdist`
- `rlogin`
- `rsh`
- `ssh`
- `telnet`

Estos programas tienen funciones que utilizan de forma transparente los tickets de Kerberos para negociar la autenticación y el cifrado opcional con el host remoto. En la mayoría de los casos, sólo observará que ya no tiene que escribir la contraseña para utilizarlos, ya que Kerberos proporciona prueba de su identidad.

Los programas de red Kerberos V5 incluyen opciones que permiten realizar lo siguiente:

- Reenviar los tickets al otro host (si inicialmente obtuvo tickets reenviables).
- Cifrar datos transmitidos entre usted y el host remoto.

---

**Nota** – En esta sección, se asume que ya está familiarizado con las versiones no Kerberizadas de estos programas, y se resalta la funcionalidad de Kerberos agregada por el paquete Kerberos V5. Para obtener descripciones detalladas de los comandos que se describen aquí, consulte las respectivas páginas del comando `man`.

---

Las siguientes opciones de Kerberos se han agregado a `ftp`, `rcp`, `rlogin`, `rsh` y `telnet`:

- a                      Intenta el inicio de sesión automático usando sus tickets existentes. Utiliza el nombre de usuario devuelto por `getlogin()`, salvo que el nombre sea diferente del ID de usuario actual. Consulte la página del comando `man telnet(1)` para obtener detalles.
- f                      Reenvía un ticket *no reenviable* a un host remoto. Esta opción es mutuamente excluyente con la opción -F. No se pueden utilizar juntas en el mismo comando.

Es posible que desee reenviar un ticket si tiene motivos para creer que deberá autenticarse con otros servicios basados en Kerberos en un tercer host. Por ejemplo, es posible que desee iniciar sesión de manera remota en otro equipo y, a continuación, iniciar sesión de manera remota desde él en un tercer equipo.

Definitivamente debe usar un ticket reenviable si el directorio principal en el host remoto se monta en NFS utilizando el mecanismo Kerberos V5. De lo contrario, no podrá acceder a su directorio principal. Es decir, suponga que inicia sesión por primera vez en el sistema 1. Desde el sistema 1, inicia sesión remotamente en el equipo doméstico, el sistema 2, que monta el directorio principal del sistema 3. A menos que haya utilizado la opción -f o -F con `rlogin`, no podrá acceder al directorio principal porque el ticket no se puede reenviar al sistema 3.

De manera predeterminada, `kinit` obtiene tickets de otorgamiento de tickets (TGT) reenviables. Sin embargo, la configuración puede ser diferente en este sentido.

Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 561](#).

- F Reenvía una copia *reenviable* de su TGT a un sistema remoto. Es similar a - f, pero permite el acceso a un equipo más (es decir, un cuarto o quinto equipo). La opción - F, por lo tanto, puede considerarse un conjunto universal de la opción - f. La opción - F es mutuamente excluyente con la opción - f. No se pueden utilizar juntas en el mismo comando.
- k *dominio* Para obtener más información sobre el reenvío de tickets, consulte [“Reenvío de tickets de Kerberos” en la página 561](#). Solicita tickets para el host remoto en el *dominio* especificado, en lugar de determinar el dominio usando el archivo `krb5.conf`.
- K Utiliza sus tickets para autenticarse en el host remoto, pero no inicia sesión automáticamente.
- m *mecanismo* Especifica el mecanismo de seguridad GSS-API para utilizar, como se muestra en el archivo `/etc/gss/mech`. De manera predeterminada, este mecanismo es `kerberos_v5`.
- x Cifra esta sesión.
- X *tipo\_autenticación* Deshabilita el tipo de autenticación *tipo\_autenticación*.

En la siguiente tabla, se muestra qué comandos tienen opciones específicas. Una "X" indica que el comando tiene esa opción.

TABLA 26-1 Opciones de Kerberos para comandos de red

	ftp	rcp	rlogin	rsh	telnet
- a					X
- f	X		X	X	X
- F			X	X	X
- k		X	X	X	X
- K					X
- m	X				
- x	X	X	X	X	X
- X					X

Además, `ftp` permite que el nivel de protección de una sesión se establezca en el indicador:



clear	Establece el nivel de protección en "clear" (sin cifrar), es decir, sin protección. Este nivel de protección es el valor predeterminado.
private	Establece el nivel de protección en "private" (privado). La confidencialidad y la integridad de las transmisiones de datos se protegen mediante el cifrado. No obstante, es posible que el servicio de privacidad no esté disponible para todos los usuarios de Kerberos.
safe	Establece el nivel de protección en "safe" (seguro). La integridad de las transmisiones de datos se protege mediante la suma de comprobación criptográfica.

También puede definir el nivel de protección en el indicador ftp escribiendo `protect` seguido de cualquiera de los niveles de protección mostrados anteriormente (`clear`, `private` o `safe`).

## Reenvío de tickets de Kerberos

Como se describe en [“Descripción general de comandos Kerberizados” en la página 558](#), algunos comandos permiten reenviar tickets con la opción `-f` o `-F`. El reenvío de tickets le permite "encadenar" las transacciones de la red. Puede, por ejemplo, iniciar sesión de manera remota en un equipo y, a continuación, iniciar sesión de manera remota desde él en otro equipo. La opción `-f` permite reenviar un ticket, mientras que la opción `-F` permite reenviar un ticket reenviado.

En la [Figura 26-2](#), el usuario david obtiene un ticket de otorgamiento de tickets (TGT) no reenviable con `kinit`. El ticket no es reenviable porque no especificó la opción `-f`. En el escenario 1, puede iniciar sesión de manera remota en el equipo B, pero no puede hacer nada más. En el escenario 2, el comando `rlogin -f` falla debido a que está intentando reenviar un ticket que no es reenviable.

FIGURA 26-2 Uso de tickets no reenviables

1. (En A): `kinit david@ACME.ORG`



2. (En A): `kinit david@ACME.ORG`



En realidad, los archivos de configuración de Kerberos están configurados para que `kinit` obtenga tickets reenviables de manera predeterminada. Sin embargo, la configuración puede diferir. Para una mejor explicación, suponga que `kinit` no obtiene TGT reenviables, a menos que se invoque con `kinit -f`. Por otro lado, observe que `kinit` no tiene una opción `-F`. Los TGT son reenviables o no reenviables.

En la [Figura 26-3](#), el usuario `david` obtiene TGT reenviables con `kinit -f`. En el escenario 3, puede acceder al equipo C debido a que utiliza un ticket reenviable con `rlogin`. En el escenario 4, el segundo `rlogin` falla debido a que el ticket no es reenviable. Mediante la opción `-F`, en cambio, como en el escenario 5, el segundo `rlogin` se realiza correctamente, y el ticket se puede reenviar al equipo D.

FIGURA 26-3 Uso de tickets reenviables

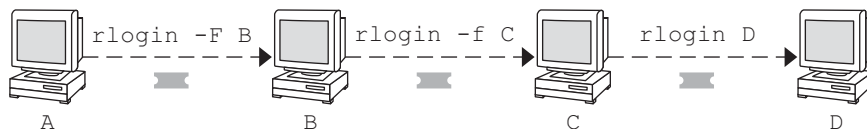
3. (En A): `kinit -f david@ACME.ORG`



4. (En A): `kinit -f david@ACME.ORG`



5. (En A): `kinit -f david@ACME.ORG`



## Uso de comandos Kerberizados (ejemplos)

Los siguientes ejemplos muestran cómo funcionan las opciones para los comandos Kerberizados.

**EJEMPLO 26-5** Uso de las opciones `-a`, `-f` y `-x` con `telnet`

En este ejemplo, el usuario `david` ya ha iniciado sesión y desea ejecutar el comando `telnet` para iniciar sesión en el equipo `denver.example.com`. Utiliza la opción `-f` para reenviar sus tickets,

**EJEMPLO 26-5** Uso de las opciones -a, -f y -x con telnet (Continuación)

la opción -x para cifrar la sesión y la opción -a para realizar el inicio de sesión automáticamente. Debido a que no planea utilizar los servicios de un tercer host, puede utilizar -f en lugar de -F.

```
% telnet -a -f -x denver.example.com
Trying 128.0.0.5...
Connected to denver.example.com. Escape character is '^]'.
[ Kerberos V5 accepts you as "david@eng.example.com" ]
[ Kerberos V5 accepted forwarded credentials ]
SunOS 5.9: Tue May 21 00:31:42 EDT 2004 Welcome to SunOS
%
```

Tenga en cuenta que el equipo de david utilizó Kerberos para autenticarlo en denver.example.com e inició sesión automáticamente como él mismo. Tenía una sesión cifrada, una copia de sus tickets esperándolo y nunca tuvo que escribir su contraseña. Si hubiera utilizado una versión de telnet no Kerberizada, se le habría solicitado la contraseña, y la contraseña se habría enviado por la red sin cifrar. En este caso, si un intruso hubiese estado observando el tráfico de la red en ese momento, habría visto la contraseña de david.

Si reenvía los tickets de Kerberos, telnet (así como los otros comandos proporcionados aquí) los destruye cuando se cierra.

**EJEMPLO 26-6** Uso de rlogin con la opción -F

Aquí, el usuario jennifer desea iniciar sesión en su propio equipo, boston.example.com. Reenvía sus tickets con la opción -F y cifra la sesión con la opción -x. Elige -F en lugar de -f porque, después de iniciar sesión en boston, es posible que desee realizar otras transacciones de la red que requieren que los tickets se reenvíen. Además, como está reenviando sus tickets existentes, no tiene que escribir la contraseña.

```
% rlogin boston.example.com -F -x
This rlogin session is using encryption for all transmissions.
Last login Mon May 19 15:19:49 from daffodil
SunOS Release 5.9 (GENERIC) #2 Tue Nov 14 18:09:3 EST 2003
%
```

**EJEMPLO 26-7** Configuración del nivel de protección en ftp

Suponga que joe desea usar ftp para obtener su correo desde el directorio ~joe/MAIL del equipo denver.example.com mediante el cifrado de la sesión. El intercambio sería de la siguiente manera:

```
% ftp -f denver.example.com
Connected to denver.example.com
220 denver.example.org FTP server (Version 6.0) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
```

**EJEMPLO 26-7** Configuración del nivel de protección en ftp *(Continuación)*

```
GSSAPI authentication succeeded Name (daffodil.example.org:joe)
232 GSSAPI user joe@MELPOMENE.EXAMPLE.COM is authorized as joe
230 User joe logged in.
Remote system type is UNIX.
Using BINARY mode to transfer files.
ftp> protect private
200 Protection level set to Private
ftp> cd ~joe/MAIL
250 CWD command successful.
ftp> get RMAIL
227 Entering Passive Mode (128,0,0,5,16,49)
150 Opening BINARY mode data connection for RMAIL (158336 bytes).
226 Transfer complete. 158336 bytes received in 1.9 seconds (1.4e+02 Kbytes/s)
ftp> quit
%
```

Para cifrar la sesión, joe establece el nivel de protección en private.

## El servicio Kerberos (referencia)

---

En este capítulo, se enumeran muchos de los archivos, comandos y daemons que forman parte del producto Kerberos. Además, se proporciona información detallada sobre cómo funciona la autenticación Kerberos.

A continuación, se indica la información de referencia contenida en este capítulo.

- “Archivos de Kerberos” en la página 565
- “Comandos de Kerberos” en la página 567
- “Daemons de Kerberos” en la página 568
- “Terminología de Kerberos” en la página 569
- “Cómo funciona el sistema de autenticación Kerberos” en la página 575
- “Obtención de acceso a un servicio con Kerberos” en la página 575
- “Uso de los tipos de cifrado de Kerberos” en la página 579
- “Tabla de uso de `gsscred`” en la página 581
- “Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos” en la página 581

## Archivos de Kerberos

TABLA 27-1 Archivos de Kerberos

Nombre de archivo	Descripción
<code>~/gkadmin</code>	Valores predeterminados para la creación de nuevos principales en la herramienta SEAM
<code>~/k5login</code>	Lista de principales que otorgan acceso a una cuenta de Kerberos
<code>/etc/krb5/kadm5.acl</code>	Archivo de lista de control de acceso de Kerberos, que incluye los nombres de principales de los administradores de KDC y sus privilegios de administración de Kerberos

TABLA 27-1 Archivos de Kerberos (Continuación)

Nombre de archivo	Descripción
/etc/krb5/kadm5.keytab	Archivo keytab para el servicio kadmind en el KDC maestro
/etc/krb5/kdc.conf	Archivo de configuración de KDC
/etc/krb5/kpropd.acl	Archivo de configuración de propagación de bases de datos de Kerberos
/etc/krb5/krb5.conf	Archivo de configuración de dominios de Kerberos
/etc/krb5/krb5.keytab	Archivo keytab para servidores de aplicaciones de redes
/etc/krb5/warn.conf	Archivo de configuración de renovación automática y advertencia de caducidad de ticket de Kerberos
/etc/pam.conf	Archivo de configuración de PAM
/tmp/krb5cc_uid	Antememoria de credenciales predeterminadas, en la que <i>uid</i> es el UID decimal del usuario
/tmp/ovsec_admin.xxxxxx	Credenciales temporales por la duración de la operación para cambio de contraseña, donde <i>xxxxxx</i> es una cadena aleatoria
/var/krb5/.k5.DOMINIO	Archivo intermedio de KDC, que contiene una copia de la clave maestra de KDC
/var/krb5/kadmind.log	Archivo de registro para kadmind
/var/krb5/kdc.log	Archivo de registro para el KDC
/var/krb5/principal	Base de datos principal de Kerberos
/var/krb5/principal.kadm5	Base de datos administrativa de Kerberos, que contiene información sobre políticas
/var/krb5/principal.kadm5.lock	Archivo de bloqueo de bases de datos administrativas de Kerberos
/var/krb5/principal.ok	Archivo de inicialización de base de datos principal de Kerberos que se crea cuando la base de datos de Kerberos se inicializa con éxito
/var/krb5/principal.ulong	Registro de actualización de Kerberos, que contiene actualizaciones para la propagación progresiva
/var/krb5/slave_datatrans	Archivo de copia de seguridad del KDC que la secuencia de comandos <i>kprop_script</i> utiliza para la propagación

TABLA 27-1 Archivos de Kerberos (Continuación)

Nombre de archivo	Descripción
<code>/var/krb5/slave_datatrans_esclavo</code>	Archivo de volcado temporal que se crea cuando se realizan las actualizaciones completas del <i>esclavo</i> especificado

## Comandos de Kerberos

En esta sección, se enumeran algunos comandos que se incluyen en el producto Kerberos.

TABLA 27-2 Comandos de Kerberos

Comando	Descripción
<code>/usr/bin/ftp</code>	Programa del protocolo de transferencia de archivos
<code>/usr/bin/kdestroy</code>	Destruye los tickets de Kerberos
<code>/usr/bin/kinit</code>	Obtiene tickets de otorgamiento de tickets de Kerberos y los almacena en la antememoria
<code>/usr/bin/klint</code>	Muestra los tickets de Kerberos actuales
<code>/usr/bin/kpasswd</code>	Cambia una contraseña de Kerberos
<code>/usr/bin/ktutil</code>	Gestiona los archivos keytab de Kerberos
<code>/usr/bin/rcp</code>	Programa de copia de archivos remota
<code>/usr/bin/rdist</code>	Programa de distribución de archivos remota
<code>/usr/bin/rlogin</code>	Programa de inicio de sesión remoto
<code>/usr/bin/rsh</code>	Programa de shell remoto
<code>/usr/bin/telnet</code>	Programa de telnet kerberizado
<code>/usr/lib/krb5/kprop</code>	Programa de propagación de bases de datos de Kerberos
<code>/usr/sbin/gkadmin</code>	Programa de interfaz gráfica de usuario de administración de bases de datos de Kerberos, que se utiliza para gestionar los principales y las políticas
<code>/usr/sbin/gsscred</code>	Gestionar las entradas de la tabla gsscred
<code>/usr/sbin/kadmin</code>	Programa de administración de bases de datos de Kerberos remoto (se ejecuta con autenticación Kerberos), que se utiliza para gestionar los principales, las políticas y los archivos keytab

TABLA 27-2 Comandos de Kerberos (Continuación)	
Comando	Descripción
/usr/sbin/kadmin.local	Programa de administración de bases de datos de Kerberos local (debe ejecutarse con la autenticación Kerberos en el KDC maestro), que se utiliza para gestionar los principales, las políticas y los archivos keytab
/usr/sbin/kclient	Secuencia de comandos de instalación de cliente Kerberos que se utiliza con o sin un perfil de instalación
/usr/sbin/kdb5_ldap_util	Crea contenedores LDAP para las bases de datos de Kerberos
/usr/sbin/kdb5_util	Crea archivos intermedios y bases de datos de Kerberos
/usr/sbin/kgcmgr	Configura KDC maestros y esclavos de Kerberos
/usr/sbin/kproplog	Contiene un resumen de las entradas del registro de actualización

## Daemons de Kerberos

La siguiente tabla enumera los daemons que utiliza el producto Kerberos.

TABLA 27-3 Daemons de Kerberos	
Daemon	Descripción
/usr/sbin/in.ftpd	Daemon del protocolo de transferencia de archivos
/usr/lib/krb5/kadmind	Daemon de administración de bases de datos de Kerberos
/usr/lib/krb5/kpropd	Daemon de propagación de bases de datos de Kerberos
/usr/lib/krb5/krb5kdc	Daemon de procesamiento de tickets de Kerberos
/usr/lib/krb5/ktkt_warnd	Daemon de renovación automática y advertencia de caducidad de ticket de Kerberos
/usr/sbin/in.rlogind	Daemon de inicio de sesión remoto
/usr/sbin/in.rshd	Daemon de shell remoto
/usr/sbin/in.telnetd	Daemon de telnet



# Terminología de Kerberos

La siguiente sección presenta los términos de Kerberos con sus definiciones. Estos términos se utilizan en toda la documentación de Kerberos. Para incorporar los conceptos de Kerberos, resulta esencial comprender estos términos.

## Terminología específica de Kerberos

Para administrar los KDC, debe comprender los términos de esta sección.

El *Centro de distribución de claves*, o *KDC*, es el componente de Kerberos que se encarga de la emisión de credenciales. Para crear estas credenciales, se utiliza la información que está almacenada en la base de datos del KDC. Cada dominio necesita al menos dos KDC, uno que sea maestro y al menos uno que sea esclavo. Todos los KDC generan credenciales, pero únicamente el KDC maestro realiza los cambios en la base de datos del KDC.

El *archivo intermedio* la clave maestra para el KDC. Esta clave se utiliza cuando se reinicia un servidor para autenticar el KDC automáticamente antes de iniciar los comandos `kadmind` y `krb5kdc`. Como este archivo contiene la clave maestra, el archivo y cualquier copia de seguridad del archivo deben permanecer seguros. El archivo se crea con permisos de sólo lectura para el usuario `root`. Para mantener el archivo seguro, no cambie los permisos. Si el archivo corre peligro, la clave podría ser utilizada para acceder a la base de datos del KDC o para modificarla.

## Terminología específica de la autenticación

Debe conocer los términos de esta sección para comprender el proceso de autenticación. Los programadores y los administradores del sistema deben estar familiarizados con estos términos.

El *cliente* es el software que se ejecuta en la estación de trabajo del usuario. El software de Kerberos que se ejecuta en el cliente realiza muchas solicitudes durante este proceso. Por lo tanto, es importante establecer la diferencia entre las acciones de este software y el usuario.

Los términos *servidor* y *servicio* suelen utilizarse de manera indistinta. El término *servidor* se utiliza para definir el sistema físico en el que se ejecuta el software de Kerberos. El término *servicio* corresponde a una determinada función que se admite en un servidor (por ejemplo, `ftp` o `nfs`). Con frecuencia, la documentación define los servidores como una parte de un servicio, pero esta definición hace que el significado de los términos sea confuso. Por lo tanto, el término *servidor* se refiere al sistema físico. El término *servicio* se refiere al software.

El producto Kerberos usa dos tipos de claves. Un tipo de clave es una clave derivada de contraseña. La clave derivada de contraseña se otorga a cada principal de usuario, y sólo el usuario y el KDC la conocen. El otro tipo de clave que el producto Kerberos utiliza es una clave aleatoria que no está asociada con una contraseña y que, por lo tanto, no es adecuada para que la

usen los principales de usuario. Por lo general, las claves aleatorias se usan para los principales de servicio que tienen entradas en un archivo keytab y claves de sesión generadas por el KDC. Los principales de servicio pueden usar claves aleatorias, ya que el servicio puede acceder a la clave que se encuentra en el archivo keytab y entonces puede ejecutarse de manera no interactiva. Las claves de sesión son generadas por el KDC (y compartidas entre el cliente y el servicio) a fin de facilitar las transacciones seguras entre un cliente y un servicio.

El *ticket* es un paquete de información que se utiliza para transferir la identidad de un usuario a un servidor o servicio de manera segura. Un ticket es válido únicamente para un solo cliente y un servicio determinado en un servidor específico. El ticket contiene:

- Nombre de principal del servicio
- Nombre de principal del usuario
- Dirección IP del host del usuario
- Indicación de hora
- Valor que define la duración del ticket
- Copia de la clave de sesión

Todos estos datos se encuentran cifrados en la clave de servicio del servidor. Tenga en cuenta que el KDC emite el ticket integrado en una credencial, que se describe en el siguiente párrafo. Una vez que se emitió un ticket, éste puede volver a usarse hasta que caduque.

La *credencial* es un paquete de información que incluye un ticket y una clave de sesión coincidente. La credencial está cifrada con la clave del principal solicitante. Generalmente, el KDC genera una credencial en respuesta a una solicitud de ticket de un cliente.

El *autenticador* es la información utilizada por el servidor para autenticar el principal del usuario cliente. El autenticador incluye el nombre de principal del usuario, la indicación de hora y otros datos. A diferencia del ticket, el autenticador puede utilizarse sólo una vez; por lo general, cuando se solicita acceso a un servicio. El autenticador se cifra mediante la clave de sesión compartida por el cliente y el servidor. Habitualmente, el cliente crea el autenticador y lo envía con el ticket de un servidor o de un servicio para que se autentique en el servidor o el servicio.

## Tipos de tickets

Los tickets tienen propiedades que establecen el modo en que pueden utilizarse. Estas propiedades se asignan al ticket en el momento que éste se crea, pero pueden modificarse más adelante. Por ejemplo, un ticket puede cambiar de `forwardable` a `forwarded`. Puede ver las propiedades del ticket con el comando `klist`. Consulte [“Visualización de tickets de Kerberos” en la página 551](#).

Los tickets pueden describirse con uno o más de los siguientes términos:

Reenviable/reenviado

El ticket reenviable puede enviarse de un host a otro, sin la necesidad de que un cliente vuelva a autenticarse. Por ejemplo, si el usuario david obtiene un ticket reenviable cuando está en el

equipo del usuario jennifer, puede iniciar sesión en su propio equipo sin obtener un ticket nuevo (ni volver a autenticarse). Consulte el [Ejemplo 26–1](#) para ver un ejemplo de un ticket reenviable.

Inicial	El ticket inicial es un ticket que se emite directamente en lugar de emitirse por medio de un ticket de otorgamiento de tickets. Algunos servicios, como las aplicaciones que cambian las contraseñas, posiblemente requieran que los tickets se marquen como iniciales para garantizar que el cliente pueda demostrar que conoce su clave secreta. El ticket inicial indica que, recientemente, el cliente se ha autenticado por sí mismo, en lugar de recurrir al ticket de otorgamiento de tickets, que quizás haya estado funcionando durante mucho tiempo.
No válido	El ticket no válido es un ticket posfechado que todavía no se puede usar. Un servidor de aplicaciones rechaza un ticket no válido hasta que se valide. Para validar un ticket, el cliente debe presentarlo al KDC en una solicitud de ticket de otorgamiento de tickets, con el indicador <code>VALIDATE</code> definido, después de que haya pasado la hora de inicio.
Posfechable/posfechado	El ticket posfechado no es válido hasta que transcurra un tiempo especificado tras su creación. Un ticket de este tipo es útil, por ejemplo, para los trabajos por lotes que deben ejecutarse tarde por la noche, ya que si el ticket es robado, no se puede utilizar hasta que se ejecute el trabajo por lotes. Los tickets posfechados se emiten como no válidos y siguen teniendo ese estado hasta que haya pasado su hora de inicio, y el cliente solicite la validación por parte del KDC. Generalmente, un ticket posfechado es válido hasta la hora de vencimiento del ticket de otorgamiento de tickets. Sin embargo, si el ticket se marca como renovable, su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets.
Que admite proxy/proxy	<p>A veces, es necesario que un principal permita que un servicio realice una operación en su nombre. El nombre de principal del proxy debe estar especificado cuando se crea el ticket. La versión de Oracle Solaris no es compatible con tickets que admiten proxy ni con tickets proxy.</p> <p>El ticket que admite proxy es similar al ticket reenviable, excepto en que sólo es válido para un único servicio, mientras que el ticket reenviable otorga al servicio el uso total de la identidad del cliente. Por lo tanto, el ticket reenviable se puede considerar como una especie de superproxy.</p>

**Renovable**

Debido a que los tickets con duraciones muy largas constituyen un riesgo de seguridad, los tickets se pueden designar como renovables. Un ticket renovable tiene dos horas de vencimiento: la hora de vencimiento de la instancia actual del ticket y la duración máxima de cualquier ticket, que es de una semana. Si un cliente desea seguir utilizando un ticket, debe renovarlo antes del primer vencimiento. Por ejemplo, un ticket puede ser válido por una hora, pero todos los tickets tienen una duración máxima de diez horas. Si el cliente que tiene el ticket desea conservarlo durante más de una hora, debe renovarlo dentro de esa hora. Cuando un ticket alcanza la duración máxima (diez horas), vence automáticamente y no se puede renovar.

Para obtener más información sobre cómo ver los atributos de tickets, consulte [“Visualización de tickets de Kerberos” en la página 551](#).

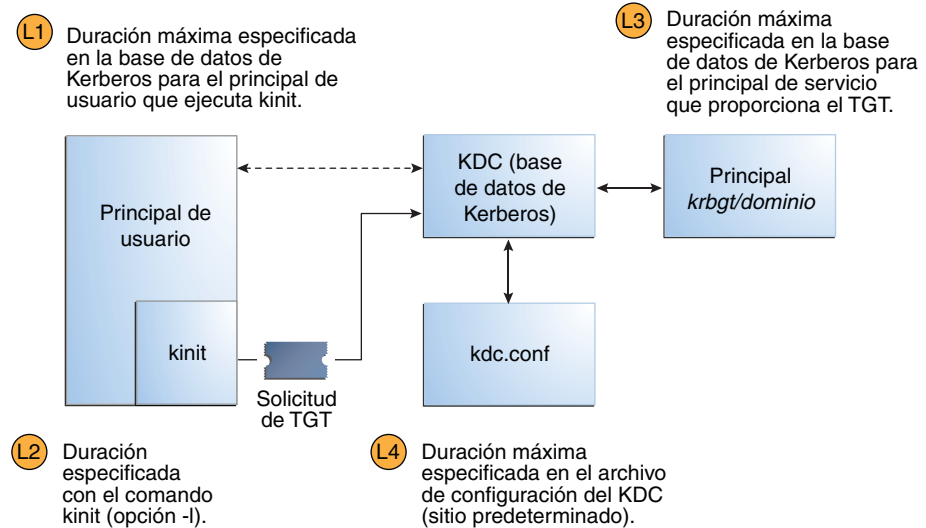
**Duración de los tickets**

En cualquier momento que un principal obtenga un ticket, incluido un ticket de otorgamiento de tickets (TGT), la duración del ticket se establece como el menor de los siguientes valores de duración:

- El valor de duración que establece la opción `-l` de `kinit`, si se usa `kinit` para obtener el ticket. De manera predeterminada, `kinit` usó el valor de duración máxima.
- El valor de duración máxima (`max_life`) que se encuentra especificado en el archivo `kdc.conf`.
- El valor de duración máxima que se especifica en la base de datos de Kerberos para el principal de servicio que proporciona el ticket. En el caso de `kinit`, el principal de servicio es `krbtgt/ dominio`.
- El valor de duración máxima que se especifica en la base de datos de Kerberos para el principal de usuario que solicita el ticket.

La [Figura 27-1](#) muestra cómo se determina la duración de un TGT y de dónde provienen los cuatro valores de duración. Aunque esta figura muestra cómo se determina la duración de un TGT, básicamente, ocurre lo mismo cuando algún principal obtiene un ticket. Las únicas diferencias radican en que `kinit` no proporciona un valor de duración, y el principal de servicio que otorga el ticket proporciona un valor de duración máxima (en lugar del principal `krbtgt/ dominio`).

FIGURA 27-1 Cómo se determina la duración de un TGT



Duración del ticket = valor mínimo de L1, L2, L3 y L4

La duración del ticket renovable también se determina a partir del mínimo de los cuatro valores, pero en su lugar se utilizan los valores de duración renovables, de la siguiente manera:

- El valor de duración renovable que especifica la opción -r de kinit, si kinit se utiliza para obtener o renovar el ticket.
- El valor de duración máxima renovable (`max_renewable_life`) que se especifica en el archivo `kdc.conf`.
- El valor de duración máxima renovable que se especifica en la base de datos de Kerberos para el principal de servicio que proporciona el ticket. En el caso de kinit, el principal de servicio es `krbtgt/ dominio`.
- El valor de duración máxima renovable que se especifica en la base de datos de Kerberos para el principal de usuario que solicita el ticket.

## Nombres de principales de Kerberos

Cada ticket se identifica con un nombre de principal. El nombre de principal puede identificar un usuario o un servicio. A continuación se muestran ejemplos de varios nombres de principal.

TABLA 27-4 Ejemplos de nombres de principales de Kerberos

Nombre de principal	Descripción
changepw/kdc1.example.com@EXAMPLE.COM	Un principal para el servidor KDC maestro que permite el acceso al KDC cuando se cambian las contraseñas.
clntconfig/admin@EXAMPLE.COM	Un principal que es empleado por la utilidad de instalación <code>kclient</code> .
ftp/boston.example.com@EXAMPLE.COM	Un principal que es empleado por el servicio ftp. Este principal puede utilizarse en lugar de un principal de host.
host/boston.example.com@EXAMPLE.COM	Un principal que es empleado por las aplicaciones de Kerberos (por ejemplo, <code>klist</code> y <code>kprop</code> ) y los servicios (como <code>ftp</code> y <code>telnet</code> ). Este principal se llama principal de host o de servicio. El principal se utiliza para autenticar los montajes de NFS. Este principal también lo utilizan los clientes para verificar que el TGT que reciben provenga del KDC correspondiente.
K/M@EXAMPLE.COM	El nombre de principal clave maestro. Se asocia un nombre de principal clave maestro con cada KDC maestro.
kadmin/history@EXAMPLE.COM	Un principal que incluye una clave utilizada para mantener los historiales de las contraseñas de otros principales. Cada KDC maestro tiene uno de los siguientes principales.
kadmin/kdc1.example.com@EXAMPLE.COM	Un principal para el servidor KDC maestro que permite el acceso al KDC con <code>kadmin</code> .
kadmin/changepw.example.com@EXAMPLE.COM	Un principal que se utiliza para aceptar solicitudes de cambio de contraseña de clientes que no están ejecutando una versión de Oracle Solaris.
krbtgt/EXAMPLE.COM@EXAMPLE.COM	Este principal se utiliza cuando se genera un ticket de otorgamiento de tickets.
krbtgt/EAST.EXAMPLE.COM@WEST.EXAMPLE.COM	Este principal es un ejemplo de un ticket de otorgamiento de tickets entre dominios.
nfs/boston.example.com@EXAMPLE.COM	Un principal que emplea el servicio NFS. Este principal puede utilizarse en lugar de un principal de host.
root/boston.example.com@EXAMPLE.COM	Un principal que está asociado a la cuenta root en un cliente. Este principal se denomina principal de root y proporciona acceso root a los sistemas de archivos montados en NFS.
<i>nombre_de_usuario</i> @EXAMPLE.COM	Un principal para un usuario.
<i>nombre_de_usuario</i> /admin@EXAMPLE.COM	Un principal de admin que se puede utilizar para administrar la base de datos del KDC.

## Cómo funciona el sistema de autenticación Kerberos

Las aplicaciones le permiten iniciar sesión en un sistema remoto si puede proporcionar un ticket que demuestre su identidad y una clave de sesión coincidente. La clave de sesión contiene información que es específica del usuario y del servicio al que se accede. El KDC crea un ticket y una clave de sesión para todos los usuarios cuando inician sesión por primera vez. El ticket y la clave de sesión coincidente constituyen una credencial. Mientras utilice varios servicios de red, el usuario puede recopilar muchas credenciales. El usuario debe tener una credencial para cada servicio que se ejecute en un servidor determinado. Por ejemplo, para acceder al servicio `ftp` en un servidor que se llama `boston` se requiere una credencial. Para acceder al servicio `ftp` en otro servidor se necesita la credencial correspondiente.

El proceso de creación y almacenamiento de las credenciales es transparente. Las credenciales las crea el KDC que las envía al solicitante. Cuando se recibe, la credencial se almacena en una antememoria de credenciales.

## Cómo interactúa el servicio Kerberos con el DNS y el archivo `nsswitch.conf`

El servicio Kerberos se compila a fin de usar el DNS para resolver nombres de host. El archivo `nsswitch.conf` no se consulta nunca cuando la resolución del nombre de host está lista.

## Obtención de acceso a un servicio con Kerberos

Para acceder a un servicio específico en un servidor específico, el usuario debe obtener dos credenciales. La primera credencial es para el ticket de otorgamiento de tickets (conocido como el TGT). Una vez que el servicio de otorgamiento de tickets descifra esta credencial, el servicio crea una segunda credencial para el servidor al que el usuario solicita acceso. Esta segunda credencial se puede utilizar para solicitar acceso al servicio en el servidor. Después de que el servidor descifra correctamente la segunda credencial, se le otorga el acceso al usuario. En las siguientes secciones, se describe este proceso de manera más detallada.

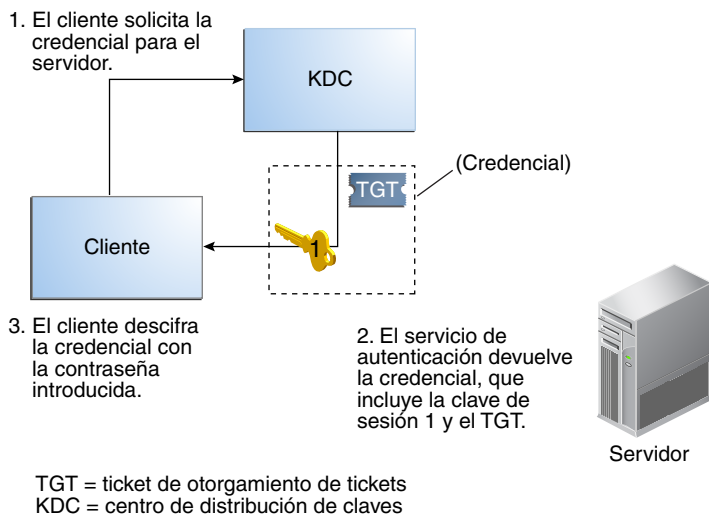
### Obtención de una credencial para el servicio de otorgamiento de tickets

1. A fin de iniciar el proceso de autenticación, el cliente envía una solicitud al servidor de autenticación para un principal de usuario específico. Esta solicitud se envía sin cifrado. En la solicitud no se incluye ninguna información que deba permanecer segura, por lo que no es necesario utilizar el cifrado.

2. Una vez que el servicio de autenticación recibe la solicitud, el nombre de principal del usuario se consulta en la base de datos del KDC. Si un principal coincide con la entrada en la base de datos, el servicio de autenticación obtiene la clave privada de ese principal. Luego, el servicio de autenticación genera una clave de sesión que utilizarán el cliente y el servicio de otorgamiento de tickets (Clave de sesión 1) y un ticket para el servicio de otorgamiento de tickets (Ticket 1). A este ticket también se lo conoce como *ticket de otorgamiento de tickets* (TGT). Tanto la clave de sesión como el ticket se cifran con la clave privada del usuario, y la información se envía de vuelta al cliente.
3. El cliente utiliza esta información para descifrar la Clave de sesión 1 y el Ticket 1 con la clave privada para el principal de usuario. Como únicamente el usuario y la base de datos del KDC deben conocer la clave privada, la información que se encuentra en el paquete debe permanecer segura. El cliente almacena la información en la antememoria de credenciales.

Durante este proceso, por lo general, al usuario se le solicita una contraseña. Si la contraseña que el usuario especifica es la misma que la que se ha utilizado para crear la clave privada almacenada en la base de datos del KDC, el cliente puede descifrar correctamente la información que envía el servicio de autenticación. Así, el cliente obtiene una credencial para utilizar con el servicio de otorgamiento de tickets. El cliente está listo para solicitar una credencial para un servidor.

FIGURA 27-2 Obtención de una credencial para el servicio de otorgamiento de tickets



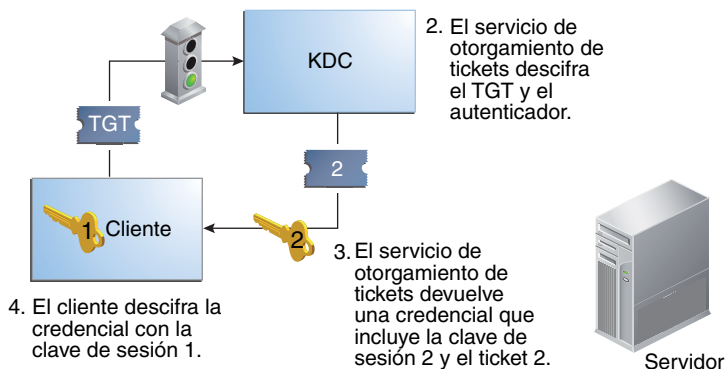


## Obtención de una credencial para un servidor

1. Para solicitar acceso a un servidor específico, el cliente debe haber obtenido primero una credencial para ese servidor desde el servicio de autenticación. Consulte [“Obtención de una credencial para el servicio de otorgamiento de tickets” en la página 575](#). Luego, el cliente envía una solicitud al servicio de otorgamiento de tickets, que incluye el nombre de principal del servicio (Ticket 1) y un autenticador que fue cifrado con la Clave de sesión 1. Originalmente, el servicio de autenticación cifró el Ticket 1 con la clave de servicio del servicio de otorgamiento de tickets.
2. El Ticket 1 se puede descifrar porque el servicio de otorgamiento de tickets conoce la clave de servicio del servicio de otorgamiento de tickets. La información del Ticket 1 incluye la Clave de sesión 1, por lo que el servicio de otorgamiento de tickets puede descifrar el autenticador. En este punto, el principal de usuario se autentica con el servicio de otorgamiento de tickets.
3. Una vez que la autenticación se realiza correctamente, el servicio de otorgamiento de tickets genera una clave de sesión para el principal de usuario y para el servidor (Clave de sesión 2), y un ticket para el servidor (Ticket 2). Luego, la Clave de sesión 2 y el Ticket 2 se cifran con la Clave de sesión 1. Como sólo el cliente y el servicio de otorgamiento de tickets conocen la Clave de sesión 1, esta información es segura y se puede enviar a través de la red con seguridad.
4. Cuando recibe este paquete de información, el cliente descifra la información con la Clave de sesión 1, que había almacenado en la antememoria de credenciales. El cliente obtuvo una credencial para usarla con el servidor. Ahora el cliente está listo para solicitar acceso a un servicio determinado en ese servidor.

FIGURA 27-3 Obtención de una credencial para un servidor

1. El cliente envía el TGT y el autenticador cifrados con la clave de sesión 1 al KDC.

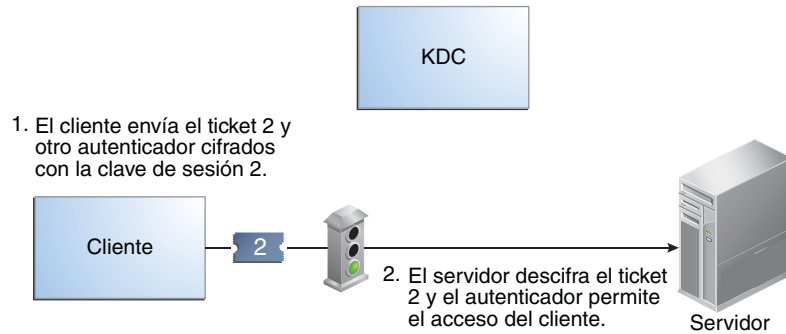


TGT = ticket de otorgamiento de tickets  
KDC = centro de distribución de claves

## Obtención de acceso a un servicio específico

1. Para solicitar acceso a un servicio específico, el cliente debe haber obtenido antes una credencial para el servicio de otorgamiento de tickets del servidor de autenticación y un servidor credenciales del servicio de otorgamiento de tickets. Consulte [“Obtención de una credencial para el servicio de otorgamiento de tickets” en la página 575](#) y [“Obtención de una credencial para un servidor” en la página 577](#). A continuación, el cliente puede enviar al servidor una solicitud que incluya el Ticket 2 y otro autenticador. El autenticador se cifra con la Clave de sesión 2.
2. El Ticket 2 se cifró mediante el servicio de otorgamiento de tickets con la clave de servicio para el servicio. Como el principal de servicio conoce la clave de servicio, el servicio puede descifrar el Ticket 2 y obtener la Clave de sesión 2. Luego, la Clave de sesión 2 puede usarse para descifrar el autenticador. Si el autenticador se descifra correctamente, el cliente obtiene acceso al servicio.

FIGURA 27-4 Obtención de acceso a un servicio específico



## Uso de los tipos de cifrado de Kerberos

Los tipos de cifrado identifican los algoritmos criptográficos y el modo en que se deben usar cuando se realizan las operaciones criptográficas. Los tipos de cifrado `aes`, `des3-cbc-sha1` y `rc4-hmac` permiten la creación de claves que se pueden utilizar para las operaciones criptográficas más resistentes. Estas operaciones más resistentes mejoran la seguridad general del servicio Kerberos.

**Nota** – En las versiones anteriores a la versión Solaris 10 8/07, el tipo de cifrado `aes256-cts-hmac-sha1-96` se puede utilizar con el servicio Kerberos si los paquetes de criptografía resistente que están desempaquetados se encuentran instalados.

Cuando un cliente solicita un ticket del KDC, el KDC debe usar claves cuyo tipo de cifrado sea compatible tanto con el cliente como con el servidor. Mientras que el protocolo Kerberos permite al cliente solicitar que el KDC utilice determinados tipos de cifrado para la parte del cliente de la respuesta de ticket, el protocolo no permite que el servidor especifique tipos de cifrado para el KDC.

**Nota** – Si tiene instalado un KDC maestro que no ejecuta la versión Solaris 10, los KDC esclavos deben actualizarse a la versión Solaris 10 antes de actualizar el KDC maestro. Un KDC maestro de Solaris 10 utilizará los nuevos tipos de cifrado, que un esclavo anterior no podrá manejar.

A continuación se enumeran algunos de los problemas que deben tenerse en cuenta antes de cambiar los tipos de cifrado.

- El KDC supone que el servidor admite el primer conjunto de claves y tipos de cifrado asociados a la entrada del principal de servidor en la base de datos del principal.

- En el KDC, debe asegurarse de que las claves generadas para el principal sean compatibles con los sistemas en los que se autenticará el principal. De manera predeterminada, el comando `kadmin` crea claves para todos los tipos de cifrado admitidos. Si los sistemas en los que se utiliza el principal no admiten este conjunto de tipos de cifrado predeterminado, debe restringir los tipos de cifrado cuando crea un principal. Puede restringir los tipos de cifrado mediante el uso del indicador `-e` en `kadmin addprinc` o la definición del parámetro `supported_encetypes` en el archivo `kdc.conf` de este subconjunto. El parámetro `supported_encetypes` debe utilizarse cuando la mayoría de los sistemas de un dominio Kerberos admiten un subconjunto del conjunto predeterminado de tipos de cifrado. Al definir `supported_encetypes`, se especifica el conjunto predeterminado de tipos de cifrado que `kadmin addprinc` utiliza cuando crea un principal para un dominio en particular. Como regla general, es mejor controlar los tipos de cifrado utilizados por Kerberos con alguno de estos dos métodos.
- Cuando vaya a determinar los tipos de cifrado que admite un sistema, tenga en cuenta la versión de Kerberos que se ejecuta en el sistema y los algoritmos criptográficos que admite la aplicación de servidor para la que se crea un principal de servidor. Por ejemplo, cuando se crea un principal de servicio `nfs/hostname`, debe restringir los tipos de cifrado para los tipos que admite el servidor NFS en ese host. Tenga en cuenta que, en la versión Solaris 10, el servidor NFS también admite todos los tipos de cifrado de Kerberos.
- El parámetro `master_key_encype` del archivo `kdc.conf` se puede utilizar para controlar el tipo de cifrado de la clave maestra que cifra las entradas de la base de datos del principal. No utilice este parámetro si la base de datos del principal del KDC ya se ha creado. El parámetro `master_key_encype` se puede usar en el momento de la creación de la base de datos para cambiar el tipo de cifrado predeterminado para la clave maestra, de `des-cbc-crc` a un tipo de cifrado más resistente. Cuando configure los KDC esclavos, asegúrese de que todos admitan el tipo de cifrado seleccionado y tengan una entrada `master_key_encype` idéntica en su archivo `kdc.conf`. Asimismo, asegúrese de que `master_key_encype` se encuentre definido en uno de los tipos de cifrado en `supported_encetypes` si `supported_encetypes` está definido en `kdc.conf`. Si alguno de estos problemas no se trata adecuadamente, es posible que el KDC maestro no pueda trabajar con los KDC esclavos.
- En el cliente, puede controlar qué tipos de cifrado el cliente solicita cuando obtiene los tickets procedentes del KDC mediante algunos parámetros de `krb5.conf`. El parámetro `default_tkt_encetypes` especifica los tipos de cifrado que el cliente está dispuesto a utilizar cuando el cliente solicita un ticket de otorgamiento de tickets (TGT) desde el KDC. El cliente utiliza el TGT para adquirir otros tickets del servidor con más eficacia. Se define `default_tkt_encetypes` a fin de otorgarle al cliente un poco de control sobre los tipos de cifrado que se utilizan para proteger la comunicación entre el cliente y el KDC cuando el cliente solicita un ticket de servidor con el TGT (esto se llama solicitud TGS). Tenga en cuenta que los tipos de cifrado especificados en `default_tkt_encetypes` deben coincidir, al menos, con uno de los tipos de cifrado de la clave de principal en la base de datos del principal que se almacena en el KDC. De lo contrario, la solicitud TGT fallará. En la mayoría de las situaciones, es mejor no definir `default_tkt_encetypes`, porque este parámetro puede generar problemas de interoperabilidad. De manera predeterminada, el código de

cliente pide que todos los tipos de cifrado admitidos y el KDC seleccionen los tipos de cifrado en función de las claves que el KDC encuentre en la base de datos del principal.

- El parámetro `default_tgs_etypes` restringe los tipos de cifrado que el cliente solicita en sus solicitudes TGS, que se utilizan para adquirir tickets de servidor. Este parámetro también restringe los tipos de cifrado que el KDC utiliza cuando crea la clave de sesión que el cliente y el servidor comparten. Por ejemplo, si un cliente quiere usar solamente el cifrado 3DES cuando emplea NFS seguro, debe definir `default_tgs_etypes = des3-cbc-sha1`. Asegúrese de que los principales de servidor y de cliente tengan una clave `des3-cbc-sha1` en la base de datos del principal. Al igual que con `default_tkt_etype`, probablemente sea mejor, en la mayoría de los casos, no establecer esto, ya que puede provocar problemas de interoperabilidad si las credenciales no están configuradas correctamente en el KDC o en el servidor.
- En el servidor, puede controlar los tipos de cifrado aceptados por el servidor con `permitted_etypes` en `kdc.conf`. Además, puede especificar los tipos de cifrado utilizados en la creación de entradas `keytab`. Por lo general, es mejor no utilizar ninguno de estos métodos para controlar los tipos de cifrado y, en su lugar, dejar que el KDC determine los tipos de cifrado que se usarán, porque el KDC no se comunica con la aplicación del servidor para determinar qué clave o tipo de cifrado se usarán.

## Tabla de uso de `gsscred`

Un servidor NFS utiliza la tabla `gsscred` cuando el servidor intenta identificar un usuario de Kerberos si las asignaciones predeterminadas no son suficientes. El servicio NFS utiliza los ID de UNIX para identificar a los usuarios. Estos ID no forman parte de un principal de usuario ni de una credencial. La tabla `gsscred` proporciona asignaciones adicionales de las credenciales GSS a los UID de UNIX (desde el archivo de contraseñas). La tabla debe crearse y administrarse una vez que se haya rellenado la base de datos del KDC. Consulte [“Asignación de credenciales GSS a credenciales UNIX” en la página 416](#) para obtener más información.

Cuando se recibe una solicitud de cliente, el servicio NFS intenta asignar el nombre de la credencial a un ID de UNIX. Si la asignación falla, se comprueba la tabla `gsscred`.

## Diferencias importantes entre Oracle Solaris Kerberos y MIT Kerberos

La versión de Solaris 10 del servicio Kerberos se basa en la versión 1.2.1 de MIT Kerberos. A continuación, se enumeran las mejoras incluidas en la versión de Solaris 10 que no se incluyen en la versión 1.2.1 del MIT:

- Compatibilidad de Kerberos con las aplicaciones remotas de Oracle Solaris
- Propagación progresiva para la base de datos del KDC

- Secuencia de comandos de configuración del cliente
- Mensajes de errores localizados
- Compatibilidad del registro de auditoría de BSM
- Uso seguro de subprocesos de Kerberos con GSS-API
- Uso de la estructura de cifrado para la criptografía

Además, esta versión incluye algunas correcciones de errores posteriores al MIT Kerberos 1.2.1. En especial, se incorporaron correcciones de errores de 1.2.5 btree y la admisión de 1.3 TCP.

## P A R T E   V I I

# Auditoría de Oracle Solaris

En esta sección se proporciona información acerca de la configuración, la gestión y el uso del subsistema de auditoría de Oracle Solaris.

- [Capítulo 28, “Auditoría de Oracle Solaris \(descripción general\)”](#)
- [Capítulo 29, “Planificación de la auditoría de Oracle Solaris”](#)
- [Capítulo 30, “Gestión de la auditoría de Oracle Solaris \(tareas\)”](#)
- [Capítulo 31, “Auditoría de Oracle Solaris \(referencia\)”](#)





## Auditoría de Oracle Solaris (descripción general)

---

La auditoría de Oracle Solaris mantiene un registro de cómo se utiliza el sistema. El servicio de auditoría incluye herramientas para ayudar con el análisis de los datos de auditoría.

En este capítulo, se introduce cómo funciona la auditoría en el Oracle Solaris. A continuación, se presenta la información que se incluye en este capítulo.

- “¿Qué es la auditoría?” en la página 585
- “¿Cómo funciona la auditoría?” en la página 587
- “¿Cómo se relaciona la auditoría con la seguridad?” en la página 588
- “Conceptos y terminología de auditoría” en la página 588
- “Auditoría en un sistema con zonas de Oracle Solaris” en la página 596
- “Mejoras de la auditoría en la versión Solaris 10” en la página 597

Para obtener sugerencias de planificación, consulte el [Capítulo 29, “Planificación de la auditoría de Oracle Solaris”](#). Para obtener procedimientos para configurar la auditoría en el sitio, consulte el [Capítulo 30, “Gestión de la auditoría de Oracle Solaris \(tareas\)”](#). Para obtener información de referencia, consulte el [Capítulo 31, “Auditoría de Oracle Solaris \(referencia\)”](#).

### ¿Qué es la auditoría?

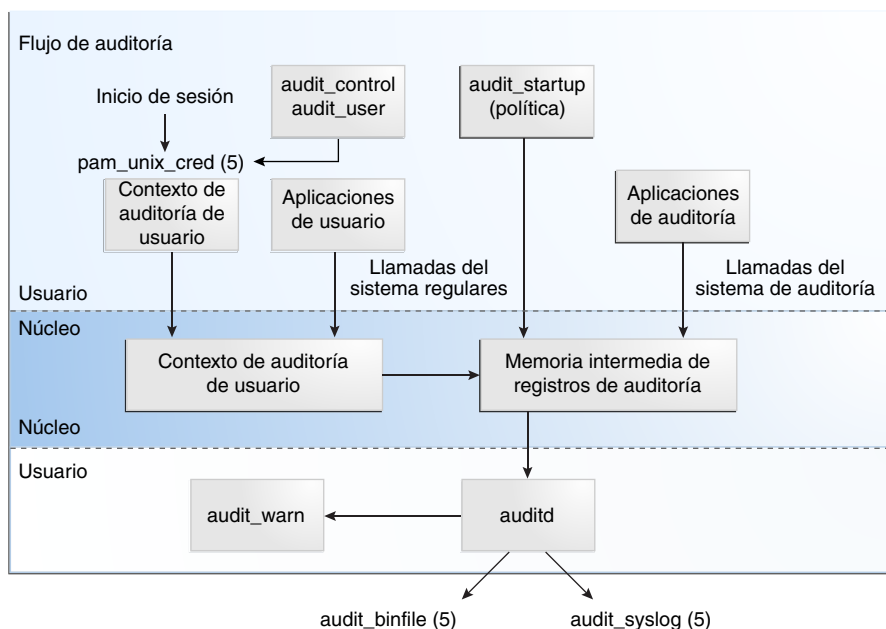
La auditoría es la recopilación de datos sobre el uso de los recursos del sistema. Los datos de auditoría proporcionan un registro de los eventos del sistema relacionados con la seguridad. Estos datos se pueden utilizar para asignar responsabilidad para acciones que ocurren en un host. La auditoría correcta comienza con dos funciones de seguridad: identificación y autenticación. En cada inicio de sesión, después de que un usuario proporciona un nombre de usuario y una contraseña, un único ID de sesión de auditoría se genera y se asocia con el proceso del usuario. El ID de sesión de auditoría es heredado por cada proceso que se inicia durante la sesión de inicio de sesión. Incluso si un usuario cambia la identidad dentro de una única sesión, todas las acciones del usuario se rastrean con el mismo ID de sesión de auditoría. Para obtener más detalles sobre cómo cambiar la identidad, consulte la página del comando `man su(1M)`.

El servicio de auditoría hace que lo siguiente sea posible:

- Supervisión de eventos relacionados con la seguridad que ocurren en el host
- Registro de los eventos en una pista de auditoría de toda la red
- Detección de uso incorrecto o actividad no autorizada
- Revisión de patrones de acceso e historiales de acceso de personas y objetos
- Detección de intentos para eludir los mecanismos de protección
- Detección de uso ampliado de privilegio que se produce cuando un usuario cambia la identidad

Durante la configuración del sistema, preselecciona las clases de registros de auditoría que desea supervisar. También puede ajustar el grado de auditoría que se realiza para usuarios individuales. En la siguiente figura, se muestran los detalles del flujo de auditoría de Oracle Solaris.

FIGURA 28-1 El flujo de auditoría



Después de que los datos de auditoría se recopilan en el núcleo, los complementos distribuyen los datos a las ubicaciones adecuadas. A continuación, las herramientas de postselección permiten reducir y examinar partes interesantes de la pista de auditoría. Por ejemplo, puede elegir revisar registros de auditoría de usuarios individuales o grupos específicos. Puede

examinar todos los registros de un tipo determinado de evento en un día específico. O puede seleccionar registros que se han generado a una hora determinada del día.

Los sistemas que instalan zonas no globales pueden auditar todas las zonas de forma idéntica desde la zona global. Estos sistemas también se pueden configurar para recopilar diferentes registros en las zonas no globales. Para obtener más información, consulte [“Auditoría y zonas de Oracle Solaris” en la página 678](#).

## ¿Cómo funciona la auditoría?

La auditoría genera registros de auditoría cuando se producen eventos especificados. Habitualmente, los eventos que generan registros de auditoría incluyen los siguientes:

- Inicio y cierre del sistema
- Inicio y cierre de sesión
- Creación o destrucción de proceso, o creación o destrucción de subproceso
- Apertura, cierre, creación, destrucción o cambio de nombre de objetos
- Uso de capacidades de privilegio o control de acceso basado en roles (RBAC)
- Acciones de identificación y de autenticación
- Cambios de permiso por un proceso o usuario
- Acciones administrativas, como la instalación de un paquete
- Aplicaciones específicas de sitio

Los registros de auditoría se generan a partir de tres orígenes:

- Por una aplicación
- Como resultado de un [evento asíncrono de auditoría](#)
- Como resultado de una llamada del sistema de proceso

Una vez que la información de evento pertinente se ha capturado, la información se formatea en un registro de auditoría. El registro luego se escribe en archivos de auditoría. Los registros de auditoría completos se almacenan en formato binario. Con la versión Solaris 10, los registros de auditoría también pueden ser registrados por la utilidad `syslog`.

Los archivos de auditoría en formato binario se pueden almacenar en un sistema de archivos local. Los archivos también se pueden almacenar en servidores de archivos montados en NFS. La ubicación puede incluir varias particiones en el mismo sistema, particiones en distintos sistemas o particiones en sistemas de redes diferentes, pero enlazadas. La recopilación de archivos de auditoría que están enlazados se considera una *pista de auditoría*. Los registros de auditoría se acumulan en archivos de auditoría cronológicamente. En cada registro de auditoría, se incluye información que identifica el evento, qué generó el evento, la hora del evento y otra información relevante.

Los registros de auditoría también se pueden supervisar mediante la utilidad `syslog`. Estos registros de auditoría se pueden almacenar de forma local o se pueden enviar a un sistema remoto por medio del protocolo UDP. Para obtener más información, consulte [“Registros de auditoría” en la página 593](#).

## ¿Cómo se relaciona la auditoría con la seguridad?

La auditoría de Oracle Solaris ayuda a detectar posibles brechas de seguridad al revelar patrones sospechosos o anómalos del uso del sistema. La auditoría de Oracle Solaris también proporciona un medio para rastrear acciones sospechosas de un usuario concreto, lo que sirve como elemento de disuasión. Es decir, es menos probable que los usuarios que saben que sus actividades se están auditando intenten realizar actividades maliciosas.

Para proteger un sistema informático, especialmente un sistema en una red, se requieren mecanismos que controlan las actividades antes de que comiencen los procesos del sistema o del usuario. La seguridad requiere herramientas que supervisan las actividades a medida que se producen. También requiere informes de actividades después de que las actividades ocurren. La configuración inicial de la auditoría de Oracle Solaris requiere que los parámetros se establezcan antes de que los usuarios inicien sesión o los procesos del sistema comiencen. La mayoría de las actividades de auditoría implican la supervisión de eventos actuales y la generación de informes de los eventos que cumplen con los parámetros especificados. Cómo la auditoría de Oracle Solaris supervisa e informa estos eventos se trata detalladamente en el [Capítulo 29, “Planificación de la auditoría de Oracle Solaris”](#) y el [Capítulo 30, “Gestión de la auditoría de Oracle Solaris \(tareas\)”](#).

La auditoría no puede evitar que los piratas informáticos entren de manera no autorizada. Sin embargo, el servicio de auditoría puede informar, por ejemplo, que un usuario específico realizó acciones específicas a una hora y en una fecha concretas. El informe de auditoría puede identificar al usuario por ruta de entrada y nombre de usuario. Dicha información se puede informar de inmediato en su terminal y en un archivo para su análisis posterior. Por lo tanto, el servicio de auditoría proporciona datos que ayudan a determinar lo siguiente:

- Cómo se comprometió la seguridad del sistema
- Qué espacios de bucle se deben cerrar para garantizar el nivel de seguridad deseado

## Conceptos y terminología de auditoría

Los siguientes términos se usan para describir el servicio de auditoría. Algunas definiciones incluyen enlaces a descripciones más completas.

TABLA 28-1 Términos de auditoría de Oracle Solaris

Término	Definición
Clase de auditoría	Una agrupación de eventos de auditoría. Las clases de auditoría proporcionan una forma de seleccionar un grupo de eventos que se van a auditar. Para obtener más información, consulte <a href="#">“Clases de auditoría y preselección” en la página 591</a> .
Directorio de auditoría	Un depósito de archivos de auditoría en formato binario. Para obtener una descripción de los tipos de directorios de auditoría, consulte <a href="#">“Registros de auditoría” en la página 593</a> .
Evento de auditoría	Una acción del sistema relacionada con la seguridad, que se audita. Para una mayor facilidad de selección, los eventos se agrupan en clases de auditoría. Para ver una explicación de las acciones del sistema que se pueden auditar, consulte <a href="#">“Eventos de auditoría” en la página 590</a> .
Política de auditoría	Un conjunto de opciones de auditoría que puede habilitar o deshabilitar en el sitio. Estas opciones incluyen si se desean registrar o no determinados tipos de datos de auditoría. Las opciones también incluyen si se desean suspender o no acciones auditables cuando la pista de auditoría está llena. Para obtener más información, consulte <a href="#">“Determinación de política de auditoría” en la página 605</a> .
Registro de auditoría	Datos de auditoría que se almacenan en archivos de auditoría. Un registro de auditoría describe un único evento de auditoría. Cada registro de auditoría se compone de tokens de auditoría. Para obtener más información sobre los registros de auditoría, consulte <a href="#">“Registros de auditoría y tokens de auditoría” en la página 592</a> .
Token de auditoría	Un campo de un evento o registro de auditoría. Cada token de auditoría describe un atributo de un evento de auditoría, como un usuario, un programa u otro objeto. Para obtener descripciones de todos los tokens de auditoría, consulte <a href="#">“Formatos de token de auditoría” en la página 686</a> .
Pista de auditoría	Una colección de uno o más archivos de auditoría que almacenan los datos de auditoría de todos los sistemas que ejecutan el servicio de auditoría. Para obtener más información, consulte <a href="#">“Pista de auditoría” en la página 683</a> .
Preselección	Preselección es la selección de las clases de auditoría que se van a supervisar antes de habilitar el servicio de auditoría. Los eventos de auditoría de clases de auditoría preseleccionadas aparecen en la pista de auditoría. Las clases de auditoría que no se preseleccionan, no se auditan, por lo que sus eventos no aparecen en la pista de auditoría. Una herramienta de postselección, el comando <code>audit reduce</code> , selecciona registros de la pista de auditoría. Para obtener más información, consulte <a href="#">“Clases de auditoría y preselección” en la página 591</a> .
Objetos públicos	Un objeto público es un archivo que es propiedad del usuario <code>root</code> y que todo el mundo puede leer. Por ejemplo, los archivos en el directorio <code>/etc</code> y el directorio <code>/usr/bin</code> son objetos públicos. Los objetos públicos no se auditan en eventos de sólo lectura. Por ejemplo, incluso si la clase de auditoría <code>file_read(fr)</code> está preseleccionada, la lectura de objetos públicos no se audita. Puede sustituir el valor predeterminado cambiando la opción de política de auditoría <code>public</code> .

TABLA 28-1 Términos de auditoría de Oracle Solaris (Continuación)

Término	Definición
Complementos de auditoría	Módulos que transfieren los registros de auditoría en la cola del núcleo a una ubicación especificada. El complemento <code>audit_binfile.so</code> crea archivos de auditoría binarios (la pista de auditoría). El complemento <code>audit_syslog.so</code> filtra registros de auditoría seleccionados en los registros <code>syslog</code> . Para obtener más información, consulte <a href="#">“Módulos de complemento de auditoría” en la página 593</a> .

## Eventos de auditoría

Las acciones del sistema relacionadas con la seguridad se pueden auditar. Estas acciones auditables se definen como *eventos de auditoría*. Los eventos de auditoría se muestran en el archivo `/etc/security/audit_event`. Cada uno de los eventos de auditoría se define en el archivo mediante un número de evento, un nombre simbólico, una descripción breve y el conjunto de clases de auditoría al que pertenece el evento. Para obtener más información sobre el archivo `audit_event`, consulte la página del comando `man audit_event(4)`.

Por ejemplo, la entrada siguiente define el evento de auditoría para la llamada del sistema `exec()`:

```
7:AUE_EXEC:exec(2):ps,ex
```

Al preseleccionar para la auditoría la clase de auditoría `ps` o la clase de auditoría `ex`, las llamadas del sistema `exec()` se registran en la pista de auditoría.

La auditoría de Oracle Solaris maneja eventos *atribuibles* y *no atribuibles*. La política de auditoría divide los eventos en *síncronos* y *asíncronos*, de la siguiente manera:

- **Eventos atribuibles:** eventos que se pueden atribuir a un usuario. La llamada del sistema `exec()` se puede atribuir a un usuario, por lo tanto, se considera un evento atribuible. Todos los eventos atribuibles son eventos síncronos.
- **Eventos no atribuibles:** eventos que ocurren en el nivel de interrupción de núcleo o antes de que un usuario sea autenticado. La clase de auditoría `na` maneja los eventos de auditoría que no son atribuibles. Por ejemplo, el inicio del sistema es un evento no atribuible. La mayoría de los eventos no atribuibles son eventos asíncronos. Sin embargo, los eventos no atribuibles que tienen procesos asociados, como inicios de sesión fallidos, son eventos síncronos.
- **Eventos síncronos:** eventos que están asociados con un proceso en el sistema. La mayoría de los eventos del sistema son eventos síncronos.
- **Eventos asíncronos:** eventos que no están asociados con ningún proceso, por lo que no hay ningún proceso disponible para bloquear y más tarde reactivar. Los eventos de salida y entrada de la PROM, y de inicio del sistema inicial son ejemplos de eventos asíncronos.

Cuando la clase a la que un evento de auditoría pertenece está preseleccionada para la auditoría, el evento se registra en la pista de auditoría. Por ejemplo, al preseleccionar las clases de auditoría

ps y na para la auditoría, las llamadas del sistema `exec()` y las acciones de inicio del sistema, entre otros eventos, se registran en la pista de auditoría.

Además de los eventos de auditoría que define el servicio de auditoría de Oracle Solaris, las aplicaciones de terceros pueden generar eventos de auditoría. Los números de evento de auditoría de 32768 a 65535 están disponibles para aplicaciones de terceros.

## Clases de auditoría y preselección

Cada uno de los eventos de auditoría pertenece a una *clase de auditoría* o a clases de auditoría. Las clases de auditoría son contenedores prácticos para un gran número de eventos de auditoría. Cuando se *preselecciona* una clase para auditar, se especifica que todos los eventos de esa clase se deben registrar en la pista de auditoría. Puede preseleccionar para eventos de un sistema y para eventos iniciados por un usuario concreto. Una vez que el servicio de auditoría se está ejecutando, puede agregar clases de auditoría a las clases preseleccionadas o eliminarlas de dichas clases de manera dinámica.

- **Preselección de todo el sistema:** especifique valores predeterminados de todo el sistema para la auditoría en las líneas `flags`, `naflags` y `plugin` del archivo `audit_control`. El archivo `audit_control` se describe en [“Archivo audit\\_control” en la página 673](#). Consulte también la página del comando `man audit_control(4)`.
- **Preselección específica de usuario:** especifique adiciones a los valores predeterminados de auditoría de todo el sistema para usuarios individuales en la base de datos `audit_user`.  
La máscara de preselección de auditoría determina las clases de eventos que se auditarán para un usuario. La máscara de preselección de auditoría del usuario es una combinación de valores predeterminados de todo el sistema y las clases de auditoría que se especifican para el usuario. Para obtener información más detallada, consulte [“Características de auditoría de proceso” en la página 683](#).  
La base de datos `audit_user` puede ser administrada localmente o por un servicio de nombres. Solaris Management Console proporciona la interfaz gráfica de usuario (GUI) para administrar la base de datos. Para obtener detalles, consulte la página del comando `man audit_user(4)`.
- **Preselección dinámica:** especifique clases de auditoría como argumentos para el comando `auditconfig` a fin de agregar esas clases de auditoría a un proceso o una sesión, o eliminarlas de un proceso o una sesión. Para obtener más información, consulte la página del comando `man auditconfig(1M)`.

Un comando de postselección, `auditreduce`, permite seleccionar registros de los registros de auditoría preseleccionados. Para obtener más información, consulte [“Examen de la pista de auditoría” en la página 595](#) y la página del comando `man auditreduce(1M)`.

Las clases de auditoría se definen en el archivo `/etc/security/audit_class`. Cada entrada contiene la máscara de auditoría para la clase, el nombre para la clase y un nombre descriptivo para la clase. Por ejemplo, las definiciones de clase `ps` y `na` aparecen en el archivo `audit_class`, de la siguiente manera:

```
0x00100000:ps:process start/stop
0x00000400:na:non-attribute
```

Hay 32 clases de auditoría posibles. Las clases incluyen las dos clases globales: `all` y `no`. Las clases de auditoría se describen en la página del comando `man audit_class(4)`.

La asignación de eventos de auditoría a clases es configurable. Puede eliminar eventos de una clase, agregar eventos a una clase y crear una nueva clase para colocar eventos seleccionados. Para conocer el procedimiento, consulte [“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 623](#).

## Registros de auditoría y tokens de auditoría

Cada *registro de auditoría* registra la aparición de un único evento auditado. El registro incluye información, como quién realizó la acción, qué archivos fueron afectados, qué acción se intentó realizar y dónde y cuándo ocurrió la acción. El siguiente ejemplo muestra un registro de auditoría `login`:

```
header,81,2,login - local,,2003-10-13 11:23:31.050 -07:00
subject,root,root,other,root,other,378,378,0 0 example_system
text,successful login
return,success,0
```

El tipo de información que se guarda para cada uno de los eventos de auditoría se define mediante un conjunto de *tokens de auditoría*. Cada vez que un registro de auditoría se crea para un evento, el registro contiene algunos de los tokens o todos los tokens que se definen para el evento. La naturaleza del evento determina qué tokens se registran. En el ejemplo anterior, cada línea empieza con el nombre del token de auditoría. El contenido del token de auditoría sigue al nombre. Juntos, los cuatro tokens de auditoría componen el registro de auditoría `login`.

Para obtener una descripción detallada de la estructura de cada token de auditoría con un ejemplo de salida de `praudit`, consulte [“Formatos de token de auditoría” en la página 686](#). Para obtener una descripción de la cadena binaria de tokens de auditoría, consulte la página del comando `man audit.log(4)`.



## Módulos de complemento de auditoría

Puede especificar módulos de complemento de auditoría para manejar los registros que la preselección ha colocado en la cola de la auditoría. Los complementos son entradas en el archivo `audit_control`.

- Complemento `audit_binfile`. so: maneja la entrega de la cola de la auditoría a los archivos de auditoría binarios. En el archivo `audit_control`, si no se especifica ningún complemento y la entrada `dir` tiene un valor, el daemon de auditoría utiliza este complemento.
- Complemento `audit_syslog`. so: maneja la entrega de registros seleccionados de la cola de la auditoría a los registros `syslog`.

Para ver la sintaxis del archivo `audit_control`, consulte la página del comando `man audit_control(4)`. Para obtener más ejemplos, consulte las tareas en “Configuración de archivos de auditoría (mapa de tareas)” en la página 614.

Para obtener información sobre los complementos, consulte las páginas del comando `man audit_binfile(5)`, `audit_syslog(5)` y `audit_control(4)`.

## Registros de auditoría

Los registros de auditoría se recopilan en registros de auditoría. La auditoría de Oracle Solaris proporciona dos modos de salida para registros de auditoría. Los registros que se denominan *archivos de auditoría* almacenan registros de auditoría en formato binario. El conjunto de archivos de auditoría de un sistema o sitio proporcionan un registro de auditoría completo. El registro de auditoría completo se denomina *pista de auditoría*.

La utilidad `syslog` recopila y almacena resúmenes en versión de texto del registro de auditoría. Un registro `syslog` no está completo. El siguiente ejemplo muestra una entrada `syslog` para un registro de auditoría login:

```
Oct 13 11:24:11 example_system auditd: [ID 6472 audit.notice] \
login - login ok session 378 by root as root:other
```

Un sitio puede almacenar registros de auditoría en ambos formatos. Puede configurar los sistemas del sitio para utilizar el modo binario, para utilizar el modo `syslog` o para utilizar ambos modos. En la siguiente tabla, se comparan registros de auditoría binarios con registros de auditoría `syslog`.

TABLA 28–2 Comparación de registros de auditoría binarios con registros de auditoría `syslog`

Función	Registros binarios	Registros <code>syslog</code>
Protocolo	Escribe en el sistema de archivos	Utiliza UDP para el registro remoto
Tipo de datos	Binarios	Texto

TABLA 28-2 Comparación de registros de auditoría binarios con registros de auditoría syslog  
(Continuación)

Función		Registros binarios	Registros syslog
Longitud de registro		Sin límite	Hasta 1024 caracteres por registro de auditoría
Ubicación		Se almacenan en el disco local y en los directorios que se montan mediante NFS	Se almacenan en una ubicación que se especifica en el archivo syslog.conf
Cómo configurar		Edite el archivo audit_control y proteja y monte en NFS directorios de auditoría	Edite el archivo audit_control y el archivo syslog.conf
Cómo leer		Normalmente, en modo de proceso por lotes	En tiempo real o se buscan mediante secuencias de comandos creadas para syslog
		Salida del navegador en XML	Salida de texto sin formato
Integridad		Se garantiza que estén completos y que aparezcan en el orden correcto	No se garantiza que estén completos
Indicación de hora		Hora del meridiano de Greenwich (GMT)	Hora en el sistema que se audita

Los registros binarios proporcionan la mayor seguridad y cobertura. La salida binaria cumple los requisitos de certificaciones de seguridad, como el perfil de protección de acceso controlado de criterios comunes (CAPP). Los registros se escriben en un sistema de archivos que se protege para evitar que sea espiado. En un único sistema, todos los registros binarios se recopilan y se muestran en orden. La indicación de hora del GMT en registros binarios permite realizar una comparación exacta cuando los sistemas en una pista de auditoría se distribuyen entre zonas horarias. El comando `praudit -x` permite ver los registros en un explorador, en XML. También puede utilizar secuencias de comandos para analizar la salida XML.

En contraste, los registros syslog proporcionan una mayor comodidad y flexibilidad. Por ejemplo, puede recopilar los datos de syslog de un gran variedad de orígenes. Además, al supervisar eventos `audit.notice` en el archivo `syslog.conf`, la utilidad `syslog` registra un resumen de registros de auditoría con la indicación de hora actual. Puede utilizar las mismas herramientas de análisis y de gestión que ha desarrollado para mensajes syslog de una gran variedad de orígenes, incluidos estaciones de trabajo, servidores, cortafuegos y enrutadores. Los registros se pueden consultar en tiempo real y se pueden almacenar en un sistema remoto.

Si usa `syslog.conf` para almacenar registros de auditoría de manera remota, está protegiendo los datos del registro para evitar que los modifique o elimine un agresor. Por otro lado, cuando los registros de auditoría se almacenan de manera remota, los registros son susceptibles a ataques de red, como denegación de servicio y direcciones de origen simuladas. También, el UDP puede eliminar paquetes o puede entregar paquetes que no funcionan. El límite en entradas syslog es de 1024 caracteres, por lo que algunos registros de auditoría podrían estar truncados en el registro. En un único sistema, no se recopilan todos los registros de auditoría. Los registros podrían no aparecer en orden. Debido a que cada registro de auditoría se indica

con la fecha y la hora del sistema local, usted no se puede basar en la indicación de hora para construir una pista de auditoría para varios sistemas.

Para obtener más información sobre registros de auditoría, consulte lo siguiente:

- `audit_syslog(5)`
- `audit.log(4)`
- “Cómo configurar registros de auditoría `syslog`” en la página 617

## Almacenamiento de la pista de auditoría

Un *directorio de auditoría* contiene archivos de auditoría en formato binario. Una instalación típica utiliza muchos directorios de auditoría. El contenido de todos los directorios de auditoría compone la *pista de auditoría*. Los registros de auditoría se almacenan en directorios de auditoría en el siguiente orden:

- **Directorio de auditoría principal:** un directorio donde los archivos de auditoría de un sistema se colocan en condiciones normales.
- **Directorio de auditoría secundario:** un directorio donde los archivos de auditoría de un sistema se colocan si el directorio de auditoría principal está lleno o no está disponible.
- **Directorio de último recurso:** un directorio de auditoría local que se usa si el directorio de auditoría principal y todos los directorios de auditoría secundarios no están disponibles.

Los directorios se especifican en el archivo `audit_control`. Un directorio no se utiliza hasta que un directorio que está antes en la lista está lleno. Para obtener un archivo `audit_control` anotado con una lista de entradas de directorio, consulte el [Ejemplo 30–3](#).

Colocar los archivos de auditoría en el directorio root de auditoría predeterminado ayuda al revisor de auditoría cuando revisa la pista de auditoría. El comando `auditreduce` usa el directorio root de auditoría para encontrar todos los archivos en la pista de auditoría. El directorio root de auditoría predeterminado es `/etc/security/audit`. Este directorio está simbólicamente enlazado a `/var/audit`. Los archivos de auditoría en directorios que se denominan `/var/audit/nombre de host/archivos` son fácilmente encontrados por el comando `auditreduce`. Para obtener más información, consulte “Comando `auditreduce`” en la página 667.

## Examen de la pista de auditoría

El servicio de auditoría proporciona comandos para combinar y reducir archivos de la pista de auditoría. El comando `auditreduce` puede fusionar archivos de auditoría de la pista de auditoría. El comando también puede filtrar archivos para localizar eventos particulares. El comando `praudit` lee los archivos binarios. Las opciones para el comando `praudit` ofrecen una salida que es adecuada para las secuencias de comandos y para la presentación del explorador.

## Auditoría en un sistema con zonas de Oracle Solaris

Una zona es un entorno de sistema operativo virtualizado que se crea dentro de una única instancia del SO Oracle Solaris. El servicio de auditoría realiza la auditoría de la totalidad del sistema, incluidas las actividades en las zonas. Un sistema que ha instalado zonas no globales puede ejecutar un solo servicio de auditoría para auditar todas las zonas de manera idéntica o puede configurar un servicio de auditoría por zona, incluida la zona global.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un solo servicio de auditoría:

- El sitio requiere una pista de auditoría de única imagen.
- Las zonas no globales se utilizan como contenedores de aplicaciones. Las zonas forman parte de un dominio administrativo. Es decir, ninguna zona no global tiene archivos personalizados de servicio de nombres.

Si todas las zonas en un sistema están dentro de un dominio administrativo, la política de auditoría zonename se puede utilizar para distinguir eventos de auditoría que se ejecutan en zonas distintas.

- Los administradores desean una baja sobrecarga de auditoría. El administrador de la zona global audita todas las zonas de manera idéntica. Además, el daemon de auditoría de la zona global presta servicio a todas las zonas en el sistema.

Los sitios que cumplen con las siguientes condiciones pueden ejecutar un servicio de auditoría por zona:

- El sitio no requiere una pista de auditoría de única imagen.
- Las zonas no globales tienen archivos personalizados de servicio de nombres. Esos dominios administrativos separados, normalmente, funcionan como servidores.
- Los administradores de zonas individuales desean controlar la auditoría en las zonas que administran. En la auditoría por zona, los administradores de zonas pueden decidir habilitar o deshabilitar la auditoría para la zona que administran.

Las ventajas de la auditoría por zona son una pista de auditoría personalizada para cada zona y la capacidad de deshabilitar la auditoría en una zona por zona. Estas ventajas pueden ser contrarrestadas por la sobrecarga administrativa. El administrador de zonas personaliza cada archivo de configuración de auditoría. Cada zona ejecuta su propio daemon de auditoría y tiene su propia cola de auditoría y sus propios registros de auditoría. Los archivos de registro de auditoría de la zona deben ser administrados.

# Mejoras de la auditoría en la versión Solaris 10

Desde la versión Solaris 9, las siguientes funciones se han introducido para la auditoría:

- La auditoría puede utilizar la utilidad `syslog` para almacenar registros de auditoría en formato de texto. Para obtener más información, consulte [“Registros de auditoría” en la página 593](#). Para configurar el archivo `audit_control` para que use la utilidad `syslog`, consulte [“Cómo configurar registros de auditoría syslog” en la página 617](#).
- El comando `praudit` tiene un formato adicional de salida, XML. XML es un formato estándar, portátil y procesable. Este formato permite leer la salida en un explorador y proporciona el origen de secuencias de comandos XML para informes. La opción `-x` para el comando `praudit` se describe en [“Comando praudit” en la página 669](#).
- Se ha reestructurado el conjunto predeterminado de clases de auditoría. Las metaclasses de auditoría proporcionan un marco para clases de auditoría más detalladas. Para obtener una lista del conjunto predeterminado de clases, consulte [“Definiciones de clases de auditoría” en la página 679](#).
- El comando `bsmconv` ya no deshabilita el uso de la clave Stop-A. El evento Stop-A se puede auditar.
- La indicación de hora en los registros de auditoría se notifica en formato ISO 8601. Para obtener información sobre el estándar, consulte <http://www.iso.org>.
- Tres opciones de política de auditoría se han agregado:
  - **pública:** los objetos públicos ya no se auditan en los eventos de sólo lectura. Al no auditar archivos públicos, el tamaño del registro de auditoría se reduce drásticamente. Por este motivo, los intentos de leer archivos confidenciales son más sencillos de supervisar. Para obtener más información sobre objetos públicos, consulte [“Conceptos y terminología de auditoría” en la página 588](#).
  - **por zona:** la política `perzone` tiene efectos amplios. Un daemon independiente de auditoría se ejecuta en cada zona. El daemon usa archivos de configuración de auditoría que son específicos para la zona, al igual que lo es la cola de la auditoría. Para obtener detalles, consulte las páginas del comando `man auditd(1M)` y `auditconfig(1M)`. Para obtener más información sobre las zonas, consulte [“Auditoría y zonas de Oracle Solaris” en la página 678](#). Para obtener más información sobre las políticas, consulte [“Cómo planificar auditoría en zonas” en la página 600](#).
  - **nombre de zona:** el nombre de la zona de Oracle Solaris en la que ocurrió un evento de auditoría se puede incluir en registros de auditoría. Para obtener más información sobre las zonas, consulte [“Auditoría y zonas de Oracle Solaris” en la página 678](#). Para ver una explicación de cuándo se debe utilizar la opción, consulte [“Determinación de política de auditoría” en la página 605](#).
- Cinco tokens de auditoría se han agregado:
  - El token `cmd` registra la lista de argumentos y la lista de variables de entorno que están asociadas con un comando. Para obtener más información, consulte [“Token cmd” en la página 690](#).

- El token `path_attr` registra la secuencia de objetos de archivo de atributos que están por debajo del objeto del token `path`. Para obtener más información, consulte [“Token path\\_attr” en la página 697](#).
- El token `privilege` registra el uso de privilegio en un proceso. Para obtener más información, consulte [“Token privilege” en la página 697](#).
- El token `uauth` registra el uso de autorización con un comando o una acción. Para obtener más información, consulte [“Token uauth” en la página 705](#).
- El token `zonename` registra el nombre de la zona no global en la que se produjo un evento de auditoría. La opción de política de auditoría `zonename` determina si el token `zonename` se incluye en el registro de auditoría. Para obtener más información, consulte [“Token zonename” en la página 705](#).

Para obtener información de referencia, consulte [“Auditoría y zonas de Oracle Solaris” en la página 678](#). Para obtener información sobre las zonas, consulte la [Parte II, “Zonas” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

## Planificación de la auditoría de Oracle Solaris

En este capítulo se describe cómo configurar el servicio de auditoría para la instalación de Oracle Solaris. En particular, el capítulo abarca cuestiones que se deben tener en cuenta antes de habilitar el servicio de auditoría. A continuación, se presenta la información de planificación que se incluye en este capítulo:

- “Planificación de auditoría de Oracle Solaris (mapa de tareas)” en la página 599
- “Determinación de política de auditoría” en la página 605
- “Control de costos de auditoría” en la página 609
- “Auditoría eficaz” en la página 610

Para obtener una descripción general de la auditoría, consulte el [Capítulo 28, “Auditoría de Oracle Solaris \(descripción general\)”](#). Para obtener información sobre procedimientos para configurar la auditoría en su sitio, consulte el [Capítulo 30, “Gestión de la auditoría de Oracle Solaris \(tareas\)”](#). Para obtener información de referencia, consulte el [Capítulo 31, “Auditoría de Oracle Solaris \(referencia\)”](#).

### Planificación de auditoría de Oracle Solaris (mapa de tareas)

El siguiente mapa de tareas hace referencia a las tareas principales necesarias para planificar el espacio en disco y los eventos que se deben registrar.

Tarea	Para obtener instrucciones
Determinar la estrategia de auditoría para zonas no globales	“Cómo planificar auditoría en zonas” en la página 600
Planificar espacio de almacenamiento para la pista de auditoría	“Cómo planificar el almacenamiento para registros de auditoría” en la página 601
Determinar a quién y qué auditar	“Cómo planificar a quién y qué auditar” en la página 602

## Planificación de la auditoría de Oracle Solaris (tareas)

Desea ser selectivo sobre los tipos de actividades que se auditan. Al mismo tiempo, desea recopilar información de auditoría útil. Los archivos de auditoría pueden crecer rápidamente y llenar el espacio disponible, por lo que debe asignar suficiente espacio en disco. También debe planificar cuidadosamente a quién auditar y qué auditar.

### ▼ Cómo planificar auditoría en zonas

Si el sistema ha implementado zonas, tiene dos posibilidades de configuración de auditoría:

- Puede configurar un único servicio de auditoría en la zona global para todas las zonas.
- Puede configurar un servicio de auditoría por zona.

Para ver una explicación de las compensaciones, consulte [“Auditoría en un sistema con zonas de Oracle Solaris” en la página 596](#).

#### ● Opte por uno de los métodos siguientes.

##### ■ OPCIÓN 1: Configurar un único servicio de auditoría para todas las zonas.

Auditar todas las zonas de manera idéntica puede crear una pista de auditoría de imagen única. Una pista de auditoría de imagen única se produce cuando todas las zonas de un sistema forman parte de un dominio administrativo. Los registros de auditoría se pueden comparar fácilmente porque los registros en cada zona están preseleccionados con valores de configuración idénticos.

Esta configuración trata todas las zonas como parte de un sistema. La zona global ejecuta el único daemon de auditoría en un sistema y recopila registros de auditoría para cada zona. Se personalizan archivos de configuración de auditoría sólo en la zona global, luego se copian los archivos de configuración de auditoría en cada zona no global.

##### a. Copie el archivo `audit_control` de la zona global a cada zona no global.

##### b. Utilice la misma base de datos `audit_user` para cada zona.

La base de datos `audit_user` puede ser un archivo local o se puede obtener de un servicio de nombres compartido.

##### c. Habilite los registros de auditoría para que se puedan seleccionar por zona.

Para colocar el nombre de zona como parte del registro de auditoría, establezca la política `zonename` en la zona global. El comando `audit reduce` podrá seleccionar luego los eventos de auditoría por zona de la pista de auditoría. Si desea ver un ejemplo, consulte la página del comando `man auditreduce(1M)`.



Para planificar una pista de auditoría de imagen única, consulte [“Cómo planificar a quién y qué auditar” en la página 602](#). Comience con el primer paso. El administrador de la zona global también debe dejar a un lado el almacenamiento, como se describe en [“Cómo planificar el almacenamiento para registros de auditoría” en la página 601](#).

#### ■ OPCIÓN 2: Configurar un servicio de auditoría por zona.

Opte por configurar la auditoría por zona si diferentes zonas tienen diferentes archivos de servicio de nombres o si los administradores de zonas desean controlar la auditoría en sus zonas.

- Cuando configura la auditoría por zona, debe configurar la zona global para auditoría. Establezca la política de auditoría perzone en la zona global. Para establecer una política de auditoría, consulte [“Cómo configurar la auditoría por zona” en la página 639](#).

---

**Nota** – Si los archivos de servicio de nombres están personalizados en zonas no globales y la política perzone no está establecida, se requiere el uso cuidadoso de herramientas de auditoría para seleccionar registros utilizables. Un ID de usuario en una zona puede hacer referencia a un usuario diferente del mismo ID en una zona diferente.

---

- Para generar registros que puedan rastrearse a sus respectivas zonas de origen, establezca la política de auditoría zonename en la zona global. En la zona global, ejecute el comando `auditreduce` con la opción `zonename`. A continuación, en la zona `zonename`, ejecute el comando `praudit` en la salida `auditreduce`.
- Cada administrador de zona configura los archivos de auditoría para la zona.  
Un administrador de zona no global puede establecer todas las opciones de política excepto `perzone` y `ahlt`.
- Cada administrador de zona puede habilitar o deshabilitar la auditoría en la zona.

Si personaliza archivos de configuración de auditoría en cada zona, utilice [“Cómo planificar a quién y qué auditar” en la página 602](#) para planificar cada zona. Puede saltar el primer paso. Cada administrador de zona también debe dejar a un lado el almacenamiento de cada zona, como se describe en [“Cómo planificar el almacenamiento para registros de auditoría” en la página 601](#).

## ▼ Cómo planificar el almacenamiento para registros de auditoría

La pista de auditoría requiere espacio de archivo dedicado. El espacio de archivo dedicado para los archivos de auditoría debe estar disponible y debe ser seguro. Cada sistema debe tener varios directorios de auditoría configurados para archivos de auditoría. Debe decidir cómo configurar los directorios de auditoría como una de las primeras tareas antes de habilitar la auditoría en

cualquier sistema. El siguiente procedimiento trata los problemas que debe resolver cuando planifica el almacenamiento de la pista de auditoría.

**Antes de empezar** Si implementa zonas no globales, complete [“Cómo planificar auditoría en zonas” en la página 600](#) antes de utilizar este procedimiento.

**1 Determine cuánta auditoría necesita el sitio.**

Equilibre las necesidades de seguridad del sitio con la disponibilidad de espacio en disco para la pista de auditoría.

Para obtener indicaciones acerca de cómo reducir los requisitos de espacio manteniendo la seguridad del sitio y cómo diseñar el almacenamiento de auditoría, consulte [“Control de costos de auditoría” en la página 609](#) y [“Auditoría eficaz” en la página 610](#).

**2 Determine los sistemas que se van a auditar.**

En esos sistemas, asigne espacio para al menos un directorio de auditoría local. Para especificar los directorios de auditoría, consulte el [Ejemplo 30–3](#).

**3 Determine los sistemas que van a almacenar archivos de auditoría.**

Decida qué servidores contendrán los directorios de auditoría primarios y secundarios. Para ver ejemplos acerca de cómo configurar discos para directorios de auditoría, consulte [“Cómo crear particiones para los archivos de auditoría” en la página 625](#).

**4 Nombre los directorios de auditoría.**

Cree una lista de todos los directorios de auditoría que se va a utilizar. Para obtener directrices de nombres, consulte [“Almacenamiento de la pista de auditoría” en la página 595](#) y [“Comando audit reduce” en la página 667](#).

**5 Determine qué directorios de auditoría se van a utilizar y qué sistemas van a utilizarlos.**

Crear un mapa que muestre el directorio de auditoría que se va a utilizar y el sistema que va a utilizarlo. El mapa le ayuda a equilibrar la actividad de auditoría. Para ver una ilustración, consulte la [Figura 31–1](#) y la [Figura 31–2](#).

## ▼ **Cómo planificar a quién y qué auditar**

**Antes de empezar** Si implementa zonas no globales, complete [“Cómo planificar auditoría en zonas” en la página 600](#) antes de utilizar este procedimiento.

**1 Determine si desea una pista de auditoría de imagen de sistema único.**

Los sistemas dentro de un único dominio administrativo pueden crear una pista de auditoría de imagen de sistema único. Si los sistemas utilizan diferentes servicios de nombres, comience con el siguiente paso. Deberá completar el resto de los pasos de planificación para cada sistema.

Una pista de auditoría de imagen de sistema único trata los sistemas que se auditan como un equipo. Para crear una pista de auditoría de imagen de sistema único para un sitio, cada sistema en la instalación debe configurarse como se indica a continuación:

- Utilice el mismo servicio de nombres.  
Para interpretar los registros de auditoría se utilizan dos comandos, `auditreduce` y `praudit`. Para una correcta interpretación de los registros de auditoría, los archivos `passwd`, `hosts` y `audit_user` deben ser consistentes.
- Utilice los mismos archivos `audit_warn`, `audit_event`, `audit_class` y `audit_startup` como cualquier otro sistema.
- Utilice la misma base de datos `audit_user`. La base de datos puede estar en un servicio de nombres como NIS o LDAP.
- Tenga entradas `flags`, `naflags` y `plugin` idénticas en el archivo `audit_control`.

## 2 Determine la política de auditoría.

Utilice el comando `auditconfig -lspolicy` para ver una breve descripción de opciones de políticas disponibles. De manera predeterminada, sólo la política `cnt` está activada. Para obtener más información, consulte el [Paso 8](#).

Para ver los efectos de las opciones de política, consulte [“Determinación de política de auditoría” en la página 605](#). Para establecer una política de auditoría, consulte [“Cómo configurar la política de auditoría” en la página 629](#).

## 3 Determine si desea modificar asignaciones evento-clase.

En muchas situaciones, la asignación predeterminada es suficiente. Sin embargo, si agrega nuevas clases, cambia definiciones de clase o determina que un registro de una llamada del sistema específica no es útil, es posible que también necesite mover un evento a una clase diferente.

Para obtener un ejemplo, consulte [“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 623](#).

## 4 Determine las clases de auditoría que se van preseleccionar.

El mejor momento para agregar clases de auditoría o para cambiar las clases predeterminadas es antes de iniciar el servicio de auditoría.

Los valores de clases de auditoría de las entradas `flags`, `naflags` y `plugin` en el archivo `audit_control` se aplican a todos los usuarios y procesos. Las clases preseleccionadas determinan si una clase de auditoría se audita correctamente, con errores o ambos.

Para preseleccionar clases de auditoría, consulte [“Cómo modificar el archivo `audit\_control`” en la página 615](#).

**5 Determine excepciones de usuario para las clases de auditoría preseleccionadas en todo el sistema.**

Si decide que algunos usuarios deben auditarse de manera distinta de las clases de auditoría preseleccionadas en todo el sistema, modifique las entradas de los usuarios individuales en la base de datos `audit_user`.

Para obtener un ejemplo, consulte [“Cómo cambiar las características de auditoría de un usuario” en la página 620](#).

**6 Determine el nivel mínimo de espacio libre en disco.**

Cuando el espacio en disco de un sistema de archivos de auditoría cae por debajo del porcentaje `minfree`, el daemon `auditd` cambia al siguiente directorio de auditoría disponible. A continuación, el daemon envía una advertencia de que el límite de aviso se ha excedido.

Para establecer el espacio en disco mínimo disponible, consulte el [Ejemplo 30–4](#).

**7 Decida cómo gestionar el alias de correo electrónico `audit_warn`.**

La secuencia de comandos `audit_warn` se ejecuta siempre que el sistema de auditoría necesita notificarle de una situación que requiere atención administrativa. De manera predeterminada, la secuencia de comandos `audit_warn` envía un correo electrónico al alias `audit_warn` y envía un mensaje a la consola.

Para configurar el alias, consulte [“Cómo configurar el alias de correo electrónico `audit\_warn`” en la página 629](#).

**8 Decida la acción que se llevará a cabo cuando todos los directorios de auditoría estén completos.**

De manera predeterminada, cuando la pista de auditoría se desborda, el sistema sigue funcionando. El sistema cuenta los registros de auditoría que se descartan, pero no registra los eventos. Para mayor seguridad, puede deshabilitar la política `cnt` y habilitar la política `ahlt`. La política `ahlt` detiene el sistema cuando un evento asíncrono no se puede ubicar en la cola de auditoría.

Para ver una explicación de estas opciones de política, consulte [“Políticas de auditoría para eventos síncronos y asíncronos” en la página 607](#). Para configurar estas opciones de política, consulte el [Ejemplo 30–16](#).

**9 Decida si se deben recopilar registros de auditoría en formato binario, en formato `syslog` o en ambos formatos.**

Para obtener una descripción general, consulte [“Registros de auditoría” en la página 593](#).

Para obtener un ejemplo, consulte [“Cómo configurar registros de auditoría `syslog`” en la página 617](#).

# Determinación de política de auditoría

La política de auditoría determina las características de los registros de auditoría para el sistema local. Las opciones de política se definen por una secuencia de comandos de inicio. La secuencia de comandos `bsmconv`, que habilita el servicio de auditoría, crea la secuencia de comandos `/etc/security/audit_startup`. La secuencia de comandos `audit_startup` ejecuta el comando `auditconfig` para establecer la política de auditoría. Para obtener detalles sobre la secuencia de comandos, consulte la página del comando `man audit_startup(1M)`.

La mayoría de las opciones de política de auditoría están deshabilitadas de manera predeterminada para minimizar los requisitos de almacenamiento y las demandas de procesamiento del sistema. Puede habilitar y deshabilitar de manera dinámica las opciones de política de auditoría con el comando `auditconfig`. Puede habilitar y deshabilitar de manera permanente las opciones de política con la secuencia de comandos `audit_startup`.

Utilice la siguiente tabla para determinar si las necesidades de su sitio justifican la sobrecarga adicional que se genera como resultado de la habilitación de una o más opciones de política de auditoría.

TABLA 29-1 Efectos de opciones de política de auditoría

Nombre de política	Descripción	¿Por qué cambiar la opción de política?
ahlt	Esta política se aplica sólo a eventos asíncronos. Cuando está deshabilitada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría.	La opción deshabilitada tiene sentido cuando la disponibilidad del sistema es más importante que la seguridad.
	Cuando está habilitada, esta política detiene el sistema cuando los sistemas de archivos de auditoría están completos. La intervención administrativa es necesaria para limpiar la cola de auditoría, liberar espacio para los registros de auditoría y reiniciar. Esta política sólo puede habilitarse en la zona global. La política afecta todas las zonas.	La opción habilitada tiene sentido en un entorno donde la seguridad es primordial.
arge	Cuando está deshabilitada, esta política omite variables de entorno de un programa ejecutado del registro de auditoría <code>exec</code> .	La opción deshabilitada recopila mucho menos información que la opción habilitada.
	Cuando está habilitada, esta política agrega variables de entorno de un programa ejecutado al registro de auditoría <code>exec</code> . Los registros de auditoría resultantes contienen más detalles que cuando esta política está deshabilitada.	La opción habilitada tiene sentido cuando audita a unos pocos usuarios. La opción también resulta útil cuando hay sospechas sobre las variables de entorno que se utilizan en programas <code>exec</code> .

TABLA 29-1 Efectos de opciones de política de auditoría (Continuación)

Nombre de política	Descripción	¿Por qué cambiar la opción de política?
argv	<p>Cuando está deshabilitada, esta política omite argumentos de un programa ejecutado del registro de auditoría exec.</p> <p>Cuando está habilitada, esta política agrega argumentos de un programa ejecutado al registro de auditoría exec. Los registros de auditoría resultantes contienen más detalles que cuando esta política está deshabilitada.</p>	<p>La opción deshabilitada recopila mucho menos información que la opción habilitada.</p> <p>La opción habilitada tiene sentido cuando audita a unos pocos usuarios. La opción también resulta útil cuando tiene motivos para creer que se ejecutan programas exec poco usuales.</p>
cnt	<p>Cuando está deshabilitada, esta política bloquea un usuario o una aplicación para que no se ejecute. El bloqueo ocurre cuando los registros de auditoría no se agregan a la pista de auditoría porque no hay espacio en disco disponible.</p> <p>Cuando está habilitada, esta política permite que se complete el evento sin que se haya generado un registro de auditoría. La política mantiene un recuento de registros de auditoría que se descartan.</p>	<p>La opción deshabilitada tiene sentido en un entorno donde la seguridad es primordial.</p> <p>La opción habilitada tiene sentido cuando la disponibilidad del sistema es más importante que la seguridad.</p>
group	<p>Cuando está deshabilitada, esta política no agrega una lista de grupos a los registros de auditoría.</p> <p>Cuando está habilitada, esta política agrega una lista de grupos a cada registro de auditoría como un token especial.</p>	<p>La opción deshabilitada normalmente satisface los requisitos de seguridad del sitio.</p> <p>La opción habilitada tiene sentido cuando necesita auditar los grupos que generan eventos de auditoría.</p>
path	<p>Cuando está deshabilitada, esta política registra en un registro de auditoría una ruta como máximo que se utiliza durante una llamada del sistema.</p> <p>Cuando está habilitada, esta política registra cada ruta que se utiliza junto con un evento de auditoría para cada registro de auditoría.</p>	<p>La opción deshabilitada ubica como máximo una ruta en un registro de auditoría.</p> <p>La opción habilitada introduce cada nombre de archivo o ruta que se utiliza durante una llamada del sistema en el registro de auditoría como un token path.</p>
perzone	<p>Cuando está deshabilitada, esta política mantiene una única configuración de auditoría para un sistema. Un daemon de auditoría se ejecuta en la zona global. Los eventos de auditoría en zonas no globales se pueden ubicar en el registro de auditoría mediante la preselección del token de auditoría zonename.</p> <p>Cuando está habilitada, esta política mantiene una configuración de auditoría, una cola de auditoría y registros de auditoría independientes para cada zona. Una versión independiente del daemon de auditoría se ejecuta en cada zona. Esta política se puede habilitar sólo en la zona global.</p>	<p>La opción deshabilitada es útil cuando no tiene una razón en especial para mantener un registro de auditoría, una cola y un daemon independientes para cada zona.</p> <p>La opción habilitada es útil cuando no puede supervisar el sistema eficazmente mediante la preselección del token de auditoría zonename.</p>

TABLA 29-1 Efectos de opciones de política de auditoría (Continuación)

Nombre de política	Descripción	¿Por qué cambiar la opción de política?
<code>public</code>	<p>Cuando está deshabilitada, esta política no agrega eventos de sólo lectura de objetos públicos a la pista de auditoría cuando la lectura de archivos está preseleccionada. Las clases de auditoría que contienen eventos de sólo lectura incluyen <code>fr</code>, <code>fa</code> y <code>cl</code>.</p> <p>Cuando está habilitada, esta política registra todos los eventos de auditoría de sólo lectura de objetos públicos si una clase de auditoría apropiada está preseleccionada.</p>	<p>La opción deshabilitada normalmente satisface los requisitos de seguridad del sitio.</p> <p>La opción habilitada rara vez es útil.</p>
<code>seq</code>	<p>Cuando está deshabilitada, esta política no agrega un número de secuencia a cada registro de auditoría.</p> <p>Cuando está habilitada, esta política agrega un número de secuencia a cada registro de auditoría. El token <code>sequence</code> contiene el número de secuencia.</p>	<p>La opción deshabilitada es suficiente si la auditoría se ejecuta sin problemas.</p> <p>La opción habilitada tiene sentido cuando la política <code>cnt</code> está habilitada. La política <code>seq</code> le permite determinar cuándo se descartan los datos.</p>
<code>trail</code>	<p>Cuando está deshabilitada, esta política no agrega un token <code>trailer</code> a los registros de auditoría.</p> <p>Cuando está habilitada, esta política agrega un token <code>trailer</code> a cada registro de auditoría.</p>	<p>La opción deshabilitada crea un registro de auditoría más pequeño.</p> <p>La opción habilitada marca claramente el final de cada registro de auditoría con un token <code>trailer</code>. El token <code>trailer</code> se suele utilizar junto con el token <code>sequence</code>. El token <code>trailer</code> proporciona una resincronización de registros de auditoría más fácil y precisa.</p>
<code>zonename</code>	<p>Cuando está deshabilitada, esta política no incluye un token <code>zonename</code> en los registros de auditoría.</p> <p>Cuando está habilitada, esta política incluye un token <code>zonename</code> en cada registro de auditoría de una zona no global.</p>	<p>La opción deshabilitada es útil cuando no necesita comparar el comportamiento de auditoría entre zonas.</p> <p>La opción habilitada es útil cuando necesita aislar y comparar el comportamiento de auditoría entre zonas.</p>

## Políticas de auditoría para eventos síncronos y asíncronos

Juntas, la política `ahlt` y la política `cnt` rigen lo que ocurre cuando la cola de auditoría está completa y no puede aceptar más eventos. Las políticas son independientes y están relacionadas. Las combinaciones de las políticas tienen los siguientes efectos:

- `-ahlt +cnt` es la política predeterminada que se envía. Este valor predeterminado le permite a un evento auditado ser procesado incluso si el evento no se puede registrar. La política `-ahlt` indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará los eventos y continuará el procesamiento. En la zona global, el contador `as_dropped` registra el recuento.

La política +cnt indica que si llega un evento síncrono y el evento no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento. El contador `as_dropped` de la zona registra el recuento.

La configuración -ahlt +cnt se usa generalmente en sitios donde el procesamiento debe continuar, incluso si continuar con el procesamiento puede producir una pérdida de registros de auditoría. El campo `auditstat drop` muestra el número de registros de auditoría que se descartan en una zona.

- La política +ahlt -cnt indica que el procesamiento se detiene cuando un evento no se puede agregar a la cola de auditoría de núcleo.

La política +ahlt indica que si un registro de auditoría de un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, todo el procesamiento se detiene. El sistema entrará en estado de alerta. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.

La política -cnt indica que si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.

La configuración +ahlt -cnt se usa generalmente en sitios donde un registro de cada evento de auditoría tiene prioridad sobre disponibilidad del sistema. Los programas parecerán bloquearse hasta que el espacio de auditoría pase a estar disponible. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.

Sin embargo, si un evento asíncrono se produce, el sistema entrará en estado de alerta, lo que lleva a una interrupción. La cola de núcleo de eventos de auditoría se puede recuperar manualmente de un volcado de bloqueo guardado. El evento asíncrono no estará en la cola de auditoría y se debe recuperar de punteros en la pila de llamadas.

- La política -ahlt -cnt indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el evento se contará y continuará el procesamiento. Cuando un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el subproceso que intenta entregar el evento se bloqueará. El subproceso se coloca en una cola inactiva hasta que el espacio de auditoría pase a estar disponible. Ningún recuento se mantiene. Los programas podrían parecer bloquearse hasta que el espacio de auditoría pase a estar disponible.

La configuración -ahlt -cnt se usa generalmente en los sitios donde el registro de todos los eventos de auditoría síncronos tiene prioridad sobre alguna posible pérdida de registros de auditoría asíncronos. El campo `auditstat wblk` muestra el número de veces que los subprocesos se bloquearon.

- La política +ahlt +cnt indica que si un evento asíncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema entrará en estado de alerta. Si un evento síncrono no se puede ubicar en la cola de auditoría de núcleo, el sistema contará el evento y continuará el procesamiento.



## Control de costos de auditoría

Debido a que la auditoría consume recursos del sistema, debe controlar el grado de detalle que se registra. Cuando decide lo que se debe auditar, tenga en cuenta los siguientes costos de auditoría:

- Costo de mayor tiempo de procesamiento
- Costo de análisis de datos de auditoría
- Costo de almacenamiento de datos de auditoría

### Costo de mayor tiempo de procesamiento de datos de auditoría

El costo de mayor tiempo de procesamiento es el menos significativo de los costos de auditoría. La primera razón es que la auditoría por lo general no se produce durante tareas de cálculos intensivos, como procesamiento de imágenes, cálculos complejos, etc. La otra razón es que el costo de sistemas de un único usuario suele ser lo suficientemente pequeño como para ignorarse.

### Costo de análisis de datos de auditoría

El costo de análisis es más o menos proporcional a la cantidad de datos de auditoría que se recopilan. El costo de análisis incluye el tiempo que se necesita para fusionar y revisar los registros de auditoría. El costo también incluye el tiempo que se necesita para archivar los registros y mantener los registros en un lugar seguro.

Cuantos menos registros se generan, menor es el tiempo que se necesita para analizar la pista de auditoría. En las próximas secciones, [“Costo de almacenamiento de datos de auditoría” en la página 609](#) y [“Auditoría eficaz” en la página 610](#), se describen maneras de auditar de manera eficaz. La auditoría eficaz reduce la cantidad de datos de auditoría al tiempo que se sigue proporcionando suficiente cobertura para lograr los objetivos de seguridad del sitio.

### Costo de almacenamiento de datos de auditoría

El costo de almacenamiento es el costo más significativo de la auditoría. La cantidad de datos de auditoría depende de lo siguiente:

- Número de usuarios
- Número de sistemas
- Cantidad de uso
- Grado de rastreabilidad y responsabilidad necesario

Debido a que estos factores varían de sitio en sitio, ninguna fórmula puede predeterminar la cantidad de espacio en disco que se debe destinar al almacenamiento de datos de auditoría. Utilice la siguiente información como guía:

- Preseleccione las clases de auditoría con cuidado para reducir el volumen de registros que se generan.

La auditoría completa, es decir, con la clase `all` llena los discos rápidamente. Incluso una simple tarea, como compilar un programa podría generar un archivo de auditoría de gran tamaño. Un programa de tamaño moderado podría generar miles de registros de auditoría en menos de un minuto.

Por ejemplo, si se omite la clase de auditoría `file_read`, `fr`, puede reducir significativamente el volumen de auditoría. Si selecciona auditar operaciones fallidas, sólo a veces puede reducir el volumen de auditoría. Por ejemplo, si realiza una auditoría de operaciones fallidas `file_read`, `-fr`, puede generar muchos menos registros que si realiza una auditoría de todos los eventos `file_read`.

- La gestión de archivos de auditoría eficaz también es importante. Después de que se crean registros de auditoría, la gestión de archivos reduce la cantidad de almacenamiento que se requiere.

- Comprenda las clases de auditoría.

Antes de configurar la auditoría, debe comprender los tipos de eventos que las clases contienen. Puede cambiar las asignaciones de evento-clase de auditoría para optimizar la recopilación de registros de auditoría.

- Desarrolle una filosofía de auditoría para su sitio.

Base la filosofía en medidas razonables. Tales medidas incluyen el importe de rastreabilidad que su sitio requiere y los tipos de usuarios que administra.

## Auditoría eficaz

Las siguientes técnicas lo pueden ayudar a lograr los objetivos de seguridad de su organización y al mismo tiempo auditar de manera más eficaz.

- Audite de manera aleatoria sólo un determinado porcentaje de usuarios a la vez.
- Reduzca los requisitos de almacenamiento en disco para archivos de auditoría mediante la combinación, reducción y compresión de los archivos. Desarrolle procedimientos para archivar los archivos, para transferir los archivos a soportes extraíbles y para almacenar los archivos fuera de línea.
- Supervise los datos de auditoría en tiempo real para comportamientos poco usuales. Puede ampliar las herramientas de análisis y de gestión que ya haya desarrollado para gestionar los registros de auditoría en archivos `syslog`.

También puede configurar procedimientos para supervisar la pista de auditoría para ciertas actividades. Puede escribir una secuencia de comandos para impulsar un aumento automático de la auditoría de determinados usuarios o determinados sistemas en respuesta a la detección de eventos poco usuales.

Por ejemplo, puede escribir una secuencia de comandos que haga lo siguiente:

1. Supervise la creación de archivos de auditoría en todos los servidores de archivos de auditoría.

2. Procese los archivos de auditoría con el comando `tail`.

La conducción de la salida del comando `tail -0f` mediante el comando `praudit` pueden producir un flujo de registros de auditoría a medida que los registros se generan. Para obtener más información, consulte la página del comando `man tail(1)`.

3. Analice este flujo para tipos de mensajes poco usuales u otros indicadores y entregue el análisis al auditor.

O bien, la secuencia de comandos se puede utilizar para desencadenar respuestas automáticas.

4. Supervise constantemente los directorios de auditoría en busca de nuevos archivos de auditoría `not_terminated`.
5. Termine procesos `tail` pendientes cuando no se esté escribiendo en los archivos.



## Gestión de la auditoría de Oracle Solaris (tareas)

Este capítulo presenta procedimientos para ayudarlo a configurar y gestionar un sistema Oracle Solaris que se ha auditado. En este capítulo también se incluyen instrucciones para administrar la pista de auditoría. A continuación, se presenta la información que se incluye en este capítulo.

- “Auditoría de Oracle Solaris (mapa de tareas)” en la página 613
- “Configuración de archivos de auditoría (mapa de tareas)” en la página 614
- “Configuración y habilitación del servicio de auditoría (mapa de tareas)” en la página 624
- “Gestión de registros de auditoría (mapa de tareas)” en la página 640
- “Resolución de problemas de la auditoría de Oracle Solaris (mapa de tareas)” en la página 651

Para obtener una descripción general del servicio de auditoría, consulte el [Capítulo 28](#), “Auditoría de Oracle Solaris (descripción general)”. Para obtener sugerencias de planificación, consulte el [Capítulo 29](#), “Planificación de la auditoría de Oracle Solaris”. Para obtener información de referencia, consulte el [Capítulo 31](#), “Auditoría de Oracle Solaris (referencia)”.

### Auditoría de Oracle Solaris (mapa de tareas)

El siguiente mapa de tareas hace referencia a las tareas principales necesarias para gestionar la auditoría. Las tareas están ordenadas.

Tarea	Descripción	Para obtener instrucciones
1. Plan para auditoría	Contiene los asuntos de configuración que debe decidir antes de configurar el servicio de auditoría.	<a href="#">“Planificación de auditoría de Oracle Solaris (mapa de tareas)” en la página 599</a>
2. Configuración de archivos de auditoría	Define qué eventos, clases y usuarios requieren la auditoría.	<a href="#">“Configuración de archivos de auditoría (mapa de tareas)” en la página 614</a>

Tarea	Descripción	Para obtener instrucciones
3. Configuración y habilitación de la auditoría	Configura el espacio en disco de cada host y otros requisitos de servicio de auditoría. A continuación, inicia el servicio de auditoría.	“Configuración y habilitación del servicio de auditoría (mapa de tareas)” en la página 624
	En un host con zonas no globales instaladas, configure un servicio de auditoría para el sistema, o un servicio de auditoría por zona.	“Configuración del servicio de auditoría en las zonas (tareas)” en la página 636
4. Gestión de registros de auditoría	Recopila y analiza los datos de auditoría.	“Gestión de registros de auditoría (mapa de tareas)” en la página 640

## Configuración de archivos de auditoría (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para que los archivos de configuración personalicen la auditoría en su sitio. La mayoría de las tareas son opcionales.

Tarea	Descripción	Para obtener instrucciones
Selección de clases de auditoría y personalización de valores de <code>audit_control</code>	Implica lo siguiente: <ul style="list-style-type: none"><li>■ Preseleccionar clases de auditoría en todo el sistema.</li><li>■ Especificar los directorios de auditoría para cada sistema.</li><li>■ Configurar los límites de espacio en disco en sistemas de archivos de auditoría.</li></ul>	“Cómo modificar el archivo <code>audit_control</code> ” en la página 615
(Opcional) Eventos de auditoría de registros en dos modos	Le permite supervisar los eventos de auditoría en tiempo real, además de almacenar los registros de auditoría en formato binario.	“Cómo configurar registros de auditoría <code>syslog</code> ” en la página 617
(Opcional) Cambiar características de auditoría para los usuarios	Permite configurar excepciones específicas para los usuarios para las clases de auditoría preseleccionadas en todo el sistema.	“Cómo cambiar las características de auditoría de un usuario” en la página 620
(Opcional) Agregar clases de auditoría	Permite reducir el número de registros de auditoría mediante la creación de una nueva clase de auditoría para retener eventos.	“Cómo agregar un clase de auditoría” en la página 622
(Opcional) Cambiar asignaciones de evento-clase	Reduce el número de registros de auditoría mediante el cambio de la asignación de evento-clase.	“Cómo cambiar una pertenencia a clase de un evento de auditoría” en la página 623

# Configuración de archivos de auditoría (tareas)

Antes de habilitar la auditoría en su red, puede personalizar los archivos de configuración de auditoría para los requisitos de auditoría de su sitio. También puede reiniciar el servicio de auditoría o el sistema local para leer los archivos de configuración cambiados después de que el servicio de auditoría se haya habilitado. Sin embargo, la práctica recomendada es personalizar su configuración de auditoría en la medida que sea posible antes de iniciar el servicio de auditoría.

Si ha implementado zonas, puede seleccionar si desea auditar todas las zonas desde la zona global. Para diferenciar entre zonas en la salida de auditoría, puede definir la opción de la política `zonename`. Como alternativa, para auditar las zonas no globales por separado, puede establecer la política `perzone` en la zona global y personalizar los archivos de configuración de auditoría en las zonas no globales. Para obtener una descripción general, consulte [“Auditoría y zonas de Oracle Solaris” en la página 678](#). Para obtener información sobre planificación, consulte [“Cómo planificar auditoría en zonas” en la página 600](#). Para obtener información sobre los procedimientos, consulte [“Configuración del servicio de auditoría en las zonas \(tareas\)” en la página 636](#).

## ▼ Cómo modificar el archivo `audit_control`

El archivo `/etc/security/audit_control` configura la auditoría en todo el sistema. El archivo determina qué eventos de auditan, cuándo se emiten advertencias de auditoría y dónde están los archivos de auditoría.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

### 2 (Opcional) Guarde una copia de seguridad del archivo `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.orig
```

### 3 Modifique el archivo `audit_control` para su sitio.

Cada entrada tiene el siguiente formato:

*keyword*: *value*

*palabra clave*      Define el tipo de línea. Los tipos son `dir`, `flags`, `minfree`, `naflags` y `plugin`. En la versión Solaris 10, las líneas `dir` y `minfree` se descartaron.

Para obtener explicaciones de las palabras clave, consulte los siguientes ejemplos.

*valor*              Especifica los datos asociados con el tipo de línea.

---

**Nota** – Para especificar las ubicaciones de los directorios de auditoría, use el atributo `p_dir` en el complemento `audit_binfile.so`. Para especificar el espacio libre mínimo, utilice el atributo `p_minfree`.

---

#### 4 (Opcional) Compruebe la sintaxis del archivo.

```
# audit -v /etc/security/audit_control
syntax ok
```

#### Ejemplo 30–1 Preselección de clases de auditoría para todos los usuarios

La línea `flags` en el archivo `audit_control` define qué clases de eventos atribuibles se auditan para todos los usuarios en el sistema. Las clases se separan por comas. Se permite agregar espacios en blanco. En este ejemplo, los eventos en las clases `lo` y `ap` se auditan para todos los usuarios.

```
## audit_control file
flags:lo,ap
naflags:lo
plugin:name=...
```

Para ver qué eventos están asignados a una clase, lea el archivo `audit_event`. También puede utilizar el comando `bsmrecord`, como se muestra en el [Ejemplo 30–27](#).

#### Ejemplo 30–2 Preselección de eventos no atribuibles

En este ejemplo, se auditan todos los eventos de la clase `na` y todos eventos `login` que no son atribuibles.

```
## audit_control file
flags:lo
naflags:lo,na
plugin:name=...
```

#### Ejemplo 30–3 Especificación de la ubicación de datos de auditoría binarios

El indicador `p_dir` del complemento `audit_binfile.so` muestra qué sistemas de archivos de auditoría usar para los datos de auditoría binarios. En este ejemplo, se pueden definir tres ubicaciones para datos de auditoría binarios. Los directorios se muestran en orden, del directorio principal al directorio de último recurso. La línea `plugin` no contiene un salto de línea.

```
## audit_control file
##
flags:lo
naflags:lo,na
```



```
plugin:name=audit_binfile.so; p_dir=/var/audit/egret.1/files,  
/var/audit/egret.2/files,/var/audit
```

Para configurar sistemas de archivos para que retengan datos de auditoría binarios, consulte [“Cómo crear particiones para los archivos de auditoría” en la página 625](#).

### Ejemplo 30-4 Cambiar el límite de aviso para las advertencias

En este ejemplo, está configurado el nivel mínimo de espacio libre para todos los sistemas archivos de auditoría de modo que se emite una advertencia cuando sólo queda disponible el 10% del sistema de archivos.

La línea plugin no contiene un salto de línea.

```
## audit_control file  
#  
flags:lo  
naflags:lo,na  
plugin:name=audit_binfile.so; p_dir=/var/audit/examplehost.1/files,  
/var/audit/examplehost.2/files,/var/audit/localhost/files; p_minfree=10
```

El alias `audit_warn` recibe la advertencia. Para configurar el alias, consulte [“Cómo configurar el alias de correo electrónico `audit\_warn`” en la página 629](#).

## ▼ Cómo configurar registros de auditoría syslog

Puede indicar al servicio de auditoría que copie algunos o todos los registros de auditoría recopilados en la cola de auditoría en syslog. En el siguiente procedimiento, guarda datos de auditoría binarios y datos de auditoría textuales. Los datos de auditoría textuales recolectados son un subconjunto de los datos binarios.

#### Antes de empezar

Debe preseleccionar las clases de auditoría. Las clases de auditoría preseleccionadas se especifican en la línea `flags` y en la línea `naflags` del archivo `audit_control`. También puede preseleccionar clases de usuarios individuales en el archivo `audit_user` y agregar dinámicamente clases de auditoría con el comando `auditconfig`.

#### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

#### 2 (Opcional) Guarde una copia de seguridad del archivo `audit_control`.

```
# cp /etc/security/audit_control /etc/security/audit_control.save
```

### 3 Agregue una entrada de complemento `audit_syslog.so`.

```
## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so;p_dir=/var/audit; p_minfree=20;
plugin:name=audit_syslog.so;p_flags=+lo,-ss
```

Una entrada `plugin` tiene el siguiente formato:

```
plugin:name=name; qsize=max-queued-records;p_*=value
```

- `name=nombre`: muestra el nombre del complemento. Los valores válidos son `audit_binfile.so` y `audit_syslog.so`.
- `qsize=máximo_registrosCola`: especifica el número máximo de registros que se pueden poner en cola para los datos de auditoría que se envían al complemento. Este atributo es opcional.
- `p_*=valor`: especifica los atributos específicos del complemento. El complemento `audit_syslog.so` acepta `p_flags`. El complemento `audit_binfile.so` acepta `p_dir`, `p_minfree` y `p_fsize`. El atributo `p_fsize` se introdujo en Solaris 10 10/08.

Para obtener más información acerca de los atributos específicos del complemento, consulte la sección `OBJECT ATTRIBUTES` de las páginas del comando `man audit_binfile(5)` y `audit_syslog(5)`.

### 4 Agregue una entrada `audit.notice` al archivo `syslog.conf`.

La entrada incluye la ubicación del archivo de registro.

```
# cat /etc/syslog.conf
...
audit.notice      /var/adm/auditlog
```

No almacene registros textuales donde se almacenan los archivos de auditoría binarios. El comando `auditreduce`, que lee archivos de auditoría binarios, asume que todos los archivos en una partición de auditoría son archivos de auditoría binarios.

### 5 Cree el archivo de registro.

```
# touch /var/adm/auditlog
```

### 6 Actualice la información de configuración para el servicio `syslog`.

```
# svcadm refresh system/system-log
```

### 7 Archive con regularidad los archivos de registro `syslog`.

El servicio de auditoría puede generar muchas salidas. Para gestionar los registros, consulte la página del comando `man logadm(1M)`.

### Ejemplo 30-5 Especificación de clases de auditoría para salida de `syslog`

En el siguiente ejemplo, la utilidad `syslog` recopila un subconjunto de las clases de auditoría preseleccionadas.

```
## audit_user file
jdoe:pf

## audit_control file
flags:lo,ss
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit/host.1/files,
/var/audit/host.2/files,/var/audit/localhost/files; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,-na,-ss,+pf
```

Las entradas `flags` y `naflags` indican al sistema que recolecte todos los registros de auditoría de inicio de sesión/cierre de sesión, eventos no atribuibles y cambios de estado de sistema en formato binario. La entrada de complemento `audit_syslog.so` indica a la utilidad `syslog` que recolecte sólo los errores con fallos, los eventos no atribuibles con fallos y los cambios de estado de sistema con fallos. Para el usuario `jdoe`, el registro de auditoría binario incluye todos los usos de un shell que reconoce perfiles. La utilidad `syslog` recopila comandos que reconocen perfiles correctos. La clase `pf` se crea en el [Ejemplo 30-10](#).

### Ejemplo 30-6 Colocar registros de auditoría `syslog` en un sistema remoto

Puede cambiar la entrada `audit.notice` en el archivo `syslog.conf` para que haga referencia a un sistema remoto. En este ejemplo, el nombre del sistema local es `example1`. El sistema remoto es `remote1`.

```
example1 # cat /etc/syslog.conf
...
audit.notice      @remote1
```

La entrada `audit.notice` en el archivo `syslog.conf` en el sistema `remote1` hace referencia al archivo de registro.

```
remote1 # cat /etc/syslog.conf
...
audit.notice      /var/adm/auditlog
```

### Ejemplo 30-7 Uso de complementos en el archivo `audit_control`

El método preferido para especificar información no de indicadores en el archivo `audit_control` es utilizar la entrada `plugin`. En este ejemplo, los indicadores de auditoría están seleccionados y, por lo tanto, se muestra la información del complemento.

```
## audit_control file
flags:lo,ss
```

```
naflags:lo,na
plugin:name=audit_binfile.so;p_minfree=10; p_dir=/var/audit
plugin:name=audit_syslog.so; p_flags=+lo
```

## ▼ Cómo cambiar las características de auditoría de un usuario

Las definiciones para cada usuario se almacenan en la base de datos `audit_user`. Estas definiciones modifican, para el usuario especificado, las clases preseleccionadas en el archivo `audit_control`. El archivo `nsswitch.conf` determina si se utiliza un archivo local o una base de datos de servicio de nombres. Para calcular la máscara de preselección de auditoría final del usuario, consulte [“Características de auditoría de proceso” en la página 683](#).

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

### 2 (Opcional) Guarde una copia de seguridad de la base de datos `audit_user`.

```
# cp /etc/security/audit_user /etc/security/audit_user.orig
```

### 3 Agregue las nuevas entradas a la base de datos `audit_user`.

En la base de datos local, cada entrada tiene el siguiente formato:

```
username:always-audit:never-audit
```

*nombre\_usuario*      Selecciona el nombre del usuario que se van a auditar.

*siempre\_auditar*      Selecciona la lista de clases de auditoría que siempre se deben auditar para el usuario especificado.

*nunca\_auditar*      Selecciona la lista de clases de auditoría que nunca se deben auditar para el usuario especificado.

Puede especificar varias clases si separa las clases de auditoría con comas.

Las entradas `audit_user` entran en vigencia a partir del siguiente inicio de sesión del usuario.

## Ejemplo 30–8 Cambiar qué eventos se auditan para un usuario

En este ejemplo, el archivo `audit_control` contiene las clases de auditoría preseleccionadas para el sistema:

```
## audit_control file
...
```

```
flags:lo,ss
naflags:lo,na
```

El archivo `audit_user` muestra una excepción. Cuando el usuario `jdoe` utiliza un shell de perfil, ese uso es auditado:

```
## audit_user file
jdoe:pf
```

La máscara de preselección de auditoría para `jdoe` es una combinación de la configuración de `audit_user` y la configuración de `audit_control`. El comando `auditconfig -getaudit` muestra la máscara de preselección para `jdoe`:

```
# auditconfig -getaudit
audit id = jdoe(1234567)
process preselection mask = ss,pf,lo(0x13000,0x13000)
terminal id (maj,min,host) = 242,511,example1(192.168.160.171)
audit session id = 2138517656
```

### Ejemplo 30–9 Sólo usuarios de auditoría, no el sistema

En este ejemplo, se auditan sólo el inicio de sesión y las actividades de rol de cuatro usuarios en este sistema. El archivo `audit_control` no preselecciona clases de auditoría para el sistema.

```
## audit_control file
...
flags:
naflags:
```

El archivo `audit_user` preselecciona dos clases de auditoría para cuatro usuarios, de la siguiente manera:

```
## audit_user file
jdoe:lo,pf
kdoe:lo,pf
pdoe:lo,pf
sdoe:lo,pf
```

El siguiente archivo `audit_control` registra intrusiones injustificadas. En combinación con el archivo `audit_user`, este archivo protege el sistema más que el primer archivo `audit_control` en este ejemplo.

```
## audit_control file
...
flags:
naflags:lo
plugin:name=...
```

## ▼ Cómo agregar un clase de auditoría

Cuando crea su propia clase de auditoría, puede colocar en ella sólo los eventos de auditoría que desea auditar para su sitio. Al agregar la clase en un sistema, deberá copiar el cambio en todos los sistemas que se están auditando.

**1 Asuma el rol de administrador principal o conviértase en superusuario.**

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

**2 (Opcional) Guarde una copia de seguridad del archivo `audit_class`.**

```
# cp /etc/security/audit_class /etc/security/audit_class.orig
```

**3 Agregue las nuevas entradas al archivo `audit_class`.**

Cada entrada tiene el siguiente formato:

*0xnumber: name: description*

*0x*                      Identifica *número* como hexadecimal.

*número*                Define la máscara de clase de auditoría única.

*nombre*                Define el nombre de letra de la clase de auditoría.

*descripción*        Define el nombre descriptivo de la clase de auditoría.

La entrada debe ser única en el archivo. No utilice máscaras de clase de auditoría existentes.

### **Ejemplo 30–10** Creación de una clase de auditoría nueva

En este ejemplo se crea una clase para mantener un pequeño conjunto de eventos de auditoría. La entrada agregada al archivo `audit_class` se muestra a continuación:

```
0x10000000:pf:profile command
```

La entrada crea una nueva clase de auditoría llamada `pf`. En el [Ejemplo 30–11](#) se rellena clase de auditoría nueva.

**Errores más frecuentes**

Si personalizó el archivo `audit_class`, asegúrese de que todas las modificaciones de `audit_user` sean coherentes con las clases de auditoría nuevas. Los errores se producen cuando las clases de auditoría en `audit_user` no son un subconjunto de la base de datos `audit_class`.

## ▼ Cómo cambiar una pertenencia a clase de un evento de auditoría

Puede que desee cambiar la pertenencia de clase de un evento de auditoría para reducir el tamaño de una clase de auditoría existente o colocar el evento en una clase propio. Cuando reconfigura asignaciones de evento-clase de auditoría en un sistema, debe copiar el cambio a todos los sistemas que se auditan.

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 (Opcional) Guarde una copia de seguridad del archivo `audit_event`.

```
# cp /etc/security/audit_event /etc/security/audit_event.orig
```

### 3 Cambie la clase a la que pertenecen los eventos determinados; para esto, cambie la *lista\_clase* de los eventos.

Cada entrada tiene el siguiente formato:

*number: name: description: class-list*

*número*            Es el ID de evento de auditoría.

*nombre*            Es el nombre del evento de auditoría.

*descripción*      Normalmente, la llamada de sistema o el ejecutable que desencadena la creación de un registro de auditoría.

*lista\_clase*        Es una lista separada por comas de las clases de auditoría.

## Ejemplo 30–11 Asignación de eventos de auditoría existentes a una nueva clase

Este ejemplo asigna un evento de auditoría existente a la nueva clase creada en [Ejemplo 30–10](#). En el archivo `audit_control`, el registro binario de auditoría captura éxitos y fracasos de eventos en la clase `pf`. El registro de auditoría `syslog` contiene solamente fracasos de eventos en la clase `pf`.

```
# grep pf | /etc/security/audit_class
0x10000000:pf:profile command
# vi /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
# vi audit_control
...
flags:lo,pf
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,-pf
```

Ejemplo 30–12 Auditoría del uso de programas setuid

En este ejemplo se crea una clase para retener eventos que supervisan las llamadas a los programas setuid y setgid. El registro de auditoría binario captura los éxitos y fracasos de los eventos en las clases lo y na, y los éxitos de los eventos en la clase st. El registro de auditoría syslog contiene solamente éxitos de eventos en la clase st.

```
# vi /etc/security/audit_class
0x00000800:st:setuid class
# vi /etc/security/audit_event
26:AUE_SETGROUPS:setgroups(2):st
27:AUE_SETPGRP:setpgrp(2):st
40:AUE_SETREUID:setreuid(2):st
41:AUE_SETREGID:setregid(2):st
214:AUE_SETEGID:setegid(2):st
215:AUE_SETEUID:seteuid(2):st

# vi audit_control
## audit_control file
flags:lo,+st
naflags:lo,na
plugin:name=audit_binfile.so; p_dir=/var/audit; p_minfree=10
plugin:name=audit_syslog.so; p_flags=-lo,+st
```

Configuración y habilitación del servicio de auditoría (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para configurar y habilitar el servicio de auditoría. Las tareas están ordenadas.

Tarea	Descripción	Para obtener instrucciones
1. (Opcional) Cambiar los archivos de configuración de auditoría	Selecciona qué eventos, clases y usuarios requieren la auditoría.	<a href="#">“Configuración de archivos de auditoría (mapa de tareas)” en la página 614</a>
2. Crear particiones de auditoría	Crea espacio en disco para los archivos de auditoría y los protege con los permisos de archivo.	<a href="#">“Cómo crear particiones para los archivos de auditoría” en la página 625</a>
3. Crear el alias audit_warn	Define quién debe recibir advertencias por correo electrónico cuando el servicio de auditoría necesita atención.	<a href="#">“Cómo configurar el alias de correo electrónico audit_warn ” en la página 629</a>
4. (Opcional) Cambiar la política de auditoría	Define datos adicionales de auditoría que el sitio necesita.	<a href="#">“Cómo configurar la política de auditoría” en la página 629</a>



Tarea	Descripción	Para obtener instrucciones
6. Configurar la auditoría en zonas no globales	Permite habilitar zonas no globales para recopilar registros de auditoría.	<a href="#">“Configuración del servicio de auditoría en las zonas (tareas)” en la página 636</a>
7. Habilitar la auditoría.	Activa el servicio de auditoría.	<a href="#">“Cómo habilitar el servicio de auditoría” en la página 632</a>
	Cuando perzone está activado, habilita la auditoría en una zona no global.	<a href="#">Ejemplo 30–20</a>
8. (Opcional) Deshabilitar la auditoría.	Desactiva el servicio de auditoría.	<a href="#">“Cómo deshabilitar el servicio de auditoría” en la página 634</a>
	Cuando perzone está activado, deshabilita la auditoría en una zona no global.	<a href="#">Ejemplo 30–25</a>
9. (Opcional) Volver a leer los cambios de configuración de auditoría	Lee los cambios de configuración de la auditoría en el núcleo mientras el daemon <code>audited</code> se está ejecutando.	<a href="#">“Cómo actualizar el servicio de auditoría” en la página 635</a>

## Configuración y habilitación del servicio de auditoría (tareas)

Después de que los archivos de configuración hayan sido configurados para la ubicación, debe configurar el espacio en disco para los archivos de auditoría. También tendrá que configurar otros atributos del servicio de auditoría y, a continuación, habilitar el servicio. Esta sección también contiene los procedimientos para actualizar el servicio de auditoría cuando cambia los valores de configuración.

Cuando se instala una zona no global, puede seleccionar auditar la zona exactamente como se audita la zona global. Como alternativa, para auditar la zona no global por separado, puede modificar los archivos de configuración de auditoría en la zona no global. Para personalizar los archivos de configuración de auditoría, consulte [“Configuración de archivos de auditoría \(mapa de tareas\)” en la página 614](#).

### ▼ Cómo crear particiones para los archivos de auditoría

El procedimiento siguiente muestra cómo crear particiones para los archivos de auditoría, así como los sistemas de archivos y directorios correspondientes. Omita los pasos según sea necesario, según tenga una partición vacía o ya haya montado un sistema de archivos vacío.

#### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)” de Guía de administración del sistema: administración básica](#).

**2 Determine la cantidad de espacio en disco que sea necesaria.**

Asigne por lo menos 200 Mbytes de espacio en disco por host. Sin embargo, la cantidad de auditoría que necesita es la que dicta los requisitos de espacio en disco. Por lo tanto, los requisitos de espacio en disco pueden ser mucho mayores que esta figura. Recuerde incluir una partición local de un directorio de último recurso.

**3 Cree particiones de auditoría dedicadas, según sea necesario.**

Este paso se realiza más fácilmente durante la instalación del servidor. También puede crear las particiones en discos que aún no se hayan montado en el servidor. Para obtener instrucciones completas sobre cómo crear las particiones, consulte el [Capítulo 11, “Administering Disks \(Tasks\)”](#) de *System Administration Guide: Devices and File Systems*.

```
# newfs /dev/rdisk/cwtxdysz
```

donde `/dev/rdisk/cwt xdysz` es el nombre del dispositivo sin formato para la partición.

Si el host local se va a auditar, cree también un directorio de auditoría de último recurso para el host local.

**4 Cree puntos de montaje para cada nueva partición.**

```
# mkdir /var/audit/server-name.n
```

donde *nombre\_servidor.n* es el nombre del servidor más un número que identifica cada partición. El número es opcional, pero es útil cuando hay muchos directorios de auditoría.

**5 Agregue entradas para que monte automáticamente las nuevas particiones.**

Agregue una línea al archivo `/etc/vfstab` como la siguiente:

```
/dev/dsk/cwtxdysz /dev/rdisk/cwtxdysz /var/audit/server-name.n ufs 2 yes
```

**6 (Opcional) Elimine el umbral de espacio libre mínimo en cada partición.**

Si utiliza la configuración predeterminada, se genera una advertencia cuando el directorio está un 80% completo. La advertencia elimina el motivo para reservar espacio libre en la partición.

```
# tuneufs -m 0 /var/audit/server-name.n
```

**7 Monte las nuevas particiones de auditoría.**

```
# mount /var/audit/server-name.n
```

**8 Cree directorios de auditoría en las nuevas particiones.**

```
# mkdir /var/audit/server-name.n/files
```

**9 Corrija los permisos en los puntos de montaje y los directorios nuevos.**

```
# chmod -R 750 /var/audit/server-name.n/files
```

## 10 En un servidor de archivos, defina los sistemas de archivos para que estén disponibles para otros hosts.

A menudo, se instalan conjuntos de discos para almacenar los registros de auditoría. Si un directorio de auditoría va a ser usado por varios sistemas, el directorio debe estar compartido a través del servicio NFS. Agregue una entrada similar a la siguiente para cada directorio en el archivo `/etc/dfs/dfstab`:

```
share -F nfs /var/audit/server-name.n/files
```

## 11 En un servidor de archivos, reinicie el servicio NFS.

Si este comando es el primer comando `share` o conjuntos de comandos `share` que ha iniciado, es posible que los daemons NFS no se ejecuten.

### ■ Si el servicio NFS está fuera de línea, habilite el servicio.

```
% svcs \*nfs\*
disabled      Nov_02   svc:/network/nfs/rquota:default
offline       Nov_02   svc:/network/nfs/server:default
# svcadm enable network/nfs/server
```

### ■ Si el servicio NFS se está ejecutando, reinicie el servicio.

```
% svcs \*nfs\*
online        Nov_02   svc:/network/nfs/client:default
online        Nov_02   svc:/network/nfs/server:default
# svcadm restart network/nfs/server
```

Para obtener más información sobre el servicio NFS, consulte [“Configuración de servicios NFS” de Guía de administración del sistema: servicios de red](#). Para obtener información sobre la gestión de servicios persistentes, consulte el [Capítulo 18, “Gestión de servicios \(descripción general\)” de Guía de administración del sistema: administración básica](#) y la página del comando `man smf(5)`.

## Ejemplo 30–13 Creación de un directorio de auditoría de último recurso

Todos los sistemas que ejecutan el servicio de auditoría deben tener un sistema de archivos local que se pueda utilizar si no hay ningún otro sistema de archivos disponible. En este ejemplo, se agrega un sistema de archivos a un sistema denominado `egret`. Como este sistema de archivos sólo se utiliza localmente, no es necesario realizar ninguno de los pasos para un servidor de archivos.

```
# newfs /dev/rdisk/c0t2d0
# mkdir /var/audit/egret
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1 /dev/rdisk/c0t2d0s1 /var/audit/egret ufs 2 yes -
# tuneufs -m 0 /var/audit/egret
# mount /var/audit/egret
# mkdir /var/audit/egret/files
# chmod -R 750 /var/audit/egret/files
```

### Ejemplo 30-14 Creación de nuevas particiones auditoría

En este ejemplo, se crea un sistema de archivos nuevo en dos discos nuevos que van a ser utilizados por otros sistemas en la red.

```
# newfs /dev/rdisk/c0t2d0
# newfs /dev/rdisk/c0t2d1
# mkdir /var/audit/egret.1
# mkdir /var/audit/egret.2
# grep egret /etc/vfstab
/dev/dsk/c0t2d0s1 /dev/rdisk/c0t2d0s1 /var/audit/egret.1 ufs 2 yes -
/dev/dsk/c0t2d1s1 /dev/rdisk/c0t2d1s1 /var/audit/egret.2 ufs 2 yes -
# tuneufs -m 0 /var/audit/egret.1
# tuneufs -m 0 /var/audit/egret.2
# mount /var/audit/egret.1
# mount /var/audit/egret.2
# mkdir /var/audit/egret.1/files
# mkdir /var/audit/egret.2/files
# chmod -R 750 /var/audit/egret.1/files /var/audit/egret.2/files
# grep egret /etc/dfs/dfstab
share -F nfs /var/audit/egret.1/files
share -F nfs /var/audit/egret.2/files
# svcadm enable network/nfs/server
```

### Ejemplo 30-15 Creación de particiones de auditoría ZFS

En este ejemplo, el administrador ejecuta el comando `script` después de que se crean las particiones de auditoría ZFS. A continuación se muestra la salida del comando:

```
# zpool create auditf mirror c0t4d0 c0t5d0
# zfs create -o mountpoint=/audit auditf/audit
# zfs create auditf/audit/noddy
# zfs create auditf/audit/noddy/files
# zfs create auditf/audit/blinken
# zfs create auditf/audit/blinken/files
# zfs set devices=off auditf/audit
# zfs set exec=off auditf/audit
# zfs set setuid=off auditf/audit
# zfs set sharenfs=on auditf/audit
# share
-          /audit/blinken/files  rw  ""
-          /audit/noddy        rw  ""
-          /audit/blinken      rw  ""
-          /audit/noddy/files   rw  ""
-          /audit              rw  ""
# ^D
script done on Fri Apr 10 10:10:20 2009
```

Luego, el administrador visualiza los montajes desde el sistema remoto, `remotesys`.

```
# dfshares remotesys
```

RESOURCE	SERVER	ACCESS	TRANSPORT
remotesys:/audit/blinken/files	remotesys	-	-
remotesys:/audit/noddy	remotesys	-	-
remotesys:/audit/blinken	remotesys	-	-

```
remotesys:/audit/noddy/files      remotesys  -      -
remotesys:/audit                 remotesys  -      -
```

Por último, el administrador monta el sistema de archivos /audit en /var/audit.

```
# mount remotesys:/audit /var/audit
# ls /var/audit
blinken  noddy
```

## ▼ Cómo configurar el alias de correo electrónico `audit_warn`

La secuencia de comandos `audit_warn` genera un correo electrónico para un alias de correo electrónico denominado `audit_warn`. Para enviar este correo electrónico a una dirección de correo electrónico válida, puede seguir una de las opciones que se describen en el [Paso 2](#):

### 1 Asuma el rol de administrador principal o conviértase en superusuario.

El rol de administrador principal incluye el perfil de administrador principal. Para crear el rol y asignarlo a un usuario, consulte el [Capítulo 2, “Trabajo con Solaris Management Console \(tareas\)”](#) de *Guía de administración del sistema: administración básica*.

### 2 Configure el alias de correo electrónico `audit_warn`.

Elija una de las siguientes opciones:

- **OPCIÓN 1** – Reemplace el alias de correo electrónico `audit_warn` con otra cuenta de correo electrónico en la secuencia de comandos `audit_warn`.

Cambie el alias de correo electrónico en la siguiente línea de la secuencia de comandos:

```
ADDRESS=audit_warn           # standard alias for audit alerts
```

- **OPCIÓN 2** – Redirija el correo electrónico `audit_warn` a otra cuenta de correo.

En este caso, debe agregar el alias de correo electrónico `audit_warn` al archivo de alias adecuado. Puede agregar el alias al archivo local `/etc/mail/aliases` o a la base de datos `mail_aliases` en el nombre de espacio. La nueva entrada es similar a la siguiente si la cuenta de correo `root` se ha agregado como miembro del alias de correo electrónico `audit_warn`:

```
audit_warn: root
```

## ▼ Cómo configurar la política de auditoría

La política de auditoría determina las características de los registros de auditoría para el host local. Cuando se habilita la auditoría, el contenido del archivo `/etc/security/audit_startup` determina la política de auditoría.

Puede inspeccionar y cambiar las opciones de la política de auditoría actual con el comando `auditconfig`. También puede modificar las opciones de política del comando `auditconfig` en la secuencia de comandos `audit_startup` para hacer permanentes los cambios de política de auditoría.

**1 Asuma un rol que incluya el perfil de control de auditoría o conviértase en superusuario.**

Para crear un rol que incluya el perfil de control de auditoría y para asignar el rol a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

**2 Revise la política de auditoría.**

Antes de que se habilite la auditoría, el contenido del archivo `audit_startup` determina la política de auditoría:

```
#!/bin/sh
...
/usr/bin/echo "Starting BSM services."
/usr/sbin/auditconfig -setpolicy +cnt      Counts rather than drops records
/usr/sbin/auditconfig -conf               Configures event-class mappings
/usr/sbin/auditconfig -aconf              Configures nonattributable events
```

**3 Vea las opciones de política disponibles.**

```
$ auditconfig -lspolicy
```

---

**Nota** – Las opciones de política `perzone` y `ahlt` solamente se pueden configurar en la zona global.

---

**4 Habilite o deshabilite las opciones de política de auditoría seleccionadas.**

```
# auditconfig -setpolicy prefixpolicy
prefix      Un valor + de prefijo habilita la opción de política. Un valor - de prefijo deshabilita la opción de política.
```

```
política    Selecciona la política que se habilitará o deshabilitará.
```

La política está vigente hasta el siguiente inicio o hasta que la política sea modificada por el comando `auditconfig -setpolicy`.

Para obtener una descripción de cada opción de política, consulte [“Determinación de política de auditoría” en la página 605](#).

**Ejemplo 30–16 Configuración de las opciones de política de auditoría `cnt` y `ahlt`**

En este ejemplo, la política `cnt` está deshabilitada y la política `ahlt` está habilitada. Con estos valores, el uso del sistema se detiene cuando las particiones de auditoría están llenas y se

produce un evento asíncrono. Cuando se produce un evento síncrono, se bloquea el proceso que creó el thread. Estos valores son adecuados cuando la seguridad es más importante que la disponibilidad.

Las siguientes entradas `audit_startup` deshabilitan la opción de política `cnt` y habilitan la opción de política `ahlt` en los inicios:

```
# cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy -cnt
/usr/sbin/auditconfig -setpolicy +ahlt
```

### Ejemplo 30-17 Configuración de la política de auditoría `seq` temporalmente

En este ejemplo, el daemon `audited` se está ejecutando y la política de auditoría `ahlt` se ha definido. La política de auditoría `seq` se agrega a la política actual. La política `seq` agrega un token sequence a todos los registros de auditoría. Esto es útil para depurar el servicio de auditoría cuando los registros de auditoría están dañados o cuando los registros se descartan.

El prefijo `+` agrega la opción `seq` a la política de auditoría, en lugar de reemplazar la política de auditoría actual con `seq`. El comando `auditconfig` hace que la política esté vigente hasta la próxima invocación del comando, o hasta el próximo inicio.

```
$ auditconfig -setpolicy +seq
$ auditconfig -getpolicy
audit policies = ahalt,seq
```

### Ejemplo 30-18 Configuración de la política de auditoría `perzone`

En este ejemplo, la política de auditoría `perzone` se configura en la secuencia de comandos `audit_startup` en la zona global. Cuando se inicia una zona, la zona no global recopila los registros de auditoría según los valores de configuración de auditoría en su zona.

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +perzone
/usr/sbin/auditconfig -setpolicy +cnt
```

**Ejemplo 30–19** Cambio de política de auditoría

En este ejemplo, el daemon de auditoría se está ejecutando y la política de auditoría se ha definido. El comando `auditconfig` cambia las políticas `ahlt` y `cnt` para la duración de la sesión. Con estos valores, los registros de auditoría se descartan, pero se cuentan cuando el sistema de archivos de auditoría está lleno. Para ver las restricciones sobre la configuración de la política `ahlt`, consulte [Paso 3](#).

```
$ auditconfig -setpolicy +cnt
$ auditconfig -setpolicy -ahlt
$ auditconfig -getpolicy
audit policies = cnt,seq
```

Cuando los cambios son ubicados en el archivo `audit_startup`, las políticas quedan vigentes permanentemente:

```
$ cat /etc/security/audit_startup
#!/bin/sh
/usr/bin/echo "Starting BSM services."
/usr/sbin/deallocate -Is
/usr/sbin/auditconfig -conf
/usr/sbin/auditconfig -aconf
/usr/sbin/auditconfig -setpolicy +cnt
```

La opción `-ahlt` no tiene que especificarse en este archivo, ya que la opción de política `ahlt` está deshabilitada de manera predeterminada. Este valor es adecuado cuando la disponibilidad es más importante que la seguridad que proporcionan los registros de auditoría.

## ▼ Cómo habilitar el servicio de auditoría

Este procedimiento habilita el servicio de auditoría para todas las zonas. Para iniciar el daemon de auditoría en una zona no global, consulte [Ejemplo 30–20](#).

Cuando la auditoría está configurada de manera segura, el sistema está en modo de usuario único hasta que se habilite la auditoría. También puede habilitar la auditoría en modo multiusuario.

### Antes de empezar

Debe realizar este procedimiento como superusuario después de completar las siguientes tareas:

- Planificación – “Planificación de auditoría de Oracle Solaris (mapa de tareas)” [en la página 599](#)
- Personalización de archivos de auditoría – “Configuración de archivos de auditoría (mapa de tareas)” [en la página 614](#)
- Configuración de particiones de auditoría – “Cómo crear particiones para los archivos de auditoría” [en la página 625](#)



- Configuración de mensajes de advertencia de auditoría – “[Cómo configurar el alias de correo electrónico audit\\_warn](#)” en la página 629
- Configuración de política de auditoría – “[Cómo configurar la política de auditoría](#)” en la página 629

---

**Nota** – La conversión del nombre de host debe funcionar correctamente para que la auditoría funcione. La base de datos hosts en los servicios de nombres debe estar configurada correctamente y debe estar funcionando.

Para obtener información sobre la base de datos de hosts, consulte las páginas del comando `man nsswitch.conf(4)` y `netconfig(4)`. Para obtener información adicional, consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* o la *System Administration Guide: Naming and Directory Services (NIS+)*.

---

## 1 Ejecute la secuencia de comandos que habilita el servicio de auditoría.

Vaya al directorio `/etc/security` y ejecute allí la secuencia de comandos `bsmconv`.

```
# cd /etc/security
# ./bsmconv
This script is used to enable the Basic Security Module (BSM).
Shall we continue with the conversion now? [y/n] y
bsmconv: INFO: checking startup file.
bsmconv: INFO: turning on audit module.
bsmconv: INFO: initializing device allocation.
```

```
The Basic Security Module is ready.
If there were any errors, please fix them now.
Configure BSM by editing files located in /etc/security.
Reboot this system now to come up with BSM enabled.
```

Para ver los efectos de la secuencia de comandos, consulte la página del comando `man bsmconv(1M)`.

## 2 Reinicie el sistema.

```
# reboot
```

El archivo de inicio `/etc/security/audit_startup` hace que el daemon `auditd` se ejecute automáticamente cuando el sistema inicia el modo multiusuario.

Otro efecto de la secuencia de comandos es que activa la asignación de dispositivos. Para configurar la asignación de dispositivos, consulte “[Gestión de asignación de dispositivos \(mapa de tareas\)](#)” en la página 85.

## Ejemplo 30–20 Habilitación de la auditoría en una zona no global

En el siguiente ejemplo, el administrador de la zona global activó la política `perzone` después de que la auditoría se activó en la zona global y después de que la zona no global se inició. El

administrador de zona de la zona no global configura los archivos de auditoría de la zona y, a continuación, inicia el daemon de auditoría en la zona.

```
zone1# svcadm enable svc:/system/auditd
```

## ▼ Cómo deshabilitar el servicio de auditoría

Si el servicio de auditoría ya no es necesario en algún momento, este procedimiento devuelve el sistema al estado anterior a la habilitación de la auditoría. Si las zonas no globales se auditan, su servicio de auditoría también se deshabilita.



**Precaución** – Este comando también deshabilita la asignación de dispositivos. No ejecute este comando si desea poder asignar dispositivos. Para deshabilitar la auditoría y retener la asignación de dispositivos, consulte el [Ejemplo 30–21](#).

### 1 Conviértase en superusuario y configure el sistema en modo de usuario único.

```
% su
Password:      <Type root password>
# init S
```

Para obtener más información, consulte la página del comando `man init(1M)`.

### 2 Ejecute la secuencia de comandos para deshabilitar la auditoría.

Cambie al directorio `/etc/security` y ejecute la secuencia de comandos `bsmunconv`.

```
# cd /etc/security
# ./bsmunconv
```

Otro efecto de la secuencia de comandos es que deshabilita la asignación de dispositivos.

Para obtener información sobre todo el efecto de la secuencia de comandos `bsmunconv`, consulte la página del comando `man bsmunconv(1M)`.

### 3 Coloque el sistema en modo multiusuario.

```
# init 6
```

## Ejemplo 30–21 Deshabilitación de la auditoría y conservación de la asignación de dispositivos

En este ejemplo, el servicio de auditoría deja de recopilar registros, pero la asignación de dispositivos continúa funcionando. Se eliminan todos los valores de las entradas `flags`, `naflags` y `plugin` en el archivo `audit_control`, al igual que todas las entradas de usuarios en el archivo `audit_user`.

```
## audit_control file
flags:
```

```
naflags:
```

```
## audit_user file
```

El daemon `auditd` se ejecuta, pero no se conservan registros de auditoría.

### Ejemplo 30–22 Deshabilitación de la auditoría por zona

En este ejemplo, el servicio de auditoría deja de funcionar en `zone1`, donde el servicio de auditoría está deshabilitado. La asignación de dispositivos continúa funcionando. Cuando este comando se ejecuta en la zona global, y la política de auditoría `per zone` no está definida, la auditoría se deshabilita para todas las zonas, no sólo para la zona global.

```
zone1 # audit -t
```

## ▼ Cómo actualizar el servicio de auditoría

Este procedimiento reinicia el daemon `auditd` cuando realiza cambios para auditar archivos de configuración de auditoría después de ejecutar el daemon.

### 1 Asuma un rol que incluya el perfil de derechos de control de auditoría o conviértase en superusuario.

Para crear un rol que incluya el perfil de derechos de control de auditoría y para asignar el rol a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Elija el comando adecuado.

- Si modifica la línea `naflags` en el archivo `audit_control`, cambie la máscara del núcleo para eventos no atribuibles.

```
$ /usr/sbin/auditconfig -aconf
```

También puede reiniciar.

- Si modifica otras líneas en el archivo `audit_control`, vuelva a leer el archivo `audit_control`.

El daemon de auditoría almacena información del archivo `audit_control` internamente. Para utilizar la información nueva, reinicie el sistema o indique al daemon de auditoría que lea el archivo modificado.

```
$ /usr/sbin/audit -s
```

---

**Nota** – Los registros de auditoría se generan sobre la base de la máscara de preselección de auditoría asociada con cada proceso. La ejecución del comando `audit -s no` cambia las máscaras en procesos existentes. Para cambiar la máscara de preselección de un proceso existente, debe reiniciar el proceso. También puede reiniciar.

---

El comando `audit -s` hace que el daemon de auditoría vuelva a leer el directorio y los valores `minfree` del archivo `audit_control`. El comando cambia la generación de la máscara de preselección para los procesos reproducidos por inicios de sesión posteriores.

- **Si modifica el archivo `audit_event` o el archivo `audit_class` mientras se ejecuta el daemon de auditoría, actualice el servicio de auditoría.**

Lea las asignaciones de evento-clase modificadas en el sistema y asegúrese de que cada usuario que utiliza el equipo esté correctamente auditado.

```
$ auditconfig -conf
$ auditconfig -setumask auid classes
```

*auid*      Es el ID de usuario.

*clases*    Son las clases de auditoría preseleccionadas.

Por ejemplo, consulte [“Cómo modificar una máscara de preselección de usuario” en la página 659](#).

- **Para cambiar la política de auditoría de un sistema en ejecución, consulte el [Ejemplo 30–17](#).**

### Ejemplo 30–23 Reinicio del daemon de auditoría

En este ejemplo, el sistema se configura en modo de usuario único y luego se configura en modo de usuario múltiple. Cuando el sistema se lleva a modo multiusuario, los archivos de configuración de auditoría modificados se leen en el sistema.

```
# init 5
# init 6
```

## Configuración del servicio de auditoría en las zonas (tareas)

El servicio de auditoría audita a todo el sistema, incluidos los eventos de auditoría en las zonas. Un sistema que tenga zonas no globales instaladas puede auditar todas las zonas de forma idéntica o puede controlar la auditoría por zona. Para acceder a información básica, consulte [“Auditoría en un sistema con zonas de Oracle Solaris” en la página 596](#). Para planificar, consulte [“Cómo planificar auditoría en zonas” en la página 600](#).

## ▼ Cómo configurar todas las zonas de forma idéntica para la auditoría

Este procedimiento habilita las auditorías de cada zona de forma idéntica. Este método requiere la menor carga del equipo y los mejores recursos administrativos.

### 1 Configure la zona global para la auditoría.

- a. Complete las tareas en [“Configuración de archivos de auditoría \(mapa de tareas\)” en la página 614.](#)
- b. Complete las tareas en [“Configuración y habilitación del servicio de auditoría \(mapa de tareas\)” en la página 624,](#) con las siguientes excepciones.

- No habilite la política de auditoría per zone.
- No habilite el servicio de auditoría. Debe habilitar el servicio de auditoría después de haber configurado las zonas no globales para la auditoría.

### 2 Copie los archivos de configuración de auditoría desde la zona global para cada zona no global.

Copie cualquiera de los siguientes archivos que haya editado: `audit_class`, `audit_control`, `audit_event`, `audit_user`. No copie los archivos `audit_startup` o `audit_warn`. No tiene que copiar los archivos que no haya editado.

Dispone de dos opciones. Como superusuario, puede copiar los archivos o bien montar los archivos en bucle de retorno. La zona no global debe estar en ejecución.

#### ▪ Copie los archivos.

- a. Desde la zona global, muestre el directorio `/etc/security` en la zona no global.

```
# ls /zone/zonename/etc/security/
```

- b. Copie los archivos de configuración de auditoría al directorio `/etc/security` de la zona.

```
# cp /etc/security/audit-file /zone/zonename/etc/security/audit-file
```

Más adelante, si modifica un archivo de configuración de auditoría en la zona global, debe volver a copiar el archivo en las zonas no globales.

#### ▪ Monte en bucle de retorno los archivos de configuración.

- a. Desde la zona global, detenga la zona no global.

```
# zoneadm -z non-global-zone halt
```

- b. Cree un montaje en bucle de retorno de sólo lectura para cada archivo de configuración de auditoría que haya modificado en la zona global.**

```
# zonecfg -z non-global-zone
add fs
  set special=/etc/security/audit-file
  set dir=/etc/security/audit-file
  set type=lofs
  add options [ro,nodevices,noexec,nosuid]
end
exit
```

- c. Para que los cambios entren en vigencia, inicie la zona no global.**

```
# zoneadm -z non-global-zone boot
```

También puede reiniciar el sistema.

Más adelante, si modifica un archivo de configuración de auditoría en la zona global, debe reiniciar el sistema para actualizar los archivos montados en bucle de retorno en las zonas no globales.

### **Ejemplo 30–24** Archivos de configuración de auditoría de montaje en bucle de retorno

En este ejemplo, el administrador del sistema ha modificado los archivos `audit_class`, `audit_event`, `audit_control`, `audit_user`, `audit_startup` y `audit_warn`.

Los archivos `audit_startup` y `audit_warn` solamente se leen en la zona global, por lo que no deben estar montados en bucle de retorno en las zonas no globales.

En este sistema, `machine1`, el administrador ha creado dos zonas no globales, `machine1-webserver` y `machine1-appserver`. El administrador ha terminado de personalizar los archivos de configuración de auditoría. Si el administrador más tarde modifica los archivos, el sistema se reiniciará para que los cambios entren en vigencia.

```
# zoneadm -z machine1-webserver halt
# zoneadm -z machine1-appserver halt
# zonecfg -z machine1-webserver
add fs
  set special=/etc/security/audit_class
  set dir=/etc/security/audit_class
  set type=lofs
  add options [ro,nodevices,noexec,nosuid]
end
add fs
  set special=/etc/security/audit_event
  set dir=/etc/security/audit_event
  set type=lofs
  add options [ro,nodevices,noexec,nosuid]
end
add fs
  set special=/etc/security/audit_control
  set dir=/etc/security/audit_control
```

```

        set type=lofs
        add options [ro,nodevices,nosetuid]
    end
add fs
    set special=/etc/security/audit_user
    set dir=/etc/security/audit_user
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
exit
# zonecfg -z machine1-appserver
add fs
    set special=/etc/security/audit_class
    set dir=/etc/security/audit_class
    set type=lofs
    add options [ro,nodevices,nosetuid]
    end
...
exit

```

Cuando se reinician las zonas, los archivos de configuración de auditoría son de sólo lectura en las zonas.

## ▼ Cómo configurar la auditoría por zona

Este procedimiento permite que distintos administradores de zonas controlen el servicio de auditoría en sus zonas. Para obtener una lista completa de las opciones de política, consulte la página del comando `man auditconfig(1M)`.

- 1 En la zona global, configure la auditoría, pero no habilite el servicio de auditoría.
  - a. Complete las tareas en “[Configuración de archivos de auditoría \(mapa de tareas\)](#)” en la [página 614](#).
  - b. Complete las tareas en “[Configuración y habilitación del servicio de auditoría \(mapa de tareas\)](#)” en la [página 624](#) con las siguientes excepciones.
    - Agregue la política de auditoría `perzone`. Si desea ver un ejemplo, consulte el [Ejemplo 30–18](#).
    - No habilite el servicio de auditoría. Debe habilitar el servicio de auditoría después de haber configurado las zonas no globales para la auditoría.
- 2 En cada zona no global, configure los archivos de auditoría.

---

**Nota** – Si tiene planificado deshabilitar la auditoría en la zona no global, puede omitir este paso. Para deshabilitar la auditoría, consulte el [Ejemplo 30–25](#).

---

- a. **Complete las tareas en “Configuración de archivos de auditoría (mapa de tareas)” en la página 614.**
  - b. **Siga los procedimientos que se describen en “Configuración y habilitación del servicio de auditoría (mapa de tareas)” en la página 624.**
  - c. **No configure los valores de auditoría en todo el sistema.**  
Específicamente, no agregue la política perzone o ahl\_t al archivo audit\_startup de la zona no global. Y no ejecute el comando bsmconv desde la zona no global.
  - d. **Habilite la auditoría en su zona.**  
Cuando la zona global reinicia después de configurar la auditoría, la auditoría se habilita de forma automática en la zona.  
  
Si el administrador de la zona global activa la política de auditoría perzone después de iniciar el sistema, los administradores de zonas individuales deben habilitar la auditoría. Para obtener detalles, consulte el [Ejemplo 30–20](#).
- 3 En la zona global, habilite el servicio de auditoría.**  
Para conocer el procedimiento, consulte “[Cómo habilitar el servicio de auditoría](#)” en la [página 632](#).

**Ejemplo 30–25    Deshabilitación de la auditoría en una zona no global**

Este ejemplo funciona si la zona global tiene definida la política de auditoría perzone. El administrador de zona de zona noaudit deshabilita la auditoría para dicha zona. Como el administrador tenía previsto deshabilitar la auditoría, no editó los archivos de configuración de auditoría.

```
noauditzone # svcadm disable svc:/system/auditd
```

# Gestión de registros de auditoría (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para seleccionar, analizar y gestionar los registros de auditoría.

Tarea	Descripción	Para obtener instrucciones
Mostrar los formatos de los registros de auditoría	Muestra el tipo de información que se recopila para un evento de auditoría y el orden en que se presenta la información.	<a href="#">“Cómo visualizar formatos de registros de auditoría” en la página 641</a>



Tarea	Descripción	Para obtener instrucciones
Fusionar registros de auditoría	Combina los archivos de auditoría de varios equipos en una pista de auditoría.	<a href="#">“Cómo fusionar archivos de auditoría de la pista de auditoría” en la página 643</a>
Seleccionar los registros para examinar	Selecciona eventos determinados de estudio.	<a href="#">“Cómo seleccionar eventos de auditoría de la pista de auditoría” en la página 645</a>
Mostrar registros de auditoría	Habilita la visualización de registros de auditoría binarios.	<a href="#">“Cómo visualizar el contenido de los archivos de auditoría binarios” en la página 647</a>
Depurar archivos de auditoría denominados incorrectamente	Proporciona una indicación de hora final para auditar archivos de auditoría que quedaron abiertos inadvertidamente en el servicio de auditoría.	<a href="#">“Cómo depurar un archivo de auditoría not_terminated” en la página 649</a>
Evitar el desbordamiento de la pista de auditoría	Impide que los sistemas de archivos de auditoría se llenen.	<a href="#">“Cómo evitar el desbordamiento de la pista de auditoría” en la página 650</a>

## Gestión de registros de auditoría

Mediante la gestión de la pista de auditoría, puede supervisar las acciones de usuarios de la red. La auditoría puede generar grandes cantidades de datos. Las siguientes tareas muestran cómo trabajar con todos estos datos.

### ▼ Cómo visualizar formatos de registros de auditoría

Para escribir secuencias de comandos que puedan encontrar los datos de auditoría que desea, necesita saber el orden de los tokens en un evento de auditoría. El comando `bsmrecord` muestra el número de evento de auditoría, la clase de auditoría, la máscara de selección y el formato de registro de un evento de auditoría.

- **Coloque el formato de todos los registros de eventos de auditoría en un archivo HTML.**

La opción `-a` muestra una lista de todos los formatos de registros de eventos de auditoría. La opción `-h` coloca la lista en formato HTML, que puede visualizarse en un explorador.

```
% bsmrecord -a -h > audit.events.html
```

Cuando visualice el archivo `*html` en un explorador, use la herramienta de búsqueda del explorador para encontrar registros específicos.

Para obtener más información, consulte la página del comando `man bsmrecord(1M)`.

**Ejemplo 30–26** Visualización de los formatos de registros de auditoría de un programa

En este ejemplo, se muestra el formato de todos los registros de auditoría que se generan mediante el programa login. Los programas de inicio de sesión incluyen rlogin, telnet, newgrp, el inicio de sesión de rol en Solaris Management Console y Oracle Solaris Secure Shell.

```
% bsmrecord -p login
login: logout
  program      various          See login(1)
  event ID     6153             AUE_logout
...

newgrp
  program      newgrp           See newgrp login
  event ID     6212             AUE_newgrp_login
...

rlogin
  program      /usr/sbin/login   See login(1) - rlogin
  event ID     6155             AUE_rlogin
...

SMC: role login
  program      SMC server       See role login
  event ID     6173             AUE_role_login
...

/usr/lib/ssh/sshd
  program      /usr/lib/ssh/sshd See login - ssh
  event ID     6172             AUE_ssh
...

telnet login
  program      /usr/sbin/login   See login(1) - telnet
  event ID     6154             AUE_telnet
...
```

**Ejemplo 30–27** Visualización de formatos de registros de auditoría de una clase de auditoría

En este ejemplo, se muestra el formato de todos los registros de auditoría en la clase fd.

```
% bsmrecord -c fd

rmdir
  system call  rmdir            See rmdir(2)
  event ID     48               AUE_RMDIR
  class       fd                (0x00000020)
    header
    path
    [attribute]
    subject
    [use_of_privilege]
    return

unlink
```

```

system call unlink          See unlink(2)
event ID      6            AUE_UNLINK
...

unlinkat
system call unlinkat        See openat(2)
event ID      286          AUE_UNLINKAT
...
```

## ▼ Cómo fusionar archivos de auditoría de la pista de auditoría

Al fusionar todos los archivos de auditoría en todos los directorios de auditoría, puede analizar los contenidos de toda la pista de auditoría. El comando `auditreduce` fusiona todos los registros de los archivos de entrada en un solo archivo de salida. Entonces, los archivos de entrada se pueden suprimir. Cuando el archivo de salida está ubicado en un directorio denominado `/etc/security/audit/nombre_servidor/files`, el comando `auditreduce` puede encontrar el archivo de salida sin especificar la ruta completa.

---

**Nota** – Este procedimiento se aplica únicamente a los registros binarios de auditoría.

---

### 1 Asuma un rol que incluya el perfil de revisión de auditoría o conviértase en superusuario.

El rol de administrador del sistema incluye el perfil de revisión de auditoría. También puede crear un rol distinto que incluya el perfil de revisión de auditoría. Para crear un rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” en la [página 204](#).

### 2 Cree un directorio para almacenar los archivos de auditoría fusionados.

```
# mkdir audit-trail-directory
```

### 3 Limite el acceso al directorio.

```
# chmod 700 audit-trail-directory
# ls -la audit-trail-directory
drwx----- 3 root  sys      512 May 12 11:47 .
drwxr-xr-x  4 root  sys     1024 May 12 12:47 ..
```

### 4 Fusione los registros de auditoría en la pista de auditoría.

Cambie los directorios al `directorio_pista_auditoría` y fusione los registros de auditoría en un archivo con un sufijo con nombre. Todos los directorios que se muestran en las líneas `dir` del archivo `audit_control` en el sistema local están fusionados.

```
# cd audit-trail-directory
# auditreduce -Uppercase-option -O suffix
```

Las opciones en mayúscula del comando `auditreduce` manipulan los archivos en la pista de auditoría. Las opciones en mayúscula incluyen las siguientes:

-A      Selecciona todos los archivos en la pista de auditoría.

- C Selecciona únicamente archivos completos. Esta opción ignora los archivos con el sufijo `not_terminated`.
- M Selecciona los archivos con un sufijo determinado. El sufijo puede ser un nombre de equipo o puede ser un sufijo que haya especificado para un archivo de resumen.
- O Crea un archivo de auditoría con indicadores de hora de 14 caracteres para la hora de inicio y la hora de finalización, con el sufijo *sufijo* en el directorio actual.

### Ejemplo 30–28 Copia de archivos de auditoría a un archivo de resumen

En el siguiente ejemplo, el rol de administrador del sistema, `sysadmin`, copia todos los archivos de la pista de auditoría en un archivo fusionado.

```
$ whoami
sysadmin
$ mkdir /var/audit/audit_summary.dir
$ chmod 700 /var/audit/audit_summary.dir
$ cd /var/audit/audit_summary.dir
$ auditreduce -A -O All
$ ls *All
20100827183214.20100827215318.All
```

En el siguiente ejemplo, únicamente se copian archivos completos de la pista de auditoría a un archivo fusionado.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O Complete
$ ls *Complete
20100827183214.20100827214217.Complete
```

En el siguiente ejemplo, únicamente se copian archivos completos del equipo `example1` a un archivo fusionado.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -M example1 -O example1summ
$ ls *summ
20100827183214.20100827214217.example1summ
```

### Ejemplo 30–29 Cómo mover archivos de auditoría a un archivo de resumen

La opción `-D` del comando `auditreduce` elimina un archivo de auditoría cuando lo copia en otra ubicación. En el siguiente ejemplo, los archivos de auditoría completos de un sistema se copian en el directorio de resumen para examinarlos posteriormente.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -C -O daily_example1 -D example1
$ ls *example1
20100827183214.20100827214217.daily_example1
```

Los archivos de auditoría del sistema `example1` que se introdujeron en el archivo `*daily_example1` se eliminan cuando este comando se completa correctamente.

## ▼ Cómo seleccionar eventos de auditoría de la pista de auditoría

Puede filtrar registros de auditoría para examinarlos. Para obtener una lista completa de las opciones de filtrado, consulte la página del comando `man auditreduce(1M)`.

### 1 Asuma un rol que incluya el perfil de revisión de auditoría o conviértase en superusuario.

El rol de administrador del sistema incluye el perfil de revisión de auditoría. También puede crear un rol distinto que incluya el perfil de revisión de auditoría. Para crear un rol y asignarlo a un usuario, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” en la [página 204](#).

### 2 Seleccione los tipos de registros que desee de la pista de auditoría o de un archivo de auditoría especificado.

`auditreduce -lowercase-option argument [optional-file]`

<i>argumento</i>	Argumento específico que requiere una opción en minúscula. Por ejemplo, la opción <code>-c</code> requiere un <i>argumento</i> de una clase de auditoría, como <code>ua</code> .
<code>-d</code>	Selecciona todos los eventos en una fecha determinada. El formato de fecha de <i>argumento</i> es <code>aaammdd</code> . Otras opciones de fecha, <code>-b</code> y <code>-a</code> , seleccionan los eventos antes y después de una fecha determinada.
<code>-u</code>	Selecciona todos los eventos atribuibles a un usuario determinado. El <i>argumento</i> es un nombre de usuario. Otra opción de usuario, <code>-e</code> , selecciona todos los eventos atribuibles a un ID de usuario vigente.
<code>-c</code>	Selecciona todos los eventos de una clase de auditoría preseleccionada. El <i>argumento</i> es un nombre de clase de auditoría.
<code>-m</code>	Selecciona todas las instancias de un evento de auditoría determinado. El <i>argumento</i> es un evento de auditoría.
<i>archivo_opcional</i>	Es el nombre de un archivo de auditoría.

## Ejemplo 30–30 Combinación y reducción de archivos de auditoría

El comando `auditreduce` puede eliminar los registros menos interesantes a medida que combina los archivos de entrada. Por ejemplo, puede utilizar el comando `auditreduce` para

retener únicamente los registros de inicio y cierre de sesión en los archivos de auditoría de más de un mes. Si necesita recuperar la pista de auditoría completa, puede recuperar la pista del medio de copia de seguridad.

```
# cd /var/audit/audit_summary.dir
# auditreduce -O lo.summary -b 20100827 -c lo; compress *lo.summary
```

### **Ejemplo 30–31** Copia de registros de auditoría na en un archivo de resumen

En este ejemplo, se recopilan en un solo archivo todos los registros de eventos de auditoría no atribuibles en la pista de auditoría.

```
$ whoami
sysadmin
$ cd /var/audit/audit_summary.dir
$ auditreduce -c na -O nasumm
$ ls *nasumm
20100827183214.20100827215318.nasumm
```

El archivo de auditoría fusionado nasumm tiene un indicador de hora con la fecha de inicio y de finalización de los registros na.

### **Ejemplo 30–32** Búsqueda de eventos de auditoría en un archivo de auditoría especificado

Puede seleccionar manualmente archivos de auditoría para buscar únicamente el conjunto de los archivos denominado. Por ejemplo, puede seguir procesando el archivo \*nasumm en el ejemplo anterior para buscar eventos de inicio de sistema. Para ello, tendría que especificar el nombre de archivo como argumento final en el comando `audit reduce`.

```
$ auditreduce -m 113 -O systemboot 20100827183214.20100827215318.nasumm
20100827183214.20100827183214.systemboot
```

El archivo 20100827183214.20100827183214.systemboot contiene únicamente eventos de auditoría de inicio de sistema.

### **Ejemplo 30–33** Copia de los registros de auditoría de un usuario en un archivo de resumen

En este ejemplo, se fusionan los registros en la pista de auditoría que contienen el nombre de un usuario determinado. La opción `-e` busca el usuario vigente. La opción `-u` busca el usuario de auditoría.

```
$ cd /var/audit/audit_summary.dir
$ auditreduce -e tamiko -O tamiko
```

Puede buscar eventos específicos en este archivo. En el siguiente ejemplo, se verifica la hora en que el usuario inició y cerró sesión el 7 de septiembre de 2010, hora local. Sólo se verifican los archivos con el nombre del usuario como sufijo de archivo. La abreviatura de la fecha es *aaaammdd*.

```
# auditreduce -M tamiko -O tamikolo -d 20100907 -u tamiko -c lo
```

### Ejemplo 30-34 Copia de registros seleccionados en un archivo único

En este ejemplo, se seleccionan de la pista de auditoría los mensajes de inicio y cierre de sesión de un día determinado. Los mensajes se fusionan en un archivo de destino. El archivo de destino se escribe en un directorio distinto que el directorio root de auditoría normal.

```
# auditreduce -c lo -d 20100827 -O /var/audit/audit_summary.dir/logins
# ls /var/audit/audit_summary.dir/*logins
/var/audit/audit_summary.dir/20100827183936.20100827232326.logins
```

## ▼ Cómo visualizar el contenido de los archivos de auditoría binarios

El comando `praudit` lo habilita a ver los contenidos de los archivos de auditoría binarios. Puede redireccionar la salida del comando `auditreduce` o puede leer un archivo de auditoría determinado. La opción `-x` es útil para el procesamiento posterior.

### 1 Asuma un rol que incluya el perfil de revisión de auditoría o conviértase en superusuario.

El rol de administrador del sistema incluye el perfil de revisión de auditoría. También puede crear un rol distinto que incluya el perfil de revisión de auditoría. Para crear un rol y asignarlo a un usuario, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

### 2 Utilice uno de los siguientes comandos `praudit` para producir la mejor salida según su propósito.

Los siguientes ejemplos muestran la salida de `praudit` para el mismo evento de auditoría. Las políticas de auditoría se configuraron para incluir los tokens `sequence` y `trailer`.

- El comando `praudit -s` muestra los registros de auditoría en formato corto, un token por línea. Utilice la opción `-l` para colocar cada registro en una línea.

```
$ auditreduce -c lo | praudit -s
header,101,2,AUE_rlogin,,example1,2010-10-13 11:23:31.050 -07:00
subject,jdoe,jdoe,staff,jdoe,staff,749,749,195 1234 server1
text,successful login
return,success,0
sequence,1298
```

- El comando `praudit -r` muestra los registros de auditoría en su formato básico, un token por línea. Utilice la opción `-l` para colocar cada registro en una línea.

```
$ auditreduce -c lo | praudit -r
21,101,2,6155,0x0000,192.168.60.83,1062021202,64408258
36,2026700,2026700,10,2026700,10,749,749,195 1234 192.168.60.17
40,successful login
39,0,0
47,1298
```

- El comando `praudit -x` muestra los registros de auditoría en formato XML, un token por línea. Utilice la opción `-l` para colocar la salida XML para un registro en una línea.

```
$ auditreduce -c lo | praudit -x
<record version="2" event="login - rlogin" host="example1"
time="Wed Aug 27 14:53:22 PDT 2010" msec="64">
<subject audit-uid="jdoe" uid="jdoe" gid="staff" ruid="jdoe"
rgid="staff" pid="749" sid="749" tid="195 1234 server1"/>
<text>successful login</text>
<return errval="success" retval="0"/>
<sequence seq-num="1298"/>

</record>
```

### Ejemplo 30-35 Impresión de toda la pista de auditoría

Con un conducto al comando `lp`, la salida de toda la pista de auditoría pasa a la impresora. La impresora debe tener acceso limitado.

```
# auditreduce | praudit | lp -d example.protected.printer
```

### Ejemplo 30-36 Visualización de un archivo de auditoría específico

En este ejemplo, se examina un inicio de sesión resumido en la ventana de terminal.

```
# cd /var/audit/audit_summary.dir/logins
# praudit 20100827183936.20100827232326.logins | more
```

### Ejemplo 30-37 Cómo poner los registros de auditoría en formato XML

En este ejemplo, los registros de auditoría se convierten en formato XML.

```
# praudit -x 20100827183214.20100827215318.logins > 20100827.logins.xml
```

El archivo `*xml` se puede visualizar en un explorador. El contenido del archivo sólo puede ser operado por una secuencia de comandos para extraer la información relevante.

### Errores más frecuentes

Un mensaje similar al siguiente indica que no tiene privilegios suficientes para usar el comando `praudit`:



praudit: Can't assign 20090408164827.20090408171614.example1 to stdin.

## ▼ Cómo depurar un archivo de auditoría `not_terminated`

Ocasionalmente, existe un daemon de auditoría mientras su archivo de auditoría está abierto. O bien, un servidor pasa a estar inaccesible y fuerza al equipo a que pase a un nuevo servidor. En esos casos, un archivo de auditoría permanece con la cadena `not_terminated` como indicación de hora final, aunque el archivo ya no se utilice para los registros de auditoría. Utilice el comando `auditreduce -O` para otorgar al archivo la indicación de hora correcta.

### 1 Enumere los archivos con la cadena `not_terminated` en el sistema de archivo de auditoría según el orden de creación.

```
# ls -Rlt audit-directory*/files/* | grep not_terminated
```

-R Muestra los archivos en los subdirectorios.

-t Muestra la lista de archivos desde el más reciente hasta el más antiguo.

-l Muestra los archivos en una columna.

### 2 Depure el archivo `not_terminated` anterior.

Especifique el nombre del archivo anterior en el comando `auditreduce -O`.

```
# auditreduce -O system-name old-not-terminated-file
```

### 3 Elimine el archivo `not_terminated` anterior.

```
# rm system-name old-not-terminated-file
```

## Ejemplo 30-38 Depuración de archivos de auditoría `not_terminated` cerrados

En el siguiente ejemplo, se encontraron archivos `not_terminated`, se renombraron, y se eliminaron los originales.

```
ls -Rlt */files/* | grep not_terminated
.../egret.1/20100908162220.not_terminated.egret
.../egret.1/20100827215359.not_terminated.egret
# cd */files/egret.1
# auditreduce -O egret 20100908162220.not_terminated.egret
# ls -lt
20100908162220.not_terminated.egret      Current audit file
20100827230920.20100830000909.egret     Input (old) audit file
20100827215359.not_terminated.egret
# rm 20100827215359.not_terminated.egret
# ls -lt
20100908162220.not_terminated.egret     Current audit file
```

20100827230920.20100830000909.egret      *Cleaned up audit file*

La indicación de hora de inicio en el nuevo archivo refleja la hora del primer evento de auditoría en el archivo `not_terminated`. La indicación de hora final refleja la hora del último evento de auditoría en el archivo.

## ▼ **Cómo evitar el desbordamiento de la pista de auditoría**

Si la política de seguridad requiere que todos los datos de auditoría se guarden, realice las siguientes acciones:

### **1 Configure un programa para archivar con regularidad los archivos de auditoría.**

Almacene los archivos de auditoría mediante una copia de los archivos en los medios sin conexión. También puede mover los archivos a un sistema de archivos de almacenamiento.

Si está recopilando registros de auditoría textual con la utilidad `syslog`, archive los registros textuales. Para más información, consulte la página del comando `man logadm(1M)`.

### **2 Establezca un programa para eliminar los archivos almacenados del sistema de archivos de auditoría.**

### **3 Guarde y almacene información auxiliar.**

Archive la información que sea necesaria para interpretar los registros de auditoría junto con la pista de auditoría.

### **4 Mantenga registros de qué archivos de auditoría se han archivado.**

### **5 Almacene los medios archivados adecuadamente.**

### **6 Reduzca el volumen de los datos de auditoría que almacene mediante la creación de archivos de resumen.**

Puede extraer archivos de resumen de la pista de auditoría mediante las opciones en el comando `auditreduce`. Los archivos de resumen contienen únicamente los registros en tipos especificados de eventos de auditoría. Para extraer archivos de resumen, consulte [Ejemplo 30–30](#) y [Ejemplo 30–34](#).

## Resolución de problemas de la auditoría de Oracle Solaris (tareas)

En esta sección se tratan distintos mensajes de error de auditoría de Oracle Solaris, las preferencias y la auditoría proporcionada por otras herramientas. Estos procedimientos pueden ayudarle a registrar los eventos de auditoría que necesita en el sitio.

## Resolución de problemas de la auditoría de Oracle Solaris (mapa de tareas)

El siguiente mapa de tareas hace referencia a los procedimientos para la resolución de problemas de la auditoría de Oracle Solaris.

Problema	Solución	Para obtener instrucciones
¿Por qué no se crean los archivos de auditoría cuando tengo configurada la auditoría?	Resuelva los problemas del daemon de auditoría y los archivos de configuración de auditoría.	<a href="#">“Cómo determinar que la auditoría de Oracle Solaris se está ejecutando” en la página 652</a>
¿Cómo puedo reducir la cantidad de información sobre auditoría que se está recopilando?	Audite sólo los eventos que desea auditar.	<a href="#">“Cómo reducir el volumen de los registros de auditoría que se producen” en la página 654</a>
¿Cómo puedo auditar todo lo que un usuario hace en el sistema?	Audite uno o más usuarios para cada comando.	<a href="#">“Cómo auditar todos los comandos por usuarios” en la página 656</a>
¿Cómo puedo cambiar los eventos de auditoría que se graban y hacer que el cambio afecte las sesiones existentes?	Actualice la máscara de preselección de un usuario.	<a href="#">“Cómo modificar una máscara de preselección de usuario” en la página 659</a>
¿Cómo puedo localizar modificaciones en archivos determinados?	Audite las modificaciones en los archivos y, luego, use el comando <code>audit reduce</code> para encontrar archivos determinados.	<a href="#">“Cómo buscar registros de auditoría de los cambios realizados en archivos específicos” en la página 658</a>
¿Cómo puedo reducir el tamaño de mis archivos de auditoría?	Limite el tamaño del archivo de auditoría binario.	<a href="#">“Cómo limitar el tamaño de los archivos de auditoría binarios” en la página 661</a>
¿Cómo puedo eliminar eventos de auditoría del archivo <code>audit_event</code> ?	Actualice el archivo <code>audit_event</code> .	<a href="#">“Cómo evitar la auditoría de determinados eventos” en la página 661</a>
¿Cómo puedo auditar todos los inicios de sesión a un sistema Oracle Solaris?	Audite los inicios de sesión de cualquier sistema.	<a href="#">“Cómo auditar inicios de sesión de otros OSes” en la página 662</a>

Problema	Solución	Para obtener instrucciones
¿Por qué no se mantienen los registros de auditoría de mis transferencias de FTP?	Utilice la herramienta de auditoría adecuada para las utilidades que generan sus propios registros.	<a href="#">“Cómo auditar transferencias de archivos FTP y SFTP” en la página 662</a>

## ▼ Cómo determinar que la auditoría de Oracle Solaris se está ejecutando

Si cree que la auditoría se ha activado, pero no hay registros de auditoría en el directorio principal de auditoría, intente lo siguiente.

**Antes de empezar** Que se ha configurado correctamente la base de datos hosts en su servicio de nombres y su funcionamiento. Para depurar los problemas del servicio de nombres, consulte lo siguiente:

- `nsswitch.conf(4)`
- *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*

### 1 Determine que la auditoría se esté ejecutando.

- Compruebe que el módulo de núcleo `c2audit` esté cargado.

```
# modinfo | grep c2audit
```

Si no se proporciona ninguna lista, significa que la auditoría no se está ejecutando. La siguiente lista indica que la auditoría se está ejecutando:

```
40 132ce90 14230 186 1 c2audit (C2 system call)
```

- Compruebe que se esté ejecutando el daemon de auditoría.

Compruebe el estado del servicio `auditd`. La siguiente lista indica que la auditoría no se está ejecutando:

```
# svcs -x auditd
svc:/system/auditd:default (Solaris audit daemon)
State: disabled since Fri Aug 14 19:02:35 2009
Reason: Disabled by an administrator.
See: http://sun.com/msg/SMF-8000-05
See: auditd(1M)
See: audit(1M)
Impact: This service is not running.
```

La siguiente lista indica que el servicio de auditoría se está ejecutando:

```
# svcs auditd
STATE          STIME    FMRI
online         10:10:10 svc:/system/auditd:default
```

■ **Compruebe la condición actual de la auditoría.**

La siguiente lista indica que la auditoría no se está ejecutando:

```
# auditconfig -getcond
auditconfig: auditon(2) failed.
auditconfig: error = Operation not supported(48)
```

La siguiente lista indica que la auditoría se está ejecutando:

```
# auditconfig -getcond
audit condition = auditing
```

Si el servicio de auditoría no se está ejecutando, habilítelo. Para conocer el procedimiento, consulte [“Cómo habilitar el servicio de auditoría” en la página 632](#).

**2 Compruebe la sintaxis del archivo `audit_control`.**

```
# audit -v /etc/security/audit_control
audit: audit_control must have either a valid "dir:" entry
or a valid "plugin:" entry with "p_dir:" specified.
```

Corrija los errores. El mensaje syntax ok indica que el archivo es correcto desde el punto de vista sintáctico.

**3 Compruebe que el archivo `audit_control` tenga valores válidos para las palabras clave `flags` y `naflags`.**

```
# grep flags /etc/security/audit_control
flags:lo
naflags:na,lp
```

Si el archivo `audit_control` tiene valores no válidos, proporcione valores válidos. En el ejemplo anterior, `lp` es una clase no válida.

**4 Compruebe que el archivo `audit_user` tenga valores válidos para todos los usuarios.**

```
# tail audit_user
...
# User Level Audit User File
#
# File Format
#
#   username:always:never
#
root:lo:no
admin:lp:no
```

Si el archivo `audit_user` tiene valores no válidos, proporcione valores válidos. En el ejemplo anterior, `lp` es una clase no válida.

**5 Si crea una clase de auditoría personalizada, compruebe que haya asignado eventos a la clase.**

Por ejemplo, el siguiente archivo `audit_control` contiene una clase que el software de Oracle Solaris no entregó:

```
# grep flags /etc/security/audit_control
flags:lo,pf
naflags:na,lo
```

Para obtener una descripción de la creación de la clase `pf`, consulte [“Cómo agregar un clase de auditoría” en la página 622](#).

**a. Compruebe que la clase esté definida en el archivo `audit_class`.**

La máscara de clase de auditoría debe ser única.

```
# grep pf /etc/security/audit_class
0x10000000:pf:profile command
```

Si la clase no está definida, defínala. De lo contrario, elimine la clase de los archivos `audit_control` y `audit_user`.

**b. Compruebe que los eventos se hayan asignado a la clase.**

```
# grep pf /etc/security/audit_event
6180:AUE_prof_cmd:profile command:ua,as,pf
```

Si los eventos no están asignados a la clase, asigne los eventos adecuados a esta clase.

**6 Si los pasos anteriores no indicaban un problema, revise los archivos de registro del sistema `/var/adm/messages` y `/var/log/syslog`.****a. Localice y corrija los problemas.****b. A continuación, si el servicio de auditoría está en ejecución, reinicielo.**

```
# audit -s
```

**c. Si el servicio de auditoría no se está ejecutando, habilítelo.**

Para conocer el procedimiento, consulte [“Cómo habilitar el servicio de auditoría” en la página 632](#).

## ▼ **Cómo reducir el volumen de los registros de auditoría que se producen**

Cuando haya determinado qué eventos deben auditarse en su ubicación, use las siguientes sugerencias para crear archivos de auditoría manejables.

## 1 Utilice la política de auditoría predeterminada.

En concreto, evite agregar eventos y tokens de auditoría a la pista de auditoría. Las siguientes políticas afectan el tamaño de la pista de auditoría.

- Política `arge`: agrega variables de entorno a los eventos de auditoría `exec`.
- Política `argv`: agrega parámetros de comandos a los eventos de auditoría `exec`.
- Política `public`: si va a auditar eventos de archivos, agregue un evento a la pista de auditoría en el archivo público cada vez que ocurra un evento auditable. Las clases de archivos incluyen `fa`, `fc`, `fd`, `fm`, `fr`, `fw` y `cl`. Para la definición de un archivo público, consulte [“Conceptos y terminología de auditoría” en la página 588](#).
- Política `path`: agrega un token `path` a los eventos de auditoría que incluyen un token `pathopcional`.
- Política `group`: agrega un token de grupo a los eventos de auditoría que incluyen un token `newgroups` opcional.
- Política `seq`: agrega un token de secuencia a cada evento de auditoría.
- Política `trail`: agrega un token de ubicador a cada evento de auditoría.
- Política `windata_down`: en un sistema configurado con Trusted Extensions, agrega eventos cuando se disminuye el nivel de la información en una ventana con etiqueta.
- Política `windata_up`: en un sistema configurado con Trusted Extensions, agrega eventos cuando se aumenta el nivel de la información en una ventana con etiqueta.
- Política `zonename`: agrega el nombre de zona a cada evento de auditoría. Si la zona global es la única zona configurada, agrega `zone`, `global` a cada evento de auditoría.

El siguiente registro de auditoría muestra el uso del comando `ls`. La clase `ex` se está auditando y la política predeterminada está en uso:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

A continuación, se muestra el mismo registro cuando se activan todas las políticas:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
attribute,100555,root,bin,136,432,0
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,PATH=/usr/sbin:/usr/bin,
SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
path,/lib/ld.so.1
attribute,100755,root,bin,136,4289,0
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
group,root,other,bin,sys,adm,uucp,mail,tty,lp,nuucp,daemon
return,success,0
zone,global
sequence,313540
trailer,375
```

**2 Utilice el complemento `audit_syslog` . so para enviar algunos eventos de auditoría a `syslog`.**

Esta estrategia funciona sólo si no es necesario mantener registros binarios de los eventos de auditoría que envía a los registros `syslog`. Mediante el comando `audit reduce`, puede segregar los archivos binarios de estos registros y reducir de esta forma el tamaño de los archivos binarios.

**3 Utilice el archivo `audit_user` para auditar eventos para usuarios y roles específicos.**

Reduzca la cantidad de auditoría para todos los usuarios mediante la reducción del número de clases de auditoría en el archivo `audit_control`. En el archivo `audit_user`, puede agregar clases de auditoría para usuarios y roles específicos.

**4 Cree sus propias clases de auditoría personalizadas.**

Puede crear clases de auditoría en el sitio. En estas clases, coloque todos los eventos de auditoría que necesita supervisar. Para conocer el procedimiento, consulte [“Cómo agregar un clase de auditoría” en la página 622](#).

---

**Nota** – Si modifica asignaciones de clase de auditoría existentes, las modificaciones pueden perderse al actualizar a una versión más reciente del SO Oracle Solaris. Lea atentamente los registros de instalación.

---

## ▼ **Cómo auditar todos los comandos por usuarios**

Como parte de la política de seguridad del sitio, algunos sitios requieren registros de auditoría de todos los comandos ejecutados por el usuario `root` o por los roles administrativos. Algunos sitios también requieren registros de auditoría de todos los comandos que ejecutan los usuarios.

**1 Audite las clases `lo` y `ex`.**

La clase `ex` audita todas las llamadas a las funciones `exec()` y `execve()`. La clase `lo` audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla. La siguiente salida muestra todos los eventos de las clases `ex` y `lo`.

```
7:AUE_EXEC:exec(2):ps,ex
23:AUE_EXECVE:execve(2):ps,ex
...
6152:AUE_login:login - local:lo
6153:AUE_logout:logout:lo
6154:AUE_telnet:login - telnet:lo
6155:AUE_rlogin:login - rlogin:lo
6158:AUE_rshd:rsh access:lo
6159:AUE_su:su:lo
6162:AUE_rexecd:rexecd:lo
6163:AUE_passwd:passwd:lo
6164:AUE_rexd:rexd:lo
6165:AUE_ftpd:ftp access:lo
6171:AUE_ftpd_logout:ftp logout:lo
6172:AUE_ssh:login - ssh:lo
```



```

6173:AUE_role_login:role login:lo
6212:AUE_newgrp_login:newgrp login:lo
6213:AUE_admin_authenticate:admin login:lo
6221:AUE_screenlock:screenlock - lock:lo
6222:AUE_screenunlock:screenlock - unlock:lo
6227:AUE_zlogin:login - zlogin:lo

```

- **Para auditar estas clases para los administradores, modifique el archivo `audit_user`.**

En el siguiente ejemplo, el sitio ha creado tres roles, `sysadm`, `auditadm` y `netadm`. Estos roles y la cuenta `root` se auditan para las clases `exec` y `lo`:

```

## audit_user file
root:lo,ex:no
sysadm:lo,ex:no
auditadm:lo,ex:no
netadm:lo,ex:no

```

- **Para auditar la clase `lo` para eventos no atribuibles, modifique el archivo `audit_control`.**

```

## audit_control file
...
naflags:lo
...

```

- **Para auditar estas clases para todos los usuarios, modifique el archivo `audit_control`.**

```

## audit_control file
flags:lo,ex
naflags:lo
...

```

El resultado es similar al siguiente:

```

header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0

```

## 2 Para registrar los argumentos en los comandos, configure la política `argv`.

```

## audit_startup script
...
auditconfig -setpolicy +argv
...

```

El token `exec_args` registra los argumentos de los comandos:

```

header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0

```

## 3 Para registrar el entorno en el que se ejecuta el comando, configure la política `argv`.

```

## audit_startup script
...

```

```
auditconfig -setpolicy +arge
...
```

El token `exec_env` registra el entorno de los comandos:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

#### 4 Para registrar los argumentos y el entorno de comandos, establezca ambas políticas.

```
## audit_startup script
...
auditconfig -setpolicy +argv
auditconfig -setpolicy +arge
...
```

El resultado es similar al siguiente:

```
header,375,2,execve(2),,mach1,2009-08-06 11:19:57.388 -07:00
path,/usr/bin/ls
exec_args,1,ls
exec_env,9,HOME=/,HZ=,LANG=C,LOGNAME=root,MAIL=/var/mail/root,
PATH=/usr/sbin:/usr/bin,SHELL=/sbin/sh,TERM=xterm,TZ=US/Pacific
subject,jdoe,root,root,root,root,1401,737,0 0 mach1
return,success,0
```

## ▼ Cómo buscar registros de auditoría de los cambios realizados en archivos específicos

Si tiene como objetivo registrar las escrituras de los archivos en comparación con un número limitado de archivos, como `/etc/passwd` y los archivos en el directorio `/etc/default`, debe utilizar el comando `auditreduce` para ubicar los archivos.

### 1 Auditoría de la clase `fw`.

Si agrega la clase al archivo `audit_user`, genera menos registros que si agrega la clase al archivo `audit_control`.

#### ■ Agregue la clase `fw` al archivo `audit_user`.

```
## audit_user file
root:fw:no
sysadm:fw:no
auditadm:fw:no
netadm:fw:no
```

- **Agregue la clase `fw` al archivo `audit_control`.**

```
## audit_control file
flags:lo,fw
...
```

- 2 Para buscar los registros de auditoría para archivos específicos, utilice el comando `audit reduce`.**

```
# /usr/sbin/auditreduce -o file=/etc/passwd,/etc/default -O filechg
```

El comando `audit reduce` busca en la pista de auditoría todas las instancias del argumento `file`. El comando crea un archivo binario con el sufijo `filechg` que contiene todos los registros que incluyen los nombres de ruta de los archivos de interés. Consulte la página del comando [man `auditreduce\(1M\)`](#) para conocer la sintaxis de la opción `-o file=nombre_ruta`.

- 3 Para leer el archivo `filechg`, utilice el comando `praudit`.**

```
# /usr/sbin/praudit *filechg
```

## ▼ **Cómo modificar una máscara de preselección de usuario**

Si modifica el archivo `audit_control` o `audit_user`, la máscara de preselección de los usuarios que ya iniciaron sesión no cambia. Debe forzar la máscara de preselección para que cambie.

### **Antes de empezar**

Debe haber habilitado la auditoría, los inicios de sesión de los usuarios y, luego, debe haber cambiado el valor de `flags` o `naflags` en el archivo `audit_control`. Quiere que los usuarios que ya iniciaron sesión se auditen en estas clases de auditoría recientemente seleccionadas.

- 1 Actualice la máscara de preselección de los usuarios que ya iniciaron sesión.**

Dispone de dos opciones. Puede terminar las sesiones existentes o utilizar el comando `auditconfig` para actualizar las máscaras de preselección de los usuarios.

- **Termine las sesiones existentes de los usuarios.**

Los usuarios pueden cerrar sesión y volver a iniciarla, o el administrador puede terminar manualmente (finalizar) las sesiones activas. Las nuevas sesiones heredan la nueva máscara de preselección. Sin embargo, cerrar la sesión de los usuarios puede ser poco práctico.

- **Cambie de forma dinámica la máscara de preselección de cada usuario.**

Supongamos que el atributo `flags` en el archivo `audit_control` se ha cambiado de `lo` a `lo,ex`.

- a. **Determine el ID de auditoría del usuario y el ID de sesión de auditoría.**

En primer lugar, busque los usuarios comunes. En el siguiente ejemplo, el administrador busca todos los procesos que no sean responsabilidad de `root`, `daemon` o `lp`:

```
# /usr/bin/pgrep -v -u root,daemon,lp | more
..
3941
3948
3949
10640 ...
```

A continuación, utilice uno de los procesos de usuario para buscar ID de auditoría del usuario:

```
# auditconfig -getpinfo 3941
audit id = jdoe(1002)
process preselection mask = lo(0x1000,0x1000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 713
```

Tenga en cuenta que la máscara de preselección del usuario incluye la clase `lo` y no incluye la clase `ex` recién agregada.

El ID de auditoría del usuario es `1002`. El ID de sesión de auditoría del usuario es `713`.

## 2 Cambie la máscara de preselección del usuario.

Utilice uno de los dos métodos siguientes:

- **Utilice el ID de sesión de auditoría del usuario para cambiar la máscara de preselección del usuario.**

```
# /usr/sbin/auditconfig -setsmask lo,ex 713
```

- **Utilice el ID de auditoría del usuario para cambiar la máscara de preselección del usuario.**

```
# /usr/sbin/auditconfig -setumask lo,ex 1002
```

## 3 Compruebe que la máscara de preselección haya cambiado.

```
# auditconfig -getpinfo 3941
audit id = jdoe(1002)
process preselection mask = ex,lo(0x40001000,0x40001000)
terminal id (maj,min,host) = 9426,65559,mach1(192.168.123.234)
audit session id = 713
```

## ▼ Cómo evitar la auditoría de determinados eventos

Con fines de mantenimiento, a veces, un sitio quiere evitar que se auditen eventos de auditoría.

### 1 Cambie la clase del evento a la clase no.

Por ejemplo, los eventos 26 y 27 pertenecen a la clase pm.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):pm
27:AUE_SETPGRP:setpgrp(2):pm
28:AUE_SWAPON:swapon(2):no
...
```

Cambie estos eventos a la clase no.

```
## audit_event file
...
25:AUE_VFORK:vfork(2):ps
26:AUE_SETGROUPS:setgroups(2):no
27:AUE_SETPGRP:setpgrp(2):no
28:AUE_SWAPON:swapon(2):no
...
```

Si la clase pm está siendo auditada actualmente, las sesiones existentes aún auditarán los eventos 26 y 27. Para evitar que estos eventos se auditen, debe actualizar las máscaras de preselección de los usuarios.



**Precaución** – Nunca quite el comentario de eventos en el archivo `audit_event`. Este archivo es utilizado por el comando `praudit` para leer archivos binarios de auditoría. Los archivos de auditoría almacenados pueden contener eventos que se muestran en el archivo.

### 2 Para actualizar la preselección de máscaras de los usuarios, siga las instrucciones de [“Cómo modificar una máscara de preselección de usuario” en la página 659](#).

## ▼ Cómo limitar el tamaño de los archivos de auditoría binarios

Los archivos de auditoría binarios crecen sin límite. Para facilitar el archivado y la búsqueda, puede que desee limitar el tamaño. También puede crear archivos binarios más pequeños a partir del archivo original.

### 1 A partir de la versión Solaris 10 10/08, use el atributo `p_fsize` para limitar el tamaño de los archivos de auditoría binarios individuales.

El atributo `p_fsize` en el complemento `audit_binfile`, so lo habilita a limitar el tamaño de un archivo de auditoría. El valor predeterminado es cero (0), que le permite al archivo crecer sin

límite. El valor se especifica en bytes, de 512.000 a 2.147.483.647. Cuando se alcanza el tamaño especificado, se cierra el archivo de auditoría actual y se abre un nuevo archivo.

En el siguiente ejemplo, se limita el tamaño de un archivo de auditoría a 1 Mbyte:

```
plugin:name=audit_binfile.so; p_dir:/var/audit; p_fsize=1024000
```

## 2 Utilice el comando `audit reduce` para seleccionar registros y escribir los registros en un archivo para su análisis posterior.

Las opciones `audit reduce -minúscula` buscan registros específicos.

Las opciones `audit reduce -mayúscula` escriben las selecciones en un archivo. Para obtener más información, consulte la página del comando `man audit reduce(1M)`.

## ▼ Cómo auditar inicios de sesión de otros OSes

Oracle Solaris puede auditar todos los inicios de sesión, independientemente del origen.

### ● Audite la clase `lo` para los eventos atribuibles y no atribuibles.

Esta clase audita los inicios de sesión, los cierres de sesión y los bloqueos de pantalla.

```
## audit_control file
flags:lo
naflags:lo
...
```

---

**Nota** – Para auditar inicios de sesión `ssh`, su sistema Oracle Solaris debe ejecutar el daemon `ssh` de Oracle Solaris. Este daemon se ha modificado para la auditoría de Oracle Solaris. Para obtener más información, consulte “Oracle Solaris Secure Shell y el proyecto OpenSSH” en la página 356.

---

## ▼ Cómo auditar transferencias de archivos FTP y SFTP

El servicio FTP crea registros de sus transferencias de archivos. El servicio SFTP, que se ejecuta en el protocolo SSH, se puede auditar mediante la auditoría de Oracle Solaris. Los inicios de sesión de ambos servicios se pueden auditar mediante la auditoría de Oracle Solaris.

### 1 Para registrar los comandos y las transferencias de archivos del servicio FTP, consulte la página del comando `man ftpaccess(4)`.

Para conocer las opciones de registro disponibles, lea la sección de “capacidades de registro”. En particular, las opciones `log commands` y `log transfers` pueden proporcionar registros útiles.

## 2 Para registrar transferencias de archivos `sftp`, realice una de las siguientes acciones o ambas acciones:

### ■ Audite las lecturas de archivos.

Las transferencias de archivos a través de una conexión SSH utilizan el comando `sftp`. Estas transferencias se pueden registrar mediante el indicador de auditoría `+fr`. Para auditar las transferencias de archivos `sftp` fallidas, audite el indicador de auditoría `-fr`.

El siguiente resultado es de una sesión `sftp` satisfactoria:

```
header,138,2,open(2) - read,,ma2,2009-08-25 14:48:58.770 -07:00
path,/home/jdoe/vpn_connect
attribute,100644,jdoe,staff,391,437,0
subject,jdoe,jdoe,staff,jdoe,staff,4444,120289379,8457 65558 ma1
return,success,6
```

### ■ Utilice la opción detallada para el comando `sftp`.

La opción `-v` se puede repetir hasta tres veces.

```
# sftp -vvv [ other options ] hostname
```

## 3 Para registrar el acceso a los servicios FTP y SFTP, audite la clase `lo`.

Como indica el siguiente resultado, el inicio y cierre de sesión del daemon `ftpd` generan registros de auditoría.

```
% bsmrecord -c lo | more
...
in.ftpd
  program    /usr/sbin/in.ftpd    See ftp access
  event ID   6165                AUE_ftp
  class      lo                  (0x00001000)
    header
    subject
  [text]
  return
error message

in.ftpd
  program    /usr/sbin/in.ftpd    See ftp logout
  event ID   6171                AUE_ftp_logout
  class      lo                  (0x00001000)
    header
    subject
  return
error message
...
```

El inicio de sesión SSH registra todos los accesos al comando `sftp`.

```
...
/usr/lib/ssh/sshd
  program    /usr/lib/ssh/sshd    See login - ssh
  event ID   6172                AUE_ssh
  class      lo                  (0x00001000)
    header
    subject
  [text]
  return
error message
```





## Auditoría de Oracle Solaris (referencia)

---

En este capítulo se describen los componentes importantes de la auditoría de Oracle Solaris. A continuación puede ver una lista de la información de referencia que se ofrece en este capítulo:

- “Comandos de auditoría” en la página 665
- “Archivos utilizados en el servicio de auditoría” en la página 671
- “Perfiles de derechos para administración de auditoría” en la página 677
- “Auditoría y zonas de Oracle Solaris” en la página 678
- “Clases de auditoría” en la página 679
- “Complementos de auditoría” en la página 682
- “Política de auditoría” en la página 682
- “Características de auditoría de proceso” en la página 683
- “Pista de auditoría” en la página 683
- “Convenciones de nombres de archivos de auditoría binarios” en la página 684
- “Estructura de registro de auditoría” en la página 685
- “Formatos de token de auditoría” en la página 686

Para obtener una descripción general de la auditoría de Oracle Solaris, consulte el [Capítulo 28](#), “Auditoría de Oracle Solaris (descripción general)”. Para obtener sugerencias de planificación, consulte el [Capítulo 29](#), “Planificación de la auditoría de Oracle Solaris”. Para obtener más información sobre procedimientos para configurar la auditoría en su sitio, consulte el [Capítulo 30](#), “Gestión de la auditoría de Oracle Solaris (tareas)”.

### Comandos de auditoría

En esta sección se ofrece información acerca de los siguientes comandos:

- “Daemon auditd” en la página 666
- “Comando audit” en la página 667
- “Comando bsmrecord” en la página 667
- “Comando auditreduce” en la página 667
- “Comando praudit” en la página 669

- “Comando `auditconfig`” en la página 671

## Daemon `auditd`

La siguiente lista resume las tareas del daemon `auditd`:

- Abre y cierra archivos de auditoría en los directorios especificados en el archivo `audit_control`. Los archivos se abren en orden de mención.
- Carga uno o más complementos. `auditd` proporciona dos complementos. El complemento `audit_binfile`.so escribe datos binarios de auditoría en un archivo. El complemento `audit_syslog`.so ofrece resúmenes de texto seleccionados de los registros de auditoría al registro `syslog`.
- Lee los datos de auditoría desde el núcleo y produce los datos con un complemento `auditd`.
- Ejecuta la secuencia de comandos `audit_warn` para advertir acerca de distintas condiciones. El complemento `audit_binfile`.so ejecuta la secuencia de comandos `audit_warn`. De manera predeterminada, la secuencia de comandos envía advertencias al alias de correo electrónico `audit_warn` y a la consola. El complemento `syslog`.so no ejecuta la secuencia de comandos `audit_warn`.
- De manera predeterminada, cuando todos los directorios de auditoría están llenos, se suspenden los procesos que generan registros de auditoría. Además, el daemon `auditd` escribe un mensaje a la consola y al alias de correo electrónico `audit_warn`. En este punto, sólo el administrador del sistema puede corregir el servicio de auditoría. El administrador puede iniciar sesión para escribir archivos de auditoría en medios sin conexión, eliminar archivos de auditoría del sistema y realizar otras tareas de limpieza.

La política de auditoría se puede volver a configurar con el comando `auditconfig`.

El daemon `auditd` se puede iniciar automáticamente cuando el sistema se inicia en modo multiusuario. O bien, puede iniciar el daemon desde la línea de comandos. Cuando el daemon `auditd` se inicia, calcula la cantidad de espacio libre necesaria para los archivos de auditoría.

El daemon `auditd` usa la lista de directorios de auditoría en el archivo `audit_control` como ubicaciones posibles para crear archivos de auditoría. El daemon mantiene un puntero en esta lista de directorios, comenzando por el primer directorio. Cada vez que el daemon `auditd` necesita crear un archivo de auditoría, el daemon coloca el archivo en el primer directorio disponible en la lista. La lista se inicia en el puntero actual del daemon `auditd`. Puede restablecer el puntero al principio de la lista mediante la ejecución del comando `audit -s`. El comando `audit -n` instruye al daemon a que pase a otro archivo de auditoría. El archivo nuevo se crea en el mismo directorio que el archivo actual.

## Comando audit

El comando `audit` controla las acciones del daemon `auditd`. El comando `audit` puede realizar las siguientes tareas:

- Habilitar y deshabilitar la auditoría.
- Restablecer el daemon `auditd`.
- Ajustar la máscara de preselección de auditoría en el sistema local.
- Escribir los registros de auditoría en un archivo de auditoría diferente.

Para obtener una explicación de las opciones disponibles, consulte la página del comando `man audit(1M)`.

## Comando bsmrecord

El comando `bsmrecord` muestra el formato de los eventos de auditoría que se definen en el archivo `/etc/security/audit_event`. La salida incluye el ID de auditoría del evento, la clase de auditoría, el indicador de auditoría y los tokens de auditoría del registro en orden. Sin ninguna opción, la salida del comando `bsmrecord` se muestra en una ventana de terminal. Con la opción `-h`, la salida es adecuada para visualizarla en un explorador. Para obtener ejemplos del uso del comando `bsmrecord`, consulte “[Cómo visualizar formatos de registros de auditoría](#)” en la [página 641](#). Asimismo, consulte la página del comando `man bsmrecord(1M)`.

## Comando auditreduce

El comando `auditreduce` resume los registros de auditoría que se almacenan en formato binario. El comando puede fusionar los registros de auditoría de uno o más archivos de auditoría de entrada. El comando también se puede utilizar para realizar una selección posterior de los registros de auditoría. Los registros permanecen en formato binario. Para fusionar toda la pista de auditoría, ejecute este comando en el servidor de la auditoría. El servidor de auditoría es el sistema que monta todos los sistemas de archivos de auditoría para la instalación. Para obtener más información, consulte la página del comando `man auditreduce(1M)`.

El comando `auditreduce` lo habilita a realizar un seguimiento de todas las acciones auditadas en varios sistemas de una sola ubicación. El comando puede leer la combinación lógica de todos los archivos de auditoría como una sola pista de auditoría. De forma idéntica, debe configurar todos los sistemas en una ubicación de la auditoría y crear servidores y directorios locales para los archivos de auditoría. El comando `auditreduce` ignora cómo se generaron los registros o dónde se guardan los registros. Sin opciones, el comando `auditreduce` fusiona los registros de auditoría de todos los archivos de auditoría de todos los subdirectorios del directorio `root` de auditoría. Normalmente, el directorio `root` de auditoría es `/etc/security/audit`. El comando

`auditreduce` envía los resultados fusionados a una salida estándar. También puede colocar los resultados en un solo archivo de salida ordenado cronológicamente. El archivo contiene los datos binarios.

El comando `auditreduce` también puede seleccionar determinados tipos de registros para el análisis. Las funciones de fusión y las funciones de selección del comando `auditreduce` tienen lógica independiente. El comando `auditreduce` captura los datos de los archivos de entrada a medida que se leen los registros, antes de que los archivos sean fusionados y luego escritos en el disco.

Al especificar opciones en el comando `auditreduce`, también puede hacer lo siguiente:

- Solicitar registros de auditoría generados por clases de auditorías especificadas
- Solicitar registros de auditoría generados por un usuario particular
- Solicitar registros de auditoría generados en fechas específicas

Sin argumentos, el comando `auditreduce` comprueba los subdirectorios dentro del directorio `/etc/security/audit`, el directorio root de auditoría predeterminado. El comando comprueba que haya un directorio `files` en el que residan los archivos `start-time.end-time.hostname`. El comando `auditreduce` es muy útil cuando los datos de auditoría residen en directorios independientes. La [Figura 31-1](#) ilustra los datos de auditoría en directorios independientes para hosts diferentes. La [Figura 31-2](#) ilustra los datos de auditoría en directorios independientes para servidores de auditoría diferentes.

FIGURA 31-1 Almacenamiento de pista de auditoría por host

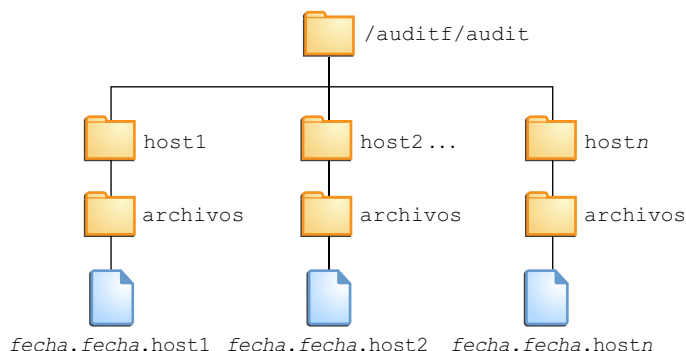
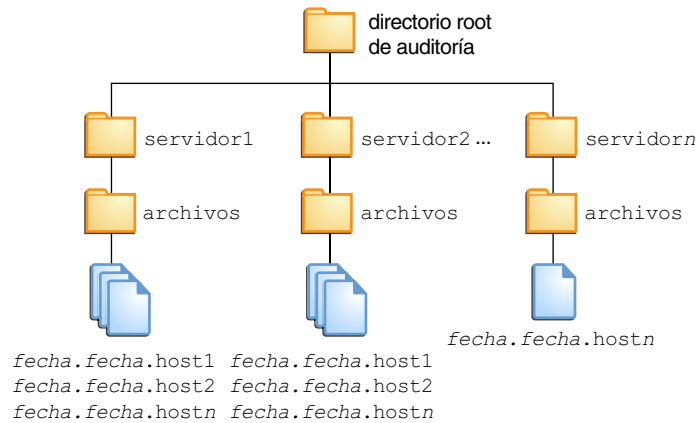


FIGURA 31-2 Almacenamiento de pista de auditoría por servidor



Si la partición para el directorio `/etc/security/audit` es muy pequeña, es posible que no necesite almacenar datos de auditoría en el directorio predeterminado. Puede transferir el comando `auditreduce` a otro directorio mediante la opción `-R`:

```
# auditreduce -R /var/audit-alt
```

También puede especificar un subdirectorio particular mediante la opción `-S`:

```
# auditreduce -S /var/audit-alt/host1
```

Para conocer otras opciones y obtener más ejemplos, consulte la página del comando [man auditreduce\(1M\)](#).

## Comando praudit

El comando `praudit` hace que la salida del comando `auditreduce` sea legible. El comando `praudit` lee los registros de auditoría en formato binario a partir de la entrada estándar y muestra los registros en un formato presentable. La entrada puede ser conducida desde el comando `auditreduce` o desde un único archivo de auditoría. La entrada también puede ser producida con el comando `cat` para concatenar varios archivos o el comando `tail` para un archivo actual de auditoría.

El comando `praudit` puede generar cuatro formatos de salida. Una quinta opción, `-l` (longitud), imprime un registro de auditoría por línea de la salida. El valor predeterminado es que coloque un token de auditoría por línea de la salida. La opción `-d` cambia el delimitador que se usa entre los campos de tokens y entre los tokens. El delimitador predeterminado es una coma.

- **Predeterminado:** el comando `praudit` sin opciones muestra un token de auditoría por línea. El comando muestra el evento de auditoría según su descripción, como la llamada del sistema `ioctl(2)`. Cualquier valor que se pueda visualizar como texto se muestra en formato de texto. Por ejemplo, un usuario se muestra como el nombre de usuario, no como el ID de usuario.
- **-r option:** la opción sin procesar muestra como un número cualquier valor que pueda ser numérico. Por ejemplo, un usuario se muestra por ID de usuario, las direcciones de Internet están en formato hexadecimal y los modos están en formato octal. El evento de auditoría se muestra como su número de evento, por ejemplo, 158.
- **-s option:** la opción de formato corto muestra el evento de auditoría según su nombre de tabla, por ejemplo, `AUE_IOCTL`. La opción muestra los otros tokens como los muestra la opción predeterminada.
- **-x option:** la opción XML muestra el registro de auditoría en formato XML. Esta opción es útil como entrada a los exploradores, o como entrada a las secuencias de comandos que manipulan XML.

El XML se describe mediante una DTD que proporciona el servicio de auditoría. El software de Oracle Solaris también proporciona una hoja de estilo. La DTD y la hoja de estilo están en el directorio `/usr/share/lib/xml`.

En el formato de salida predeterminado del comando `praudit`, cada registro se identifica fácilmente como una secuencia de tokens de auditoría. Cada token se presenta en una línea separada. Cada registro comienza con un token header. Por ejemplo, puede seguir procesando la salida con el comando `awk`.

Ésta es la salida del comando `praudit - l` para un token header:

```
header,173,2,settppriv(2),,example1,2010-10-10 10:10:02.020 -07:00
```

Ésta es la salida del comando `praudit - r` para el mismo token header:

```
121,173,2,289,0x0000,192.168.86.166,1066077962,174352445
```

#### EJEMPLO 31-1 Procesamiento de la salida de `praudit` con una secuencia de comandos

Es posible que quiera procesar la salida del comando `praudit` como líneas de texto. Por ejemplo, es posible que quiera seleccionar registros que el comando `audit` reduce no pueda seleccionar. Puede utilizar una secuencia de comandos de shell sencilla para procesar la salida del comando `praudit`. La siguiente secuencia de comandos sencilla de ejemplo coloca un registro de auditoría en una línea, busca una cadena especificada por el usuario y devuelve el archivo de auditoría a su forma original.

```
#!/bin/sh
#
## This script takes an argument of a user-specified string.
# The sed command prefixes the header tokens with Control-A
# The first tr command puts the audit tokens for one record
```

**EJEMPLO 31-1** Procesamiento de la salida de `praudit` con una secuencia de comandos (Continuación)

```
# onto one line while preserving the line breaks as Control-A
#
praudit | sed -e '1,2d' -e '$s/^file.*$//' -e 's/^header/^aheader/' \
| tr '\012\001' '\002\012' \
| grep "$1" \      Finds the user-specified string
| tr '\002' '\012' Restores the original newline breaks
```

Tenga en cuenta que `^` en la secuencia de comandos equivale a Control-A, no los dos caracteres `^` y `a`. El prefijo distingue el token `header` de la cadena `header` que podría aparecer como texto.

## Comando `auditconfig`

El comando `auditconfig` proporciona una interfaz de línea de comando para recuperar y establecer parámetros de configuración de auditoría. El comando `auditconfig` puede realizar las siguientes tareas:

- Mostrar, comprobar y configurar la política de auditoría
- Determinar si la auditoría está activada o desactivada
- Gestionar el directorio de auditoría y el archivo de auditoría
- Gestionar la cola de auditoría
- Obtener y establecer máscaras de preselección
- Obtener y establecer el evento de auditoría en las asignaciones de clase de auditoría
- Obtener y establecer información de configuración, como ID de sesión e ID de auditoría
- Configurar las características de auditoría para un proceso, un shell y una sesión
- Reiniciar estadísticas de auditoría

Para obtener una explicación de las opciones de comandos, consulte la página del comando `man auditconfig(1M)`.

## Archivos utilizados en el servicio de auditoría

El servicio de auditoría utiliza los siguientes archivos:

- “Archivo `system`” en la página 672
- “Archivo `syslog.conf`” en la página 672
- “Archivo `audit_class`” en la página 672
- “Archivo `audit_control`” en la página 673
- “Archivo `audit_event`” en la página 674
- “Secuencia de comandos `audit_startup`” en la página 674

- [“Base de datos audit\\_user” en la página 675](#)
- [“Secuencia de comandos audit\\_warn” en la página 676](#)
- [“Secuencia de comandos bsmconv” en la página 677](#)

## Archivo system

El archivo `/etc/system` contiene comandos que el núcleo lee durante la inicialización para personalizar las operaciones de sistema. Las secuencias de comandos de shell `bsmconv` y `bsmunconv`, que se usan para activar y desactivar la auditoría, modifican el archivo `/etc/system`. La secuencia de comandos de shell `bsmconv` agrega la línea siguiente al archivo `/etc/system`:

```
set c2audit:audit_load=1
```

La entrada `set c2audit:audit_load=1` hace que el módulo de núcleo para auditar se cargue al reiniciar el sistema. La secuencia de comandos `bsmunconv` deshabilita la auditoría cuando el sistema se reinicia. El comando elimina la línea `c2audit` del archivo `/etc/system`.

## Archivo syslog.conf

El archivo `/etc/syslog.conf` trabaja con el complemento `audit_syslog.so` para almacenar los registros de auditoría en texto. El archivo `syslog.conf` puede configurarse para permitir que la utilidad `syslog` almacene registros de auditoría. Para obtener un ejemplo, consulte [“Cómo configurar registros de auditoría syslog” en la página 617](#).

## Archivo audit\_class

El archivo `/etc/security/audit_class` define las clases de auditoría. Las clases de auditoría son grupos de eventos de auditoría. Utiliza el nombre de la clase en el archivo `audit_control` para preseleccionar las clases cuyos eventos desea auditar. Las clases aceptan prefijos para seleccionar sólo los eventos con fallos o sólo los eventos correctos. Para obtener más información, consulte [“Sintaxis de la clase de auditoría” en la página 680](#).

El superusuario, o un administrador en un rol equivalente, puede modificar las definiciones de las clases de auditoría. Este administrador puede definir nuevas clases de auditoría, cambiar el nombre de clases existentes o cambiar clases existentes al editar el archivo `audit_class` en un editor de texto. Para obtener más información, consulte la página del comando `man audit_class(4)`.



## Archivo `audit_control`

El archivo `/etc/security/audit_control` en cada sistema contiene información de configuración para el daemon `auditd`. El archivo permite que cada sistema monte un sistema de archivos de auditoría remoto para almacenar sus registros de auditoría.

Puede especificar cinco tipos de información en el archivo `audit_control`. Cada línea de información comienza con una palabra clave.

- **Palabra clave** `flags`: inicia la entrada que preselecciona qué clases de eventos se auditan para todos los usuarios en el sistema. Las clases de auditoría especificadas aquí determinan la *máscara de preselección de auditoría de todo el sistema*. Las clases de auditoría se separan por comas.
- **Palabra clave** `naflags`: inicia la entrada que preselecciona qué clases de eventos se auditan cuando una acción no se puede atribuir a un usuario específico. Las clases de auditoría se separan por comas. La clase de evento `na` pertenece a esta entrada. La entrada `naflags` se puede utilizar para registrar otras clases de eventos que normalmente son atribuibles, pero que no pueden ser atribuidas. Por ejemplo, si un programa que arranca en el inicio lee un archivo, entonces un `fr` en la entrada `naflags` crearía un registro para ese evento.
- **Palabra clave** `minfree`: esta palabra clave se descarta. Utilice el atributo `p_minfree` para el complemento `audit_binfile.so`.

El atributo `p_minfree` define el nivel de espacio libre mínimo para todos los sistemas de archivos de auditoría como un porcentaje. El porcentaje debe ser igual a 0 o mayor que 0. El valor predeterminado es 20%. Cuando un sistema de archivos de auditoría está un 80% completo, los datos de auditoría se almacenan en el siguiente directorio de auditoría disponible. Para obtener más información, consulte la página del comando `man audit_warn(1M)`.

- **Palabra clave** `dir`: esta palabra clave se descarta. Utilice el atributo `p_dir` para el complemento `audit_binfile.so`.

El atributo `p_dir` muestra las ubicaciones de directorio. Cada valor de línea define un sistema de archivos de auditoría y un directorio que el sistema utiliza para almacenar sus archivos de auditoría. Puede especificar una o más ubicaciones de directorio. El orden de los valores es significativo. El daemon `auditd` crea archivos de auditoría en los directorios en el orden especificado. El primer directorio es el *directorio de auditoría principal* del sistema. El segundo directorio es el *directorio de auditoría secundario* donde el daemon `auditd` crea archivos de auditoría cuando el primer directorio se llena, y así sucesivamente. Para obtener más información, consulte la página del comando `man audit(1M)`.

- **Palabra clave** `plugin`: especifica la *ruta del complemento* para los módulos de complemento `audit_binfile.so` y `audit_syslog.so`. El módulo `audit_binfile.so` maneja la creación de archivos de auditoría binarios. El módulo `audit_syslog.so` proporciona en tiempo real conversión a texto de los registros de auditoría de Oracle Solaris. Las clases de auditoría que se especifican en el atributo `p_flags` del complemento `audit_syslog.so` deben ser un subconjunto de las clases de auditoría preseleccionadas.

Para obtener más información acerca del archivo `audit_control`, consulte la página del comando `man audit_control(4)`. Para obtener más información acerca de los complementos, consulte “Complementos de auditoría” en la página 682 y las páginas del comando `man audit_binfile(5)` y `audit_syslog(5)`.

#### EJEMPLO 31-2 Muestra: archivo `audit_control`

El siguiente es un archivo de muestra `audit_control` para el sistema `noddy`. `noddy` usa dos sistemas de archivos de auditoría en el servidor de auditoría `blinken` y usa un tercer sistema de archivos de auditoría montado desde el segundo servidor de auditoría `winken`. El tercer sistema de archivos sólo se utiliza cuando los sistemas de archivos de auditoría en `blinken` se llenan o no están disponibles. El valor `minfree` de 20% especifica que la secuencia de comandos de advertencia se ejecute cuando los sistemas de archivos estén un 80% llenos. Los valores especifican que los inicios de sesión y las operaciones administrativas se van a auditar. Se auditan las operaciones para determinar si son correctas o si fallaron. Se auditan los fallos de todos los tipos, excepto los fallos para crear un objeto de sistema de archivos. También se auditan los eventos no atribuibles. El registro de auditoría `syslog` registra menos eventos de auditoría. Este registro contiene resúmenes de texto de inicios de sesión fallidos y operaciones administrativas fallidas.

En la versión Solaris 10, las líneas `dir` y `minfree` se descartaron. En el ejemplo siguiente, las líneas `plugin` no contienen un salto de línea.

```
flags:lo,am,-all,^-fc
naflags:lo,nt
plugin:name=audit_binfile.so; p_minfree=20; p_dir=/var/audit/blinken/files,
/var/audit/blinken.1/files,/var/audit/winken
plugin:name=audit_syslog.so; p_flags=-lo,-am
```

## Archivo `audit_event`

El archivo `/etc/security/audit_event` contiene las asignaciones de evento-clase de auditoría predeterminadas. Puede editar este archivo para cambiar las asignaciones de clase. Al cambiar las asignaciones de clase, debe reiniciar el sistema o ejecutar el comando `auditconfig -conf` para leer las asignaciones cambiadas en el núcleo. Para obtener más información, consulte la página del comando `man audit_event(4)`.

## Secuencia de comandos `audit_startup`

La secuencia de comandos `/etc/security/audit_startup` configura automáticamente el servicio de auditoría cuando el sistema ingresa en el modo multiusuario. El daemon `auditd` se inicia después de que la secuencia de comandos realiza las siguientes tareas:

- Configurar las asignaciones de evento-clase de auditoría
- Establecer las opciones de la política de auditoría

Para obtener más información, consulte la página del comando `man audit_startup(1M)`.

## Base de datos `audit_user`

La base de datos `/etc/security/audit_user` modifica las clases preseleccionadas de todo el sistema para un usuario individual. Las clases que agregue a una entrada de usuario en la base de datos `audit_user` modifican los valores del archivo `audit_control` de dos formas:

- Especificando las clases de auditoría que siempre se van a auditar para este usuario
- Especificando las clases de auditoría que nunca se van a auditar para este usuario

Cada entrada de usuario en la base de datos `audit_user` contiene tres campos:

*username: always-audit-classes: never-audit-classes*

Los campos de auditoría se procesan en secuencia.

- El campo *siempre\_auditar\_clases* activa la auditoría de las clases en ese campo. Utilice este campo para modificar los valores en todo el sistema. Por ejemplo, si coloca `all` en el campo *siempre\_auditar\_clases* audita todo para un usuario.
- El campo *nunca\_auditar\_clases* desactiva la auditoría de las clases en ese campo. Utilice este campo para sustituir configuraciones del sistema. Si pone `all` en el campo *nunca\_auditar\_clases*, desactiva todas las auditorías para el usuario, incluso las clases de auditoría especificadas en el archivo `audit_control`.

Suponga que desea aplicar la configuración de auditoría de todo el sistema al usuario `tamiko`, excepto para las lecturas correctas de los objetos de sistema de archivos. Tenga en cuenta los segundos dos puntos (:) en la siguiente entrada `audit_user`:

`tamiko:~+fr:no`      *modify system defaults for fr*

La entrada anterior significa “siempre auditar todo, excepto lecturas de archivos correctas”.

Si desea realizar una auditoría todo para el usuario `tamiko` con la excepción de las lecturas de archivos correctas, utilice la siguiente entrada:

`tamiko:all,~+fr:no`      *audit everything except fr*

Suponga que desea sustituir los ajustes predeterminados del sistema para las lecturas de archivos correctas del usuario `tamiko`. La siguiente entrada significa “auditar siempre todo, pero nunca lecturas de archivos correctas de auditoría”.

`tamiko:all:+fr`      *override system defaults for fr*

---

**Nota** – Los eventos correctos y los eventos con fallos se tratan por separado. Un proceso puede generar más registros de auditoría para eventos que han fallado que para eventos correctos.

---

## Secuencia de comandos `audit_warn`

La secuencia de comandos `/etc/security/audit_warn` notifica a un alias de correo electrónico cuando el daemon `auditd` encuentra una condición poco común al escribir registros de auditoría. Puede personalizar esta secuencia de comandos para su ubicación a fin de advertir acerca de las condiciones que puedan requerir intervención manual. O bien, puede especificar cómo manejar dichas condiciones automáticamente. Para todas las condiciones de error, la secuencia de comandos `audit_warn` escribe un mensaje a `syslog` con la gravedad de `daemon.alerta`. Puede utilizar `syslog.conf` para configurar la visualización de consola de los mensajes `syslog`. La secuencia de comandos `audit_warn` también envía un mensaje al alias de correo electrónico `audit_warn`. Configure este alias como parte de la configuración de auditoría.

Cuando el daemon `auditd` detecta las siguientes condiciones, el daemon invoca la secuencia de comandos `audit_warn`. La secuencia de comandos envía un correo electrónico al alias `audit_warn`.

- Un directorio de auditoría está más lleno que lo que permite el valor `minfree`. El valor `minfree` o el límite de aviso es un porcentaje del espacio disponible en un sistema de archivos de auditoría.

La secuencia de comandos `audit_warn` se invoca con la cadena `soft` y el nombre del directorio cuyo espacio disponible está por debajo del valor mínimo. El daemon `auditd` cambia automáticamente al siguiente directorio adecuado. El daemon escribe los archivos de auditoría en este nuevo directorio hasta que el directorio alcanza su límite `minfree`. Entonces el daemon `auditd` va a cada directorio restante en el orden que se muestra en el archivo `audit_control`. El daemon escribe los registros de auditoría hasta que cada directorio llegue a su límite `minfree`.

- Todos los directorios de auditoría han llegado al límite de `minfree`.

La secuencia de comandos `audit_warn` se invoca con la cadena `allsoft`. Se escribe un mensaje en la consola. También se envía el correo electrónico al alias `audit_warn`.

Cuando todos los directorios que aparecen en el archivo `audit_control` alcanzaron su límite de `minfree`, el daemon `auditd` vuelve al primer directorio. El daemon escribe registros de auditoría hasta que el directorio se llena por completo.

- Un directorio de auditoría se ha llenado y no queda espacio disponible.

La secuencia de comandos `audit_warn` se invoca con la cadena `hard` y el nombre del directorio. Se escribe un mensaje en la consola. También se envía el correo electrónico al alias `audit_warn`.

El daemon `auditd` cambia automáticamente al siguiente directorio adecuado con espacio disponible. El daemon `auditd` va a cada directorio restante en el orden que se muestra en el archivo `audit_control`. El daemon escribe registros de auditoría hasta que cada directorio se llene por completo.

- Todos los directorios de auditoría están llenos. La secuencia de comandos `audit_warn` se invoca con la cadena `allhard` como un argumento.

De manera predeterminada, se escribe un mensaje en la consola. También se envía el correo electrónico al alias `audit_warn`. Siguen ocurriendo los procesos que de lo contrario generarían registros de auditoría, pero se recuentan los registros de auditoría. No se generan registros de auditoría. Para obtener un ejemplo de cómo manejar esta situación, consulte el [Ejemplo 30–16](#) y “Cómo evitar el desbordamiento de la pista de auditoría” en la página 650.

- Ocurre un error interno. Entre los posibles errores internos se incluyen los siguientes:
  - `ebusy`: ya se está ejecutando otro proceso de daemon `auditd`
  - `tmpfile`: no se puede usar un archivo temporal
  - `postsigterm`: se recibió una señal durante el cierre de auditoría
  - `plugin nombre`: ocurrió un error durante la ejecución del complemento
- Se descubrió un problema con la sintaxis del archivo `audit_control`. De manera predeterminada, se envía un mensaje a la consola. También se envía el correo electrónico al alias `audit_warn`.

Si se establece la política de auditoría `perzone`, la instancia de la zona no global de `auditd` invoca la secuencia de comandos `audit_warn` de la zona. Para obtener más información, consulte la página del comando `man audit_warn(1M)`.

## Secuencia de comandos `bsmconv`

La secuencia de comandos `/etc/security/bsmconv` habilita el servicio de auditoría. El comando `bsmunconv` deshabilita el servicio de auditoría. Después de que se ejecuta la secuencia de comandos `bsmconv`, debe configurar los directorios de auditoría y los archivos de configuración de auditoría. Al reiniciar, se habilita la auditoría.

Para obtener más información, consulte la página del comando `man bsmconv(1M)`.

# Perfiles de derechos para administración de auditoría

Oracle Solaris proporciona perfiles de derechos para configurar el servicio de auditoría y para analizar la pista de auditoría.

- **Control de auditoría:** habilita que un rol configure la auditoría de Oracle Solaris. Este perfil de derechos concede autorizaciones para configurar archivos utilizados por el servicio de auditoría. El perfil también habilita que un rol ejecute comandos de auditoría. Un rol con el perfil de control de auditoría puede ejecutar los siguientes comandos: `audit`, `auditd`, `auditconfig`, `bsmconv` y `bsmunconv`.
- **Revisión de auditoría:** habilita que un rol analice los registros de auditoría de Oracle Solaris. Este perfil de derechos concede autorización para leer registros de auditoría con los comandos `praudit` y `auditreduce`. Un rol con este perfil de derecho también puede ejecutar el comando `auditstat`.
- **Administrador del sistema:** incluye el perfil de derechos de revisión de auditoría. Un rol con el perfil de derechos de administrador del sistema puede analizar los registros de auditoría.

Para configurar roles para manejar el servicio de auditoría, consulte [“Configuración de RBAC \(mapa de tareas\)” en la página 204](#).

## Auditoría y zonas de Oracle Solaris

Las zonas no globales se pueden auditar exactamente como se audita la zona global, o las zonas no globales pueden establecer sus propios indicadores, almacenamientos y políticas de auditoría.

Cuando todas las zonas se auditan de forma idéntica, los archivos de configuración en la zona global proporcionan la configuración para la auditoría en cada zona. La opción de política `+zonename` es útil. Cuando se establece esta opción, los registros de auditoría de todas las zonas incluyen el nombre de la zona. Los registros de auditoría se pueden postseleccionar por nombre de zona. Para comprender la política de auditoría, consulte [“Determinación de política de auditoría” en la página 605](#). Para obtener un ejemplo, consulte [“Cómo configurar la política de auditoría” en la página 629](#).

Las zonas se pueden auditar individualmente. Cuando la opción de política, `perzone`, se establece en la zona global, cada zona no global ejecuta su propio daemon de auditoría, gestiona su propia cola de auditoría y especifica el contenido y la ubicación de los registros de auditoría. Una zona no global también puede definir la mayoría de las opciones de la política de auditoría. No puede definir una política que afecte a todo el sistema, por lo que una zona no global no puede definir las políticas `ahlt` o `perzone`. Para más información, consulte [“Auditoría en un sistema con zonas de Oracle Solaris” en la página 596](#) y [“Cómo planificar auditoría en zonas” en la página 600](#).

Para obtener información sobre las zonas, consulte [Parte II, “Zonas” de Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#).

## Clases de auditoría

Los valores predeterminados en todo el sistema de la auditoría de Oracle Solaris se preseleccionan al especificar una o más clases de eventos. Las clases se preseleccionan para cada sistema en el archivo `audit_control` del sistema. Se audita cualquier persona que utilice el sistema para estas clases de eventos. El archivo se describe en [“Archivo `audit\_control`” en la página 673](#).

Puede configurar clases de auditoría y realizar nuevas clases de auditoría. Los nombres de clase de auditoría puede tener un máximo de 8 caracteres de longitud. La descripción de clase está limitada a 72 caracteres. Se permite el uso de caracteres numéricos y no alfanuméricos.

Puede modificar qué se va a auditar para usuarios individuales al agregar clases de auditoría a la entrada de un usuario en la base de datos `audit_user`. Las clases de auditoría también se utilizan como argumentos para el comando `auditconfig`. Para obtener detalles, consulte la página del comando `man auditconfig(1M)`.

## Definiciones de clases de auditoría

La siguiente tabla muestra cada clase de auditoría predefinida, el nombre descriptivo de cada clase de auditoría y una descripción breve.

TABLA 31-1 Clases de auditoría predefinidas

Clase de auditoría	Nombre descriptivo	Descripción
<code>all</code>	<code>all</code>	Todas las clases (metaclase)
<code>no</code>	<code>no_class</code>	Valor nulo para desactivar la preselección de evento
<code>na</code>	<code>non_attrib</code>	Eventos no atribuibles
<code>fr</code>	<code>file_read</code>	Lectura de datos, abierto para lectura
<code>fw</code>	<code>file_write</code>	Escritura de datos, abierto para escritura
<code>fa</code>	<code>file_attr_acc</code>	Acceso de atributos de objeto: <code>stat</code> , <code>pathconf</code>
<code>fm</code>	<code>file_attr_mod</code>	Cambio de atributos de objeto: <code>chown</code> , <code>flock</code>
<code>fc</code>	<code>file_creation</code>	Creación de objeto
<code>fd</code>	<code>file_deletion</code>	Supresión de objeto
<code>cl</code>	<code>file_close</code>	<code>close</code>
<code>ap</code>	<code>application</code>	Evento definido por la aplicación
<code>ad</code>	<code>administrative</code>	Acciones administrativas (antigua metaclase administrativa)

TABLA 31-1 Clases de auditoría predefinidas (Continuación)

Clase de auditoría	Nombre descriptivo	Descripción
am	administrative	Acciones administrativas (metaclase)
ss	system state	Cambio de estado de sistema
as	system-wide administration	Administración en todo el sistema
ua	user administration	Administración de usuarios
aa	audit administration	Utilización de auditoría
ps	process start	Inicio de proceso y detención de proceso
pm	process modify	Modificación de proceso
pc	process	Proceso (metaclase)
ex	exec	Ejecución de programa
io	ioctl	Llamada de sistema <code>ioctl()</code>
ip	ipc	Operaciones de System V IPC
lo	login_logout	Eventos de inicio y cierre de sesión
nt	network	Eventos de red: bind, connect, accept
ot	other	Otros, por ejemplo, asignación de dispositivos y <code>mknod()</code>

Puede definir nuevas clases si modifica el archivo `/etc/security/audit_class`. También puede cambiar el nombre de clases existentes. Para obtener más información, consulte la página del comando `man audit_class(4)`.

## Sintaxis de la clase de auditoría

Los eventos se pueden auditar para determinar si son correctos, si tienen fallos o ambas cosas. Sin un prefijo, una clase de eventos se audita para determinar si es correcta o si falló. Con un prefijo de signo más (+), se audita una clase de eventos únicamente para determinar si son correctos. Con un prefijo de signo menos (-), se audita una clase de los eventos únicamente para determinar si tienen fallos. La siguiente tabla muestra algunas posibles representaciones de las clases de auditoría.



TABLA 31-2 Prefijos con signo más y signo menos para clases de auditoría

[prefijo] clase	Explicación
lo	Permite auditar todos los intentos correctos para iniciar sesión y cerrar sesión, y todos los intentos fallidos para iniciar sesión. Un usuario no puede fallar en un intento para cerrar sesión.
+lo	Permite auditar todos los intentos correctos para iniciar y cerrar una sesión.
-all	Permite auditar todos los eventos con fallos.
+all	Permite auditar todos los eventos correctos.



**Precaución** – La clase `all` puede generar grandes cantidades de datos y llenar rápidamente los sistemas de archivos de auditoría. Utilice la clase `all` sólo si se tienen motivos extraordinarios para auditar todas las actividades.

Las clases de auditoría previamente seleccionadas pueden seguir modificándose con un prefijo de acento circunflejo, `^`. La siguiente tabla muestra cómo el prefijo de acento circunflejo modifica una clase de auditoría preseleccionada.

TABLA 31-3 Prefijo de acento circunflejo que modifica clases de auditoría ya especificadas

<code>^[prefijo]clase</code>	Explicación
<code>-all, ^-fc</code>	Permite auditar todos los eventos con fallos, excepto los intentos con fallos para crear objetos de archivo que no se deben auditar
<code>am, ^+aa</code>	Permite auditar todos los eventos administrativos para determinar si son correctas o si fallaron, excepto los intentos correctos de administración de auditoría que no se deben auditar
<code>am, ^ua</code>	Permite auditar todos los eventos administrativos para determinar si son correctas o si fallaron, excepto los eventos administración de usuarios que no se deben auditar

Las clases de auditoría y sus prefijos se pueden utilizar en los siguientes archivos y comandos:

- En la línea `flags` en el archivo `audit_control`
- En la línea `plugin:name=audit_syslog.so; p_flags=` en el archivo `audit_control`
- En la entrada del usuario en la base de datos `audit_user`
- Como argumentos para las opciones de comando `auditconfig`

Consulte “[Archivo `audit\_control`](#)” en la [página 673](#) para obtener un ejemplo de cómo usar los prefijos en el archivo `audit_control`.

## Complementos de auditoría

Los complementos de auditoría especifican cómo manejar los registros de auditoría en la cola de auditoría. Los complementos de auditoría se especifican por nombre en el archivo `audit_control: audit_binfile.so` y `audit_syslog.so`. Los complementos y sus parámetros pueden especificar lo siguiente:

- Dónde se deben enviar los datos binarios, mediante el complemento `audit_binfile.so`, parámetro `p_dir`
- El mínimo espacio que queda en un disco antes de que el administrador obtenga una advertencia, mediante el complemento `audit_binfile.so`, parámetro `p_minfree`
- El tamaño máximo de un archivo de auditoría, mediante el complemento `audit_binfile.so`, parámetro `p_fsize`

El complemento de parámetro `p_fsize` está disponible hasta la versión Solaris 10 10/08.

- Una selección de registros de auditoría que se enviará a `syslog` mediante el complemento `audit_syslog.so`, parámetro `p_flags`
- El número máximo de registros de auditoría que se ponen en cola para el complemento, mediante el parámetro `qsize`

Consulte las páginas del comando `man audit_binfile(5)`, `audit_syslog(5)` y `audit_control(4)`.

## Política de auditoría

La política de auditoría determina si se agrega información adicional a la pista de auditoría.

Las siguientes políticas agregan tokens a los registros de auditoría: `arge`, `argv`, `group`, `path`, `seq`, `trail`, `windata_down`, `windata_up` y `zonename`.

Las políticas restantes no agregan tokens. Las políticas `ahlt` y `cnt` determinan qué sucede si los registros de auditoría del núcleo no se pueden entregar, la política `public` limita la auditoría de los archivos públicos y la política `perzone` establece colas de auditoría separadas para las zonas no globales.

Los efectos de las diferentes opciones de políticas de auditoría se describen en “[Determinación de política de auditoría](#)” en la página 605. Para obtener una descripción de las opciones de política de auditoría, consulte la opción `-setpolicy` en la página del comando `man auditconfig(1M)`. Para obtener una lista de las opciones de política disponibles, ejecute el comando `auditconfig -lspolicy`.

## Características de auditoría de proceso

Las siguientes características de auditoría se definen en el primer inicio de sesión:

- **Máscara de preselección de proceso:** una combinación de las clases de auditoría del archivo `audit_control` y la base de datos `audit_user`. Cuando un usuario inicia sesión, el proceso de inicio de sesión combina las clases preseleccionadas para establecer la *máscara de preselección de proceso* para los procesos del usuario. La máscara de preselección de proceso especifica si los eventos en cada clase de auditoría van a generar registros de auditoría.

El siguiente algoritmo describe el modo en que el sistema obtiene la máscara de preselección de proceso del usuario:

`(flags line + always-audit-classes) - never-audit-classes`

Agregue las clases de auditoría de la línea `flags` en el archivo `audit_control` a las clases del campo *siempre\_auditar\_clases* en la entrada del usuario en la base de datos `audit_user`. Luego, reste del total las clases del campo *nunca\_auditar\_clases* del usuario.

- **ID de auditoría:** un proceso adquiere un ID de auditoría cuando el usuario inicia sesión. El ID de auditoría es heredado por todos los procesos secundarios comenzados por el proceso inicial del usuario. El ID de auditoría ayuda a aplicar responsabilidad. Incluso después de que un usuario se convierta en usuario `root`, el ID de auditoría sigue siendo el mismo. El ID de auditoría que se guarda en cada registro de auditoría siempre le permite rastrear acciones hasta el usuario original que inició sesión.
- **ID de sesión de auditoría:** el ID de sesión de auditoría se asigna cuando se inicia sesión. El ID de sesión es heredado por todos los procesos secundarios.
- **ID de terminal (ID de puerto, dirección de equipo):** el ID de terminal está formado por el nombre del host y la dirección de Internet, seguidos por un número único que identifica el dispositivo físico en el que inició sesión el usuario. La mayoría de las veces, el inicio de sesión es a través de la consola. El número que corresponde al dispositivo de la consola es 0.

## Pista de auditoría

La *pista de auditoría* contiene archivos de auditoría binarios. La pista se crea mediante el daemon `auditt`. Una vez que el servicio de auditoría se haya habilitado con el comando `order bsmconv`, el daemon `auditt` arranca cuando se inicia el sistema. El daemon `auditt` es responsable de recolectar los datos de la pista de auditoría y escribir los registros de auditoría.

Los registros de auditoría se almacenan en formato binario en los sistemas de archivos dedicados a los archivos de auditoría. Aunque se pueden ubicar físicamente directorios de auditoría en sistemas de archivos que no están dedicados a la auditoría, *no lo haga*, salvo para los directorios de último recurso. Los directorios de último recurso son directorios en los que los archivos de auditoría se escriben sólo cuando no hay ningún otro directorio adecuado disponible.

Existe otro escenario en el que ubicar directorios de auditoría fuera de los sistemas de archivos de auditoría dedicados puede ser aceptable. Puede hacerlo en un entorno de desarrollo de software en el que la auditoría sea opcional. Utilizar por completo el espacio en disco puede ser más importante que mantener una pista de auditoría. Sin embargo, en un entorno en el que la seguridad es una preocupación, colocar directorios de auditoría en otros sistemas de archivos no es aceptable.

También debe tener en cuenta los siguientes factores al administrar sistemas de archivos de auditoría:

- Un host debe tener al menos un directorio de auditoría local. El directorio local se puede utilizar como un directorio de último recurso si el host no se puede comunicar con el servidor de auditoría.
- Monte los directorios de auditoría con la opción de lectura-escritura (*rw*). Al montar directorios de auditoría de forma remota, use también las opciones *intr* y *noac*.
- Visualice los sistemas de archivos de auditoría en el servidor de auditoría en el que residen. La lista de exportación debería incluir todos los sistemas que se están auditando en la ubicación.

## Convenciones de nombres de archivos de auditoría binarios

Cada archivo de auditoría binario es una recopilación de registros autocontenidos. El nombre del archivo identifica el período durante el cual los registros se generaron y el sistema que los generó.

### Nombres de archivos de auditoría binarios

Los archivos de auditoría completos tienen la siguiente forma:

*start-time.end-time.system*

*hora\_inicio*      Es la hora en la que se generó el primer registro de auditoría en el archivo de auditoría

*hora\_fin*          Es la hora en la que se escribió el último registro en el archivo

*sistema*          Es el nombre del sistema que generó el archivo

Un archivo de auditoría que sigue estando activo tiene un nombre con la siguiente forma:

*start-time.not\_terminated.system*

Para obtener ejemplos de nombres de archivos de auditoría *not\_terminated* y cerrados, consulte [“Cómo depurar un archivo de auditoría \*not\\_terminated\*” en la página 649](#).

## Indicadores de hora de archivos de auditoría binarios

Los indicadores de hora en los nombres de los archivos son usados por el comando `auditreduce` para ubicar los registros dentro de un rango horario específico. Estos indicadores de hora son importantes porque puede haber una acumulación mensual o mayor de archivos de auditoría en línea. Buscar todos los archivos de registros generados en las últimas 24 horas sería demasiado costoso.

Las indicaciones *hora\_inicio* y *hora\_fin* son indicaciones de hora con una resolución de un segundo. Están especificadas según la hora del meridiano de Greenwich (GMT). El formato está compuesto por los cuatro dígitos del año, seguido por dos dígitos para cada mes, día, hora, minuto y segundo, de la siguiente manera:

YYYYMMDDHHMMSS

Estos indicadores de hora están en GMT para asegurarse de que estén en el orden correcto, incluso en distintas zonas horarias. Como están en GMT, para que la fecha y la hora sean significativas, se deben convertir según la zona horaria. Tenga en cuenta este punto siempre que manipule estos archivos con los comandos de archivo estándar en lugar de utilizar el comando `auditreduce`.

## Estructura de registro de auditoría

Un registro de auditoría es una secuencia de tokens de auditoría. Cada token de auditoría contiene información del evento, como ID de usuario, hora y fecha. Un token header comienza un registro de auditoría, y un token opcional trailer, lo concluye. Otras tokens de auditoría contienen información relevante para el evento de auditoría. La siguiente figura muestra un registro típico de auditoría.

FIGURA 31-3 Estructura típica de registro de auditoría

Token header
Token arg
Token data
Token subject
Token return

## Análisis de registro de auditoría

El análisis de registro de auditoría incluye postseleccionar los registros de la pista de auditoría. Puede utilizar uno de estos dos métodos para analizar los datos binarios recopilados.

- Puede analizar las secuencias de datos binarios. Para analizar la secuencia de datos, necesita saber el orden de los campos de cada token y el orden de los tokens en cada registro. También necesita conocer las variantes de un registro de auditoría. Por ejemplo, la llamada de sistema `ioctl()` crea un registro de auditoría para “nombre de archivo incorrecto” que contiene diferentes tokens del registro de auditoría para “descriptor de archivo no válido”.
  - Para obtener una descripción del orden de los datos binarios en cada token de auditoría, consulte la página del comando `man audit.log(4)`.
  - Para obtener una descripción del orden de los tokens en un registro de auditoría, use el comando `bsmrecord`. La salida del comando `bsmrecord` incluye los diferentes formatos que se producen en diferentes condiciones. Los corchetes `[ ]` indican que un token de auditoría es opcional. Para más información, consulte la página del comando `man bsmrecord(1M)`. Para obtener más ejemplos, consulte también “[Cómo visualizar formatos de registros de auditoría](#)” en la [página 641](#).
- Puede utilizar para ello el comando `praudit`. Las opciones para el comando proporcionan diferentes salidas de texto. Por ejemplo, el comando `praudit -x` proporciona XML para introducir en secuencias de comandos y exploradores. Las salidas de `praudit` no incluyen campos cuyo único propósito es ayudar a analizar los datos binarios. Los valores de salida no siguen necesariamente el orden de los campos binarios. Además, el orden y el formato de la salida de `praudit` no están garantizados entre las versiones de Oracle Solaris.

Para obtener ejemplos de la salida `praudit`, consulte “[Cómo visualizar el contenido de los archivos de auditoría binarios](#)” en la [página 647](#) y la página del comando `man praudit(1M)`.

Para obtener una descripción de la salida de `praudit` para cada token de auditoría, consulte los tokens individuales en la sección “[Formatos de token de auditoría](#)” en la [página 686](#).

## Formatos de token de auditoría

Cada token de auditoría tienen un identificador de tipo de token, que está seguido por los datos específicos para el token. Cada tipo de token tiene su propio formato. La siguiente tabla muestra los nombres de token con una breve descripción de cada uno. Los tokens obsoletos se mantienen por motivos de compatibilidad con las versiones anteriores de Solaris.

TABLA 31–4 Tokens de auditoría para la auditoría de Oracle Solaris

Nombre de token	Descripción	Para obtener más información
<code>acl</code>	Información de lista de Control de Acceso (ACL)	“ <a href="#">Token <code>acl</code></a> ” en la <a href="#">página 688</a>

TABLA 31–4 Tokens de auditoría para la auditoría de Oracle Solaris (Continuación)

Nombre de token	Descripción	Para obtener más información
arbitrary	Datos con información de formato y de tipo	<a href="#">“Token arbitrary (obsoleto)” en la página 688</a>
arg	Valor de argumento de llamada de sistema	<a href="#">“Token arg” en la página 689</a>
attribute	Tokens vnode de archivo	<a href="#">“Token attribute” en la página 690</a>
cmd	Argumentos de comandos y variables de entornos	<a href="#">“Token cmd” en la página 690</a>
exec_args	Argumentos de llamada de sistema exec	<a href="#">“Token exec_args” en la página 691</a>
exec_env	Variables de entorno de llamada de sistema exec	<a href="#">“Token exec_env” en la página 691</a>
exit	Información de salida de programa	<a href="#">“Token exit (obsoleto)” en la página 692</a>
file	Información de archivo de auditoría	<a href="#">“Token file” en la página 692</a>
group	Información de grupos de procesos	<a href="#">“Token group (obsoleto)” en la página 692</a>
groups	Información de grupos de procesos	<a href="#">“Token groups” en la página 692</a>
header	Indica el comienzo del registro de auditoría	<a href="#">“Token header” en la página 693</a>
ip_addr	Dirección de Internet	<a href="#">“Token ip_addr” en la página 694</a>
ip	Información de encabezado IP	<a href="#">“Token ip (obsoleto)” en la página 694</a>
ipc	Información de System V IPC	<a href="#">“Token ipc” en la página 694</a>
ipc_perm	Tokens de objeto de System V IPC	<a href="#">“Token ipc_perm” en la página 695</a>
ipport	Dirección de puerto de Internet	<a href="#">“Token ipport” en la página 696</a>
opaque	Datos no estructurados (sin especificar formato)	<a href="#">“Token opaque (obsoleto)” en la página 696</a>
path	Información de ruta	<a href="#">“Token path” en la página 696</a>
path_attr	Información de ruta de acceso	<a href="#">“Token path_attr” en la página 697</a>
privilege	Información de conjunto de privilegios	<a href="#">“Token privilege” en la página 697</a>
process	Información de token de proceso	<a href="#">“Token process” en la página 698</a>
return	Estado de llamada de sistema	<a href="#">“Token return” en la página 700</a>
sequence	Token de número de secuencia	<a href="#">“Token sequence” en la página 700</a>
socket	Direcciones y tipo de socket	<a href="#">“Token socket” en la página 701</a>
subject	Token subject (tiene el mismo formato que el token process)	<a href="#">“Token subject” en la página 702</a>
text	Cadena ASCII	<a href="#">“Token text” en la página 704</a>
trailer	Indica el final del registro de auditoría	<a href="#">“Token trailer” en la página 704</a>

TABLA 31–4 Tokens de auditoría para la auditoría de Oracle Solaris (Continuación)

Nombre de token	Descripción	Para obtener más información
uauth	Uso de autorización	<a href="#">“Token uauth” en la página 705</a>
upriv	Uso de privilegio	<a href="#">“Token upriv” en la página 705</a>
zonename	Nombre de la zona	<a href="#">“Token zonename” en la página 705</a>

Un registro de auditoría comienza siempre con un token header. El token header indica dónde comienza el registro de auditoría en la pista de auditoría. En el caso de eventos atribuibles, los tokens `subject` y `process` hacen referencia a los valores del proceso que causaron el evento. En el caso de eventos no atribuibles, el token `process` hace referencia al sistema.

## Token `acl`

El token `acl` registra información acerca de las listas de control de acceso (ACL).

El token `acl` está formado por cuatro campos fijos:

- Un ID de token que identifica este token como un token `acl`
- Un campo que especifica el tipo de ACL
- Un campo de valor de ACL
- Un campo en el que se muestran los permisos asociados a esta ACL

El comando `praudit -x` muestra los campos del token `acl`:

```
<acl type="1" value="root" mode="6"/>
```

## Token `arbitrary` (obsoleto)

El token `arbitrary` encapsula datos para la pista de auditoría. Este token está formado por cuatro campos fijos y una matriz de datos. Los campos fijos son los siguientes:

- Un ID de token que identifica este token como un token `arbitrary`
- Un campo de formato de impresión sugerido, por ejemplo, hexadecimal
- Un campo de tamaño de elemento que especifica el tamaño de los datos encapsulados, por ejemplo, pequeño
- Un campo de recuento que proporciona el número de elementos siguientes

El resto del token está compuesto por el *recuento* del tipo especificado. El comando `praudit` muestra el token `arbitrary` de la siguiente manera:

```
arbitrary,decimal,int,1  
42
```



La siguiente tabla muestra los valores posibles del campo de formato de impresión.

**TABLA 31-5** Valores para el campo de formato de impresión de token `arbitrary`

Valor	Acción
AUP_BINARY	Imprime la fecha en formato binario
AUP_OCTAL	Imprime la fecha en formato octal
AUP_DECIMAL	Imprime la fecha en formato decimal
AUP_HEX	Imprime la fecha en formato hexadecimal
AUP_STRING	Imprime la fecha como una cadena

La siguiente tabla muestra los posibles valores del campo de tamaño de elemento.

**TABLA 31-6** Valores para el campo de tamaño de elemento de token `arbitrary`

Valor	Acción
AUR_BYTE	Se imprimen los datos en unidades de bytes en 1 byte
AUR_SHORT	Se imprimen los datos en unidades breves en 2 bytes
AUR_LONG	Se imprimen los datos en unidades extensas en 4 bytes

## Token arg

El token `arg` contiene información sobre los argumentos de una llamada de sistema: el número de argumento de la llamada del sistema, el valor del argumento y una descripción opcional. Este token permite un argumento de llamada de sistema de número entero de 32 bits en un registro de auditoría.

El token `arg` tiene cinco campos:

- Un ID de token que identifica este token como un token `arg`
- Un ID de argumento que indica a qué argumento de llamada de sistema hace referencia el token
- El valor del argumento
- La longitud de la cadena de texto descriptivo
- La cadena de texto

El comando `praudit -x` muestra los campos del token `arg`:

```
<argument arg-num="2" value="0x0" desc="new file uid"/>
```

## Token attribute

El token `attribute` contiene información del vnode del archivo.

El token `attribute` tiene varios campos:

- Un ID de token que identifica este token como un token `attribute`
- El modo de acceso de archivo y el tipo
- El ID de usuario del responsable
- El ID de grupo del responsable
- El ID del sistema de archivos
- El ID del nodo
- El ID del dispositivo que el archivo puede representar

Para obtener más información acerca del ID de sistema de archivos y del ID de dispositivo, consulte la página del comando `man statvfs(2)`.

El token `attribute` por lo general acompaña un token `path`. El token `attribute` se produce durante búsquedas de ruta. Si ocurre un error de búsqueda de ruta, no hay un vnode disponible para obtener la información de archivo necesaria. Por lo tanto, el token `attribute` se encuentra incluido como parte del registro de auditoría. El comando `praudit -x` muestra los campos del token `attribute`:

```
<attribute mode="100644" uid="adm" gid="adm" fsid="136" nodeid="2040" device="0"/>
```

## Token cmd

El token `cmd` registra la lista de argumentos y la lista de variables del entorno asociadas con un comando.

El token `cmd` contiene los siguientes campos:

- Un ID de token que identifica este token como un token `cmd`
- Un recuento de los argumentos del comando
- La lista de argumentos
- La longitud del siguiente campo
- El contenido de los argumentos
- Un recuento de las variables de entorno
- La lista de variables de entorno
- La longitud del siguiente campo
- El contenido de las variables de entorno

El comando `praudit -x` muestra los campos del token `cmd`. El siguiente es un token `cmd` truncado. La línea se ajusta con fines de visualización.

```
<cmd><arg>WINDOWID=6823679</arg>
<arg>COLORTERM=gnome-terminal</arg>
<arg>...LANG=C</arg>...<arg>HOST=machine1</arg>
<arg>LPDEST=printer1</arg>...</cmd>
```

## Token exec\_args

El token `exec_args` registra los argumentos en una llamada de sistema `exec()`. El token `exec_args` tiene dos campos fijos:

- Un campo de ID de token que identifica al token como un token `exec_args`
- Un recuento que representa el número de argumentos que se transfieren a la llamada de sistema `exec()`

El resto de este token se compone de cadenas de *recuento*. El comando `praudit -x` muestra los campos del token `exec_args`:

```
<exec_args><arg>/usr/bin/sh</arg><arg>/usr/bin/hostname</arg></exec_args>
```

---

**Nota** – El token `exec_args` sólo se muestra cuando está activada la opción de política de auditoría `argv`.

---

## Token exec\_env

El token `exec_env` registra las variables de entorno actuales en una llamada de sistema `exec()`. El token `exec_env` tiene dos campos fijos:

- Un campo de ID de token que identifica al token como un token `exec_env`
- Un recuento que representa el número de argumentos que se transfieren a la llamada de sistema `exec()`

El resto de este token se compone de cadenas de *recuento*. El comando `praudit -x` muestra los campos del token `exec_env`. La línea se ajusta con fines de visualización.

```
<exec_env><env>_/usr/bin/hostname</env>
<env>DTXSERVERLOCATION=local</env><env>SESSIONTYPE=altDt</env>
<env>LANG=C</env><env>SDT_NO_TOOLTALK=1</env><env>SDT_ALT_HELLO=/bin/true</env>
<env>PATH=/usr/bin:/usr/openwin/bin:/usr/ucb</env>
<env>OPENWINHOME=/usr/openwin</env><env>LOGNAME=jdoe</env><env>USER=jdoe</env>
<env>DISPLAY=:0</env><env>SHELL=/bin/csh</env><env>START_SPECKEYS=no</env>
<env>SDT_ALT_SESSION=/usr/dt/config/Xsession2.jds</env><env>HOME=/home/jdoe</env>
<env>SDT_NO_DTDBCACHE=1</env><env>PWD=/home/jdoe</env><env>TZ=US/Pacific</env>
</exec_env>
```

---

**Nota** – El token `exec_env` sólo se muestra cuando está activada la opción de política de auditoría `arge`.

---

## Token `exit` (obsoleto)

El token `exit` registra el estado de salida de un programa. El token `exit` contiene los siguientes campos:

- Un ID de token que identifica este token como un token `exit`
- El estado de salida de un programa como se transfirió a la llamada de sistema `exit()`
- Un valor de retorno que describe el estado de salida o que proporciona un error de número de sistema

El comando `praudit` muestra el token `exit` de la siguiente manera:

```
exit,Error 0,0
```

## Token `file`

El token `file` es un token especial generado por el daemon `auditd`. El token marca el inicio de un nuevo archivo de auditoría y el fin de un antiguo archivo de auditoría cuando se desactiva el archivo antiguo. El token `file` inicial identifica el archivo anterior en la pista de auditoría. El token `file` final identifica el archivo siguiente en la pista de auditoría. El daemon `auditd` genera un registro de auditoría especial que contiene este token a fin de “enlazar” sucesivos archivos de auditoría con una pista de auditoría.

El comando `praudit -x` muestra los campos del token `file`. Este token identifica el siguiente archivo en la pista de auditoría. La línea se ajusta con fines de visualización.

```
<file iso8601="2009-04-08 14:18:26.200 -07:00">  
/var/audit/machine1/files/20090408211826.not_terminated.machine1</file>
```

## Token `group` (obsoleto)

Este token se ha sustituido por el token `groups`. Consulte [“Token groups” en la página 692](#).

## Token `groups`

El token `groups` sustituye el token `group`. El token `groups` registra las entradas del grupo de la credencial del proceso.

El token groups tiene dos campos fijos:

- Un campo de ID de token que identifica al token como groups
- Un recuento que representa el número de grupos que figuran en este registro de auditoría

El resto de este token se compone de entradas de grupo de *recuento*.

El comando `praudit -x` muestra los campos del token groups:

```
<group><gid>staff</gid><gid>other</gid></group>
```

---

**Nota** – El token groups sólo se muestra cuando la opción de política de auditoría group está activa.

---

## Token header

El token header es especial en cuanto marca el inicio de un registro de auditoría. El token header se combina con el token trailer para encerrar todos los tokens en el registro.

El token header tiene ocho campos:

- Un campo de ID de token que identifica al token como header
- Un recuento de bytes de la longitud total del registro de auditoría, incluidos los tokens header y trailer
- Un número de versión que identifica la versión de la estructura de registro de auditoría
- El ID de evento de auditoría que identifica el evento de auditoría que representa el registro
- El modificador de ID que identifica características especiales del evento de auditoría

El campo de modificador de ID tiene los siguientes indicadores definidos:

0x4000	PAD_NOTATTR	nonattributable event
0x8000	PAD_FAILURE	failed audit event

- El tipo de dirección, IPv4 o IPv6
- La dirección del equipo
- La fecha y la hora en las que se creó el registro

En sistemas de 64 bits, el token header se muestra con una indicación de hora de 64 bits, en lugar de la indicación de hora de 32 bits.

El comando `praudit` muestra el token header de la siguiente manera:

```
header,69,2,su,,machine1,2009-04-08 13:11:58.209 -07:00
```

El comando `praudit -x` muestra los campos del token header al comienzo del registro de auditoría. La línea se ajusta con fines de visualización.

```
<record version="2" event="su" host="machine1"
iso8601="2009-04-08 13:11:58.209 -07:00">
```

## Token `ip_addr`

El token contiene una dirección de protocolo de Internet `ip_addr`. Desde la versión Solaris 8 la dirección de Internet se puede visualizar en formato de IPv4 o formato de IPv6. La dirección IPv4 utiliza 4 bytes. La dirección IPv6 utiliza 1 byte para describir el tipo de dirección y 16 bytes para describir la dirección.

El token `in_addr` tiene tres campos:

- Un ID de token que identifica este token como un token `in_addr`
- El tipo de dirección IP, IPv4 o IPv6
- Una dirección IP

El comando `praudit -x` muestra el contenido del token `ip_addr`:

```
<ip_address>machine1</ip_address>
```

## Token `ip` (obsoleto)

El token `ip` contiene una copia de un encabezado de protocolo de Internet. El token `ip` tiene dos campos:

- Un ID de token que identifica este token como un token `ip`
- Una copia del encabezado de IP, es decir, todos los 20 bytes

El comando `praudit` muestra el token `ip` de la siguiente manera:

```
ip address,0.0.0.0
```

La estructura del encabezado de IP está definida en el archivo `/usr/include/netinet/ip.h`.

## Token `ipc`

El token `ipc` contiene el identificador de mensaje de System V IPCe, los indicadores de semáforo o el identificador de memoria compartida usado por el emisor de llamada para identificar un objeto IPC determinado.

El token `ipc` tiene tres campos:

- Un ID de token que identifica este token como un token `ipc`
- Un campo de tipo que especifica el tipo de objeto IPC
- El identificador que identifica el objeto IPC

**Nota** – Los identificadores del objeto IPC viola la naturaleza sin contexto de los tokens de auditoría de Oracle Solaris. Ningún “nombre” global identifica de forma exclusiva objetos IPC. En su lugar, los objetos IPC se identifican por sus identificadores. Los identificadores sólo son válidos durante el tiempo que los objetos IPC están activos. Sin embargo, la identificación de los objetos IPC no debería suponer ningún problema. Los mecanismos de System V IPC rara vez se utilizan, y todos los mecanismos comparten la misma clase de auditoría.

La siguiente tabla muestra los posibles valores del campo de tipo de objeto IPC. Los valores se definen en el archivo `/usr/include/bsm/audit.h`.

**TABLA 31-7** Valores para el campo de tipo de objeto IPC

Nombre	Valor	Descripción
AU_IPC_MSG	1	Objeto de mensaje IPC
AU_IPC_SEM	2	Objeto de semáforo IPC
AU_IPC_SHM	3	Objeto de memoria compartida IPC

El comando `praudit -x` muestra los campos del token `ipc`:

```
<IPC ipc-type="shm" ipc-id="15"/>
```

## Token `ipc_perm`

El token `ipc_perm` contiene una copia de los permisos de acceso de System V IPC. Este token se agrega a los registros de auditoría generados por los eventos de memoria compartida IPC, los eventos de semáforo IPC y los eventos de mensajes IPC.

El token `ipc_perm` tiene ocho campos:

- Un ID de token que identifica este token como un token `ipc_perm`
- El ID de usuario del responsable de IPC
- El ID de grupo del responsable de IPC
- El ID de usuario del creador de IPC
- El ID de grupo del creador de IPC
- El modo de acceso del IPC
- El número de secuencia del IPC
- El valor clave de IPC

El comando `praudit -x` muestra los campos del token `ipc_perm`. La línea se ajusta con fines de visualización.

```
<IPC_perm uid="jdoe" gid="staff" creator-uid="jdoe"
creator-gid="staff" mode="100600" seq="0" key="0x0"/>
```

Los valores se toman de la estructura de `ipc_perm` asociada con el objeto IPC.

## Token iport

El token `iport` contiene las direcciones de los puertos TCP o UDP.

El token `iport` tiene dos campos:

- Un ID de token que identifica este token como un token `iport`
- La dirección de los puertos TCP o UDP

El comando `praudit` muestra el token `iport` de la siguiente manera:

```
ip port,0xf6d6
```

## Token opaque (obsoleto)

El token `opaque` contiene datos sin formato como una secuencia de bytes. El token `opaque` tiene tres campos:

- Un ID de token que identifica este token como un token `opaque`
- Un recuento de bytes de los datos
- Una matriz de datos de byte

El comando `praudit` muestra el token `opaque` de la siguiente manera:

```
opaque,12,0x4f5041515545204441544100
```

## Token path

El token de auditoría `path` contiene información sobre la ruta de acceso para un objeto.

El token `path` contiene los siguientes campos:

- Un ID de token que identifica este token como un token `path`
- La longitud de ruta
- La ruta de acceso absoluta al objeto que se basa en la raíz real del sistema

El comando `praudit` muestra el token `path` sin el segundo campo, de la siguiente manera:

```
path,/etc/security/audit_user
```

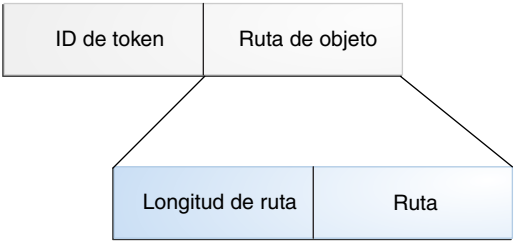
El comando `praudit -x` muestra el contenido del token `path`:



<path>/etc/security/prof\_attr</path>

La siguiente figura muestra el formato de un token path.

FIGURA 31-4 Formato de token path



## Token path\_attr

El token de auditoría `path_attr` contiene información sobre la ruta de acceso para un objeto. La ruta de acceso especifica la secuencia de los objetos de archivo de atributos en el objeto de token path. Las llamadas de sistema, como `openat()`, permiten acceder a los archivos de atributos. Para obtener más información acerca de los objetos de archivo de atributos, consulte la página del comando `man fsattr(5)`.

El token `path_attr` contiene los siguientes campos:

- Un ID de token que identifica este token como un token `path_attr`
- Un recuento que representa el número de secciones de las rutas de los archivos de atributos
- Cadenas con terminación nula *count*

El comando `praudit` muestra el token `path_attr` de la siguiente manera:

```
path_attr,1,attr_file_name
```

## Token privilege

El token `privilege` registra el uso de privilegios en un proceso. El token `privilege` no registra privilegios en la configuración básica. Si un privilegio se ha eliminado del conjunto básico por una acción administrativa, entonces la utilización de ese privilegio se registra. Para obtener más información sobre los privilegios, consulte [“Privilegios \(descripción general\)” en la página 193](#).

El token `privilege` contiene los siguientes campos:

- Un ID de token que identifica este token como un token `privilege`
- La longitud del siguiente campo
- El nombre del conjunto de privilegios

- La longitud del siguiente campo
- La lista de privilegios

El comando `praudit -x` muestra los campos del token `privilege`. La línea se ajusta con fines de visualización.

```
<privilege set-type="Effective">file_chown,file_dac_read,  
file_dac_write,net_privaddr,proc_exec,proc_fork,proc_setid</privilege>
```

## Token process

El token `process` contiene información acerca del usuario asociado con un proceso, como el destinatario de una señal.

El token `process` tiene nueve campos:

- Un ID de token que identifica este token como un token `process`
- El ID de auditoría
- El ID de usuario efectivo
- El ID de grupo efectivo
- El ID de usuario real
- El ID de grupo real
- El ID de proceso
- El ID de sesión de auditoría
- Un ID de terminal que está formado por un ID de dispositivo y una dirección del equipo

Los ID de auditoría, ID de usuario, ID de grupo, ID de proceso e ID de sesión son largos en lugar de ser cortos.

---

**Nota** – Los campos del token `process` para el ID de sesión, el ID de usuario real o el ID de grupo real pueden no estar disponibles. Entonces, el valor se establece en -1.

---

Cualquier token que contiene ID de terminal posee distintas variaciones. El comando `praudit` oculta estas variaciones. Por lo tanto, el ID de terminal se maneja de la misma manera para cualquier token que contiene un ID de terminal. El ID de terminal puede ser una dirección IP y un número de puerto, o un ID de dispositivo. Un ID de dispositivo, como el puerto de serie que está conectado a un módem, puede ser cero. El ID de terminal se especifica en uno de los diversos formatos existentes.

El ID de terminal para los números de dispositivo se especifica de la siguiente manera:

- **Aplicaciones de 32 bits:** un número de dispositivo de 4 bytes, 4 bytes sin usar
- **Aplicaciones de 64 bits:** un número de dispositivo de 8 bytes, 4 bytes sin usar

En las versiones anteriores a la versión Solaris 8, el ID de terminal para números de puerto se asigna de la siguiente manera:

- **Aplicaciones de 32 bits:** un número de puerto de 4 bytes, una dirección de IP de 4 bytes
- **Aplicaciones de 64 bits:** un número de puerto de 8 bytes, una dirección de IP de 4 bytes

Desde la versión Solaris 8, el ID de terminal para números de puerto se especifica de la siguiente manera:

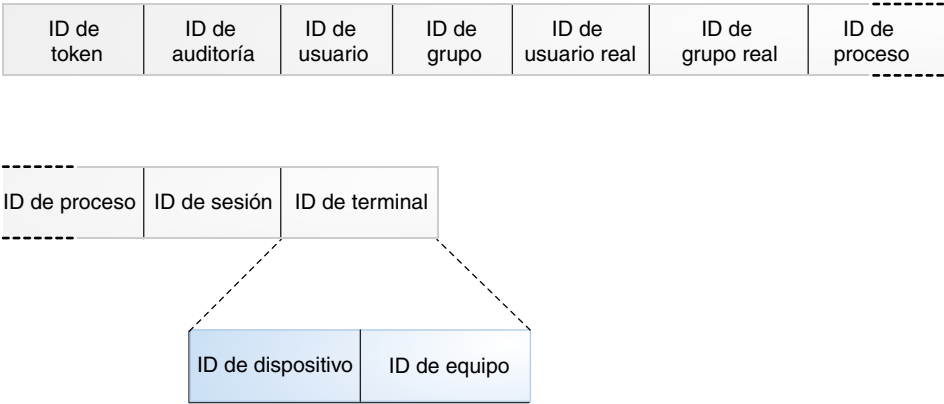
- **32-bit con IPv4:** un número de puerto de 4 bytes, un tipo de IP de 4 bytes, una dirección de IP de 4 bytes
- **32-bit con IPv6:** un número de puerto de 4 bytes, un tipo de IP de 4 bytes, una dirección de IP de 16 bytes
- **64-bit con IPv4:** un número de puerto de 8 bytes, un tipo de IP de 4 bytes, una dirección de IP de 4 bytes
- **64-bit con IPv6:** un número de puerto de 8 bytes, un tipo de IP de 4 bytes, una dirección de IP de 16 bytes

El comando `praudit -x` muestra los campos del token process. La línea se ajusta con fines de visualización.

```
<process audit-uid="-2" uid="root" gid="root" ruid="root"
rgid="root" pid="9" sid="0" tid="0 0 0.0.0.0"/>
```

La siguiente figura muestra el formato de un token process.

FIGURA 31-5 Formato de token process



## Token return

El token return contiene el estado de devolución de la llamada de sistema (`u_error`) y el valor de devolución de proceso (`u_rval1`).

El token return tiene tres campos:

- Un ID de token que identifica este token como un token return
- El estado de error de la llamada de sistema
- El valor de devolución de la llamada de sistema

El token return siempre se devuelve como parte de los registros de auditoría generadas por el núcleo para las llamadas de sistema. En la auditoría de la aplicación, este token indica el estado de salida y otros valores de devolución.

El comando `praudit` muestra el token return para una llamada de sistema de la siguiente manera:

```
return,failure: Operation now in progress,-1
```

El comando `praudit -x` muestra los campos del token return:

```
<return errval="failure: Operation now in progress" retval="-1/">
```

## Token sequence

El token sequence contiene un número de secuencia. El número de secuencia se incrementa cada vez que un registro de auditoría se agregue a la pista de auditoría. Este token es útil para la depuración.

El token sequence tiene dos campos:

- Un ID de token que identifica este token como un token sequence
- Un campo largo no asignado de 32 bits que contiene el número de secuencia

El comando `praudit` muestra el campo del token sequence:

```
sequence, 1292
```

El comando `praudit -x` muestra el contenido del token sequence:

```
<sequence seq-num="1292"/>
```

---

**Nota** – El token sequence sólo se muestra cuando está activada la opción de política de auditoría `seq`.

---

## Token socket

El token socket contiene información que describe un socket de Internet. En algunos casos, el token tiene cuatro campos:

- Un ID de token que identifica este token como un token socket
- Un campo de tipo de socket que indica el tipo de socket al que se hace referencia, TCP, UDP o UNIX
- El puerto local
- La dirección IP local

El comando `praudit` muestra esta instancia del token socket de la siguiente manera:

```
socket, 0x0002, 0x83b1, localhost
```

En la mayoría de los casos, el token tiene ocho campos:

- Un ID de token que identifica este token como un token socket
- El dominio del socket
- Un campo de tipo de socket que indica el tipo de socket al que se hace referencia, TCP, UDP o UNIX
- El puerto local
- El tipo de dirección, IPv4 o IPv6
- La dirección IP local
- El puerto remoto
- La dirección IP remota

Desde la versión Solaris 8 la dirección de Internet se puede visualizar en formato de IPv4 o formato de IPv6. La dirección IPv4 utiliza 4 bytes. La dirección IPv6 utiliza 1 byte para describir el tipo de dirección y 16 bytes para describir la dirección.

El comando `praudit` muestra el token socket de la siguiente manera:

```
socket,0x0002,0x0002,0x83cf,example1,0x2383,server1.Subdomain.Domain.COM
```

El comando `praudit -x` muestra los campos del token socket. La línea se ajusta con fines de visualización.

```
<socket sock_domain="0x0002" sock_type="0x0002" lport="0x83cf"  
laddr="example1" fport="0x2383" faddr="server1.Subdomain.Domain.COM"/>
```

## Token subject

El token subject describe un usuario que lleva a cabo o intenta llevar a cabo una operación. El formato es el mismo que el del token process.

El token subject tiene nueve campos:

- Un ID de token que identifica este token como un token subject
- El ID de auditoría
- El ID de usuario efectivo
- El ID de grupo efectivo
- El ID de usuario real
- El ID de grupo real
- El ID de proceso
- El ID de sesión de auditoría
- Un ID de terminal que está formado por un ID de dispositivo y una dirección IP del equipo

Los ID de auditoría, ID de usuario, ID de grupo, ID de proceso e ID de sesión son largos en lugar de ser cortos.

---

**Nota** – Los campos del token subject para el ID de sesión, el ID de usuario real o el ID de grupo real pueden no estar disponibles. Entonces, el valor se establece en -1.

---

Cualquier token que contiene ID de terminal posee distintas variaciones. El comando `praudit` oculta estas variaciones. Por lo tanto, el ID de terminal se maneja de la misma manera para cualquier token que contiene un ID de terminal. El ID de terminal puede ser una dirección IP y un número de puerto, o un ID de dispositivo. Un ID de dispositivo, como el puerto de serie que está conectado a un módem, puede ser cero. El ID de terminal se especifica en uno de los diversos formatos existentes.

El ID de terminal para los números de dispositivo se especifica de la siguiente manera:

- **Aplicaciones de 32 bits:** un número de dispositivo de 4 bytes, 4 bytes sin usar
- **Aplicaciones de 64 bits:** un número de dispositivo de 8 bytes, 4 bytes sin usar

En las versiones anteriores a la versión Solaris 8, el ID de terminal para números de puerto se asigna de la siguiente manera:

- **Aplicaciones de 32 bits:** un número de puerto de 4 bytes, una dirección de IP de 4 bytes
- **Aplicaciones de 64 bits:** un número de puerto de 8 bytes, una dirección de IP de 4 bytes

Desde la versión Solaris 8, el ID de terminal para números de puerto se especifica de la siguiente manera:

- **32-bit con IPv4:** un número de puerto de 4 bytes, un tipo de IP de 4 bytes, una dirección de IP de 4 bytes
- **32-bit con IPv6:** un número de puerto de 4 bytes, un tipo de IP de 4 bytes, una dirección de IP de 16 bytes
- **64-bit con IPv4:** un número de puerto de 8 bytes, un tipo de IP de 4 bytes, una dirección de IP de 4 bytes
- **64-bit con IPv6:** un número de puerto de 8 bytes, un tipo de IP de 4 bytes, una dirección de IP de 16 bytes

El token `subject` siempre se devuelve como parte de los registros de auditoría generados por el núcleo para las llamadas de sistema. El comando `praudit` muestra el token `subject` de la siguiente manera:

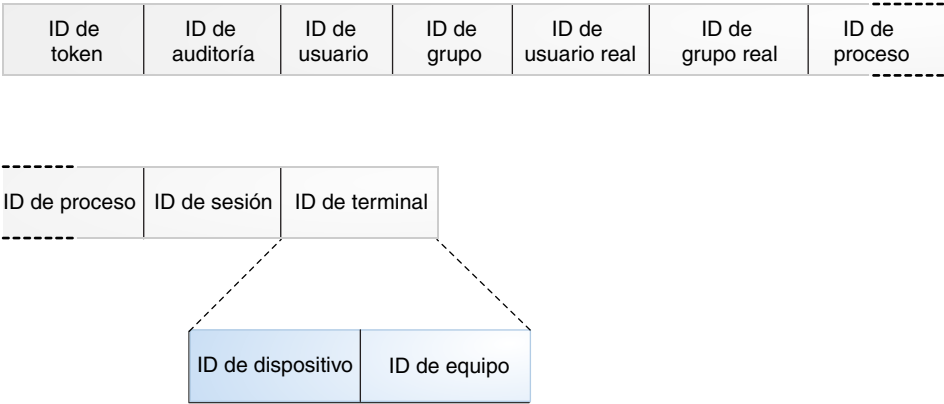
```
subject,jdoe,root,root,root,root,1631,1421584480,8243 65558 machine1
```

El comando `praudit -x` muestra los campos del token `subject`. La línea se ajusta con fines de visualización.

```
<subject audit-uid="jdoe" uid="root" gid="root" ruid="root"
rgid="root" pid="1631" sid="1421584480" tid="8243 65558 machine1"/>
```

La siguiente figura muestra el formato del token `subject`.

FIGURA 31-6 Formato de token subject



## Token text

El token text contiene una cadena de texto.

El token text tiene tres campos:

- Un ID de token que identifica este token como un token text
- La longitud de la cadena de texto
- La cadena de texto propiamente dicha

El comando `praudit -x` muestra el contenido del token text:

```
<text>booting kernel</text>
```

## Token trailer

Los dos tokens, header y trailer, son especiales en cuanto distinguen los puntos finales de un registro de auditoría y encierran todos los demás tokens. Un token header comienza un registro de auditoría. Un token trailer finaliza un registro de auditoría. El token trailer es un token opcional. El token trailer se agrega como el último token de cada registro sólo cuando la opción de política de auditoría `trail` está configurada.

Cuando un registro de auditoría se genera cuando los ubicadores están desactivados, el comando `auditreduce` puede verificar que el ubicador haga referencia correctamente al encabezado del registro. El token trailer admite búsquedas hacia atrás en la pista de auditoría.

El token trailer tiene tres campos:

- Un ID de token que identifica este token como un token trailer
- Un número de relleno para ayudar a marcar el final del registro



- El número total de caracteres en el registro de auditoría, incluidos los tokens header y trailer

El comando `praudit` muestra el token trailer de la siguiente manera:

```
trailer,136
```

## Token uauth

El token uauth registra el uso de la autorización con un comando o acción.

El token uauth contiene los siguientes campos:

- Un ID de token que identifica este token como un token uauth
- La longitud del texto en el siguiente campo
- Una lista de autorizaciones

El comando `praudit` muestra el token uauth de la siguiente manera:

```
use of authorization,solaris.admin.printer.delete
```

## Token upriv

El token upriv registra el uso del privilegio con un comando o acción.

El comando `praudit -x` muestra los campos del token upriv:

```
<use_of_privilege result="successful use of priv">proc_setid</use_of_privilege>
```

## Token zonename

El token zonename registra la zona en la que ocurrió el evento de auditoría. La cadena “global” indica los eventos de auditoría que se producen en la zona global.

El token zonename contiene los siguientes campos:

- Un ID de token que identifica este token como un token zonename
- La longitud del texto en el siguiente campo
- El nombre de la zona

El comando `praudit -x` muestra el contenido del token zonename:

```
<zone name="graphzone"/>
```



# Glosario

---

<b>AES</b>	Advanced Encryption Standard. Una técnica de cifrado de datos en bloques de 128 bits simétricos. En octubre de 2000, el gobierno de los Estados Unidos adoptó la variante Rijndael del algoritmo como estándar de cifrado. AES sustituye el cifrado <a href="#">principal de usuario</a> como estándar gubernamental.
<b>algoritmo</b>	Un algoritmo criptográfico. Se trata de un procedimiento informático establecido que realiza el cifrado o el hashing de una entrada.
<b>algoritmo criptográfico</b>	Consulte <a href="#">algoritmo</a> .
<b>ámbito del servicio de nombres</b>	El ámbito en el que un rol puede operar, es decir, un host individual o todos los hosts gestionados por un servicio de nombres especificado, como NIS, NIS+ o LDAP. Los ámbitos se aplican a las cajas de herramientas de Solaris Management Console.
<b>antememoria de credenciales</b>	Un espacio de almacenamiento (generalmente, un archivo) que contiene credenciales recibidas del KDC.
<b>aplicación con privilegios</b>	Una aplicación que puede sustituir los controles del sistema. La aplicación comprueba los atributos de seguridad, como UID, GID, autorizaciones o privilegios específicos.
<b>archivo de ticket</b>	Consulte <a href="#">antememoria de credenciales</a> .
<b>archivo intermedio</b>	Un archivo intermedio contiene una copia cifrada de la clave maestra para el KDC. Esta clave maestra se utiliza cuando un servidor se reinicia para autenticar automáticamente el KDC antes de que inicie los procesos kadmind y krb5kdc. Dado que el archivo intermedio incluye la clave maestra, el archivo y sus copias de seguridad deben mantenerse en un lugar seguro. Si el cifrado está en peligro, la clave podría utilizarse para acceder o modificar la base de datos del KDC.
<b>archivo keytab</b>	Un archivo de tabla de claves que contiene una o varias claves (principales). Un host o servicio utiliza un archivo keytab de la misma manera que un usuario utiliza una contraseña.
<b>archivos de auditoría</b>	Registros de auditoría binarios. Los archivos de auditoría se almacenan de forma independiente en una partición de auditoría.
<b>asignación de dispositivos</b>	Protección de dispositivos en el nivel de usuario. La asignación de dispositivos restringe el uso exclusivo de un dispositivo a un usuario a la vez. Los datos del dispositivo se depuran antes de volver a utilizar el dispositivo. Las autorizaciones se pueden utilizar para limitar quién tiene permiso para asignar un dispositivo.

<b>atributos de seguridad</b>	En RBAC, sustituciones a la política de seguridad que permiten que un comando administrativo se ejecute correctamente al ser ejecutado por un usuario y no por un superusuario. En el modelo de superusuario, los programas <code>setuid</code> y <code>setgid</code> son atributos de seguridad. Cuando estos atributos se aplican a un comando, el comando se ejecuta correctamente sin importar quién lo ejecuta. En el modelo de privilegios, los atributos de seguridad son privilegios. Cuando un privilegio se otorga a un comando, el comando se ejecuta correctamente. El modelo de privilegios es compatible con el modelo de superusuario, ya que el modelo de privilegios reconoce también los programas <code>setuid</code> y <code>setgid</code> como atributos de seguridad.
<b>autenticación</b>	Proceso de verificación de la identidad reclamada de un principal.
<b>autenticador</b>	Los clientes transfieren autenticadores al solicitar tickets (desde un KDC) y servicios (desde un servidor). Contienen información que se genera mediante una clave de sesión conocida sólo por el cliente y el servidor y que se puede verificar como de origen reciente, lo cual indica que la transacción es segura. Cuando se utiliza con un ticket, un autenticador sirve para autenticar un principal de usuario. Un autenticador incluye el nombre de principal del usuario, la dirección IP del host del usuario y una indicación de hora. A diferencia de un ticket, un autenticador se puede utilizar sólo una vez, generalmente, cuando se solicita acceso a un servicio. Un autenticador se cifra mediante la clave de sesión para ese cliente y ese servidor.
<b>autorización</b>	<ol style="list-style-type: none"> <li>1. En Kerberos, el proceso para determinar si un principal puede utilizar un servicio, a qué objetos puede acceder el principal y el tipo de acceso permitido para cada objeto.</li> <li>2. En el control de acceso basado en roles (RBAC), un permiso que se puede asignar a un rol o a un usuario (o que está incrustado en un perfil de derechos) para realizar una clase de acciones que, de lo contrario, están prohibidas por la política de seguridad.</li> </ol>
<b>Blowfish</b>	Algoritmo cifrado de bloques simétricos con una clave de tamaño variable que va de 32 a 448 bits. Bruce Schneier, su creador, afirma que Blowfish se optimiza en el caso de aplicaciones en que la clave se modifica con poca frecuencia.
<b>cifrado de clave privada</b>	En el cifrado de clave privada, el remitente y receptor utilizan la misma clave para el cifrado. Consulte también <a href="#">cifrado de clave pública</a> .
<b>cifrado de clave pública</b>	Un esquema de cifrado en el que cada usuario tiene dos claves, una clave pública y una clave privada. En el cifrado de clave pública, el remitente utiliza la clave pública del receptor para cifrar el mensaje y el receptor utiliza una clave privada para descifrarlo. El servicio Kerberos es un sistema de clave privada. Consulte también <a href="#">cifrado de clave privada</a> .

<b>clave</b>	<p>1. Generalmente, uno de los dos tipos principales de claves:</p> <ul style="list-style-type: none"> <li>■ <i>Clave simétrica</i>: una clave de cifrado que es idéntica a la clave de descifrado. Las claves simétricas se utilizan para cifrar archivos.</li> <li>■ <i>Claves asimétrica o clave pública</i>: una clave que se utiliza en algoritmos de clave pública, como Diffie-Hellman o RSA. Las claves públicas incluyen una clave privada que sólo conoce un usuario, una clave pública utilizada por el servidor o recurso general y un par de claves privada-pública que combina ambas. La clave privada también se denomina clave <i>secreta</i>. La clave pública también se denomina clave <i>compartida</i> o clave <i>común</i>.</li> <li>■ 2. Una entrada (nombre de principal) en un archivo keytab. Consulte también <a href="#">archivo keytab</a>.</li> </ul> <p>3. En Kerberos, una clave de cifrado, que puede ser de tres tipos:</p> <ul style="list-style-type: none"> <li>■ <i>Clave privada</i>: una clave de cifrado que comparten un principal y el KDC, y que se distribuye fuera de los límites del sistema. Consulte también <a href="#">clave privada</a>.</li> <li>■ <i>Clave de servicio</i>: esta clave tiene el mismo propósito que la clave privada, pero la utilizan servidores y servicios. Consulte también <a href="#">clave de servicio</a>.</li> <li>■ <i>Clave de sesión</i>: una clave de cifrado temporal que se utiliza entre dos principales y cuya duración se limita a la duración de una única sesión de inicio. Consulte también <a href="#">clave de sesión</a>.</li> </ul>
<b>clave de servicio</b>	Una clave de cifrado que se comparte entre un principal de servicio y el KDC, y se distribuye fuera de los límites del sistema. Consulte también <a href="#">clave</a> .
<b>clave de sesión</b>	Una clave generada por el servicio de autenticación o el servicio de otorgamiento de tickets. Una clave de sesión se genera para proporcionar transacciones seguras entre un cliente y un servicio. La duración de una clave de sesión está limitada a una única sesión de inicio. Consulte también <a href="#">clave</a> .
<b>clave privada</b>	Una clave que se asigna a cada principal de usuario y que sólo conocen el usuario del principal y el KDC. Para los principales de usuario, la clave se basa en la contraseña del usuario. Consulte también <a href="#">clave</a> .
<b>clave secreta</b>	Consulte <a href="#">clave privada</a> .
<b>cliente</b>	<p>De manera restringida, un proceso que utiliza un servicio de red en nombre de un usuario; por ejemplo, una aplicación que utiliza <code>rlogin</code>. En algunos casos, un servidor puede ser el cliente de algún otro servidor o servicio.</p> <p>De manera más amplia, un host que: a) recibe una credencial de Kerberos y b) utiliza un servicio proporcionado por un servidor.</p> <p>Informalmente, un principal que utiliza un servicio.</p>
<b>código de autenticación de mensajes (MAC)</b>	MAC proporciona seguridad en la integridad de los datos y autentica el origen de los datos. MAC no proporciona protección contra intromisiones externas.
<b>confidencialidad</b>	Consulte <a href="#">privacidad</a> .

<b>conjunto básico</b>	El conjunto de privilegios asignados al proceso de un usuario en el momento de inicio de sesión. En un sistema sin modificaciones, cada conjunto heredable inicial del usuario es equivalente al conjunto básico en el inicio de sesión.
<b>conjunto de privilegios</b>	<p>Una recopilación de privilegios. Cada proceso tiene cuatro conjuntos de privilegios que determinan si un proceso puede utilizar un privilegio determinado. Consulte <a href="#">límite definido</a>, <a href="#">conjunto vigente set</a>, <a href="#">conjunto permitido set</a> y <a href="#">conjunto heredable set</a>.</p> <p>Además, el <a href="#">conjunto básico</a> de privilegios es la recopilación de privilegios asignados al proceso de un usuario en el momento de inicio de sesión.</p>
<b>conjunto heredable</b>	El conjunto de privilegios que un proceso puede heredar a través de una llamada a <code>exec</code> .
<b>conjunto permitido</b>	El conjunto de privilegios que están disponibles para que utilice un proceso.
<b>conjunto vigente</b>	El conjunto de privilegios que actualmente están vigentes en un proceso.
<b>consumidor</b>	En la estructura criptográfica de Oracle Solaris, un consumidor es un usuario de los servicios criptográficos prestados por los proveedores. Los consumidores pueden ser aplicaciones, usuarios finales u operaciones de núcleo. Kerberos, IKE e IPsec son ejemplos de consumidores. Para ver ejemplos de proveedores, consulte <a href="#">proveedor</a> .
<b>credencial</b>	Un paquete de información que incluye un ticket y una clave de sesión coincidente. Se utiliza para autenticar la identidad de un principal. Consulte también <a href="#">ticket</a> , <a href="#">clave de sesión</a> .
<b>DES</b>	Siglas en inglés de Data Encryption Standard, estándar de cifrado de datos. Un método de cifrado de claves simétricas que se desarrolló en 1975 y que la ANSI estandarizó en 1981 como ANSI X.3.92. DES utiliza una clave de 56 bits.
<b>desfase de reloj</b>	La cantidad máxima de tiempo que pueden diferir los relojes del sistema interno de todos los hosts que participan en el sistema de autenticación Kerberos. Si el sesgo de reloj se excede entre cualquiera de los hosts participantes, las solicitudes se rechazan. El desfase de reloj se puede especificar en el archivo <code>krb5.conf</code> .
<b>dominio</b>	<ol style="list-style-type: none"><li>1. La red lógica gestionada por una única base de datos de Kerberos y un juego de centros de distribución de claves (KDC).</li><li>2. La tercera parte de un nombre de principal. Para el nombre de principal <code>jdoe/admin@ENG.EXAMPLE.COM</code>, el dominio es <code>ENG.EXAMPLE.COM</code>. Consulte también <a href="#">nombre de principal</a>.</li></ol>
<b>DSA</b>	Siglas en inglés de Digital Signature Algorithm, algoritmo de firma digital. Algoritmo de clave pública con un tamaño de clave variable que va de 512 a 4096 bits. DSS, el estándar del gobierno de los Estados Unidos, llega hasta los 1024 bits. DSA se basa en el algoritmo <a href="#">SHA1</a> para las entradas.
<b>elemento inicial</b>	Un iniciador numérico para generar números aleatorios. Cuando el iniciador comienza desde un origen aleatorio, el elemento inicial se denomina <i>elemento inicial aleatorio</i> .
<b>escalonamiento de privilegios</b>	Obtención de acceso a recursos que se encuentran fuera del rango de recursos permitidos por los atributos de seguridad asignados, incluidas las sustituciones. Como resultado, un proceso puede realizar acciones no autorizadas.

<b>evento asíncrono de auditoría</b>	Los eventos asíncronos constituyen la minoría de los eventos del sistema. Estos eventos no están asociados con ningún proceso; por lo tanto, no hay procesos disponibles para bloquear y reactivar más adelante. Los eventos de inicio del sistema y entrada y salida de la PROM son ejemplos de eventos asíncronos.
<b>evento de auditoría no atribuible</b>	Un evento de auditoría cuyo iniciador no se puede determinar, como el evento AUE_BOOT.
<b>evento síncrono de auditoría</b>	La mayoría de los eventos de auditoría. Estos eventos están asociados con un proceso en el sistema. Un evento no atribuible que está asociado con un proceso es un evento síncrono, como un error de inicio de sesión.
<b>FQDN</b>	Siglas en inglés de Fully Qualified Domain Name, nombre de dominio completo. Por ejemplo, <code>central.example.com</code> (en lugar de simplemente <code>denver</code> ).
<b>frase de contraseña</b>	Una frase que se utiliza para verificar que una clave privada haya sido creada por el usuario de la frase de contraseña. Una buena frase de contraseña tiene una longitud de 10 a 30 caracteres, combina caracteres alfabéticos y numéricos, y evita el texto y los nombres simples. Se le pedirá la frase de contraseña para autenticar el uso de la clave privada para cifrar y descifrar comunicaciones.
<b>GSS-API</b>	Generic Security Service Application Programming Interface. Una capa de red que proporciona apoyo para diversos servicios de seguridad modulares, incluido el servicio Kerberos. GSS-API proporciona servicios de privacidad, integridad y autenticación de seguridad. Consulte también <a href="#">autenticación</a> , <a href="#">integridad</a> , <a href="#">privacidad</a> .
<b>host</b>	Un sistema al que se puede acceder a través de una red.
<b>imagen de único sistema</b>	Una imagen de único sistema se utiliza en la auditoría Oracle Solaris para describir un grupo de sistemas auditados que utilizan el mismo servicio de nombres. Estos sistemas envían sus registros de auditoría a un servidor de auditoría central, donde los registros se pueden comparar como si procedieran de un sistema.
<b>instancia</b>	La segunda parte de un nombre de principal; una instancia cualifica la primera parte del nombre de principal. En el caso de un principal de servicio, la instancia es obligatoria. La instancia es el nombre de dominio completo del host, como en <code>host/central.example.com</code> . Para los principales de usuario, una instancia es opcional. Sin embargo, tenga en cuenta que <code>jdoe</code> y <code>jdoe/admin</code> son principales únicos. Consulte también <a href="#">nombre primario</a> , <a href="#">nombre de principal</a> , <a href="#">principal de servidor</a> , <a href="#">principal de usuario</a> .
<b>integridad</b>	Un servicio de seguridad que, además de la autenticación del usuario, permite validar los datos transmitidos mediante una suma de comprobación criptográfica. Consulte también <a href="#">autenticación</a> , <a href="#">privacidad</a> .
<b>KDC</b>	<p>Siglas en inglés de Key Distribution Center, centro de distribución de claves. Un equipo que tiene tres componentes Kerberos V5:</p> <ul style="list-style-type: none"> <li>■ Base de datos de claves y principal</li> <li>■ Servicio de autenticación</li> <li>■ Servicio de otorgamiento de tickets</li> </ul> <p>Cada dominio tiene un KDC maestro y debe tener uno o varios KDC esclavos.</p>
<b>KDC esclavo</b>	Una copia de un KDC maestro, que es capaz de realizar la mayoría de las funciones del maestro. Cada dominio, generalmente, tiene varios KDC esclavos (y un solo KDC maestro). Consulte también <a href="#">KDC</a> , <a href="#">KDC maestro</a> .

<b>KDC maestro</b>	El KDC maestro en cada dominio, que incluye un servidor de administración Kerberos, kadmind, y un daemon de otorgamiento de tickets y autenticación, krb5kdc. Cada dominio debe tener al menos un KDC maestro y puede tener varios KDC duplicados, o esclavos, que proporcionan servicios de autenticación a los clientes.
<b>Kerberos</b>	<p>Un servicio de autenticación, el protocolo utilizado por ese servicio o el código utilizado para implementar ese servicio.</p> <p>La implementación de Oracle Solaris Kerberos que está estrechamente basada en la implementación de Kerberos V5.</p> <p>Aunque son técnicamente diferentes, "Kerberos" y "Kerberos V5" suelen utilizarse de forma indistinta en la documentación de Kerberos.</p> <p>En la mitología griega, Kerberos (también escrito Cerberus) era un mastín feroz de tres cabezas que protegía las puertas de Hades.</p>
<b>kvno</b>	Siglas en inglés de Key Version Number, número de versión de clave. Un número de secuencia que realiza un seguimiento de una clave determinada en orden de generación. El kvno más alto corresponde a la clave más reciente y actual.
<b>límite definido</b>	El límite exterior que indica qué privilegios están disponibles para un proceso y sus procesos secundarios.
<b>Lista de control de acceso (ACL, Access Control List)</b>	Una lista de control de acceso (ACL) proporciona un nivel de seguridad de archivos más específico que la protección de archivos UNIX tradicionales. Por ejemplo, una ACL permite autorizar el acceso de lectura de grupo a un archivo, pero permitir que un solo miembro de ese grupo escriba en el archivo.
<b>MAC</b>	<ol style="list-style-type: none"><li>1. Consulte <a href="#">código de autenticación de mensajes (MAC)</a>.</li><li>2. También se denomina etiquetado. En la terminología de seguridad gubernamental, MAC significa control de acceso obligatorio (del inglés Mandatory Access Control). Etiquetas como Top Secret y Confidential son ejemplos de MAC. MAC se diferencia de DAC, que significa control de acceso discrecional (del inglés Discretionary Access Control). Los permisos UNIX son un ejemplo de DAC.</li><li>3. En hardware, la dirección única del sistema en una LAN. Si el sistema está en una Ethernet, la dirección MAC es la dirección Ethernet.</li></ol>
<b>MD5</b>	Una función de hash criptográfica iterativa utilizada para autenticar mensajes, incluso las firmas digitales. Rivest desarrolló esta función en 1991.
<b>mecanismo</b>	<ol style="list-style-type: none"><li>1. Un paquete de software que especifica técnicas criptográficas para lograr la autenticación o confidencialidad de los datos. Ejemplos: clave pública Diffie-Hellman, Kerberos V5.</li><li>2. En la estructura criptográfica de Oracle Solaris, la implementación de un algoritmo para un propósito determinado. Por ejemplo, un mecanismo DES que se aplica a la autenticación, como CKM_DES_MAC, es un mecanismo distinto de un mecanismo DES que se aplica al cifrado, CKM_DES_CBC_PAD.</li></ol>
<b>mecanismo de seguridad</b>	Consulte <a href="#">mecanismo</a> .



<b>minimización</b>	La instalación del sistema operativo mínimo necesario para ejecutar el servidor. Cualquier software que no se relacione directamente con el funcionamiento del servidor no se instala o se elimina después de la instalación.
<b>modelo de privilegios</b>	Un modelo de seguridad más estricto en un sistema informático que el modelo de superusuario. En el modelo de privilegios, los procesos requieren un privilegio para ejecutarse. La administración del sistema se puede dividir en partes discretas que se basan en los privilegios que los administradores tienen en sus procesos. Los privilegios se pueden asignar al proceso de inicio de sesión de un administrador. O bien, los privilegios se pueden asignar para que estén vigentes para determinados comandos solamente.
<b>modelo de superusuario</b>	El modelo de seguridad UNIX típico en un sistema informático. En el modelo de superusuario, un administrador tiene todo el control del sistema o ningún control (todo o nada). Generalmente, para administrar el equipo, un usuario se convierte en superusuario (root) y puede llevar a cabo todas las actividades administrativas.
<b>Módulo básico de seguridad (BSM, Basic Security Module)</b>	La asignación de dispositivos y el servicio de auditoría de Oracle Solaris. Juntas, estas funciones satisfacen el nivel de seguridad C2.
<b>nombre de principal</b>	1. El nombre de un principal, con el formato <i>nombre primario/instancia@DOMINIO</i> . Consulte también, <a href="#">instancia</a> , <a href="#">nombre primario</a> , <a href="#">dominio</a> . 2. (RPCSEC_GSS API) Consulte <a href="#">principal de cliente</a> , <a href="#">principal de servidor</a> .
<b>nombre primario</b>	La primera parte de un nombre de principal. Consulte también <a href="#">instancia</a> , <a href="#">nombre de principal</a> , <a href="#">dominio</a> .
<b>NTP</b>	Siglas en inglés de Network Time Protocol, protocolo de hora de red. Software de la Universidad de Delaware que permite gestionar la sincronización precisa del tiempo o del reloj de la red, o de ambos, en un entorno de red. Puede usar NTP para mantener el desfase de reloj en un entorno de Kerberos. Consulte también <a href="#">desfase de reloj</a> .
<b>PAM</b>	Siglas en inglés de Pluggable Authentication Module, módulo de autenticación conectable. Una estructura que permite que se utilicen varios mecanismos de autenticación sin que sea necesario recompilar los servicios que los utilizan. PAM permite inicializar la sesión de Kerberos en el momento del inicio de sesión.
<b>partición de auditoría</b>	Una partición de disco duro que está configurada para retener archivos de auditoría.
<b>perfil de derechos</b>	También se denomina derecho o perfil. Una recopilación de sustituciones utilizada en RBAC que se puede asignar a un rol o a un usuario. Un perfil de derechos puede constar de autorizaciones, privilegios, comandos con atributos de seguridad y otros perfiles de derechos.
<b>pista de auditoría</b>	La recopilación de todos los archivos de auditoría de todos los hosts.

<b>política</b>	<p>Generalmente, un plan o curso de acción que influye sobre decisiones y acciones, o las determina. Para los sistemas informáticos, la política suele hacer referencia a la política de seguridad. La política de seguridad de su sitio es el conjunto de reglas que definen la confidencialidad de la información que se está procesando y las medidas que se utilizan para proteger la información contra el acceso no autorizado. Por ejemplo, la política de seguridad puede requerir que se auditen los sistemas, que los dispositivos se protejan con privilegios y que las contraseñas se cambien cada seis semanas.</p> <p>Para la implementación de la política en áreas específicas del SO Oracle Solaris, consulte <a href="#">política de auditoría</a>, <a href="#">política en la estructura criptográfica</a>, <a href="#">política de dispositivos</a>, <a href="#">política Kerberos</a>, <a href="#">política de contraseñas</a> y <a href="#">política RBAC</a>.</p>
<b>política de auditoría</b>	<p>La configuración global y por usuario que determina qué eventos de auditoría se registran. La configuración global que se aplica al servicio de auditoría, generalmente, afecta qué información opcional se incluye en la pista de auditoría. Dos valores, <code>cnt</code> y <code>ahlt</code>, afectan al funcionamiento del sistema cuando se completa la cola de auditoría. Por ejemplo, es posible que la política de auditoría requiera que un número de secuencia forme parte de cada registro de auditoría.</p>
<b>política de contraseñas</b>	<p>Los algoritmos de cifrado que se pueden utilizar para generar contraseñas. También puede referirse a cuestiones más generales sobre las contraseñas, como la frecuencia con la que deben cambiarse las contraseñas, cuántas entradas erróneas se permiten y otras consideraciones de seguridad. La política de seguridad requiere contraseñas. La política de contraseñas requiere que las contraseñas se cifren con el algoritmo MD5 y puede exigir requisitos adicionales relacionados con la seguridad de las contraseñas.</p>
<b>política de dispositivos</b>	<p>Protección de dispositivos en el nivel de núcleo. La política de dispositivos se implementa como dos conjuntos de privilegios en un dispositivo. Un conjunto de privilegios controla el acceso de lectura al dispositivo. El segundo conjunto de privilegios controla el acceso de escritura al dispositivo. Consulte también <a href="#">política</a>.</p>
<b>política de seguridad</b>	<p>Consulte <a href="#">política</a>.</p>
<b>política en la estructura criptográfica</b>	<p>En la estructura criptográfica de Oracle Solaris, la política es la deshabilitación de mecanismos criptográficos existentes. Después de esto, los mecanismos no se pueden utilizar. La política en la estructura criptográfica puede impedir el uso de un mecanismo determinado, como <code>CKM_DES_CBC</code>, de un proveedor, como DES.</p>
<b>política Kerberos</b>	<p>Un conjunto de reglas que rige el uso de contraseñas en el servicio Kerberos. Las políticas pueden regular los accesos de los principales, o los parámetros de tickets, como la duración.</p>
<b>política para tecnologías de clave pública</b>	<p>En la estructura de gestión de claves (KMF), la política es la gestión del uso de certificados. La base de datos de políticas KMF puede limitar el uso de las claves y los certificados administrados por la biblioteca KMF.</p>
<b>política RBAC</b>	<p>La política de seguridad que está asociada a un comando. Actualmente, <code>suser</code> y <code>solaris</code> son las políticas válidas. La política <code>solaris</code> reconoce privilegios, autorizaciones y atributos de seguridad <code>setuid</code>. La política <code>suser</code> reconoce únicamente atributos de seguridad <code>setuid</code>. Los sistemas Trusted Solaris y Trusted Extensions, que pueden interoperar con un sistema Oracle Solaris, proporcionan una política <code>tsol</code>, que reconoce privilegios, atributos de seguridad <code>setuid</code> y etiquetas en los procesos.</p>

<b>principal</b>	<p>1. Un cliente o usuario con un nombre único o una instancia de servidor o servicio que participa en una comunicación de red. Las transacciones de Kerberos implican interacciones entre principales (principales de servicio y principales de usuario) o entre principales y KDC. En otras palabras, un principal es una entidad única a la que Kerberos puede asignar tickets. Consulte también <a href="#">nombre de principal</a>, <a href="#">principal de servidor</a>, <a href="#">principal de usuario</a>.</p> <p>2. (RPCSEC_GSS API) Consulte <a href="#">principal de cliente</a>, <a href="#">principal de servidor</a>.</p>
<b>principal admin</b>	Un principal de usuario con un nombre del tipo <i>nombre de usuario/admin</i> (como en <code>jdoe/admin</code> ). Un principal admin puede tener más privilegios (por ejemplo, para modificar las políticas) que un principal de usuario común. Consulte también <a href="#">nombre de principal</a> , <a href="#">principal de usuario</a> .
<b>principal de cliente</b>	(RPCSEC_GSS API) Un cliente (un usuario o una aplicación) que utiliza los servicios de red RPCSEC_GSS seguros. Los nombres de principales de cliente se almacenan con el formato <code>rpc_gss_principal_t</code> .
<b>principal de host</b>	Una instancia determinada de un principal de servicio en la que el principal (indicado por el nombre principal host) está configurado para proporcionar un rango de servicios de red, como <code>ftp</code> , <code>rcp</code> o <code>rlogin</code> . Un ejemplo de un principal de host principal es <code>host/central.example.com@EXAMPLE.COM</code> . Consulte también <a href="#">principal de servidor</a> .
<b>principal de servidor</b>	(RPCSEC_GSS API) Un principal que proporciona un servicio. El principal de servidor se almacena como una cadena ASCII con el formato <i>servicio@host</i> . Consulte también <a href="#">principal de cliente</a> .
<b>principal de servidor</b>	Un principal que proporciona autenticación Kerberos para un servicio o servicios. Para los principales de servicio, el nombre de principal es el nombre de un servicio, como <code>ftp</code> y su instancia es el nombre de host completo del sistema que proporciona el servicio. Consulte también <a href="#">principal de host</a> , <a href="#">principal de usuario</a> .
<b>principal de usuario</b>	Un principal atribuido a un usuario determinado. El nombre primario de un principal de usuario es un nombre de usuario y su instancia opcional es un nombre que se utiliza para describir el uso que se pretende hacer de las credenciales correspondientes (por ejemplo, <code>jdoe</code> o <code>jdoe/admin</code> ). También se conoce como instancia de usuario. Consulte también <a href="#">principal de servidor</a> .
<b>privacidad</b>	Un servicio de seguridad en el que los datos transmitidos se cifran antes de enviarse. La privacidad también incluye la integridad de los datos y la autenticación de usuario. Consulte también <a href="#">autenticación</a> , <a href="#">integridad</a> , <a href="#">servicio</a> .
<b>privilegio</b>	Un derecho discreto en un proceso de un sistema Oracle Solaris. Los privilegios ofrecen un control más específico de los procesos que <code>root</code> . Los privilegios se definen y se aplican en el núcleo. Para obtener una descripción completa de los privilegios, consulte la página del comando <code>man privileges(5)</code> .
<b>protección</b>	La modificación de la configuración predeterminada del sistema operativo para eliminar las vulnerabilidades de seguridad inherentes al host.
<b>protocolo de Diffie-Hellman</b>	También se lo denomina "criptografía de claves públicas". Se trata de un protocolo de claves criptográficas asimétricas que desarrollaron Diffie y Hellmann en 1976. Este protocolo permite a dos usuarios intercambiar una clave secreta mediante un medio no seguro, sin ningún otro secreto. <b>Kerberos</b> utiliza el protocolo Diffie-Hellman.

<b>proveedor</b>	En la estructura criptográfica de Oracle Solaris, un servicio criptográfico proporcionado a los consumidores. Las bibliotecas PKCS #11, los módulos criptográficos y los aceleradores de hardware son ejemplos de proveedores. Los proveedores se conectan a la estructura criptográfica y también se conocen como <i>complementos</i> . Para ver ejemplos de consumidores, consulte <a href="#">consumidor</a> .
<b>proveedor de hardware</b>	En la estructura criptográfica de Oracle Solaris, un controlador del dispositivo y su acelerador de hardware. Los proveedores de hardware descargan operaciones criptográficas costosas del sistema informático y, de esa manera, liberan los recursos de la CPU para otros usos. Consulte también <a href="#">proveedor</a> .
<b>proveedor de software</b>	En la estructura criptográfica de Oracle Solaris, un módulo de núcleo de software o una biblioteca PKCS #11 que proporciona servicios criptográficos. Consulte también <a href="#">proveedor</a> .
<b>QOP</b>	Siglas en inglés de Quality of Protection, calidad de protección. Un parámetro que se utiliza para seleccionar los algoritmos criptográficos que se utilizan junto con el servicio de integridad o de privacidad.
<b>RBAC</b>	Siglas en inglés de Role-Based Access Control, control de acceso basado en roles. Una alternativa al modelo de superusuario de todo o nada. El RBAC permite que una organización separe las capacidades de superusuario y las asigne a cuentas de usuario especiales denominadas roles. Los roles se pueden asignar a individuos específicos según sus responsabilidades.
<b>red privada virtual (VPN)</b>	Una red que proporciona comunicaciones seguras al utilizar el cifrado y el establecimiento de túneles para conectar usuarios a través de una red pública.
<b>relación</b>	Una variable de configuración o un vínculo definidos en los archivos <code>kdc.conf</code> o <code>krb5.conf</code> .
<b>resumen</b>	Consulte <a href="#">resumen de mensaje</a> .
<b>resumen de mensaje</b>	Un resumen de mensaje es un valor hash que se calcula a partir de un mensaje. El valor hash identifica el mensaje casi de manera exclusiva. Un resumen es útil para verificar la integridad de un archivo.
<b>rol</b>	Una identidad especial para ejecutar aplicaciones con privilegios que sólo los usuarios asignados pueden asumir.
<b>RSA</b>	Método para la obtención de firmas digitales y criptosistemas de claves públicas. Dicho método lo describieron sus creadores, Rivest, Shamir y Adleman, en 1978.
<b>SEAM</b>	Sun Enterprise Authentication Mechanism. El nombre del producto para las versiones iniciales de un sistema para autenticar usuarios de una red, basado en la tecnología Kerberos V5 desarrollada en el Massachusetts Institute of Technology. El producto ahora se denomina servicio Kerberos. SEAM se refiere a las partes del servicio Kerberos que no se incluyeron en las diferentes versiones de Solaris.
<b>Secure Shell</b>	Un protocolo especial para el inicio de sesión remoto seguro y otros servicios de red seguros a través de una red no segura.
<b>servicio</b>	<ol style="list-style-type: none"><li>1. Un recurso proporcionado a clientes de la red, a menudo, por más de un servidor. Por ejemplo, si ejecuta <code>rlogin</code> en el equipo <code>central.example.com</code>, ese equipo es el servidor que proporciona el servicio <code>rlogin</code>.</li><li>2. Un servicio de seguridad (ya sea de integridad o privacidad) que proporciona un nivel de protección más allá de la autenticación. Consulte también <a href="#">integridad</a> y <a href="#">privacidad</a>.</li></ol>

<b>servicio de seguridad</b>	Consulte <a href="#">servicio</a> .
<b>servidor</b>	Un principal que proporciona un recurso a los clientes de la red. Por ejemplo, si ejecuta ssh en el sistema central.example.com, ese sistema es el servidor que proporciona el servicio ssh. Consulte también <a href="#">principal de servidor</a> .
<b>servidor de aplicaciones</b>	Consulte <a href="#">servidor de aplicaciones de red</a> .
<b>servidor de aplicaciones de red</b>	Un servidor que proporciona aplicaciones de red, como ftp. Un dominio puede contener varios servidores de aplicaciones de red.
<b>SHA1</b>	Siglas en inglés de Secure Hashing Algorithm, algoritmo de hash seguro. El algoritmo funciona en cualquier tamaño de entrada que sea inferior a $2^{64}$ para generar un resumen del mensaje. El algoritmo SHA-1 es la entrada de <a href="#">DSA</a> .
<b>shell de perfil</b>	En RBAC, un shell que permite que un rol (o un usuario) ejecute desde la línea de comandos cualquier aplicación con privilegios asignada a los perfiles de derechos del rol. Los shells de perfiles son pfs, pfcs y pfks. Corresponden al shell Bourne (sh), shell C (csh) y shell Korn (ksh), respectivamente.
<b>TGS</b>	Siglas en inglés de Ticket-Granting Service, servicio de otorgamiento de tickets. La parte del KDC que es responsable de emitir tickets.
<b>TGT</b>	Siglas en inglés de Ticket-Granting Ticket, Ticket de otorgamiento de tickets. Un ticket emitido por el KDC que permite que un cliente solicite tickets para otros servicios.
<b>ticket</b>	Un paquete de información que se utiliza para transmitir de manera segura la identidad de un usuario a un servidor o servicio. Un ticket es válido únicamente para un solo cliente y un servicio determinado en un servidor específico. Un ticket contiene el nombre de principal del servicio, el nombre de principal del usuario, la dirección IP del host del usuario, una indicación de hora y un valor que define la duración del ticket. Un ticket se crea con una clave de sesión aleatoria que utilizará el cliente y el servicio. Una vez que se ha creado un ticket, se puede volver a utilizar hasta que caduque. Un ticket sólo sirve para autenticar un cliente cuando se presenta junto con un autenticador nuevo. Consulte también <a href="#">autenticador</a> , <a href="#">credencial</a> , <a href="#">servicio</a> , <a href="#">clave de sesión</a> .
<b>ticket de sustituto</b>	Un ticket que puede utilizar un servicio en nombre de un cliente para realizar una operación para el cliente. Por lo tanto, se dice que el servicio actúa como sustituto del cliente. Con el ticket, el servicio puede asumir la identidad del cliente. El servicio puede utilizar un ticket de sustituto para obtener un ticket de servicio para otro servicio, pero no puede obtener un ticket de otorgamiento de tickets. La diferencia entre un ticket de sustituto y un ticket reenviable es que un ticket de sustituto únicamente es válido para una sola operación. Consulte también <a href="#">ticket reenviable</a> .
<b>ticket inicial</b>	Un ticket que se emite directamente (es decir, que no se basa en un ticket de otorgamiento de tickets existente). Algunos servicios, como las aplicaciones que cambian las contraseñas, posiblemente requieran que los tickets se marquen como <i>iniciales</i> para garantizar que el cliente pueda demostrar que conoce su clave secreta. Esta garantía es importante porque un ticket inicial indica que el cliente se ha autenticado recientemente (en lugar de basarse en un ticket de otorgamiento de tickets, que posiblemente haya existido durante mucho tiempo).

<b>ticket no válido</b>	Un ticket posfechado que todavía no puede utilizarse. Un servidor de aplicaciones rechaza un ticket no válido hasta que se valide. Para validar un ticket no válido, el cliente debe presentarlo al KDC en una solicitud TGS, con el indicador <code>VALIDATE</code> definido, después de que haya pasado la hora de inicio. Consulte también <a href="#">ticket posfechado</a> .
<b>ticket posfechado</b>	Un ticket posfechado no es válido hasta que transcurra un tiempo especificado tras su creación. Un ticket de este tipo es útil, por ejemplo, para los trabajos por lotes que deben ejecutarse tarde por la noche, ya que si el ticket es robado, no se puede utilizar hasta que se ejecute el trabajo por lotes. Los tickets posfechados se emiten como <i>no válidos</i> y siguen teniendo ese estado hasta que: a) haya pasado su hora de inicio, y b) el cliente solicite la validación por parte del KDC. Generalmente, un ticket posfechado es válido hasta la hora de vencimiento del ticket de otorgamiento de tickets. Sin embargo, si el ticket posfechado se marca como <i>renovable</i> , su duración suele definirse para que coincida con la duración total del ticket de otorgamiento de tickets. Consulte también, <a href="#">ticket no válido</a> , <a href="#">ticket renovable</a> .
<b>ticket reenviable</b>	Un ticket que un cliente puede utilizar para solicitar un ticket en un host remoto sin que sea necesario que el cliente complete todo el proceso de autenticación en ese host. Por ejemplo, si el usuario <code>david</code> obtiene un ticket reenviable mientras está en el equipo de <code>jennifer</code> , puede iniciar sesión en su propio equipo sin tener que obtener un ticket nuevo (y, por lo tanto, autenticarse nuevamente). Consulte también <a href="#">ticket de sustituto</a> .
<b>ticket renovable</b>	Debido a que los tickets con duraciones muy largas constituyen un riesgo de seguridad, los tickets se pueden designar como <i>renovables</i> . Un ticket renovable tiene dos horas de vencimiento: a) la hora de vencimiento de la instancia actual del ticket, y b) la duración máxima de cualquier ticket. Si un cliente desea seguir utilizando un ticket, debe renovarlo antes del primer vencimiento. Por ejemplo, un ticket puede ser válido por una hora, pero todos los tickets tienen una duración máxima de diez horas. Si el cliente que tiene el ticket desea conservarlo durante más de una hora, debe renovarlo. Cuando un ticket alcanza la duración máxima, vence automáticamente y no se puede renovar.
<b>tipo</b>	Históricamente, <i>tipo de seguridad</i> y <i>tipo de autenticación</i> tenían el mismo significado; ambos indicaban el tipo de autenticación ( <code>AUTH_UNIX</code> , <code>AUTH_DES</code> , <code>AUTH_KERB</code> ). <code>RPCSEC_GSS</code> también es un tipo de seguridad, aunque proporciona servicios de privacidad e integridad, además de autenticación.
<b>tipo de seguridad</b>	Consulte <a href="#">tipo</a> .

# Índice

---

## Números y símbolos

[ ] (corchetes), salida bsmrecord, 686  
\$\$ (signo de dólar doble), número de proceso de shell principal, 257  
^ (acento circunflejo) en prefijos de clases de auditoría, 681  
@ (arroba), archivo device\_allocate, 101  
\* (asterisco)  
    archivo device\_allocate, 100, 101  
    carácter comodín  
        en ASET, 168, 170  
        en autorizaciones RBAC, 242, 246  
    comprobar en autorizaciones RBAC, 235  
\  
    archivo device\_allocate, 100  
    archivo device\_maps, 99  
.  
    (punto)  
        entrada de variable path, 51  
        separador de nombre de autorización, 242  
        visualización de archivos ocultos, 138  
;  
    (punto y coma)  
        archivo device\_allocate, 100  
        separador de atributos de seguridad, 250  
# (signo de almohadilla)  
    archivo device\_allocate, 100  
    archivo device\_maps, 99  
? (signo de interrogación), archivos de ajuste de ASET, 170  
= (signo igual), símbolo de permisos de archivo, 133  
+ (signo más)  
    archivo su\_log, 77  
    entrada de ACL, 145

+ (signo más) (*Continuación*)  
    prefijo de clase de auditoría, 680  
    símbolo de permisos de archivo, 133  
- (signo menos)  
    archivo su\_log, 77  
    prefijo de clase de auditoría, 680  
    símbolo de permisos de archivo, 133  
    símbolo de tipo de archivo, 128  
> (redirigir salida), prevención, 52  
>> (agregar salida), prevención, 52

## A

opción -A, comando auditreduce, 644  
acceso  
    acceso al servidor  
        con Kerberos, 575–578  
acceso root  
    impedir inicio de sesión (RBAC), 215–219  
    restricción, 56–57, 77–78  
    supervisión de intentos de comando su, 76–77  
    supervisión de intentos del comando su, 50  
    visualización de intentos en consola, 77–78  
autenticación de inicio de sesión con Secure Shell, 367–368  
autenticación de RPC segura, 323  
listas de control  
    Ver ACL  
obtención de acceso a un servicio específico, 578  
otorgamiento de acceso a su cuenta, 556–558

acceso (*Continuación*)

- restricción para
    - dispositivos, 47–49, 82
    - hardware del sistema, 79–80
  - restricción para servidores KDC, 490–491
  - seguridad
    - ACL, 55–56
    - ACL de UFS, 134–136
    - autenticación de inicio de sesión, 367–368
    - cliente-servidor NFS, 325–328
    - comunicación de problemas, 62
    - configuración de cortafuegos, 60
    - configuración de variable PATH, 51
    - configuración del cortafuegos, 60–61
    - control de inicio de sesión, 41
    - control de red, 57–61
    - control del uso del sistema, 50–55
    - dispositivos, 82
    - dispositivos periféricos, 47
    - guardar inicios de sesión fallidos, 67–68
    - hardware del sistema, 79–80
    - programas setuid, 52
    - restricción de acceso a archivos, 52
    - restricciones de acceso de inicio de sesión, 41
    - seguimiento de inicio de sesión root, 50
    - seguridad física, 40–41
    - sistemas remotos, 353
    - supervisión del uso del sistema, 54, 55
  - uso compartido de archivos, 56
- acento circunflejo (^) en prefijos de clases de auditoría, 681

## ACL

- archivo `kadm5.acl`, 521, 523, 527
- cambio de entradas, 147–148
- comandos, 136
- comprobación de entradas, 144–145
- configuración de entradas, 145–146
- configuración en un archivo, 145
- copia de entradas de ACL, 147
- descripción, 55–56, 134–136
- eliminación de entradas, 136, 148
- entradas de archivo válidas, 135–136
- entradas de directorio, 136
- entradas predeterminadas para directorios, 136

ACL (*Continuación*)

- formato de entradas, 134–136
  - mapa de tareas, 144–149
  - modificación de entradas, 147
  - procedimientos de usuario, 144–149
  - restricciones en copia de entradas, 135
  - visualización de entradas, 136, 148–149
- actualización
- servicio de auditoría, 635–636
  - servicios criptográficos, 310–311
- adición
- agregar
    - desde línea de comandos, 210–213
  - auditoría de zonas, 600–604
  - autenticación DH para sistemas de archivos montados, 329
  - claves para autenticación DH, 329–330
  - complemento de biblioteca, 303
  - complementos
    - estructura criptográfica, 302–303
  - contraseñas de marcación telefónica, 69–71
  - entradas de ACL, 145–146
  - mecanismos y funciones de proveedor de hardware, 309
  - módulo de cifrado de contraseña, 75–76
  - principal de servicio a archivo `keytab` (Kerberos), 543–545
  - principales de administración (Kerberos), 426, 433
  - proveedor de software, 302–303
  - proveedor de software de nivel de usuario, 303
  - seguridad para hardware del sistema, 79–80
- administración
- ACL, 144–149
  - algoritmos de contraseña, 71–72
  - almacenes de claves con KMF, 315
  - asignación de dispositivos, 85–86
  - auditoría
    - archivos de auditoría, 647–649
    - clases de auditoría, 591–592, 679
    - comando `auditreduce`, 643–645
    - control de costos, 609
    - descripción, 586
    - eficacia, 610
    - eventos de auditoría, 590



- administración, auditoría (*Continuación*)
  - mapa de tareas, 613
  - máscara de preselección de proceso, 667
  - reducción de requisitos de espacio de almacenamiento, 609–610
  - registros de auditoría, 592
  - en zonas, 596, 678
- comandos de la estructura criptográfica, 283
- estructura criptográfica y zonas, 285
- inicios de sesión de marcación telefónica, 70
- inicios de sesión remotos con Secure Shell, 363–365
- Kerberos
  - políticas, 528–537
  - principales, 514–528
  - tablas de claves, 542–548
- mapa de tareas de la estructura criptográfica, 299
- mapa de tareas de RPC segura, 328
- metarranura, 283
- permisos de archivo, 138
- política de dispositivos, 82
- Secure Shell
  - clientes, 378
  - descripción general, 375–377
  - mapa de tareas, 358
  - servidores, 378
- seguridad de archivos de cliente-servidor
  - NFS, 325–328
- administrador del sistema (RBAC)
  - asumir rol, 221
  - crear rol, 208–209
  - perfil de derechos, 239
  - protección de hardware, 79
  - rol recomendado, 183
- administrador principal (RBAC)
  - asumir rol, 220
  - contenido de perfil de derechos, 238
  - rol recomendado, 183
- administrar
  - contraseña de rol, 224–226
  - perfiles de derechos, 228–231
  - privilegios, 256
  - propiedades de un rol, 226–228
  - propiedades RBAC, 228–231
  - roles, 207–210
- administrar (*Continuación*)
  - roles para reemplazar a superusuario, 205–207
  - sin privilegios, 195
- advertencia sobre caducidad de ticket, 460
- agregar
  - atributos a un perfil de derechos, 228–231
  - atributos de seguridad a aplicaciones
    - antiguas, 233–235
  - auditoría de roles, 215
  - clases de auditoría, 622
  - directorios de auditoría, 625–629
  - dispositivo asignable, 86–87
  - módulos PAM, 340
  - nuevo perfil de derechos, 228–231
  - perfiles de derechos con Solaris Management Console, 230
  - política de auditoría, 631
  - privilegios
    - a comando, 260
    - directamente a usuario o rol, 260–261
  - propiedades RBAC a aplicaciones
    - antiguas, 233–235
  - rol cryptomgt, 214–215
  - rol de administrador del sistema, 208–209
  - rol de operador, 209
  - rol personalizado, 212–213
  - rol relacionado con seguridad, 214–215
  - roles
    - a un usuario, 210
    - con ámbito limitado, 210
    - para determinados perfiles, 207–210
  - roles personalizados (RBAC), 212–213
  - roles relacionados con seguridad, 209
  - seguridad a dispositivos, 83–84, 86–91
  - usuario local, 216
- algoritmo de cifrado 3des, archivo `ssh_config`, 379
- algoritmo de cifrado 3des-cbc, archivo `ssh_config`, 379
- algoritmo de cifrado aes128-cbc, archivo `ssh_config`, 379
- algoritmo de cifrado aes128-ctr, archivo `ssh_config`, 379
- algoritmo de cifrado arcfour, archivo `ssh_config`, 379

- algoritmo de cifrado Blowfish
  - archivo `policy.conf`, 73
  - archivo `ssh_config`, 379
- algoritmo de cifrado Blowfish, proveedor de núcleo, 300
- algoritmo de cifrado Blowfish
  - uso para contraseña, 73
- algoritmo de cifrado blowfish-cbc, archivo `ssh_config`, 379
- algoritmo de cifrado hmac-sha1, archivo `ssh_config`, 381
- algoritmo de cifrado MD5, archivo `policy.conf`, 72–73
- algoritmo de cifrado MD5, proveedor de núcleo, 300
- algoritmo de contraseña `crypt_bsdbf`, 43
- algoritmo de contraseña `crypt_bsdbf`, 43
- algoritmo de contraseña `crypt_sha256`, 43
- algoritmo de contraseña `crypt_sunmd5`, 43
- algoritmo de contraseña `crypt_unix`, 43, 72–76
- algoritmo hmac-md5, archivo `ssh_config`, 381
- algoritmos
  - cifrado de archivo, 296–298
  - cifrado de contraseña, 43
  - contraseña
    - configuración, 72–73
  - definición en la estructura criptográfica, 281
  - lista de la estructura criptográfica, 300–302
- algoritmos de contraseña de terceros, adición, 75–76
- `all audit class`, descripción, 679
- almacenaje, archivos de auditoría, 625–629
- almacenamiento
  - archivos de auditoría, 601–602
  - contraseña, 297
- almacenes de claves
  - administrados por KMF, 314
  - admitidos por KMF, 314, 315
  - enumeración de contenido, 316
  - exportación de certificados, 318–320
  - importación de certificados, 317–318
- ALTSHELL en Secure Shell, 383
- ámbito (RBAC), descripción, 192
- análisis, comando `praudit`, 669
- antememoria, credenciales, 575
- aplicación con privilegios
  - comprobación de autorizaciones, 190
  - comprobación de ID, 189
  - comprobación de privilegios, 189
  - descripción, 185
- archivo, archivos de auditoría, 650
- archivo `~/.gkadmin`, descripción, 565
- archivo `~/.k5login`, descripción, 565
- archivo `~/.rhosts`, descripción, 385
- archivo `~/.shosts`, descripción, 385
- archivo `~/.ssh/authorized_keys`
  - descripción, 385
  - valor de sustitución, 386
- archivo `~/.ssh/config`
  - descripción, 386
  - valor de sustitución, 386
- archivo `~/.ssh/environment`, descripción, 386
- archivo `~/.ssh/id_dsa`, valor de sustitución, 386
- archivo `~/.ssh/id_rsa`, valor de sustitución, 386
- archivo `~/.ssh/identity`, valor de sustitución, 386
- archivo `~/.ssh/known_hosts`
  - descripción, 385
  - valor de sustitución, 387
- archivo `~/.ssh/rc`, descripción, 386
- archivo `.cshrc`, entrada de variable `path`, 51
- archivo `/etc/d_passwd`
  - creación, 70
  - deshabilitación de inicios de sesión de marcación telefónica temporalmente, 71
  - y archivo `/etc/passwd`, 46
- archivo `/etc/default/kbd`, 80
- archivo `/etc/default/login`
  - configuración predeterminada de inicio de sesión, 68
  - descripción, 385
  - restricción de acceso root remoto, 77–78
  - Secure Shell y, 382–383
- archivo `/etc/default/su`
  - supervisión de comando `su`, 76–77
  - supervisión de intentos de acceso, 77–78
  - visualización de intentos de comando `su`, 77–78
- archivo `/etc/dfs/dfstab`
  - modos de seguridad, 451
  - uso compartido de archivos, 56

- archivo /etc/dialups, creación, 70
- archivo /etc/group, comprobaciones de ASET, 156
- archivo /etc/hosts.equiv, descripción, 386
- archivo /etc/krb5/kadm5.acl, descripción, 565
- archivo /etc/krb5/kadm5.keytab, descripción, 566
- archivo /etc/krb5/kdc.conf, descripción, 566
- archivo /etc/krb5/kpropd.acl, descripción, 566
- archivo /etc/krb5/krb5.conf, descripción, 566
- archivo /etc/krb5/krb5.keytab, descripción, 566
- archivo /etc/krb5/warn.conf, descripción, 566
- archivo /etc/logindevperm, 46
- archivo /etc/nologin
  - descripción, 385
  - deshabilitación temporal de inicios de sesión de usuario, 66–67
- archivo /etc/nsswitch.conf, 41
- archivo /etc/pam.conf, Kerberos y, 566
- archivo /etc/passwd, comprobaciones de ASET, 156
- archivo /etc/publickey, autenticación DH y, 325
- archivo /etc/security/audit\_event, eventos de auditoría y, 590
- archivo /etc/security/audit\_startup, 674–675
- archivo /etc/security/crypt.conf
  - cambio con nuevo módulo de contraseña, 75–76
  - módulos de contraseña de terceros, 75–76
- archivo /etc/security/device\_allocate, 100
- archivo /etc/security/device\_maps, 99
- archivo /etc/security/policy.conf, configuración de algoritmos, 72–73
- archivo /etc/ssh\_host\_dsa\_key.pub,
  - descripción, 385
- archivo /etc/ssh\_host\_key.pub, descripción, 385
- archivo /etc/ssh\_host\_rsa\_key.pub,
  - descripción, 385
- archivo /etc/ssh/shosts.equiv, descripción, 386
- archivo /etc/ssh/ssh\_config
  - configuración de Secure Shell, 378
  - descripción, 386
  - palabras clave, 378–383
  - parámetros específicos de host, 382
  - valor de sustitución, 386
- archivo /etc/ssh/ssh\_host\_dsa\_key,
  - descripción, 385
- archivo /etc/ssh/ssh\_host\_key
  - descripción, 385
  - valor de sustitución, 386
- archivo /etc/ssh/ssh\_host\_rsa\_key,
  - descripción, 385
- archivo /etc/ssh/ssh\_known\_hosts
  - control de distribución, 383
  - descripción, 385
  - distribución segura, 384
  - valor de sustitución, 386
- archivo /etc/ssh/sshd\_config
  - descripción, 385
  - palabras clave, 378–383
- archivo /etc/ssh/sshr, descripción, 386
- archivo /etc/syslog.conf
  - auditoría y, 618, 672
  - inicios de sesión fallidos y, 68–69
  - mensajes de pilas ejecutables y, 137
  - PAM y, 341
- archivo /etc/system, 672
- archivo .gkadmin
  - descripción, 565
  - herramienta SEAM y, 512
- archivo .k5.DOMINIO, descripción, 566
- archivo .k5login
  - descripción, 556–558, 565
  - en lugar de revelar la contraseña, 557
- archivo .profile, entrada de variable path, 51
- archivo .rhosts, descripción, 385
- archivo .shosts, descripción, 385
- archivo /tmp/krb5cc\_uid, descripción, 566
- archivo /tmp/ovsec\_adm.xxxxx, descripción, 566
- archivo /usr/aset/asetenv, 162
- archivo /usr/aset/masters/uid\_alias, 161
- archivo /var/adm/auditlog, registros de auditoría textual, 618
- archivo /var/adm/loginlog, guardar intentos de inicio de sesión fallidos, 67–68
- archivo /var/adm/messages
  - mensajes de pilas ejecutables, 137
  - resolución de problemas de la auditoría, 654
- archivo /var/adm/sulog, supervisión de contenido de, 76
- archivo /var/krb5/.k5.DOMINIO, descripción, 566

- archivo `/var/krb5/kadmin.log`, descripción, 566
- archivo `/var/krb5/kdc.log`, descripción, 566
- archivo `/var/krb5/principal`, descripción, 566
- archivo `/var/krb5/principal.kadm5`, descripción, 566
- archivo `/var/krb5/principal.kadm5.lock`, descripción, 566
- archivo `/var/krb5/principal.ok`, descripción, 566
- archivo `/var/krb5/principal.ulo`, descripción, 566
- archivo `/var/krb5/slave_datatrans`, descripción, 566
- archivo `/var/krb5/slave_datatrans_esclavo`, descripción, 567
- archivo `/var/log/authlog`, inicios de sesión fallidos, 68–69
- archivo `/var/log/syslog`, resolución de problemas de la auditoría, 654
- archivo `/var/run/sshd.pid`, descripción, 385
- archivo `audit_class`
  - agregar una clase, 622
  - descripción, 672
  - resolución de problemas, 622
- archivo `audit_control`
  - advertencia `minfree`, 676
  - auditoría de todo el sistema, 591
  - cambio de máscara de núcleo para eventos no atribuibles, 635
  - comprobación de clases, 653
  - comprobar sintaxis, 616
  - configuración, 615–617
  - descripción, 673
  - ejemplos, 674
  - entradas, 673
  - entradas y zonas, 678
  - excepciones a `flags` en base de datos
    - `audit_user`, 675–676
  - línea `flags`
    - máscara de preselección de proceso, 683
  - línea `plugin`, 618
  - prefijos en línea `flags`, 681
  - problema de sintaxis, 677
  - relectura de `daemon` de auditoría tras edición, 635
- archivo `audit_event`
  - cambio de pertenencia de clase, 623–624
- archivo `audit_event` (*Continuación*)
  - descripción, 590
  - eliminación de eventos de forma segura, 661
- archivo `auditlog`, registros de auditoría textual, 618
- archivo `authlog`, guardar intentos de inicio de sesión fallidos, 68–69
- archivo `authorized_keys`, descripción, 385
- archivo `cklist.rpt`, 156, 160
- archivo `crypt.conf`
  - cambio con nuevo módulo de contraseña, 75–76
  - módulos de contraseña de terceros, 75–76
- archivo `d_passwd`
  - creación, 70
  - descripción, 46
  - deshabilitación de inicios de sesión de marcación telefónica temporalmente, 71
- archivo de configuración de auditoría, *Ver* archivo `audit_control`
- archivo de reglas (BART), 107–108
- archivo de ticket, *Ver* antememoria de credenciales
- archivo `default/login`, descripción, 385
- archivo `device_allocate`
  - descripción, 100–101
  - ejemplo, 89, 100
  - formato, 100
- archivo `device_maps`
  - descripción, 99
  - entradas de ejemplo, 99
  - formato, 99
- archivo `dfstab`
  - modos de seguridad, 451
  - uso compartido de archivos, 56
- archivo `dialups`, creación, 70
- archivo `eeeprom.rpt`, 157, 160
- archivo `env.rpt`, 157, 160
- archivo `firewall.rpt`, 157, 160
- archivo `hosts.equiv`, descripción, 386
- archivo intermedio
  - creación, 440, 483
  - definición, 569
- archivo `kadm5.acl`
  - descripción, 565
  - entrada de KDC maestro, 425, 433, 471
  - formato de las entradas, 527

- archivo `kadm5.acf` (*Continuación*)
  - nuevos principales y, 521, 523
- archivo `kadm5.keytab`
  - descripción, 542, 566
- archivo `kadmin.log`, descripción, 566
- archivo `kbd`, 80
- archivo `kdc.conf`
  - descripción, 566
  - duración de tickets y, 572
- archivo `kdc.log`, descripción, 566
- archivo `keytab`
  - adición de principal de servicio a, 542, 543–545
  - adición del principal host del KDC maestro al, 428, 436
  - administración, 542–548
  - administración mediante el comando `ktutil`, 542
  - creación, 426, 434
  - eliminación de principales con el comando `ktremove`, 545
  - eliminación de un principal de servicio del, 545–546
  - inhabilitación de un servicio de host con el comando `delete_entry`, 548
  - lectura en memoria intermedia de `keytab` con el comando `read_kt`, 546
  - lectura en memoria intermedia de lista de claves con el comando `read_kt`, 547
  - visualización de contenido con el comando `ktutil`, 545
  - visualización de memoria intermedia de lista de claves con el comando `list`, 546, 547
  - visualización del contenido con el comando `ktutil`, 546–547
- archivo `known_hosts`
  - control de distribución, 383
  - descripción, 385
- archivo `kpropd.acf`, descripción, 566
- archivo `krb5.conf`
  - definición de puertos, 414
  - descripción, 566
  - edición, 424, 432
  - sección `domain_realm`, 413
- archivo `krb5.keytab`, descripción, 566
- archivo `krb5cc_uid`, descripción, 566
- archivo `login`
  - configuración predeterminada de inicio de sesión, 68
  - restricción de acceso root remoto, 77–78
- archivo `loginlog`, guardar intentos de inicio de sesión fallidos, 67–68
- archivo `nologin`, descripción, 385
- archivo `nsswitch.conf`, restricciones de acceso de inicio de sesión, 41
- archivo `ovsec_admin.xxxxx`, descripción, 566
- archivo `pam.conf`, Ver archivo de configuración de PAM
- archivo `passwd`
  - comprobaciones de ASET, 156
  - y archivo `/etc/d_passwd`, 46
- archivo `policy.conf`
  - adición de módulo de cifrado de contraseña, 75–76
  - descripción, 250–251, 251
  - especificación de algoritmo de contraseña en servicios de nombres, 73
  - especificación de algoritmos de cifrado en, 72–73
  - especificación de algoritmos de contraseña, 72–73
  - palabras clave
    - para algoritmos de contraseña, 44
    - para autorizaciones RBAC, 250
    - para perfiles de derechos, 250
    - para privilegios, 250, 272
  - perfil de derechos de usuario de Solaris básico, 240
- archivo principal, descripción, 566
- archivo `principal.kadm5`, descripción, 566
- archivo `principal.kadm5.lock`, descripción, 566
- archivo `principal.ok`, descripción, 566
- archivo `principal.ulong`, descripción, 566
- archivo `privileges`, descripción, 195
- archivo `shosts.equiv`, descripción, 386
- archivo `slave_datatrans`
  - descripción, 566
  - propagación de KDC y, 473–474
- archivo `slave_datatrans_esclavo`, descripción, 567
- archivo `ssh_config`
  - configuración de Secure Shell, 378
  - palabras clave, 378–383
    - Ver palabra clave específica
  - parámetros específicos de host, 382

archivo `ssh_config` (*Continuación*)

- valor de sustitución, 386

archivo `ssh_host_dsa_key`, descripción, 385archivo `ssh_host_dsa_key.pub`, descripción, 385archivo `ssh_host_key`

- descripción, 385

- valor de sustitución, 386

archivo `ssh_host_key.pub`, descripción, 385archivo `ssh_host_rsa_key`, descripción, 385archivo `ssh_host_rsa_key.pub`, descripción, 385archivo `ssh_known_hosts`, 385archivo `sshd_config`

- descripción, 385

- palabras clave, 378–383

  - Ver palabra clave específica

- valores de sustitución de entradas

  - `/etc/default/login`, 382–383

archivo `sshd.pid`, descripción, 385archivo `sshrd`, descripción, 386archivo `su`, supervisión de comando `su`, 76–77archivo `sulog`, 76–77

- supervisión de contenido de, 76

archivo `sysconf.rpt`, 157, 160archivo `syslog.conf`

- entrada `priv.debug`, 273

- guardar intentos de inicio de sesión fallidos, 68–69

- mensajes de pilas ejecutables, 137

- nivel `audit.notice`, 618

- nivel `kern.notice`, 137

- registros de auditoría, 588

- y auditoría, 672

archivo `system`, efecto `bsmconv en`, 672archivo `tune.rpt`, 155, 160archivo `uid_aliases` (ASET), 161, 164archivo `usrgrp.rpt`

- descripción, 156, 160

- ejemplo, 160

archivo `warn.conf`, descripción, 566archivo `audit_user`, comprobación de clases, 653

archivos

- archivo `syslog.conf`, 672

- archivos especiales, 129–131

- auditoría de modificaciones de, 658–659

- búsqueda de archivos con permisos `setuid`, 150

archivos (*Continuación*)

- cálculo de MAC de, 295–296

- cálculo de resúmenes de, 293–294, 294

- cálculo de un resumen, 293–294

- cambio de ACL, 147–148

- cambio de permisos de archivo especiales, 143–144

- cambio de propiedad, 128, 139–140

- cambio de propiedad de grupo, 140–141

- cifrado, 288, 296–298

- comprobaciones de ASET, 156

- con información de privilegios, 272–273

- configuración de ACL, 145–146

- copia con Secure Shell, 371–372

- copia de entradas de ACL, 147

- descifrado, 297

- determinar si tiene ACL, 144–145

- eliminación de ACL, 148

- entradas de ACL

  - adición o modificación, 147–148

  - comprobación, 144–145

  - configuración, 145–146

  - eliminación, 136, 148

  - entradas válidas, 135–136

  - visualización, 136, 148–149

hashing, 288

`kdc.conf`, 572

Kerberos, 565–567

manifiestos (BART), 123

manifiestos de BART, 123

montaje con autenticación DH, 333

objetos públicos, 589

para administrar Secure Shell, 384

permisos

- bit de permanencia, 131

- cambio, 128, 132–134, 141–142

- descripción, 129

- modo absoluto, 132, 142–143

- modo simbólico, 132, 133, 141–142

- `setgid`, 130–131

- `setuid`, 130

- valor `umask`, 131–132

- valores predeterminados, 131–132

PKCS #12, 319

privilegios relacionados con, 194

## archivos (*Continuación*)

- propiedad
    - y permiso `setgid`, 130–131
    - y permiso `setuid`, 130
  - protección con ACL, 144–149
  - protección con permisos UNIX, 138–144
  - resumen de, 293–294
  - seguridad
    - ACL, 55–56
    - cambio de permisos, 132–134, 141–142
    - cambio de propiedad, 139–140
    - cifrado, 55, 288
    - clases de usuario, 128
    - permisos de archivo, 129
    - permisos de archivo especiales, 133
    - permisos de directorio, 129
    - permisos UNIX, 127–134
    - restricción de acceso, 52
    - tipos de archivo, 128
    - `umask` predeterminado, 131–132
    - visualización de información de archivos, 128, 139
  - símbolos de tipo de archivo, 128
  - tipos de archivo, 128
  - uso compartido con autenticación DH, 333–334
  - verificación de la integridad mediante
    - `digest`, 293–294
  - visualización de archivos ocultos, 138
  - visualización de entradas de ACL, 148–149
  - visualización de información de archivos, 138–139
  - visualización de información sobre, 128
- archivos `/usr/aset/masters/tune`
- descripción, 161
  - modificación, 164
  - reglas, 170
- archivos `crontab`
- autorizaciones requeridas, 253
  - detención de ejecución periódica de ASET, 174
  - ejecución de ASET periódicamente, 154
- archivos de ajuste (ASET)
- descripción, 161
  - ejemplos, 170, 171
  - modificación, 164
  - reglas, 170
- archivos de auditoría
- alternar a archivo nuevo, 666
  - comando `auditreduce`, 667
  - combinación, 643–645, 667
  - configuración, 615–624
  - copia de mensajes en un solo archivo, 647
  - disco de partición para, 625–629
  - espacio libre mínimo para sistemas de archivos, 673
  - gestión, 650
  - impresión, 648
  - indicaciones de hora, 685
  - indicadores de hora, 685
  - limitar el tamaño de, 661–662
  - nombres, 684, 685
  - orden de abertura, 673
  - reducción, 643–645, 667
  - reducción de requisitos de espacio de almacenamiento, 609–610, 610
- archivos de configuración
- archivo `audit_class`, 672
  - archivo `audit_control`, 615–617, 666, 673
  - archivo `audit_event`, 674
  - archivo `device_maps`, 99
  - archivo `nsswitch.conf`, 41
  - archivo `policy.conf`, 43, 72–73, 251
  - archivo `syslog.conf`, 273, 672
  - archivo `system`, 672
  - ASET, 154
  - base de datos `audit_user`, 675–676
  - con información de privilegios, 272–273
  - para algoritmos de contraseña, 43
  - secuencia de comandos `audit_startup`, 674–675
  - Secure Shell, 376
- archivos de identidad (Secure Shell), convenciones de denominación, 384
- archivos de registro
- BART
    - salida detallada, 125–126
    - salida programática, 125–126
  - configuración de servicio de auditoría, 617–620
  - espacio para registros de auditoría, 666
  - examen de registros de auditoría, 667
  - intentos de inicio de sesión fallidos, 68–69
  - registro de ejecución (ASET), 158



archivos de registro (*Continuación*)

- registros de auditoría, 593, 648
- registros de auditoría syslog, 672
- supervisión de comando su, 76–77
- /var/adm/messages, 654
- /var/log/syslog, 654

## archivos maestros (ASET), 156, 161

## archivos PKCS #12 files, protección, 319

## arroba (@), archivo device\_allocate, 101

## ASET

- archivo asetenv, 162
- archivo de alias
  - descripción, 161
  - ejemplos, 171
  - variable UID\_ALIASES, 164
- archivo de entorno, 162
- archivo uid\_aliases, 161
- archivos de ajuste, 161, 164
- archivos maestros, 156, 161
- comando aset
  - inicio, 154
  - opción -p, 173
  - versión interactiva, 172–173
- comando aset.restore, 165
- configuración, 162–165, 165
- descripción, 53, 153–171
- detención de ejecución periódica, 174
- directorio de trabajo, 167
- ejecución periódica, 173
- ejecución periódica de ASET, 173
- ejemplos de archivos de ajuste, 170
- la ejecución interactiva, 172–173
- los servicios NFS y, 165
- mapa de tareas, 171–175
- mensajes de error, 175
- programación de ejecución de ASET, 164, 168
- recopilación de informes, 174–175
- registro de ejecución, 158
- resolución de problemas, 175
- restauración de estado original de sistema, 165
- variable ASETDIR, 167
- variable ASETSECLEVEL, 167
- variable CKLISTPATH\_level, 169
- variable PERIODIC\_SCHEDULE, 164, 168

ASET (*Continuación*)

- variable TASKS, 163, 169
- variable UID\_ALIASES, 161, 164, 169
- variable YPCHECK, 164, 169
- variables de entorno, 166

## asignación

- de UID a principales de Kerberos, 581
- nombres de host en dominios (Kerberos), 413

## asignación de credenciales GSS, 416

## asignación de dispositivos

- agregar dispositivos, 85–86
- archivo de configuración, 99
- archivo device\_allocate, 100–101
- archivo device\_maps, 99–100
- asignación forzada de dispositivos, 88–89
- asignar dispositivos, 91–92
- auditoría, 90–91
- autorización de usuarios para asignar, 87
- autorizaciones para comandos, 98
- cambio de dispositivos asignables, 89–90
- comando allocate, 98
- comando deallocate, 98
  - secuencias de comandos device-clean y, 103
  - uso, 94–95
- comandos, 97
- componentes del mecanismo, 97
- desasignación de dispositivos, 94–95
- desasignación forzada de dispositivos, 89
- deshabilitación, 634
- desmontaje de un dispositivo asignado, 95
- dispositivos asignables, 101
- ejemplos, 92
- estado de error de asignación, 98–99
- forzada, 88–89
- gestión de dispositivos, 85–86
- habilitación, 86–87
- mapa de tareas, 85–86, 91
- montaje de dispositivos, 92–94
- no requieren autorización, 90
- permisos de resolución de problemas, 88
- permitir asignación de dispositivos, 86–87
- por usuarios, 91–92
- prevención, 90
- procedimientos de usuario, 91



- asignación de dispositivos (*Continuación*)
  - requiere autorización, 89–90
  - resolución de problemas, 92, 94
  - secuencias de comandos device-clean
    - descripción, 101–103
    - dispositivos de audio, 102
    - opciones, 103
  - redacción de secuencias de comandos
    - nuevas, 103
  - unidades de CD-ROM, 102
  - unidades de cinta, 101
  - unidades de cintas, 102
  - unidades de disquete, 102
- servicios asignables, 101
- uso, 91
- uso del comando `allocate`, 91–92
- visualización de información, 88
- asignaciones, eventos a clases (auditoría), 592
- asignar
  - privilegios a comandos en un perfil de derechos, 260
  - privilegios a comandos en una secuencia de comandos, 263–264
  - privilegios a usuario o rol, 260–261
  - rol a un usuario, 208, 210
  - rol a un usuario localmente, 213–215
- asterisco (\*)
  - archivo `device_allocate`, 100, 101
  - carácter comodín
    - en ASET, 168, 170
  - en autorizaciones RBAC, 242, 246
  - comprobar en autorizaciones RBAC, 235
- asumir rol
  - administrador del sistema, 221
  - administrador principal, 220
  - cómo, 205–219, 219
  - en Solaris Management Console, 222–223
  - en una ventana de terminal, 219–221
  - root, 221
- atributo `p_minfree`, condición `audit_warn`, 676
- atributo `qsize`, entrada `plugin`, 618
- atributos, palabra clave en BART, 124
- atributos de archivo de reglas, *Ver* palabras clave
- atributos de seguridad
  - comprobar, 189
- atributos de seguridad (*Continuación*)
  - consideraciones al asignar directamente, 192–193
  - descripción, 185
  - ID especial en comandos, 189
  - perfil de derechos de seguridad de la red, 187
  - privilegios en comandos, 189
  - uso para montar dispositivo asignado, 87
- auditar, roles, 215
- auditoría
  - actualización de información, 635–636
  - asignación de dispositivos, 90–91
  - cambios en la versión actual, 597–598
  - cambios en política de dispositivos, 84
  - configuración en la zona global, 600
  - configuración en zona global, 630–631
  - configuración idéntica para todas las zonas, 637–639
  - configuración por zona, 639–640
  - definición de preselección, 589
  - deshabilitación, 634–635
  - encontrar cambios en archivos específicos, 658–659
  - habilitar, 632–634
  - inicios de sesión, 662
  - perfiles de derechos para, 677–678
  - planificación, 600–604
  - planificación en zonas, 600–601
  - prerrequisito de base de datos `hosts`, 633
  - privilegios y, 273–274
  - resolución de problemas, 651–663
  - resolución de problemas de comando `praudit`, 648
  - todos los comandos por usuarios, 656–658
  - transferencias de archivos `sftp`, 662–663
  - zonas y, 596, 678
- autenticación
  - archivos montados en NFS, 333
  - autenticación DH, 324–328
  - configuración entre dominios, 441–443
  - descripción, 58–59
  - descripción general de Kerberos, 575
  - deshabilitación con la opción `-X`, 560
  - Kerberos y, 393
  - RPC segura, 323
  - Secure Shell
    - métodos, 354–356

autenticación, Secure Shell (*Continuación*)

- proceso, 376–377
  - seguridad de red, 58–59
  - servicios de nombres, 323
  - sesión cliente-servidor AUTH\_DH, 325–328
  - terminología, 569–570
  - tipos, 58–59
  - uso con NFS, 323
- autenticación AUTH\_DES, *Ver* autenticación AUTH\_DH
- autenticación AUTH\_DH, y NFS, 323
- autenticación basada en host
- configuración en Secure Shell, 358–360
  - descripción, 354
- autenticación de clave pública, Secure Shell, 354
- autenticación de contraseña, Secure Shell, 354
- autenticación DH
- configuración en NIS, 331–332
  - configuración en NIS+, 329–330
  - descripción, 324–328
  - montaje de archivos con, 333
  - para cliente NIS, 331–332
  - para cliente NIS+, 330
  - uso compartido de archivos con, 333–334
- autenticación Diffie-Hellman, *Ver* autenticación DH
- autenticación entre dominios, configuración, 441–443
- autenticación Kerberos
- opción de archivo `dfstab`, 451
  - y RPC segura, 324
- autenticador
- en Kerberos, 570, 577
- automatización de la creación de principales, 515–516
- autorización `solaris.device.revoke`, 98
- autorizaciones
- Kerberos y, 393
  - tipos, 58–59
- autorizaciones (RBAC)
- base de datos, 243–251
  - comandos que requieren autorizaciones, 252–253
  - comprobar caracteres comodín, 235
  - comprobar en aplicación con privilegios, 190
  - convención de denominación, 242
  - definición, 188
  - delegar, 243
  - descripción, 184, 242–243

autorizaciones (RBAC) (*Continuación*)

- granularidad, 243
  - no requieren asignación de dispositivos, 90
  - para asignación de dispositivos, 98
  - para asignar dispositivos, 87
  - `solaris.device.allocate`, 87, 98
  - `solaris.device.revoke`, 98
- ayuda
- herramienta SEAM, 512
  - herramienta SEAM, 512
  - URL en línea, 419–420
- ayuda contextual, herramienta SEAM, 512
- ayuda en pantalla
- herramienta SEAM, 512
  - URL para, 419–420

**B**

## BART

- componentes, 106–108
  - consideraciones de seguridad, 109–110
  - descripción general, 105–108
  - mapa de tareas, 108–109
  - salida detallada, 126
  - salida programática, 126
- base de datos, para RPC segura `cred`, 325
- base de datos `audit_user`
- campos de auditoría de usuarios, 675–676
  - especificación de excepciones de usuario, 620–621
  - máscara de preselección de proceso, 683
- base de datos `auth_attr`
- descripción, 246–247
  - resumen, 243
- base de datos `cred`
- adición de credencial de cliente, 330
  - adición de credencial de usuario, 331
  - autenticación DH, 324–328
- base de datos de usuario (RBAC), *Ver* base de datos `user_attr`
- base de datos `exec_attr`
- descripción, 249–250
  - resumen, 244
- base de datos `prof_attr`
- descripción, 248–249

- base de datos `prof_attr` (*Continuación*)
    - resumen, 243
  - base de datos `user_attr`
    - descripción, 243, 245–246
    - palabra clave `defaultpriv`, 273
    - palabra clave `limitpriv`, 273
    - palabra clave `privs`, 273
    - relaciones de RBAC, 244–245
  - base de datos `audit_user`
    - excepción a clases de auditoría de todo el sistema, 591
    - prefijos para clases, 681
  - bases de datos
    - `audit_user`, 675–676
    - `auth_attr`, 246–247
    - claves secretas NFS, 325
    - con información de privilegios, 272–273
    - copia de seguridad y propagación de KDC, 473–474
    - creación de KDC, 425
    - cred para RPC segura, 330
    - `exec_attr`, 249–250
    - para RPC segura `publickey`, 325
    - `prof_attr`, 248–249
    - propagación KDC, 417
    - RBAC, 243–251
    - `user_attr`, 245–246
  - biblioteca `/usr/lib/libsasl.so`, descripción
    - general, 349
  - biblioteca PKCS #11
    - adición de biblioteca de proveedor, 303
    - en la estructura criptográfica de Oracle Solaris, 280
  - bibliotecas, proveedores de nivel de usuario, 300
- C**
- C opción, `auditreduce` comando, 644
  - shell C, versión con privilegios, 192
  - caballo de Troya, 51
  - cadena `allhard`, secuencia de comandos
    - `audit_warn`, 677
  - cadena `allsoft`, secuencia de comandos
    - `audit_warn`, 676
  - cadena `ebusy`, secuencia de comandos
    - `audit_warn`, 677
  - cadena `hard`, secuencias de comandos `audit_warn`, 676
  - cadena `postsigterm`, secuencia de comandos
    - `audit_warn`, 677
  - cadena `soft`, secuencia de comandos `audit_warn`, 676
  - cadena `tmpfile`, secuencia de comandos
    - `audit_warn`, 677
  - cálculo
    - clave secreta, 288–290, 290–293
    - MAC de un archivo, 295–296
    - resumen de un archivo, 293–294
  - cambiar
    - contenido de perfil de derechos, 228–231
    - contraseña de rol, 224–226
    - perfil de derechos desde línea de comandos, 230
    - propiedades de rol, 226–228
    - propiedades de usuario desde línea de comandos, 233
    - usuario `root` a rol, 215–219
  - cambio
    - algoritmo de contraseña para un dominio, 73
    - algoritmo de contraseña predeterminado, 71–72
    - archivo `audit_class`, 622
    - archivo `audit_control`, 615–617
    - archivo `audit_event`, 623–624
    - dispositivos asignables, 89–90
    - entradas de ACL, 147–148
    - la frase de contraseña para Secure Shell, 365–366
    - mapa de tareas de algoritmo de contraseña, 71–72
    - permisos de archivo
      - especiales, 143–144
      - modo absoluto, 142–143
      - modo simbólico, 141–142
    - permisos de archivo especiales, 143–144
    - política de dispositivos, 83–84
    - propiedad de archivo, 139–140
    - propiedad de grupo de archivo, 140–141
    - su contraseña con `kpasswd`, 554
    - su contraseña con `passwd`, 554
  - campo de formato de impresión, `token arbitrary`, 689
  - campo de tamaño de elemento, `token arbitrary`, 688
  - campos de auditoría de usuarios, base de datos
    - `audit_user`, 675–676
  - caracteres comodín
    - en archivos de ajuste de ASET, 170

caracteres comodín (*Continuación*)

- en archivos de ASET, 168
- en autorizaciones RBAC, 242
- para hosts en Secure Shell, 372

## características de auditoría

- ID de auditoría, 683
- ID de sesión, 683
- ID de terminal, 683
- máscara de preselección de proceso, 667
- máscara de preselección de proceso de usuario, 683
- procesos, 683

## características de auditoría de proceso

- ID de auditoría, 683
- ID de sesión de auditoría, 683
- ID de terminal, 683
- máscara de preselección de proceso, 683

Centro de distribución de claves, *Ver* KDC

## certificados

- exportación para uso por parte de otro sistema, 318–320
- generación con el comando `pktool`
  - `gencert`, 316–317
- importación a almacén de claves, 317–318

## cierre, señal recibida durante cierre de auditoría, 677

## cifrado

- algoritmo de contraseña, 43
- algoritmo DES, 324
- algoritmos
  - Kerberos y, 419
- archivos, 55, 288, 296–298
- clave privada del usuario NIS, 332
- comando `encrypt`, 296–298
- con la opción `-x`, 560
- contraseñas, 71–72
- especificación de algoritmo de contraseña
  - localmente, 71–72
- especificación de algoritmos de contraseña en el archivo `policy.conf`, 43
- especificación de algoritmos en archivo `ssh_config`, 379
- generación de clave simétrica
  - uso del comando `dd`, 288–290
  - uso del comando `pktool`, 290–293

cifrado (*Continuación*)

- instalación de módulos de contraseña de terceros, 75–76
  - las comunicaciones entre hosts, 367
  - lista de algoritmos de contraseña, 43
  - modos
    - Kerberos y, 419
  - NFS seguro, 324
  - servicio de privacidad, 393
  - tipos
    - Kerberos y, 419, 579–581
  - tráfico de red entre hosts, 353–356
  - uso de comandos de nivel de usuario, 283–284
- cifrado DES, NFS seguro, 324
- cifrado DES, proveedor de núcleo, 300
- clase de auditoría `administrative`, 680
- clase de auditoría `administrative (old)`, 679
- clase de auditoría `all`, precaución de uso, 681
- clase de auditoría `application`, 679
- clase de auditoría `audit administration`, 680
- clase de auditoría `exec`, 680
- clase de auditoría `file_attr_acc`, 679
- clase de auditoría `file_attr_mod`, 679
- clase de auditoría `file_close`, 679
- clase de auditoría `file_creation`, 679
- clase de auditoría `file_deletion`, 679
- clase de auditoría `file_write`, 679
- clase de auditoría `ioctl`, 680
- clase de auditoría `ipc`, 680
- clase de auditoría `login_logout`, 680
- clase de auditoría `network`, 680
- clase de auditoría `no_class`, 679
- clase de auditoría `non_attrib`, 679
- clase de auditoría `null`, 679
- clase de auditoría `other`, 680
- clase de auditoría `process`, 680
- clase de auditoría `process modify`, 680
- clase de auditoría `process start`, 680
- clase de auditoría `system state`, 680
- clase de auditoría `system-wide administration`, 680
- clase de auditoría `user administration`, 680
- clase `file_read audit`, 679
- clases, *Ver* clases de auditoría

- clases de auditoría
  - agregar, 622
  - asignación de eventos, 592
  - definición en todo el sistema, 679
  - definiciones, 679
  - descripción, 589, 590
  - descripción general, 591–592
  - en todo el sistema, 673
  - entradas en archivo `audit_control`, 673
  - excepciones a valores de todo el sistema, 591
  - excepciones en base de datos `audit_user`, 675–676
  - máscara de preselección de proceso, 683
  - modificar predeterminado, 622
  - prefijos, 680
  - preselección, 589, 615–617
  - sintaxis, 680, 681
- clases de usuario de archivos, 128
- clases no atribuibles, 673
- claves
  - clave de servicio, 542–548
  - claves de sesión
    - autenticación Kerberos y, 575
  - creación de clave DH para usuario NIS, 332–333
  - creación para Secure Shell, 363–365
  - definición en Kerberos, 569
  - generación de clave simétrica
    - uso del comando `pktool`, 290–293
  - generación de claves simétricas
    - uso del comando `dd`, 288–290
  - generación para Secure Shell, 363–365
  - uso para MAC, 296
- claves comunes
  - autenticación DH y, 324–328
  - cálculo, 327
- claves de conversación
  - descifrado en RPC segura, 327
  - generación en RPC segura, 326
- claves de servicio, definición en Kerberos, 569
- claves de sesión
  - autenticación Kerberos y, 575
  - definición en Kerberos, 569
- claves privadas
  - Ver también* claves secretas
  - archivos de identidad de Secure Shell, 384
- claves privadas (*Continuación*)
  - definición en Kerberos, 569
- claves públicas
  - archivos de identidad de Secure Shell, 384
  - autenticación DH y, 324–328
  - cambio de frase de contraseña, 365–366
  - generación de par de clave pública y clave privada, 363–365
- claves secretas
  - creación, 288–290, 290–293
  - generación
    - uso del comando `dd`, 288–290
    - uso del comando `pktool`, 290–293
  - generación para RPC segura, 325
- clientes
  - configuración de Kerberos, 452–466
  - configuración para Secure Shell, 376, 378
  - definición en Kerberos, 569
  - sesión cliente-servidor `AUTH_DH`, 325–328
- código de autenticación de mensajes (MAC), cálculo
  - para archivo, 295–296
- comando `/usr/bin/ftp`, Kerberos y, 567
- comando `/usr/bin/kdestroy`, Kerberos y, 567
- comando `/usr/bin/kinit`, Kerberos y, 567
- comando `/usr/bin/klist`, Kerberos y, 567
- comando `/usr/bin/kpasswd`, Kerberos y, 567
- comando `/usr/bin/ktutil`, Kerberos y, 567
- comando `/usr/bin/rcp`, Kerberos y, 567
- comando `/usr/bin/rdist`, Kerberos y, 567
- comando `/usr/bin/rlogin`, Kerberos y, 567
- comando `/usr/bin/rsh`, Kerberos y, 567
- comando `/usr/bin/telnet`, Kerberos y, 567
- comando `/usr/lib/kprop`, descripción, 567
- comando `/usr/sbin/gkadmin`, descripción, 567
- comando `/usr/sbin/kadmin`, descripción, 567
- comando `/usr/sbin/kadmin.local`, descripción, 568
- comando `/usr/sbin/kclient`, descripción, 568
- comando `/usr/sbin/kdb5_ldap_util`,
  - descripción, 568
- comando `/usr/sbin/kdb5_util`, descripción, 568
- comando `/usr/sbin/kgcmgr`, descripción, 568
- comando `/usr/sbin/kproplog`, descripción, 568
- comando `add_drv`, descripción, 96

- comando `allocate`
  - autorización de usuario, 87
  - autorizaciones para, 98
  - autorizaciones requeridas, 253
  - descripción, 98
  - estado de error de asignación, 99
  - unidad de cinta, 92
  - uso, 91–92
- comando `at`, autorizaciones requeridas, 252
- comando `atq`, autorizaciones requeridas, 252
- comando `audit`
  - actualización de servicio de auditoría, 635–636
  - comprobar sintaxis del archivo `audit_control` (opción `-v`), 616
  - descripción, 667
  - máscara de preselección para procesos existentes (opción `-s`), 635
  - relectura de archivos de auditoría (opción `-s`), 666
  - restablecer puntero de directorio (opción `-n`), 666
- comando `auditconfig`
  - clases de auditoría como argumentos, 591, 679
  - configuración de política de auditoría, 657
  - configurar política de auditoría, 631
  - descripción, 671
  - prefijos para clases, 681
- comando `auditreduce`, 667
  - depuración de archivos editados, 649–650
  - descripción, 667
  - ejemplos, 643–645
  - filtrado de opciones, 645
  - fusión de registros de auditoría, 643–645
  - opción `-c`, 647
  - opción `-O`, 643–645
  - opciones, 668
  - selección de registros de auditoría, 645–647
  - sin opciones, 668
  - tokens trailer y, 704
  - uso de indicación de hora, 685
  - uso de opciones en mayúscula, 643
  - uso de opciones en minúscula, 645
- comando `auths`, descripción, 251
- comando `bart`, 105
- comando `bart compare`, 107
- comando `bart create`, 106–107, 110
- comando `bsmrecord`
  - [ ] (corchetes) en salida, 686
  - descripción, 667
  - ejemplo, 641
  - lista de formatos de clase, 642–643
  - lista de formatos de programa, 642
  - lista de todos los formatos, 641
  - tokens opcionales ([ ]), 686
  - visualización de formatos de registros de auditoría, 641–643
- comando `cd rw`, autorizaciones requeridas, 252
- comando `chgrp`
  - descripción, 128
  - sintaxis, 141
- comando `chkey`, 325, 332
- comando `chmod`
  - cambio de permisos especiales, 143–144, 144
  - descripción, 128
  - sintaxis, 143
- comando `chown`, descripción, 128
- comando `crypt`, seguridad de archivos, 55
- comando `cryptoadm`
  - descripción, 282
  - inhabilitación de mecanismos criptográficos, 304, 305
  - inhabilitación de mecanismos de hardware, 308–310
  - instalación de una biblioteca PKCS #11, 303
  - lista de proveedores, 300
  - opción `-m`, 304, 305
  - opción `-p`, 304, 306
  - restauración de un proveedor de software de núcleo, 306
- comando `cryptoadm install`, instalación de una biblioteca PKCS #11, 303
- comando `csh`, versión con privilegios, 192
- comando `dd`, generación de claves secretas, 288–290
- comando `deallocate`
  - autorizaciones para, 98
  - autorizaciones requeridas, 253
  - descripción, 98
  - estado de error de asignación, 98–99, 99
  - secuencias de comandos `device-clean y`, 103
  - uso, 94–95

- comando `decrypt`
  - descripción, 283
  - sintaxis, 297
- comando `delete_entry`, comando `ktutil`, 548
- comando `devfsadm`, descripción, 96
- comando `digest`
  - descripción, 283
  - ejemplo, 294
  - sintaxis, 293
- comando `dminfo`, 99
- comando `eeprom`, 41, 79–80
- comando `eject`, limpieza de dispositivos y, 102
- comando `elfsign`
  - descripción, 282, 284
- comando `encrypt`
  - descripción, 283
  - mensajes de error, 298
  - resolución de problemas, 298
  - sintaxis, 289
- comando `find`, búsqueda de archivos con permisos `setuid`, 150
- comando `ftp`
  - configuración de nivel de protección en, 560
  - Kerberos y, 558–561, 567
  - registro de transferencias de archivos, 662–663
- comando `getdevpolicy`, descripción, 96
- comando `getfacl`
  - descripción, 136
  - ejemplos, 148–149
  - opción `-a`, 148
  - opción `-d`, 149
  - verificación de entradas de ACL, 146
  - visualización de entradas de ACL, 148–149
- comando `gkadmin`
  - Ver también* herramienta SEAM
  - descripción, 567
- comando `gsscred`, descripción, 567
- comando `kadmin`
  - comando `ktadd`, 543–545
  - comando `ktremove`, 545
  - creación de principal `host`, 428, 435
  - descripción, 567
  - eliminación de principales de `keytab` con, 545–546
  - herramienta SEAM y, 510
- comando `kadmin.local`
  - adición de principales de administración, 426, 433
  - automatización de la creación de principales, 515
  - creación de archivo `keytab`, 426, 434
  - descripción, 568
- comando `kclient`, descripción, 568
- comando `kdb5_ldap_util`, descripción, 568
- comando `kdb5_util`
  - creación de archivo intermedio, 440, 483
  - creación de base de datos KDC, 425
  - descripción, 568
- comando `kdestroy`
  - ejemplo, 552
  - Kerberos y, 567
- comando `keylogin`
  - uso para RPC segura, 325
  - verificación de configuración de autenticación DH, 330
- comando `kgcmgr`, descripción, 568
- comando `kinit`
  - duración de `ticket`, 572
  - ejemplo, 550
  - Kerberos y, 567
  - opción `-F`, 550
- comando `klist`
  - ejemplo, 551–552
  - Kerberos y, 567
  - opción `-f`, 551–552
- comando `kmfcfg`, 314
- comando `kpasswd`
  - comando `passwd` y, 554
  - ejemplo, 555
  - Kerberos y, 567
  - mensaje de error, 554
- comando `kprop`, descripción, 567
- comando `kproplog`, descripción, 568
- comando `ksh`, versión con privilegios, 192
- comando `ktadd`
  - adición de principal de servicio, 542, 543–545
  - sintaxis, 544
- comando `ktremove`, 545
- comando `ktutil`
  - administración del archivo `keytab`, 542
  - comando `delete_entry`, 548



- comando ktutil (*Continuación*)
  - comando list, 546, 547
  - comando read\_kt, 546, 547
  - Kerberos y, 567
  - visualización de la lista de principales, 546–547
  - visualización de lista de principales, 545
- comando list, 546, 547
- comando list\_devices
  - autorizaciones para, 98
  - autorizaciones requeridas, 253
  - descripción, 98
- comando logadm, archivado de archivos de auditoría textual, 650
- comando logins
  - sintaxis, 65
  - visualización de estado de inicio de sesión de usuario, 64–65, 65
  - visualización de usuarios sin contraseñas, 66
- comando mac
  - descripción, 283
  - sintaxis, 295
- comando makedbm, descripción, 251
- comando mount, con atributos de seguridad, 87
- comando mt, limpieza de dispositivo de cinta y, 102
- comando newkey
  - creación de clave para usuario NIS, 332–333
  - generación de claves, 325
- comando nisaddcred
  - adición de credencial de cliente, 330
  - generación de claves, 325
- comando pam\_roles, descripción, 251
- comando passwd
  - cambiar contraseña de rol, 224–226
  - y el comando kpasswd, 554
  - y servicios de nombres, 42
- comando perfiles, descripción, 251
- comando pfcsh, descripción, 192
- comando pfexec, descripción, 251
- comando pfksh, descripción, 192
- comando pfsh, descripción, 192
- comando pkgadd
  - instalación de proveedores de terceros, 302
  - instalación de software de terceros, 75
- comando pktool
  - administración de objetos PKI, 314
  - creación de un certificado autofirmado, 316–317
  - generación de claves secretas, 290–293
  - subcomando export, 318–320
  - subcomando gencert, 316–317
  - subcomando import, 317–318
  - subcomando list, 316
  - subcomando setpin, 320
- comando ppriv
  - enumerar privilegios, 256
  - para depuración, 258
- comando praudit
  - conversión de registros de auditoría a formato legible, 648, 669
  - DTD para opción -x, 670
  - formato XML, 648
  - formatos de salida, 669
  - opciones, 669
  - redirección de salida a auditreduce, 648
  - sin opciones, 670
  - uso en una secuencia de comandos, 670–671
  - visualización de registros de auditoría, 647–649
- comando rcp
  - Kerberos y, 558–561, 567
- comando rdist, Kerberos y, 567
- comando read\_kt, 546, 547
- comando rem\_drv, descripción, 96
- comando rlogin
  - Kerberos y, 558–561, 567
- comando roleadd
  - descripción, 252
  - usar, 211
- comando roledel, descripción, 252
- comando rolemod
  - cambiar propiedades de rol, 227
  - descripción, 252
- comando roles
  - descripción, 252
  - usar, 220
- comando rsh
  - Kerberos y, 558–561, 567
- comando rsh (shell restringido), 51



- comando scp
  - copia de archivos con, 371–372
  - descripción, 387
- comando sendmail, autorizaciones requeridas, 253
- comando setfacl
  - descripción, 136
  - ejemplos, 147–148
  - opción -d, 148
  - opción -f, 147
  - sintaxis, 145–146
- comando sftp
  - auditoría de transferencias de archivos, 662–663
  - copia de archivos con, 372
  - descripción, 388
- comando sh, versión con privilegios, 192
- comando smattrpop, descripción, 252
- comando smexec, descripción, 252
- comando smmultiuser, descripción, 252
- comando smprofile
  - cambiar perfil de derechos, 229
  - descripción, 252
- comando smrole
  - cambiar propiedades de rol, 225, 227
  - descripción, 252
  - usar, 212–213
- comando smuser
  - cambiar propiedades RBAC de usuario, 232
  - descripción, 252
- comando ssh
  - descripción, 387
  - opciones de reenvío del puerto, 369–371
  - uso, 366–367
  - uso de un comando de proxy, 373
  - valores de sustitución de palabras clave, 388
- comando ssh-add
  - almacenamiento de claves privadas, 367–368
  - descripción, 387
  - ejemplo, 367–368, 368
- comando ssh-agent
  - configuración para CDE, 368–369
  - descripción, 387
  - desde la línea de comandos, 367–368
  - en secuencias de comandos, 368–369
- comando ssh-keygen
  - descripción, 387
  - uso, 363–365
- comando ssh-keyscan, descripción, 387
- comando ssh-keysign, descripción, 387
- comando sshd, descripción, 387
- comando su
  - en asunción de roles, 219–221, 222–223
  - supervisión de uso, 76–77
  - visualización de intentos de acceso en consola, 77–78
- comando svcadm
  - actualización de la estructura criptográfica, 302–303
  - administración de la estructura criptográfica, 282, 283
  - habilitación de daemon de servidor de claves, 329
  - habilitación de la estructura criptográfica, 310–311
  - reiniciar servicio de nombres, 208
  - reinicio
    - daemon syslog, 69
    - Secure Shell, 362
  - reinicio de daemon syslog, 618
  - reinicio de servidor NFS, 627
- comando svcs
  - lista de servicios criptográficos, 310–311
  - listado de servicio de servidor de claves, 329
- comando tail, ejemplo de uso, 611
- comando taskstat (ASET), 155, 158
- comando telnet
  - Kerberos y, 558–561, 567
- comando truss, para depuración de privilegios, 258
- comando umount, con atributos de seguridad, 87
- comando update\_drv
  - descripción, 96
  - uso, 83–84
- comando useradd
  - agregar usuario local, 216
  - descripción, 252
- comando userdel, descripción, 252
- comando usermod
  - cambiar propiedades RBAC de usuario, 232
  - descripción, 252
  - usar para asignar rol, 213–215

- comando `uucico`, programa de inicio de sesión, 70
- comando `xauth`, reenvío de X11, 382
- comandos
  - Ver también* comandos individuales
  - comandos criptográficos de nivel de usuario, 283–284
  - comandos de ACL, 136
  - comandos de administración de RBAC, 251–252
  - comandos de asignación de dispositivos, 97
  - comandos de auditoría, 665–671
  - comandos de la estructura criptográfica, 283
  - comandos de política de dispositivos, 95–96
  - comandos de protección de archivos, 127
  - comandos de RPC segura, 325
  - comandos de Secure Shell, 387–389
  - determinar comandos con privilegios de usuario, 266–267
  - Kerberos, 567–568
  - para administrar privilegios, 271
  - que asignan privilegios, 199
  - que comprueban privilegios, 189
- comandos de Kerberos, 558–564
  - sólo habilitación de Kerberizadas, 490
- comandos de shell
  - entradas de archivo `/etc/d_passwd`, 47
  - transferir número de proceso de shell principal, 257
- comandos Kerberizados, ejemplos, 562–564
- combinación de archivos de auditoría
  - comando `auditreduce`, 643–645, 667
- combinación de archivos de auditoría, desde distintas zonas, 678
- complemento `crammd5.so.1`, SASL y, 350
- complemento de mecanismo de seguridad EXTERNAL, SASL y, 350
- complemento `digestmd5.so.1`, SASL y, 350
- complemento `gssapi.so.1`, SASL y, 350
- complemento INTERNAL, SASL y, 350
- complemento `plain.so.1`, SASL y, 350
- complementos
  - cargado por `daemon auditd`, 666
  - en servicio de auditoría, 618
  - estructura criptográfica, 280
  - SASL y, 350
- complementos de auditoría, resumen, 682
- componentes
  - BART, 106–108
  - mecanismo de asignación de dispositivos, 97
  - RBAC, 184–187
  - sesión de usuario de Secure Shell, 377
- comprobación de privilegios, en aplicaciones, 189
- con fallos, prefijo de clase de auditoría, 680
- conexión segura
  - inicio de sesión, 366–367
  - por medio de un cortafuegos, 372
- configuración
  - archivo `audit_class`, 622
  - archivo `audit_event`, 623–624
  - archivo `audit_control`, 615–617
  - archivos de auditoría, 615–624
  - ASET, 162–165, 165
  - asignación de dispositivos, 85–86
  - auditoría en zonas, 596, 678
  - auditoría idéntica para zonas no globales, 637–639
  - auditoría por zona, 639–640
  - autenticación basada en host para Secure Shell, 358–360
  - base de datos `audit_user`, 620–621
  - clave DH en NIS, 331–332
  - clave DH en NIS+, 329–330
  - clave DH para usuario NIS, 332–333
  - clave DH para usuario NIS+, 330–331
  - comando `auditconfig`, 671
  - contraseña para acceso al hardware, 79–80
  - `daemon ssh-agent`, 368–369
  - inicios de sesión de marcación telefónica, 70
- Kerberos
  - adición de principales de administración, 426, 433
  - autenticación entre dominios, 441–443
  - clientes, 452–466
  - descripción general, 421–492
  - mapa de tareas, 421–422
  - servidor KDC esclavo, 437–440
  - servidor KDC maestro, 423–429
  - servidor KDC maestro con LDAP, 429–436
  - servidores NFS, 446–448
  - mapa de tareas de archivos de auditoría, 614
  - mapa de tareas de dispositivos, 81

- configuración (*Continuación*)
  - mapa de tareas de Secure Shell, 358
  - mapa de tareas de servicio de auditoría, 624–625
  - política arge, 657
  - política argv, 657
  - política de auditoría, 629–632
  - política de auditoría ahl\_t, 630–631
  - política de auditoría perzone, 631
  - política de auditoría temporalmente, 631
  - política de dispositivos, 82
  - prevención de desbordamiento de la pista de auditoría, 650
  - reenvío del puerto en Secure Shell, 361–362
  - registros de auditoría textual, 617–620
  - secuencia de comandos audit\_startup, 629–632
  - secuencia de comandos audit\_warn, 629
  - Secure Shell, 357–358
    - clientes, 378
    - servidores, 378
  - seguridad del hardware, 79–80
  - valores predeterminado de principal (Kerberos), 525–526
- configuración de archivos, archivo
  - syslog.conf, 68–69
- configuración de servidores de aplicaciones, 444–445
- configuración del cortafuegos de Internet, 60–61
- configuración manual
  - Kerberos
    - servidor KDC esclavo, 437–440
    - servidor KDC maestro, 423–429
    - servidor KDC maestro con LDAP, 429–436
- configurar
  - mapa de tareas de RBAC, 204–205
  - perfil de derechos desde línea de comandos, 230
  - perfiles de derechos, 228–231
  - RBAC, 205–219
  - roles, 207–210, 226–228
    - desde línea de comandos, 210–213
  - roles personalizados, 212–213
  - servicio de nombres, 217
  - usuario root como rol, 215–219
- conjunto básico de privilegios, 198
- conjunto heredable de privilegios, 197
- conjunto límite de privilegios, 198
- conjunto permitido de privilegios, 197
- conjunto vigente de privilegios, 197
- conjuntos de privilegios
  - agregar privilegios a, 200
  - básicos, 198
  - eliminar privilegios de, 200
  - enumerar, 198
  - heredables, 197
  - límite, 198
  - permitidos, 197
  - vigentes, 197
- consola, visualización de intentos de comando
  - su, 77–78
- CONSOLE en Secure Shell, 383
- consumidores, definición en la estructura
  - criptográfica, 281
- contraseñas
  - acceso al hardware y, 79–80
  - algoritmos de cifrado, 43
  - autenticación en Secure Shell, 354
  - búsqueda de usuarios sin contraseñas, 66
  - cambiar contraseña de rol, 224–226
  - cambio con el comando kpasswd, 554
  - cambio con el comando passwd, 554
  - cambio con el comando passwd -r, 42
  - contraseñas de acceso telefónico
    - archivo /etc/d\_passwd, 46
  - contraseñas de marcación telefónica
    - deshabilitación temporal, 71
  - creación para marcación telefónica, 69–71
  - descifrado de clave secreta para RPC segura, 325
  - deshabilitación de marcación telefónica
    - temporalmente, 71
  - eliminación en Secure Shell, 367–368
  - eliminación en Secure Shell en CDE, 368–369
  - especificación de algoritmo, 72–73
    - en servicios de nombres, 73
    - localmente, 71–72
  - gestión, 553–558
  - inicios de sesión en el sistema, 42
  - instalación de módulo de cifrado de terceros, 75–76
  - LDAP, 42
    - especificación de nuevo algoritmo de contraseña, 74–75

contraseñas (*Continuación*)

- locales, 42
- mapa de tareas, 64
- modificación de la contraseña de un principal, 524
- modo de seguridad de PROM, 41, 79–80
- NIS, 42
  - especificación de nuevo algoritmo de contraseña, 73
- NIS+, 42
  - especificación de nuevo algoritmo de contraseña, 74
- otorgamiento de acceso sin revelar, 556–558
- políticas y, 554
- protección
  - almacén de claves, 319
  - archivo PKCS #12, 319
- requerir para acceso al hardware, 79–80
- seguridad de inicio de sesión, 41, 42
- sugerencias para la elección, 553–554
- UNIX y Kerberos, 553–558
- uso de algoritmo de cifrado Blowfish para, 73
- uso de algoritmo de cifrado MD5 para, 72–73
- uso de nuevo algoritmo, 73
- visualización de usuarios sin contraseñas, 66

contraseñas de acceso telefónico

- archivo `/etc/d_passwd`, 47
- deshabilitación, 47
- seguridad, 46–47

contraseñas de marcación telefónica

- creación, 69–71
- deshabilitación temporal, 71

control

- acceso al sistema, 63–64
- uso del sistema, 50–55

control de acceso basado en roles, *Ver* RBAC

control de costos, y auditoría, 609

control de recursos

- `project.max-locked-memory`, 181, 196–197

control de recursos `zone.max-locked-memory`, 181, 196–197

controlador ncp

- complemento de hardware para estructura criptográfica, 280
- lista de mecanismos, 308

controlador ncp

- complemento de hardware para estructura criptográfica, 280
- lista de mecanismos, 308

controlar, acceso a hardware del sistema, 79

controles de recursos

- privilegios y, 181, 196–197
- `project.max-locked-memory`, 181, 196–197
- `zone.max-locked-memory`, 181, 196–197

convenciones de denominación

- archivos de auditoría, 684
- archivos de identidad de Secure Shell, 384
- autorizaciones RBAC, 242
- devices, 88
- directorios de auditoría, 616, 674

conversión

- registros de auditoría a formato legible, 669
- registros de auditoría en formato legible, 648

copia

- archivos con Secure Shell, 371–372
- entradas de ACL, 147

copia de mensajes de auditoría en un solo archivo, 647

copia de seguridad

- base de datos de Kerberos, 473–474
- KDC esclavos, 415

corchetes ([ ]), salida `bsmrecord`, 686

correctos

- desactivar clases de auditoría para, 681
- prefijo de clase de auditoría, 680

correo, uso con Secure Shell, 370

costos de almacenamiento, y auditoría, 609–610

costos de tiempo de procesamiento, de servicio de auditoría, 609

creación

- archivo `/etc/d_passwd`, 70
- archivo `d_passwd`, 70
- archivo intermedio, 440, 483
- archivo `keytab`, 426, 434
- claves de Secure Shell, 363–365
- claves secretas
  - para cifrado, 288–290, 290–293
- contraseñas de marcación telefónica, 69–71
- contraseñas para usuario temporal, 70
- nueva política (Kerberos), 520, 533–534

creación (*Continuación*)  
 nuevo principal (Kerberos), 520–522  
 particiones de archivos de auditoría  
   binarios, 625–629  
 pista de auditoría  
   daemon auditd, 683  
   rol de daemon auditd, 666  
 resúmenes de archivos, 293–294  
 secuencias de comandos device-clean nuevas, 103  
 tabla de credenciales, 448  
 tickets con kinit, 550

crear  
 perfiles de derechos, 228–231  
 perfiles de derechos con Solaris Management  
   Console, 230  
 rol de administrador del sistema, 208–209  
 rol de operador, 209  
 rol personalizado, 212–213  
 roles  
   con ámbito limitado, 210  
   en línea de comandos, 210–213  
   para determinados perfiles, 207–210  
 roles relacionados con seguridad, 209  
 usuario local, 216  
 usuario root como rol, 215–219

credencial  
 descripción, 326, 570  
 o tickets, 395  
 obtención para un servidor, 577  
 obtención para un TGS, 575–576

credenciales  
 antememoria, 575  
 asignación, 416

criptografía de clave pública  
 base de datos de claves públicas para RPC  
   segura, 325  
 claves comunes  
   cálculo, 327  
 claves secretas NFS, 325  
 generación de claves  
   claves de conversación para NFS seguro, 326  
   uso de Diffie-Hellman, 325  
 modificación de claves públicas y claves secretas  
   NFS, 325

criptografía de clave pública (*Continuación*)  
 sesión cliente-servidor AUTH\_DH, 325–328  
 Cryptoki, Ver biblioteca PKCS #11  
 cuenta root, descripción, 45  
 cuentas de usuario  
   comprobación de ASET, 156  
   visualización de estado de inicio de sesión, 64–65,  
   65  
 cuentas de usuarios  
   Ver también usuarios

## D

opción -D  
 comando auditreduce, 644  
 comando ppriv, 258

daemon /usr/lib/krb5/kadmind, Kerberos y, 568  
 daemon /usr/lib/krb5/kpropd, Kerberos y, 568  
 daemon /usr/lib/krb5/krb5kdc, Kerberos y, 568  
 daemon /usr/lib/krb5/ktkt\_warnd, Kerberos y, 568  
 daemon /usr/sbin/in.ftpd, Kerberos y, 568  
 daemon /usr/sbin/in.rlogind, Kerberos y, 568  
 daemon /usr/sbin/in.rshd, Kerberos y, 568  
 daemon /usr/sbin/in.telnetd, Kerberos y, 568

daemon auditd  
 complementos cargados por, 666  
 creación de pista de auditoría, 666, 683  
 funciones, 666  
 relectura del archivo audit\_control, 635  
 relectura del archivo audit\_control, 635  
 se abren los archivos de auditoría de orden, 673  
 secuencia de comandos audit\_warn  
   descripción, 676  
   ejecución de, 666

daemon de agente, Secure Shell, 367–368  
 daemon de auditd, relectura de información para el  
   núcleo, 635  
 daemon de auditoría, Ver daemon auditd  
 daemon ftpd, Kerberos y, 568  
 daemon gssd, Kerberos y, 568  
 daemon in.ftpd, Kerberos y, 568  
 daemon in.rlogind, Kerberos y, 568  
 daemon in.rshd, Kerberos y, 568  
 daemon in.telnetd, Kerberos y, 568

- daemon kadmind
  - KDC maestro y, 569
  - Kerberos y, 568
- daemon kcfld, 283, 310–311
- daemon keysevr, 329
- daemon kpropd, Kerberos y, 568
- daemon krb5kdc
  - inicio, 440, 483
  - KDC maestro y, 569
  - Kerberos y, 568
- daemon ktkk\_warnd, Kerberos y, 568
- daemon rlogind, Kerberos y, 568
- daemon rshd, Kerberos y, 568
- daemon telnetd, Kerberos y, 568
- daemon vold, desactivado por la asignación de dispositivos, 87
- daemons
  - auditd, 666
  - ejecutar con privilegios, 195
  - kcfld, 283
  - keysevr, 329
  - nscd (daemon de antememoria de servicio de nombres), 208, 251
  - rpc.nispasswd, 74
  - ssh-agent, 367–368
  - sshd, 375–377
  - tabla de Kerberos, 568
  - vold, 87
- decisiones de configuración
  - algoritmo de contraseña, 43
  - auditoría
    - a quién y qué auditar, 602–604
    - almacenamiento de archivos, 601–602
    - política, 605–608
    - zonas, 600–601
  - Kerberos
    - asignación de nombres de host en dominios, 413
    - clientes, 417–418
    - dominios, 412–413
    - jerarquía de dominios, 413
    - KDC esclavos, 415
    - nombres de dominio, 412
    - nombres de principal de servicio y cliente, 414
    - número de dominios, 412–413
  - decisiones de configuración, Kerberos (*Continuación*)
    - propagación de base de datos, 417
    - puertos, 414
    - servidor KDC, 418
    - sincronización de reloj, 417
    - tipos de cifrado, 419
- delegar, autorizaciones RBAC, 243
- depuración
  - archivos de auditoría binarios, 649–650
  - privilegios, 258
- derecho, *Ver* perfiles de derechos
- desasignación
  - dispositivos, 94–95
  - forzada, 89
  - micrófono, 95
- descifrado
  - archivos, 297
  - claves de conversación para RPC segura, 327
  - claves secretas, 325
  - claves secretas NFS, 325
- desfase de reloj, Kerberos y, 466–467
- deshabilitación
  - acceso root remoto, 77–78
  - archivos ejecutables que ponen en riesgo la seguridad, 137
  - asignación de dispositivos, 634
  - cierre del teclado, 80
  - cómo impedir que programas usen pilas ejecutables, 151–152
  - contraseñas de marcación telefónica, 71
  - inicios de sesión de marcación telefónica temporalmente, 71
  - inicios de sesión de usuario, 66–67
  - inicios de sesión temporalmente, 66–67
  - interrupción del teclado, 80
  - pilas ejecutables, 151–152
  - política de auditoría, 629–632
  - registro de mensajes de pilas ejecutables, 152
  - secuencia de interrupción, 80
  - secuencia de interrupción del sistema, 80
  - servicio de auditoría, 634–635
- desinstalación, proveedores criptográficos, 305
- desmontaje, dispositivos asignados, 95
- destrucción, tickets con kdestroy, 552

- detención, inicios de sesión de marcación telefónica temporalmente, 71
- determinación
  - archivos con permisos `setuid`, 150
  - ID de auditoría de un usuario, 660
  - los indicadores de `audit_useron` correctos, 653
  - si el archivo tiene una ACL, 144–145
- determinar
  - `audit_control` indicadores correctos, 653
  - `c2audit` módulo cargado, 652
  - la auditoría se está ejecutando, 652–654
  - mapa de tareas de privilegios, 264
  - privilegios en un proceso, 256–258
- direcciones IP, comprobación de Secure Shell, 379
- directorio `/usr/aset`, 154
- directorio `/usr/aset/reports`, estructura, 159
- directorio `/usr/aset/reports/latest`, 159
- directorio `/usr/share/lib/xml`, 670
- directorio de auditoría
  - creación, 627
  - descripción, 589
  - estructura modelo, 668
  - partición para, 625–629
- directorio de auditoría principal, 673
- directorio de auditoría secundario, 673
- directorios
  - Ver también* archivos
  - archivos maestros (ASET), 161
  - configuración de tarea de lista de comprobación (ASET), 163, 169
  - definiciones de archivos `audit_control`, 673
  - directorio de trabajo (ASET), 167, 172–173
  - directorios de auditoría llenos, 666, 677
  - directorios públicos, 131
  - entradas de ACL, 136
  - informes (ASET), 159
  - montaje de directorios de auditoría, 684
  - permisos
    - descripción, 129
    - valores predeterminados, 131–132
  - puntero de `daemon auditd`, 666
  - puntero de `daemon auditd`, 666
  - visualización de archivos e información relacionada, 128, 138–139
- directorios públicos
  - auditoría, 589
  - bit de permanencia y, 131
- disco duro, requisitos de espacio para auditoría, 609–610
- dispositivo `/dev/arp`, obtención de información MIB-II IP, 84–85
- dispositivo `/dev/urandom`, 288–290
- dispositivos
  - agregar una política de dispositivos, 83–84
  - asignación de dispositivos
    - Ver* asignación de dispositivos
  - asignación forzada, 88–89
  - asignación para uso, 91
  - auditoría de asignación, 90–91
  - auditoría de cambios en política, 84
  - autorización de usuarios para asignar, 87
  - cambio de los que se pueden asignar, 89–90
  - cambio de política de dispositivos, 83–84
  - comandos de política, 95–96
  - control de acceso de inicio de sesión, 46
  - desasignación de un dispositivo, 94–95
  - desasignación forzada, 89
  - desmontaje de un dispositivo asignado, 95
  - dispositivo `/dev/urandom`, 288–290
  - eliminación de política, 84
  - enumeración, 82–83
  - enumeración de nombres de dispositivos, 88
  - gestión, 82
  - gestión de asignación de, 85–86
  - modelo de privilegios y, 201
  - modelo de superusuario y, 201
  - montaje de dispositivos asignados, 92–94
  - no requieren autorización para uso, 90
  - obtención de información MIB-II IP, 84–85
  - permitir asignación, 86–87
  - prevención de uso de algunos, 90
  - prevención de uso de todos, 90
  - protección en el núcleo, 47
  - protección por asignación de dispositivos, 47
  - seguridad, 47–49
  - visualización de información de asignación, 88
  - visualización de política de dispositivos, 82–83
  - zonas y, 48



- dispositivos de audio, seguridad, 102
- dispositivos SCSI, secuencia de comandos
  - st\_clean, 101
- DNS, Kerberos y, 414
- documentación de tarjeta inteligente, puntero hacia, 34
- dominios (Kerberos)
  - asignación de nombres de host en, 413
  - configuración de autenticación entre dominios, 441–443
  - contenidos de, 400
  - decisiones de configuración, 412–413
  - directos, 442–443
  - en nombres de principales, 399
  - jerarquía, 413
  - jerárquicos, 441–442
  - jerárquicos o no jerárquicos, 399–400
  - nombres, 412
  - número de, 412–413
  - servidores y, 400
  - solicitud de tickets para dominios específicos, 560
- dominios directos, 442–443
- dominios jerárquicos
  - configuración, 441–442
  - en Kerberos, 399–400, 413
- dominios no jerárquicos, en Kerberos, 399–400
- DTD para comando praudit, 670
- duplicación, principales (Kerberos), 523
- duración de tickets, en Kerberos, 572–573

## E

- eficacia, auditoría y, 610
- ejecución de comandos, Secure Shell, 377
- ejecución interactiva de ASET, 172–173
- elección, su contraseña, 553–554
- eliminación
  - archivos de auditoría, 643
  - archivos de auditoría almacenados, 650
  - archivos de auditoría not\_terminated, 649–650
  - entradas de ACL, 136, 148
  - eventos de auditoría de archivo audit\_event, 661
  - política de dispositivos, 84
  - principal de servicio del archivo keytab, 545–546

- eliminación (*Continuación*)
  - principales con el comando ktremove, 545
  - proveedores criptográficos, 305
  - proveedores de software
    - permanente, 307
    - temporal, 306
- eliminar
  - perfiles de derechos, 229
  - privilegios de conjunto básico, 262
  - privilegios de conjunto límite, 262
- enlaces simbólicos, permisos de archivo, 129
- entrada audit.notice, archivo syslog.conf, 618
- entrada c2audit:audit\_load, archivo system, 672
- entrada kern.notice, archivo syslog.conf, 137
- entrada priv.debug, archivo syslog.conf, 273
- entradas de ACL de grupo
  - configuración, 145–146
  - descripción, 135–136
  - entradas predeterminadas para directorios, 136
- entradas de ACL de máscara
  - configuración, 145–146
  - descripción, 135–136
  - entradas predeterminadas para directorios, 136
- entradas de ACL de usuario
  - configuración, 145–146
  - descripción, 135–136
  - entradas predeterminadas para directorios, 136
- enumeración
  - contenido de almacenes de claves, 316
  - política de dispositivos, 82–83
- enumerar
  - roles que puede asumir, 220, 252
- Equipo de Respuesta ante Emergencias Informáticas/Centro de Coordinación (CERT/CC), 62
- equivalentes de línea de comandos de la herramienta SEAM, 511–512
- errores
  - directorios de auditoría llenos, 666, 677
  - errores internos, 677
  - estado de error de asignación, 98–99
- estado de error de asignación, 98–99
- Estándar de cifrado de datos, Ver cifrado DES



estructura criptográfica

- actualización, 310–311
- administrar con rol, 214–215
- biblioteca PKCS #11, 280
- comando `cryptoadm`, 282, 283
- comando `elfsign`, 282, 284
- comandos de nivel de usuario, 283–284
- complementos de hardware, 280
- conexión de proveedores, 284
- consumidores, 280
- definición de términos, 281
- descripción, 280
- instalación de proveedores, 284
- interacción con, 282
- lista de proveedores, 300–302
- mapas de tareas, 287
- mensajes de error, 298
- proveedores, 280, 281
- registro de proveedores, 284
- reinicio, 310–311
- zonas y, 285, 310–311

estructura criptográfica de Oracle Solaris, *Ver* estructura criptográfica

estructura de directorios `/usr/aset/reports`, 158

estructura de gestión de claves (KMF), *Ver* KMF

evento, descripción, 590

eventos de auditoría

- archivo `audit_event`, 590
- asignación a clases, 592
- cambio de pertenencia de clase, 623–624
- descripción, 590
- resumen, 589
- selección de pista de auditoría, 645–647
- selección desde pista de auditoría en zonas, 678
- visualización de archivos binarios, 647–649

evitar, desbordamiento de la pista de auditoría, 650

## F

opción -f

- comando `setfacl`, 147
- comandos Kerberizados, 559, 561–562
- secuencia de comandos `st_clean`, 103

opción -F

- comando `deallocate`, 98–99
- comandos Kerberizados, 560, 561–562

fallo, desactivar clases de auditoría para, 681

fin, señal recibida durante cierre de auditoría, 677

flecha de adición (>), prevención de adición, 52

flecha de redirección (>), prevención de redirección, 52

formato de archivo de reglas (BART), 124–125

formato de registro de auditoría legible

- conversión de registros de auditoría a, 669
- conversión de registros de auditoría en, 648

formato de registro de auditorías, comando

- `bsmrecord`, 641

formato de salida de `praudit corto`, 670

formato de salida `praudit` sin procesar, 670

formato `syslog`, registros de auditoría, 672

formato XML, registros de auditorías, 648

FQDN (nombre de dominio completo), en Kerberos, 414

frases de contraseña

- almacenamiento seguro, 297
- comando `encrypt`, 296
- comando `mac`, 295
- generación en KMF, 320
- uso en Secure Shell, 365
- uso para MAC, 295–296

frases de contraseñas

- cambio para Secure Shell, 365–366
- ejemplo, 366
- uso en Secure Shell, 367–368

funciones nuevas

- BART, 105–126

comandos

- `bart create`, 106–107
- `getdevpolicy`, 82–83
- `ppriv`, 256–258

gestión de derechos de procesos, 193–202

mejoras de la seguridad del sistema, 39–40

mejoras de PAM, 337–338

privilegios, 193–202

fusión, registros de auditoría binarios, 643–645

**G**

## generación

- certificados con el comando `pktool`, 316–317
- clave simétrica
  - uso del comando `dd`, 288–290
  - uso del comando `pktool`, 290–293
- claves de Secure Shell, 363–365
- claves para Secure Shell, 363–365
- claves secretas NFS, 325
- frases de contraseña con el comando `pktool`, 320
- número aleatorio
  - uso del comando `dd`, 288–290
  - uso del comando `pktool`, 290–293

Generic Security Service API, *Ver* GSS-API

## gestión

*Ver también* administración

- archivos de auditoría, 643–645, 650
- auditoría, 613
  - prevención de desbordamiento de la pista de auditoría, 650
- auditoría en zonas, 596, 600–601, 678
- contraseñas con Kerberos, 553–558
- desbordamiento de la pista de auditoría, 650
- dispositivos, 85–86
- mapa de tareas de asignación de dispositivos, 85–86
- mapa de tareas de registros de auditoría, 640–641
- permisos de archivo, 138

## gestión de criptografía (RBAC)

- crear rol, 214–215
- uso de perfil de derechos, 304, 305

gestión de derechos de procesos, *Ver* privilegiosgestión de derechos de usuarios, *Ver* privilegios

## gestión de DHCP (RBAC), crear rol, 210

gestión de dispositivos, *Ver* política de dispositivos

## gestión de impresoras (RBAC), contenido de perfil de derechos, 240

## gestionar

- mapa de tareas de privilegios, 256
- mapa de tareas de RBAC, 223–224

## grupos, cambio de propiedad de archivo, 140–141

## GSS-API

- autenticación en Secure Shell, 354
- credenciales en RPC segura, 329–330
- credenciales en Secure Shell, 376

GSS-API (*Continuación*)

Kerberos y, 394, 409

guardar, intentos de inicio de sesión fallidos, 67–68

**H**

## habilitación

- asignación de dispositivo, 86–87
- asignación de dispositivos, 86
- interrupción del teclado, 80
- mapa de tareas de servicio de auditoría, 624–625
- mecanismos criptográficos, 305
- mecanismos y funciones en el proveedor de hardware, 309
- sólo aplicaciones Kerberizadas, 490
- uso de un proveedor de software de núcleo, 306

## habilitación de auditoría automática, 674–675

## habilitar

- auditoría, 632–634
- servicio de auditoría, 632–634

## hardware

- lista de aceleradores de hardware conectados, 308
- protección, 40–41, 79–80
- requerir contraseña para acceso, 79–80

## hardware del sistema, control de acceso a, 79–80

## hash

- algoritmos
- Kerberos y, 419

## hashing, archivos, 288

## Help Contents, herramienta SEAM, 512

Herramienta automatizada de mejora de la seguridad, *Ver* ASETHerramienta básica de creación de informes de auditoría, *Ver* BARTherramienta de creación de informes, *Ver* bart

*compare*

## herramienta Rights, descripción, 228–231

## herramienta SEAM

- archivo `.gkadmin`, 512
- archivos modificados por, 512
- ayuda contextual, 512
- campo Filter Pattern, 517
- comando `gkadmin`, 509
- comando `kadmin`, 509

## herramienta SEAM (*Continuación*)

- configuración de valores predeterminados de principal, 525–526
  - creación de un nuevo principal, 520–522
  - creación de una nueva política, 520, 533–534
  - descripción de paneles, 537–540
  - descripción general, 510–514
  - duplicación de un principal, 523
  - efecto de los privilegios, 541
  - equivalentes de línea de comandos, 511–512
  - Help Contents, 512
  - inicio, 513–514
  - modificación de un principal, 523–524
  - modificación de una política, 535–536
  - o comando `kadmin`, 510
  - privilegios, 540
  - supresión de políticas, 536–537
  - supresión de un principal, 525
  - tabla de paneles, 537–540
  - valores predeterminados, 514
  - ventana de inicio de sesión, 513
  - visualización de atributos de política, 531–533
  - visualización de la lista de políticas, 529–531
  - visualización de la lista de principales, 516–518
  - visualización de los atributos de un principal, 518–520
  - visualización de sublista de principales, 517
  - y privilegios de administración limitados, 540–541
  - y privilegios de lista, 540
  - y sistema de ventanas X, 511–512
- herramienta User Accounts, descripción, 231–233
- herramienta SEAM
- ayuda, 512
  - ayuda en pantalla, 512
- hosts
- hosts de confianza, 60
  - hosts de Secure Shell, 354
  - inhabilitación de servicio de Kerberos en, 547–548
  - prerrequisito de auditoría, 633
- hosts de confianza, 60

## I

- opción -I
  - comando `bart create`, 110
  - secuencia de comandos `st_clean`, 103
- ID
  - asignación de UNIX a principales de Kerberos, 581
  - auditoría
    - descripción general, 585–587
- ID de auditoría
  - descripción general, 585–587
  - mecanismo, 683
- ID de sesión, auditoría, 683
- ID de sesión de auditoría, 683
- ID de terminal, auditoría, 683
- ID de usuario
  - en servicios NFS, 448
  - ID de auditoría y, 585–587, 683
- identificadores
  - auditoría
    - mecanismo, 683
    - sesión de auditoría, 683
- idioma de especificación de archivo de reglas, *Ver*
  - sintaxis de comillas
- impedir
  - acceso a hardware del sistema, 79
  - cómo impedir que archivos ejecutables pongan en riesgo la seguridad, 137
  - uso de mecanismo de hardware, 308–310
  - uso de un proveedor de software de núcleo, 305–307
- impresión, registro de auditoría, 648
- indicaciones de hora, informes de ASET, 159
- indicador de control binding, PAM, 343
- indicador de control include, PAM, 343
- indicador de control optional, PAM, 343
- indicador de control required, PAM, 344
- indicador de control requisite, PAM, 344
- indicador de control sufficient, PAM, 344
- indicadores de campo de modificador de evento (token header), 693
- indicadores de hora, archivos de auditoría, 685
- informática, clave DH, 331
- informes
  - ASET, 159, 160–161, 166

informes (*Continuación*)

- BART, 105
- comparación (ASET), 161
- directorío (ASET), 159

## inhabilitación

- mecanismos criptográficos, 304
- mecanismos de hardware, 308–310
- servicio en un host (Kerberos), 547–548

## iniciar sesión

- auditoría de inicios de sesión, 662
- conjunto básico de privilegios del usuario, 198

## inicio

- ASET de shell, 154
- ASET interactivamente, 172–173
- asignación de dispositivo, 86–87
- auditoría, 632–634
- daemon de auditoría, 636
- daemon del KDC, 440, 483
- ejecución periódica de ASET, 173
- servidor de claves RPC segura, 329

## inicio de sesión

- con Secure Shell, 366–367
- deshabilitación temporal, 66–67
- inicio de sesión root

- restricción a consola, 77–78
- seguimiento, 50

## mapa de tareas, 64

## registro de inicios de sesión fallidos, 68–69

## seguridad

- control de acceso al sistema, 41
- control de acceso en dispositivos, 46
- guardar intentos fallidos, 67–68
- restricciones de acceso, 41
- seguimiento de inicio de sesión root, 50
- supervisión de fallos, 67–68
- visualización de estado de inicio de sesión de usuario, 64–65, 65

## y AUTH\_DH, 325

## inicio de sesión automático

- deshabilitación, 560
- habilitación, 559

## inicios de sesión remotos

- autenticación, 58–59
- autorización, 58–59

inicios de sesión remotos (*Continuación*)

- evitar que el superusuario, 77–78
- seguridad y, 327

## instalación

- módulo de cifrado de contraseña, 75–76
- proveedores en la estructura criptográfica, 284
- seguridad predeterminada, 53

## instancias, en nombres de principales, 399

## integridad

- Kerberos y, 393
- servicio de seguridad, 401

## intentos de inicio de sesión fallidos

- archivo loginlog, 67–68
- archivo syslog.conf, 68–69

## intercambio de KDC maestros y esclavos, 468–473

**K**

## opción -k

- comando encrypt, 297
- comando mac, 295
- comandos Kerberizados, 560

## opción -K

- comando usermod, 261
- comandos Kerberizados, 560

## KDC

- configuración de esclavo
  - manual, 437–440
- configuración de maestro
  - manual, 423–429
- configuración de servidor maestro
  - con LDAP, 429–436
- copia de archivos de administración del esclavo al maestro, 438, 482
- copia de seguridad y propagación, 473–474
- creación de base de datos, 425
- creación de principal host, 428, 435
- esclavo, 415
  - definición, 569
- esclavo o maestro, 423
- esclavos o maestro, 400
- inicio de daemon, 440, 483
- intercambio de maestro y esclavo, 468–473

**KDC (Continuación)**

- maestro
  - definición, 569
  - planificación, 415
  - propagación de base de datos, 417
  - puertos, 414
  - restricción de acceso a servidores, 490–491
  - sincronización de relojes
    - KDC esclavo, 440, 483
    - KDC maestro, 429, 436

**KDC esclavos**

- configuración, 437–440
- definición, 569
- intercambio con KDC maestro, 468–473
- KDC maestro y, 400
- o maestro, 423
- planificación para, 415

**KDC maestro**

- configuración con LDAP, 429–436
- configuración manual, 423–429
- definición, 569
- intercambio con KDC esclavo, 468–473
- KDC esclavos y, 400, 423

**Kerberos**

- administración, 509–548
- aplicaciones remotas, 398
- archivos, 565–567
- ayuda pantalla, 419–420
- comandos, 558–564, 567–568
- componentes de, 402–403
- configuración de servidores KDC, 423–441
- daemons, 568
- decisiones de configuración, 411–420
- descripción general
  - comandos Kerberizados, 558–561
  - sistema de autenticación, 394–400, 575
- dominios
  - Ver dominios (Kerberos)*
- ejemplos de uso de comandos
  - Kerberizados, 562–564
- gestión de contraseñas, 553–558
- herramienta de administración
  - Ver herramienta SEAM*
- mensajes de error, 493–506

**Kerberos (Continuación)**

- obtención de acceso al servidor, 575–578
- opción de archivo `dfstab`, 451
- opciones para comandos Kerberizados, 559
- otorgamiento de acceso a su cuenta, 556–558
- planificación para, 411–420
- protocolo Kerberos V5, 393
- referencia, 565–582
- resolución de problemas, 506
- sólo habilitación de aplicaciones Kerberizadas, 490
- tabla de opciones de comandos de red, 560
- terminología, 569–575
- tipos de cifrado
  - descripción general, 419
  - uso, 579–581
- uso, 549–564

**keystores, protección con contraseña en KMF, 320****kit de herramientas JASS, puntero a, 53****KMF**

- administración
  - almacenes de claves, 315
  - política PKI, 314
  - tecnologías de clave pública (PKI), 313
- almacenes de claves, 314, 315
- biblioteca, 314
- creación
  - certificado autofirmado, 316–317
  - contraseña para almacén de claves, 320
  - frases de contraseña para almacenes de claves, 315
- exportación de certificados, 318–320
- importación de certificados a almacén de claves, 317–318
- utilidades, 314

**L**

- opción `-L`, comando `ssh`, 369–371
- `-l` opción, comando `encrypt`, 289
- las claves de servicio, archivos `keytab` y, 542–548
- LDAP, configuración de KDC maestro con, 429–436
- limitación, tamaño de archivo de auditoría, 661–662
- limitar, uso de privilegios por usuario o rol, 261–263

## límite de aviso

- condición `audit_warn`, 676
- descripción de línea `minfree`, 673

## limpieza estándar, secuencia de comandos

- `st_clean`, 103

## limpieza forzada, secuencia de comandos

- `st_clean`, 103

línea `dir`, archivo `audit_control`, 673línea `flags`

- archivo `audit_control`, 673
- máscara de preselección de proceso, 683

línea `minfree`

- archivo `audit_control`, 673
- condición `audit_warn`, 676

línea `naflags`, archivo `audit_control`, 673línea `plugin`

- archivo `audit_control`, 673
- atributo `qsize`, 618
- atributos `p_*`, 618

## lista

- proveedores de estructura criptográfica, 308
- proveedores de hardware, 308
- proveedores de la estructura criptográfica, 300–302
- proveedores disponibles de la estructura criptográfica, 300–302
- usuarios sin contraseñas, 66

## lista de control de acceso

*Ver* ACL

listas de control de acceso (ACL), *Ver* ACL

## llamadas de sistema

- `ioctl()`, 680
- llamada de sistema `close`, 679
- token de auditoría `arg`, 689
- token de auditoría `exec_args`, 691
- token de auditoría `exec_env`, 691–692
- token de auditoría `return`, 700

llamadas de sistema `ioctl()`, 680llamadas del sistema, `ioctl` para limpiar dispositivo de audio, 102llamadas del sistema `ioctl()`, `AUDIO_SETINFO()`, 102archivo `.login`, entrada de variable `path`, 51**M**opción `-M`, comando `auditreduce`, 644

## manifiestos

*Ver también* `bart create`

- control, 105
- de prueba, 107
- formato de archivo, 123
- personalización, 112–115

## manifiestos de control (BART), 105

## manifiestos de prueba, 107

## mapa de tareas

- auditoría, 613
- configuración de archivos de auditoría, 614
- dispositivos, 81

## mapa de tareas de auditoría de Solaris, 613

## mapa de tareas de ejecución de ASET, 171–175

mapa `publickey`, autenticación DH, 324–328

## mapas de tarea

- gestión de registros de auditoría, 640–641
- resolución de problemas de auditoría de Solaris, 651–663

## mapas de tareas

- acceso al sistema, 63–64
- administración de la estructura criptográfica, 299
- administración de políticas (Kerberos), 528–529
- administración de principales (Kerberos), 514–515
- administración de RPC segura, 328
- ASET, 171–175
- asignación de dispositivos, 85–86, 91
- cambio de algoritmo predeterminado para cifrado de contraseña, 71–72
- configuración de dispositivos, 81
- configuración de Kerberos, 421–422
- configuración de política de dispositivos, 82
- configuración de Secure Shell, 358
- configuración de servicio de auditoría, 624–625
- configuración de servidores NFS con Kerberos, 446
- configurar RBAC, 204–205
- control de acceso a hardware del sistema, 79
- ejecución de ASET, 171–175
- estructura criptográfica, 287
- gestión de asignación de dispositivos, 85–86
- gestión de política de dispositivos, 82
- gestionar RBAC, 223–224

- mapas de tareas (*Continuación*)
  - gestionar y usar privilegios, 255
  - habilitación de servicio de auditoría, 624–625
  - mantenimiento de Kerberos, 422
  - PAM, 338
  - planificación de auditoría, 599–600
  - política de dispositivos, 82
  - protección contra programas con riesgo de seguridad, 150
  - protección de archivos, 138
  - protección de archivos con ACL, 144
  - protección de archivos con mecanismos criptográficos, 288
  - protección de archivos con permisos UNIX, 138
  - protección de hardware del sistema, 79
  - protección de inicios de sesión y contraseñas, 64
  - protección de sistemas, 63–64
  - Secure Shell, 357–358
  - supervisión y restricción de superusuario, 76
  - usar RBAC, 203–204
  - usar roles, 219
  - uso de la asignación de dispositivos, 91
  - uso de la estructura criptográfica, 287
  - uso de la estructura de gestión de claves (mapa de tareas), 315–316
  - uso de Secure Shell, 362–363
  - Uso del mapa de tareas de BART, 108–109
- máscara (auditoría)
  - descripción de preselección de proceso, 683
  - preselección de proceso en todo el sistema, 673
- máscara de preselección (auditoría)
  - descripción, 683
  - en todo el sistema, 673
  - reducción de costos de almacenamiento, 667
- máscara de preselección de auditoría
  - modificación para usuarios existentes, 659–660
  - modificación para usuarios individuales, 620–621
- máscara de preselección de proceso, descripción, 683
- mecanismo, definición en la estructura criptográfica, 281
- mecanismo de seguridad, especificación con la opción -m, 560
- mecanismo mech\_dh
  - credenciales GSS-API, 377
- mecanismo mech\_dh (*Continuación*)
  - RPC segura, 329–330
- mecanismo mech\_krb, credenciales GSS-API, 377
- mecanismos
  - habilitación de algunos en el proveedor de hardware, 309
  - inhabilitación de todo en el proveedor de hardware, 308–310
- mediante
  - ACL, 145–146
  - permisos de archivo, 138
- mensajes de auditoría, copia en un solo archivo, 647
- mensajes de error
  - comando encrypt, 298
  - con kpasswd, 554
  - Kerberos, 493–506
- mensajes file, mensajes de pilas ejecutables, 137
- metarranura
  - administración, 283
  - definición en la estructura criptográfica, 281
- métodos de autenticación
  - basada en host en Secure Shell, 358–360
  - basado en host en Secure Shell, 355
  - claves públicas en Secure Shell, 355
  - contraseña en Secure Shell, 355
  - credenciales GSS-API en Secure Shell, 354
  - Secure Shell, 354–356
  - teclado interactivo en Secure Shell, 355
- MIB-II IP, obtención de información de /dev/arp, 84–85
- micrófono
  - asignación, 92
  - desasignación, 95
- modificación
  - claves secretas NFS, 325
  - contraseña de principal (Kerberos), 524
  - políticas (Kerberos), 535–536
  - principales (Kerberos), 523–524
- modificar
  - asignación de rol a un usuario, 210
  - roles (RBAC), 226–228
  - usuarios (RBAC), 231–233
- modo, definición en la estructura criptográfica, 281



modo absoluto  
 cambio de permisos de archivo, 132, 142–143  
 cambio de permisos de archivo especiales, 143–144  
 configuración de permisos especiales, 133  
 descripción, 132  
 modo de seguridad de PROM, 79–80  
 modo simbólico  
 cambio de permisos de archivo, 133, 141–142  
 descripción, 132  
 modos de permiso de archivo  
 modo absoluto, 132  
 modo simbólico, 133  
 modos de seguridad, configuración de entorno con  
 varios, 450–452  
 módulo básico de seguridad (BSM)  
*Ver* asignación de dispositivos  
*Ver* auditoría  
 módulo c2audit, verificar que esté cargado, 652  
 módulo de autenticación conectable, *Ver* PAM  
 módulos, cifrado de contraseña, 43  
 montaje  
 archivos con autenticación DH, 333  
 CD-ROM asignado, 94  
 directorios de auditoría, 684  
 dispositivos asignados, 92–94  
 disquete asignado, 93–94  
 mostrar  
 roles que puede asumir, 220, 252

## N

NFS seguro, 324  
 nivel de protección  
 configuración en ftp, 560  
 privado, 561  
 seguro, 561  
 sin cifrar, 561  
 nivel de protección privado, 561  
 nivel de protección seguro, 561  
 nivel de protección sin cifrar, 561  
 nivel de seguridad alto de ASET, 155  
 nivel de seguridad bajo de ASET, 154  
 nivel de seguridad medio de ASET, 154

nombres  
 archivos de auditoría, 684  
 clases de auditoría, 679  
 nombres de dispositivos  
 archivo device\_maps, 99, 100  
 nombres de cliente, planificación en Kerberos, 414  
 nombres de host  
 asignación en dominios, 413  
 prerequisite de auditoría, 633  
 nsd (daemon de antememoria de servicio de nombres)  
 iniciar con comando svcadm, 208  
 usar, 251  
 NSS, administración de almacén de claves, 315  
 NTP  
 KDC esclavo y, 440, 483  
 KDC maestro y, 429, 436  
 planificación Kerberos y, 417  
 nuevas funciones  
 comandos  
 cryptoadm, 299  
 kclient, 405  
 kproxd, 405  
 praudit -x, 648  
 ssh-keyscan, 387  
 ssh-keysign, 387  
 estructura criptográfica, 279–285  
 estructura criptográfica de Oracle Solaris, 279–285  
 mejoras de Kerberos, 405–407  
 mejoras de la auditoría, 597–598  
 mejoras de Secure Shell, 356–357  
 metarranura, 279  
 SASL, 349  
 número de secuencia de depuración, 700–701  
 números aleatorios  
 comando dd, 288–290  
 comando pkttool, 290–293  
 números de ID de usuario (UID), cuentas especiales  
 y, 45  
 nunca\_auditar\_clases, base de datos audit\_user, 675

## O

opción -O, comando auditreduce, 643–645  
 objetos públicos, auditoría, 589



- obtención
  - acceso a un servicio específico, 578
  - credencial para un servidor, 577
  - credencial para un TGS, 575–576
  - tickets con kinit, 550
  - tickets reenviables, 550
- obtener
  - comandos con privilegios, 226–228
  - privilegios, 198, 199, 260–261
  - privilegios en un proceso, 256–258
- opción -a
  - comando bsmrecord, 641
  - comando digest, 294
  - comando encrypt, 297
  - comando getfacl, 148
  - comando mac, 295
  - comando smrole, 212–213
  - comandos Kerberizados, 559
- opción -b, comando auditreduce, 645
- opción -c
  - comando auditreduce, 646, 647
- opción -d
  - comando auditreduce, 647
  - comando getfacl, 149
  - comando praudit, 669
  - comando setfacl, 148
- opción -e
  - comando auditreduce, 646
  - comando ppriv, 258
- opción -h, comando bsmrecord, 641
- opción -i
  - comando bart create, 110, 115
  - comando encrypt, 297
  - secuencia de comandos st\_clean, 103
- opción -l
  - comando digest, 293
  - comando mac, 295
  - comando praudit, 669
- opción -m
  - comando cryptoadm, 304, 305
  - comandos Kerberizados, 560
- opción -n
  - comando audit, 666
  - comando bart create, 110
- opción -o, comando encrypt, 297
- opción -p
  - bart create, 115
  - comando aset, 173
  - comando bsmrecord, 642
  - comando cryptoadm, 304, 306
  - comando logins, 66
- opción -r
  - bart create, 115
  - comando passwd, 42
  - comando praudit, 670
- opción -s
  - comando audit, 666
  - comando praudit, 670
- opción -v
  - comando audit, 616
  - comando digest, 294
  - comando mac, 295
  - comando ppriv, 257
- opción -x
  - comando praudit, 670
  - comandos Kerberizados, 560
- opción auto\_transition, SASL y, 351
- opción auxprop\_login, SASL y, 351
- opción -c, comando bsmrecord, 642–643
- opción canon\_user\_plugin, SASL y, 351
- opción de instalación con seguridad
  - predeterminada, 53
- opción de instalación netservices limited, 53
- opción keytab, SASL y, 351
- opción log\_level, SASL y, 351
- opción mech\_list, SASL y, 351
- opción plugin\_list, SASL y, 351
- opción pwcheck\_method, SASL y, 351
- opción reauth\_timeout, SASL y, 351
- opción rewoffl
  - comando mt
    - limpieza de dispositivo de cinta y, 102
- opción saslauthd\_path, SASL y, 351
- opción use\_authid, SASL y, 351
- opción XML, comando praudit, 670
- opciones para comandos Kerberizados, 559
- OpenSSH, Ver Secure Shell
- OpenSSL, administración de almacén de claves, 315

- operador (RBAC)
  - contenido de perfil de derechos, 239
  - crear rol, 209
  - rol recomendado, 183
- operador personalizado (RBAC), crear rol, 212–213
- otorgamiento de acceso a su cuenta, 556–558
- otras entradas de ACL, descripción, 135–136

## P

- palabra clave AllowGroups, archivo sshd\_config, 379
- palabra clave AllowTcpForwarding
  - archivo sshd\_config, 379
  - cambio, 362
- palabra clave AllowUsers, archivo sshd\_config, 379
- palabra clave AuthorizedKeysFile, archivo sshd\_config, 379
- palabra clave AUTHS\_GRANTED, archivo policy.conf, 250
- palabra clave Banner, archivo sshd\_config, 379
- palabra clave Batchmode, archivo ssh\_config, 379
- palabra clave BindAddress, archivo ssh\_config, 379
- palabra clave ChallengeResponseAuthentication, *Ver* palabra clave KbdInteractiveAuthentication
- palabra clave CheckHostIP, archivo ssh\_config, 379
- palabra clave ChrootDirectory, archivo ssh\_config, 379
- palabra clave Cipher, archivo ssh\_config, 379
- palabra clave Ciphers, Secure Shell, 379
- palabra clave ClearAllForwardings, reenvío del puerto de Secure Shell, 379
- palabra clave ClientAliveCountMax, archivo ssh\_config, 379
- palabra clave ClientAliveInterval, archivo ssh\_config, 379
- palabra clave Compression, Secure Shell, 379
- palabra clave CompressionLevel, archivo ssh\_config, 379
- palabra clave ConnectionAttempts, archivo ssh\_config, 379
- palabra clave CRYPT\_ALGORITHMS\_ALLOW, archivo policy.conf, 44
- palabra clave CRYPT\_ALGORITHMS\_DEPRECATED, archivopolicy.conf, 44

- palabra clave CRYPT\_DEFAULT, archivo policy.conf, 44
- palabra clave defaultpriv, base de datos user\_attr, 273
- palabra clave DenyGroups, archivo sshd\_config, 379
- palabra clave DenyUsers, archivo sshd\_config, 379
- palabra clave DSAAAuthentication, *Ver* palabra clave PubkeyAuthentication
- palabra clave DynamicForward, archivo ssh\_config, 379
- palabra clave EscapeChar, archivo ssh\_config, 379
- palabra clave FallBackToRsh, archivo ssh\_config, 379
- palabra clave ForwardAgent, autenticación de reenvío de Secure Shell, 379
- palabra clave ForwardX11, reenvío del puerto de Secure Shell, 379
- palabra clave GatewayPorts, Secure Shell, 380
- palabra clave GlobalKnownHostsFile
  - Ver* palabra clave GlobalKnownHostsFile
  - archivo ssh\_config, 380
- palabra clave GSSAPIAuthentication, Secure Shell, 380
- palabra clave GSSAPIDelegateCredentials, archivo ssh\_config, 380
- palabra clave GSSAPIKeyExchange, Secure Shell, 380
- palabra clave GSSAPIStoreDelegatedCredentials, archivo sshd\_config, 380
- palabra clave Host
  - archivo ssh\_config, 380, 382
- palabra clave HostbasedAuthentication, Secure Shell, 380
- palabra clave HostbasedUsesNameFromPacketOnly, archivo sshd\_config, 380
- palabra clave HostKey, archivo sshd\_config, 380
- palabra clave HostKeyAlgorithms, archivo ssh\_config, 380
- palabra clave HostKeyAlias, archivo ssh\_config, 380
- palabra clave HostName, archivo ssh\_config, 380
- palabra clave IdentityFile, archivo ssh\_config, 380
- palabra clave IgnoreRhosts, archivo sshd\_config, 380
- palabra clave IgnoreUserKnownHosts, archivo sshd\_config, 380

- palabra clave KbdInteractiveAuthentication, Secure Shell, 380
- palabra clave KeepAlive, Secure Shell, 380
- palabra clave KeyRegenerationInterval, archivo sshd\_config, 380
- palabra clave limitpriv, base de datos user\_attr, 273
- palabra clave ListenAddress, archivo sshd\_config, 380
- palabra clave LocalForward, archivo ssh\_config, 380
- palabra clave LoginGraceTime, archivo sshd\_config, 381
- palabra clave LogLevel, Secure Shell, 381
- palabra clave LookupClientHostnames, archivo sshd\_config, 381
- palabra clave MACS, Secure Shell, 381
- palabra clave MaxAuthTries, archivo sshd\_config, 381
- palabra clave MaxAuthTriesLog, archivo sshd\_config, 381
- palabra clave MaxStartups, archivo sshd\_config, 381
- palabra clave NoHostAuthenticationForLocalHost, archivo ssh\_config, 381
- palabra clave NumberOfPasswordPrompts, archivo ssh\_config, 381
- palabra clave PAMAuthenticationViaKBDInt, archivo sshd\_config, 381
- palabra clave PasswordAuthentication, Secure Shell, 381
- palabra clave PermitEmptyPasswords, archivo sshd\_config, 381
- palabra clave PermitRootLogin, archivo sshd\_config, 381
- palabra clave PermitUserEnvironment, archivo sshd\_config, 381
- palabra clave PidFile, Secure Shell, 381
- palabra clave Port, Secure Shell, 381
- palabra clave PreferredAuthentications, archivo ssh\_config, 381
- palabra clave PrintLastLog, archivo ssh\_config, 381
- palabra clave PrintMotd, archivo sshd\_config, 381
- palabra clave PRIV\_DEFAULT
  - archivo policy.conf, 250, 272
- palabra clave PRIV\_LIMIT
  - archivo policy.conf, 250, 272
- palabra clave privs, base de datos user\_attr, 273
- palabra clave PROFS\_GRANTED, archivo policy.conf, 250
- palabra clave Protocol, Secure Shell, 381
- palabra clave ProxyCommand, archivo ssh\_config, 381
- palabra clave PubkeyAuthentication, Secure Shell, 381
- palabra clave RemoteForward, archivo ssh\_config, 381
- palabra clave RhostsAuthentication, Secure Shell, 381
- palabra clave RhostsRSAAuthentication, Secure Shell, 381
- palabra clave RSAAuthentication, Secure Shell, 381
- palabra clave StrictHostKeyChecking, archivo ssh\_config, 382
- palabra clave StrictModes, archivo sshd\_config, 382
- palabra clave Subsystem, archivo sshd\_config, 382
- palabra clave SyslogFacility, archivo sshd\_config, 382
- palabra clave UseLogin, archivo sshd\_config, 382
- palabra clave UseOpenSSLEngine, Secure Shell, 382
- palabra clave UsePrivilegedPort, Secure Shell, 382
- palabra clave User, archivo ssh\_config, 382
- palabra clave UserKnownHostsFile, archivo ssh\_config, 382
- palabra clave UserKnownHostsFile2, *Ver* palabra clave UserKnownHostsFile
- palabra clave UserRsh, archivo ssh\_config, 382
- palabra clave VerifyReverseMapping, archivo ssh\_config, 382
- palabra clave X11DisplayOffset, archivo sshd\_config, 382
- palabra clave X11Forwarding, archivo sshd\_config, 382
- palabra clave X11UseLocalHost, archivo sshd\_config, 382
- palabra clave XAuthLocation, reenvío del puerto de Secure Shell, 382
- palabras clave
  - Ver también* palabra clave específica
  - atributo en BART, 124
  - Secure Shell, 378–383

palabras clave (*Continuación*)

- valores de sustitución de línea de comandos en Secure Shell, 388

## PAM

- agregar un módulo, 340
- archivo `/etc/syslog.conf`, 341
- archivo de configuración
  - diagramas de apilamiento, 344
  - ejemplo de apilamiento, 346
  - explicación del apilamiento, 342
  - indicadores de control, 343
  - introducción, 341
  - Kerberos y, 566
  - sintaxis, 342
- descripción general, 335
- estructura, 336
- Kerberos y, 403, 408
- mapa de tareas, 338
- planificar, 339
- paneles, tabla de la herramienta SEAM, 537–540
- paquetes, Secure Shell, 384
- partición de disco, para archivos de auditoría
  - binarios, 625–629
- PASSREQ en Secure Shell, 383
- PATH en Secure Shell, 383
- perfil de derechos de control de auditoría, 678
- perfil de derechos de copia de seguridad de medios
  - asignar a usuarios de confianza, 183, 213
- perfil de derechos de revisión de auditoría, 678
- perfiles, *Ver* perfiles de derechos
- perfiles de derechos
  - administrador del sistema, 237, 239
  - asignar a usuarios de confianza, 183, 213
  - para servicio de auditoría, 677–678
  - bases de datos
    - Ver* base de datos `prof_attr` y base de datos `exec_attr`
  - cambiar contenido de, 228–231
  - cambiar desde línea de comandos, 230
  - contenido de perfiles típicos, 237
  - crear
    - en línea de comandos, 229
    - en Solaris Management Console, 230
  - crear roles para, 207–210

perfiles de derechos (*Continuación*)

- descripción, 185, 190
  - descripciones de principales perfiles de derechos, 237
  - evitar escalada de privilegios, 183, 213
  - gestión de impresoras, 238, 240
  - métodos de creación, 228–231
  - modificar, 228–231
  - operador, 237, 239
  - orden, 241–242
  - resolución de problemas, 231
  - todos, 238, 241
  - uso de perfil de administrador del sistema, 79
  - usuario de Solaris básico, 238, 240
  - ver contenido, 242
- permisos
- ACL de UFS y, 134–136
  - ACL y, 55–56
  - archivos de ajuste (ASET), 161, 164, 165
  - bit de permanencia, 131
  - búsqueda de archivos con permisos `setuid`, 150
  - cambio de permisos de archivo
    - comando `chmod`, 128
    - modo absoluto, 132, 142–143
    - modo simbólico, 132, 133, 141–142
  - clases de usuario y, 128
  - los permisos de archivo
    - modo absoluto, 132
  - manejo de ASET de, 154, 155
  - permisos de archivo
    - cambio, 132–134, 141–142
    - descripción, 129
    - modo absoluto, 142–143
    - modo simbólico, 132, 133, 141–142
    - permisos especiales, 131, 133
  - permisos de archivo especiales, 129–131, 131, 133
  - permisos de directorio, 129
  - permisos `setgid`
    - descripción, 130–131
    - modo absoluto, 133, 144
    - modo simbólico, 133
  - permisos `setuid`
    - descripción, 130
    - modo absoluto, 133, 144

- permisos, permisos setuid (*Continuación*)
  - modo simbólico, 133
  - riesgos de seguridad, 130
  - valor umask, 131–132
  - valores predeterminados, 131–132
- permisos de archivo UNIX, *Ver* archivos, permisos
- permisos de bit de permanencia
  - descripción, 131
  - modo absoluto, 133, 144
  - modo simbólico, 133
- permisos de ejecución, modo simbólico, 133
- permisos de escritura, modo simbólico, 133
- permisos de lectura, modo simbólico, 133
- permisos especiales
  - bit de permanencia, 131
  - permisos setgid, 130–131
  - permisos setuid, 130
- permisos setgid
  - descripción, 130–131
  - modo absoluto, 133, 144
  - modo simbólico, 133
  - riesgos de seguridad, 131
- permisos setuid
  - búsqueda de archivos con permisos
    - establecidos, 150
  - descripción, 130
  - modo absoluto, 133, 144
  - modo simbólico, 133
  - riesgos de seguridad, 52, 130
- personalización, manifiestos, 112–115
- personalización de un informe (BART), 121–122
- pilas ejecutables
  - deshabilitación de registro de mensajes, 152
  - protección contra, 137, 151–152
  - registro de mensajes, 137
- pista de auditoría
  - análisis con comando praudit, 669
  - costos de análisis, 609
  - creación
    - rol de daemon auditd, 666
  - depuración de archivos no terminados, 649–650
  - descripción, 589
  - descripción general, 587
  - efecto de política de auditoría en, 605
  - pista de auditoría (*Continuación*)
    - eventos incluidos, 592
    - evitar desbordamiento, 650
    - fusión de todos los archivos, 668
    - selección de eventos de, 645–647
    - sin objetos públicos, 589
    - supervisión en tiempo real, 610
    - vista de eventos desde distintas zonas, 678
    - visualización de eventos de, 647–649
- PKCS #11 tokens de software, administración de
  - almacén de claves, 315
- PKI
  - administración por KMF, 313
  - política administrada por KMF, 314
- placa Crypto Accelerator 1000 de Sun, lista de
  - mecanismos, 308–310
- placa Crypto Accelerator 6000 de Sun
  - complemento de hardware para estructura
    - criptográfica, 280
  - lista de mecanismos, 308
- planificación
  - auditoría, 600–604
  - auditoría en zonas, 600–601
- Kerberos
  - decisiones de configuración, 411–420
  - dominios, 412–413
  - jerarquía de dominios, 413
  - KDC esclavos, 415
  - nombres de dominio, 412
  - nombres de principal de servicio y cliente, 414
  - número de dominios, 412–413
  - propagación de base de datos, 417
  - puertos, 414
  - sincronización de reloj, 417
  - mapa de tareas de auditoría, 599–600
- planificar
  - PAM, 339
  - RBAC, 205–207
- política
  - definición en la estructura criptográfica, 281
  - definición en Oracle Solaris, 35–36
- política de auditoría
  - actualización dinámica, 636
  - configuración, 629–632

política de auditoría (*Continuación*)

- configuración `ahlt`, 630–631
- configuración de `arge`, 657
- configuración de `argv`, 657
- configuración en zona global, 596, 678
- configuración `perzone`, 631
- descripción, 589
- efectos de, 605–608
- `public`, 607
- que no afecta tokens, 682
- tokens agregados por, 682
- tokens de auditoría de, 682
- valores predeterminados, 605–608

política de auditoría `ahlt`

- configuración, 630–631
- descripción, 605

política de auditoría `arge`, configuración, 657política de auditoría `arge`

- descripción, 605
- y token `exec_env`, 691–692

política de auditoría `argv`, configuración, 657política de auditoría `argv`

- descripción, 606
- y token `exec_args`, 691

política de auditoría `cnt`, descripción, 606política de auditoría `group`

- descripción, 606
- y token `groups`, 606, 693

política de auditoría `path`, descripción, 606política de auditoría `perzone`

- cuándo utilizar, 596
- descripción, 606
- uso, 601, 639–640, 678

política de auditoría `public`

- descripción, 607
- eventos de sólo lectura, 607

política de auditoría `seq`

- descripción, 607
- y token `sequence`, 607, 701

política de auditoría `trail`

- descripción, 607
- y token `trailer`, 607

política de auditoría `zonename`

- descripción, 607

política de auditoría `zonename` (*Continuación*)

- uso, 601, 678

política de auditoría `aperzone`, configuración, 631

## política de dispositivos

- auditoría de cambios, 84
- cambio, 83–84
- comando `add_drv`, 95
- comando `update_drv`, 83–84, 95
- comandos, 95
- configuración, 82–85
- descripción general, 47–49
- eliminación de dispositivo, 84
- gestión de dispositivos, 82
- mapa de tareas, 82
- protección en núcleo, 95–103
- visualización, 82–83

## política de seguridad, predeterminada (RBAC), 244

política de seguridad `solaris`, 249política de seguridad `suser`, 249

## políticas

- administración, 509–548
- contraseñas y, 554
- creación (Kerberos), 520
- creación de nuevas (Kerberos), 533–534
- descripción general, 35–36
- en dispositivos, 82–83
- especificación de algoritmo de contraseña, 71–72
- mapa de tareas para administrar, 528–529
- modificación, 535–536
- paneles de la herramienta SEAM para, 537–540
- para auditoría, 605–608
- supresión, 536–537
- visualización de atributos, 531–533
- visualización de la lista de, 529–531

## prefijos para clases de auditoría, 680

prerrequisito de auditoría, base de datos de `hosts` con configuración correcta, 633

## preselección, clases de auditoría, 615–617

## preselección de clases de auditoría, efecto en objetos públicos, 589

## preselección en auditoría, 589

## prevención de desbordamiento, pista de auditoría, 650

## prevención de desbordamiento de almacenamiento, pista de auditoría, 650

- primario, en nombres de principales, 399
- principal
  - adición de principal de servicio a keytab, 542, 543–545
  - adición de principales de administración, 426, 433
  - administración, 509–548
  - automatización de la creación de, 515–516
  - comparación de ID de usuario, 448
  - configuración de valores predeterminados, 525–526
  - creación, 520–522
  - creación de `clntconfig`, 428, 436
  - creación de host, 428, 435
  - duplicación, 523
  - eliminación de un principal de servicio de keytab, 545–546
  - eliminación del archivo keytab, 545
  - Kerberos, 399
  - mapa de tareas para administrar, 514–515
  - modificación, 523–524
  - nombre de principal, 399
  - paneles de la herramienta SEAM para, 537–540
  - principal de servicio, 399
  - principal de usuario, 399
  - supresión, 525
  - visualización de atributos, 518–520
  - visualización de la lista de, 516–518
  - visualización de sublista de principales, 517
- principal `changepw`, 542
- principal `clntconfig`
  - creación, 428, 436
- principal de servicio
  - adición a archivo keytab, 542, 543–545
  - descripción, 399
  - eliminación del archivo keytab, 545–546
  - planificación para nombres, 414
- principal de usuario, descripción, 399
- principal host
  - creación, 428, 435
- principal `kadmind`, 542
- principal `root`, adición a keytab de host, 542
- principio de privilegio mínimo, 194
- privacidad
  - disponibilidad, 561
  - Kerberos y, 393
  - privacidad (*Continuación*)
    - servicio de seguridad, 401
- privilegio de lista, herramienta SEAM y, 540
- privilegio mínimo, principio de, 194
- privilegio `PRIV_PROC_LOCK_MEMORY`, 181, 196–197
- privilegios
  - administrar, 256
  - agregar a comando, 260
  - archivos, 272–273
  - asignar a secuencia de comandos, 201
  - asignar a un comando, 199
  - asignar a un usuario, 199
  - asignar a usuario o rol, 260–261
  - auditoría y, 273–274
  - buscar faltantes, 258–259
  - categorías, 194
  - comandos, 271
  - cómo usar, 264
  - depuración, 202, 258
  - descripción, 184, 185, 194
  - determinar privilegios asignados
    - directamente, 265–266
  - diferencias con modelo de superusuario, 195
  - dispositivos y, 201
  - efectos en la herramienta SEAM, 541
  - ejecutar comandos con privilegios, 200
  - eliminar de conjunto básico, 262
  - eliminar de conjunto límite, 262
  - eliminar de un usuario, 200
  - en comparación con modelo de superusuario, 193–202
  - enumerar en un proceso, 256–258
  - escalada, 274
  - heredados por procesos, 198
  - implementados en conjuntos, 197
  - limitar uso por usuario o rol, 261–263
  - mapa de tareas, 255
  - `PRIV_PROC_LOCK_MEMORY`, 181, 196–197
  - procesos con privilegios asignados, 198
  - programas para privilegios, 199
  - proteger procesos del núcleo, 193
  - resolución de problemas de requisitos
    - para, 258–259
  - usar en secuencia de comandos de shell, 263–264



- privilegios de proceso, 195
- privilegios FILE, 194
- privilegios IPC, 194
- privilegios NET, 195
- privilegios PROC, 195
- privilegios SYS, 195
- procedimientos de usuario
  - asignación de dispositivos, 91
  - asumir un rol, 205–219, 219
  - cálculo de MAC de un archivo, 295–296
  - cálculo de resumen de un archivo, 293–294
  - cifrado de archivos, 288
  - cifrado de clave privada del usuario NIS, 332
  - comando chkey, 333
  - creación de un certificado autofirmado, 316–317
  - descifrado de archivos, 296–298
  - exportación de certificados, 318–320
  - generación de frase de contraseña para almacén de claves, 320
  - generación de una clave simétrica
    - uso del comando dd, 288–290
    - uso del comando pktool, 290–293
  - importación de certificados, 317–318
  - protección de archivos, 138–144
  - usar un rol asignado, 205–219, 219
  - uso de ACL, 144–149
  - uso de Secure Shell, 362–363
  - uso del comando pktool, 315–316
- proceso de shell, enumerar sus privilegios, 256–258
- programas
  - comprobar autorizaciones RBAC, 234
  - para privilegios, 197, 199
- propagación
  - base de datos de Kerberos, 473–474
  - base de datos KDC, 417
- propiedad de archivos
  - ACL de UFS y, 134–136
  - ACL y, 55–56
  - cambio, 128, 139–140
  - cambio de propiedad de grupo, 140–141
- propiedades del sistema, privilegios relacionados
  - con, 195
- protección
  - archivos con estructura criptográfica, 288
  - protección (*Continuación*)
    - BIOS, puntero hacia, 79–80
    - contenido de almacén de claves, 319
    - mapa de tareas de contraseñas, 64
    - mapa de tareas de inicios de sesión, 64
    - mediante contraseñas con estructura criptográfica, 315–316
    - PROM, 79–80
  - protección de sistema contra programas riesgosos, 150–152
  - red durante la instalación, 53
- protección de archivos
  - con ACL, 144–149
  - con ACL de UFS, 134–136
  - con mapa de tareas de ACL, 144
  - con permisos UNIX, 127–134, 138–144
  - mapa de tareas, 138
  - mapa de tareas con permisos UNIX, 138
  - procedimientos de usuario, 138–144
- proteger, secuencias de comandos, 234
- protocolo de hora de red, *Ver* NTP
- protocolo v1, Secure Shell, 354
- protocolo v2, Secure Shell, 354
- proveedor de nivel de usuario pkcs11\_kernel.so, 300
- proveedor de nivel de usuario
  - pkcs11\_softtoken.so, 300
- proveedor de núcleo AES, 300
- proveedor de núcleo ARCFOUR, 300
- proveedor de núcleo RSA, 300
- proveedor de núcleo SHA1, 300
- proveedores
  - adición de biblioteca, 303
  - adición de proveedor de software, 302–303
  - adición de un proveedor de software de nivel de usuario, 303
  - conexión a la estructura criptográfica, 284
  - definición como complementos, 280
  - definición como componentes, 281
  - definición en la estructura criptográfica, 281
  - impedir el uso de un proveedor de software de núcleo, 305–307
  - inhabilitación de mecanismos de hardware, 308–310
  - instalación, 284



proveedores (*Continuación*)

- lista de la estructura criptográfica, 300–302
- lista de proveedores de hardware, 308
- registro, 284
- restauración del uso de un proveedor de software de núcleo, 306

## proveedores de hardware

- carga, 308
- habilitación de mecanismos y funciones en, 309
- inhabilitación de mecanismos criptográficos, 308–310
- lista, 308

## proveedores de núcleo, lista, 300

## pseudo-tty, uso en Secure Shell, 377

puertas de enlace, *Ver* sistemas de cortafuegos

## puertos, para KDC Kerberos, 414

## puertos con privilegios, alternativa a RPC seguras, 59

## punto (.)

- entrada de variable path, 51
- separador de nombre de autorización, 242
- visualización de archivos ocultos, 138

## punto y coma (;)

- archivo `device_allocate`, 100
- separador de atributos de seguridad, 250

**R**

## opción -R

- `bart create`, 110, 115
- comando `ssh`, 369–371

## ranura, definición en la estructura criptográfica, 282

## RBAC

- agregar nuevo perfil de derechos, 230
- agregar roles, 207–210
- agregar roles desde línea de comandos, 210–213
- agregar roles personalizados, 212–213
- auditar roles, 215
- autorizaciones, 188
- base de datos de autorización, 246–247
- base de datos de perfil de derechos, 248–249
- bases de datos, 243–251
- cambiar contraseñas de rol, 224–226
- cambiar propiedades de usuario desde línea de comandos, 233

RBAC (*Continuación*)

- comandos de administración, 251–252
- comandos para gestionar, 251–252
- comprobar autorizaciones en secuencias de comandos o programas, 234
- conceptos básicos, 184–187
- configurar, 205–219
- editar perfiles de derechos, 228–231
- elementos, 184–187
- en comparación con modelo de superusuario, 182–184
- modificar roles, 226–228
- modificar usuarios, 231–233
- perfiles de auditoría, 678
- perfiles de derechos, 190
- planificar, 205–207
- proteger secuencias de comandos, 234
- relaciones entre bases de datos, 244–245
- servicios de nombres y, 245
- shells de perfil, 192
- usar aplicaciones con privilegios, 222–223

RC4, *Ver* proveedor de núcleo ARCFOUR

## red, privilegios relacionados con, 195

## reducción

- archivos de auditoría, 643–645, 667
- requisitos de espacio de almacenamiento para archivos de auditoría, 610

## reemplazar, superusuario con roles, 205–207

## reenvío de datos, Secure Shell, 377

## reenvío de X11

- configuración en archivo `ssh_config`, 379
- en Secure Shell, 377

## reenvío del puerto

- configuración en Secure Shell, 361–362
- Secure Shell, 370, 371

## registro, transferencias de archivos ftp, 662–663

## registro de auditorías, ejemplo de formato, 641

## registro de ejecución (ASET), 158

## registro de proveedores

- estructura criptográfica, 284

## registros de auditoría

- Ver también* archivos de auditoría
- archivo `/var/adm/auditlog`, 618
- archivo `syslog.conf`, 588

registros de auditoría (*Continuación*)

- comparación binaria y textual, 593
  - configuración de registros de auditoría textual, 617–620
  - conversión a formato legible, 648, 669
  - descripción, 589
  - descripción general, 592
  - directorios de auditoría llenos, 666, 677
  - en texto, 673
  - eventos que generan, 587
  - formato, 685
  - formatos de visualización de
    - procedimiento, 641–643
  - fusión, 643–645
  - modos, 593
  - mostrar formatos de
    - resumen, 667
  - reducción de archivos de auditoría, 643–645
  - secuencia de tokens, 685
  - visualización, 647–649
  - visualización de formatos de un programa, 642
  - visualización de formatos de una clase de auditoría, 642–643
  - visualización en formato XML, 648
- reinicio
- daemon de auditoría, 635
  - daemon sshd, 362
  - servicio ssh, 362
  - servicios criptográficos, 310–311
- requisitos de espacio en disco, 609–610
- requisitos de reutilización de objetos
- para dispositivos, 101–103
  - secuencias de comandos device-clean
    - redacción de secuencias de comandos nuevas, 103
    - unidades de cinta, 101
- resolución de problemas
- acceso remoto de superusuario, 78
  - asignación de un dispositivo, 92
  - auditoría, 651–663
  - búsqueda de archivos con permisos setuid, 150
  - capacidades de rol, 210
  - clases de auditoría
    - personalizadas, 654

resolución de problemas, clases de auditoría (*Continuación*)

- personalizado, 622
  - comando `encrypt`, 298
  - comando `list_devices`, 88
  - cómo impedir que programas usen pilas ejecutables, 151–152
  - convertirse en superusuario, 219
  - errores de ASET, 175
  - falta de privilegio, 258–259
  - intentos de entrada ilegal a equipos, 67–68
  - Kerberos, 506
  - montaje de un dispositivo, 94
  - perfiles de derechos, 231
  - praudit, 648
  - requisitos de privilegios, 258–259
  - root como un rol, 219
  - terminal donde el comando `su` se originó, 77
  - usuario que ejecuta comandos con privilegios, 266–267
- restauración, proveedores criptográficos, 306
- restricción
- acceso remoto de superusuario, 77–78
  - mapa de tareas de superusuario, 76
- restricción de acceso para servidores KDC, 490–491
- restringir, privilegios de usuario, 262
- resúmenes
- cálculo para archivo, 293–294
  - de archivos, 293–294, 294
- RETRIES en Secure Shell, 383
- rol de usuario root
- rol proporcionado, 183
  - rol recomendado, 183
- rol root (RBAC)
- asumir rol, 221
  - cambiar de nuevo a usuario root, 218
  - resolución de problemas, 219
- roles
- agregar desde línea de comandos, 210–213
  - agregar para determinados perfiles, 207–210
  - agregar roles personalizados, 212–213
  - asignar con comando `usermod`, 213–215
  - asignar privilegios a, 260–261
  - asumir, 219–221, 222–223

## roles (*Continuación*)

- asumir en Solaris Management Console, 222–223
- asumir en una ventana de terminal, 192, 219–221
- asumir rol de administrador del sistema, 221
- asumir rol de administrador principal, 220
- asumir rol root, 221
- asumir tras inicio de sesión, 191
- auditar, 215
- cambiar contraseña de, 224–226
- cambiar propiedades de, 226–228
- convertir usuario root en rol, 215–219
- crear
  - en línea de comandos, 210–213
  - para determinados perfiles, 207–210
  - rol con ámbito limitado, 210
  - rol de administrador del sistema, 208–209
  - rol de gestión de criptografía, 214–215
  - rol de gestión de DHCP, 210
  - rol de operador, 209
  - rol de operador personalizado, 212–213
  - rol de seguridad de dispositivos, 209
  - rol de seguridad de la red, 209
  - rol root, 215–219
  - roles relacionados con seguridad, 209
- descripción, 190–191
- determinar comandos con privilegios de rol, 267–269
- determinar privilegios asignados
  - directamente, 265–266
- enumerar roles locales, 220, 252
- modificar, 226–228
- modificar asignación a un usuario, 210
- resolución de problemas, 210
- resumen, 185
- roles recomendados, 182
- usar un rol asignado, 219–221, 222–223
- uso en RBAC, 182
- uso para acceder al hardware, 79–80

## RPC segura

- alternativa, 59
- descripción, 323
- descripción general, 58–59
- implementación de, 325–328
- servidor de claves, 325

## RPC segura (*Continuación*)

- y Kerberos, 324
- RPCSEC\_GSS API, Kerberos y, 409

## S

- opción -S, secuencia de comandos `st_clean`, 103
- SASL
  - complementos, 350
  - descripción general, 349
  - opciones, 351–352
  - variable de entorno, 350
- señal recibida durante cierre de auditoría, 677
- sección `admin_server`
  - archivo `krb5.conf`, 424, 432
- sección `default_realm`
  - archivo `krb5.conf`, 424, 432
- sección `domain_realm`
  - archivo `krb5.conf`, 413, 424, 432
- secuencia de comandos `.dtpfile`, uso en Secure Shell, 368–369
- secuencia de comandos
  - `/etc/security/audit_warn`, 676
- secuencia de comandos
  - `/etc/security/bsmconv`, 99–100
  - descripción, 677
- secuencia de comandos `audit_startup`
  - configuración, 629–632
  - descripción, 674–675
- secuencia de comandos `audit_warn`
  - condiciones que invocan, 676
  - configuración, 629
  - daemon `auditd`, ejecución de, 666
  - descripción, 676
  - secuencias de comandos, 677
- secuencia de comandos `bsmconv`
  - creación del archivo `device_maps`, 99–100
  - descripción, 677
  - habilitar servicio de auditoría, 632–634
- secuencia de comandos `bsmunconv`, deshabilitación de servicio de auditoría, 634–635
- secuencia de comandos `device-clean` para unidad de cinta Archive, 101

- secuencia de comandos device-clean para unidad de cinta Xylogics, 101
- secuencia de comandos fd\_clean, descripción, 102
- secuencia de comandos sr\_clean, descripción, 102
- secuencia de comandos st\_clean
  - descripción, 102
  - para unidades de cinta, 101
- secuencias de comandos
  - bsmconv para asignación de dispositivos, 86
  - comando bsmconv para habilitar auditoría, 632–634
  - comprobar autorizaciones RBAC, 234
  - efecto bsmconv, 672
  - ejecutar con privilegios, 201
  - ejemplo de supervisión de archivos de auditoría, 611
  - para limpieza de dispositivos, 101–103
  - procesamiento de salida praudit, 670–671
  - proteger, 234
  - secuencia de comandos audit\_startup, 674–675
  - secuencia de comandos audit\_warn, 676
  - secuencia de comandos bsmconv, 677
  - secuencias de comandos device-clean
    - Ver también* secuencias de comandos device-clean
  - uso de privilegios en, 263–264
- secuencias de comandos de shell, escribir con privilegios, 263
- secuencias de comandos de usuario, configuración para daemon ssh-agent en CDE, 368–369
- secuencias de comandos device-clean
  - descripción, 101–103
  - dispositivos de audio, 102
  - opciones, 103
  - redacción de secuencias de comandos nuevas, 103
  - unidades de CD-ROM, 102
  - unidades de cinta, 101
  - unidades de cintas, 102
  - unidades de disquete, 102
  - y reutilización de objetos, 101–103
- Secure Shell
  - adición al sistema, 384
  - administración, 375–377
  - archivos, 384

- Secure Shell (*Continuación*)
  - autenticación
    - requisitos para, 354–356
    - autenticación de clave pública, 354
    - base de OpenSSH, 356–357
    - cambio de frase de contraseña, 365–366
    - cambios en la versión actual, 356–357
    - comando scp, 371–372
    - conexión fuera de cortafuegos
      - de archivo de configuración, 372–373
      - desde la línea de comandos, 373
    - conexión por medio de un cortafuegos, 372
    - configuración de clientes, 378
    - configuración de reenvío del puerto, 361–362
    - configuración de servidor, 378
    - copia de archivos, 371–372
    - creación de claves, 363–365
    - denominación de archivos de identidad, 384
    - descripción, 353
    - ejecución de comandos, 377
    - generación de claves, 363–365
    - inicio de sesión en host remoto, 366–367
    - mapa de tareas de administrador, 357–358, 358
    - menos indicadores de inicio de sesión, 367–368
    - métodos de autenticación, 354–356
    - palabras clave, 378–383
    - paquetes, 384
    - pasos de autenticación, 376–377
    - procedimientos de usuario, 362–363
    - reenvío de correo, 370
    - reenvío de datos, 377
    - reenvío del puerto local, 370, 371
    - reenvío del puerto remoto, 371
    - sesión típica, 375–377
    - TCP y, 361
    - uso de reenvío del puerto, 369–371
    - uso sin contraseña, 367–368
    - variables de entorno de inicio de sesión y, 382–383
    - versiones de protocolo, 354
  - seguridad
    - archivos de cifrado, 296–298
    - auditoría y, 588
    - autenticación DH, 325–328
    - autenticación Kerberos, 451

seguridad (*Continuación*)

- BART, 105–126
- cálculo de MAC de archivos, 295–296
- cálculo de resumen de archivos, 293–294
- cifrado de contraseña, 43
- cliente-servidor NFS, 325–328
- descripción general de políticas, 35–36
- dispositivos, 47–49
- estructura criptográfica, 279–285
- estructura de gestión de claves, 313–320
- evitar inicio de sesión remoto, 77–78
- hardware del sistema, 79–80
- opción de instalación netservices limited, 53
- opciones de instalación, 53
- por medio de red no segura, 372
- protección contra caballos de Troya, 51
- protección contra denegación del servicio, 54
- protección de dispositivos, 101–103
- protección de hardware, 79–80
- protección de PROM, 79–80
- puntero al kit de herramientas JASS, 53
- Secure Shell, 353–373
- seguridad predeterminada, 53
- sistemas, 39
- seguridad de dispositivos (RBAC), crear rol, 209
- seguridad de la máquina, *Ver* seguridad del sistema
- seguridad de la red (RBAC), crear rol, 209
- seguridad de red
  - autenticación, 58–59
  - autorizaciones, 58–59
  - comunicación de problemas, 62
  - control de acceso, 57–61
  - descripción general, 57
  - sistemas de cortafuegos
    - hosts de confianza, 60
    - interceptación de paquetes, 61
    - necesidad de, 60
- seguridad del equipo, *Ver* seguridad del sistema
- seguridad del sistema
  - acceso, 39
  - acceso al equipo, 40–41
  - ACL de UFS, 134–136
  - cifrado de contraseña, 43
  - contraseñas, 42

seguridad del sistema (*Continuación*)

- contraseñas de marcación telefónica
  - deshabilitación temporal, 71
- contraseñas e inicios de sesión de acceso telefónico, 46–47
- control de acceso basado en roles (RBAC), 50
- control de accesos basado en roles (RBAC), 182–184
- cuentas especiales, 45
- descripción general, 39, 40
- guardar intentos de inicio de sesión fallidos, 67–68
- mapa de tareas, 150
- privilegios, 193–202
- protección contra programas riesgosos, 150–152
- protección de hardware, 40–41, 79–80
- restricción de acceso root remoto, 77–78
- restricciones de acceso de inicio de sesión, 41
- restricciones de acceso root, 56–57, 77–78
- shell restringido, 51, 52
- sistemas de cortafuegos, 60–61
- supervisión de comando su, 76–77
- supervisión del comando su, 50
- visualización
  - estado de inicio de sesión de usuario, 64–65, 65
  - usuarios sin contraseñas, 66
- seguridad física, descripción, 40–41
- selección
  - clases de auditoría, 615–617
  - eventos de pista de auditoría, 645–647
  - registros de auditoría, 645–647
- servicio
  - definición en Kerberos, 569
  - inhabilitación en un host, 547–548
  - obtención de acceso a un servicio específico, 578
- servicio de nombres LDAP
  - contraseñas, 42
  - especificación de algoritmo de contraseña, 74–75
- servicio de nombres NIS
  - autenticación, 323
  - contraseñas, 42
  - especificación de algoritmo de contraseña, 73
- servicio de nombres NIS+
  - adición de usuario autenticado, 331
  - autenticación, 323

servicio de nombres NIS+ (*Continuación*)

- base de datos cred, 331
- comprobaciones de ASET, 164
- contraseñas, 42
- especificación de algoritmo de contraseña, 74
- tabla cred, 325

servicio de otorgamiento de tickets, *Ver* TGS

## servicio de seguridad, Kerberos y, 401

servicios criptográficos, *Ver* estructura criptográfica

## servicios de nombres

*Ver* servicios de nombres individuales

ámbito y RBAC, 192

## servidor de aplicaciones, configuración, 444–445

## servidor de claves

descripción, 325

inicio, 329

## servidores

configuración para Secure Shell, 378

definición en Kerberos, 569

dominios y, 400

obtención de acceso con Kerberos, 575–578

obtención de credencial para, 577

sesión cliente-servidor AUTH\_DH, 325–328

## servidores NFS, configuración para Kerberos, 446–448

## sesgo de reloj, planificación Kerberos y, 417

## shell, versiones con privilegios, 192

## shell Bourne, versión con privilegios, 192

## shell Korn, versión con privilegios, 192

## shell restringido (rsh), 51

## shells de perfil, descripción, 192

## siempre\_auditar\_clases

base de datos audit\_user, 675

máscara de preselección de proceso, 683

## signo de almohadilla (#)

archivo device\_allocate, 100

archivo device\_maps, 99

## signo de dólar doble (\$\$), número de proceso de shell principal, 257

## signo de interrogación (?), en archivos de ajuste de ASET, 170

## signo igual (=), símbolo de permisos de archivo, 133

## signo más (+)

entrada de ACL, 145

entrada en archivo su\_log, 77

signo más (+) (*Continuación*)

prefijo de clase de auditoría, 680

símbolo de permisos de archivo, 133

## signo menos (-)

entrada en archivo su\_log, 77

prefijo de clase de auditoría, 680

símbolo de permisos de archivo, 133

símbolo de tipo de archivo, 128

## sincronización de reloj

KDC esclavo con Kerberos y, 440

KDC maestro con Kerberos y, 429, 436

planificación Kerberos y, 417

servidor esclavo con Kerberos y, 483

## sincronización de relojes

descripción general, 466–467

KDC esclavo, 440, 483

KDC maestro, 429, 436

## sintaxis de comillas en BART, 125

## sistema de archivos TMPFS, seguridad, 131

## sistema de inicio de sesión único, 558–564

Kerberos y, 393

## sistema de ventana X, y herramienta SEAM, 511–512

## sistemas, protección contra programas

riesgosos, 150–152

## sistemas de archivos

NFS, 323

## seguridad

autenticación y NFS, 323

sistema de archivos TMPFS, 131

TMPFS, 131

uso compartido de archivos, 56

## sistemas de archivos NFS

acceso seguro con AUTH\_DH, 333

ASET y, 165

autenticación, 323

proporcionar seguridad cliente-servidor, 325–328

## sistemas de cortafuegos

conexión desde fuera, 373

conexiones seguras de host, 372

configuración de ASET, 157

fuera de conexiones con Secure Shell

de archivo de configuración, 372–373

desde la línea de comandos, 373

hosts de confianza, 60

sistemas de cortafuegos (*Continuación*)

- interceptación de paquetes, 61
- seguridad, 60–61
- transferencias de paquetes, 61

## SMF

- Ver también* utilidad de gestión de servicios
- administración de la configuración de seguridad predeterminada, 53
- servicio de estructura criptográfica, 283
- servicio kcf, 283
- servicio ssh, 362

## archivo .ssh/config

- descripción, 386
- valor de sustitución, 386

## archivo .ssh/environment, descripción, 386

## archivo .ssh/id\_dsa, 386

## archivo .ssh/id\_rsa, 386

## archivo .ssh/identity, 386

## archivo .ssh/known\_hosts

- descripción, 385
- valor de sustitución, 387

## archivo .ssh/rc, descripción, 386

## subcomando export, comando pktool, 318–320

## subcomando gencert, comando pktool, 316–317

## subcomando import, comando pktool, 317–318

## subcomando install, comando cryptoadm, 303

## subcomando list, comando pktool, 316

## subcomando setpin, comando pktool, 320

## SUPATH en Secure Shell, 383

## superusuario

- diferencias con modelo de privilegios, 195
- eliminar en RBAC, 191
- en comparación con modelo de privilegios, 193–202
- en comparación con modelo RBAC, 182–184
- resolución de problemas de acceso remoto, 78
- resolución de problemas para convertirse en root como un rol, 219
- supervisión de intentos de acceso, 77–78

## supervisión

- inicios de sesión fallidos, 67–68
- intentos de acceso de superusuario, 77–78
- intentos de comando su, 76–77
- intentos del comando su, 50

supervisión (*Continuación*)

- mapa de tareas de superusuario, 76
- pista de auditoría en tiempo real, 610
- uso de comandos con privilegios, 215
- uso del sistema, 54, 55

## supresión

- políticas (Kerberos), 536–537
- principal (Kerberos), 525
- servicio de host, 548

## SYSLOG\_FAILED\_LOGINS

- en Secure Shell, 383
- variable del sistema, 68

## System V IPC

- clase de auditoría ipc, 680
- privilegios, 194
- token de auditoría ipc, 694–695
- token de auditoría ipc\_perm, 695–696

## T

## tabla cred

- autenticación DH y, 325
  - información almacenada por el servidor, 327
- tabla de credenciales, adición de una sola entrada a, 448–449

## tabla gsscred, uso, 581

## tablas, gsscred, 581

## tamaño de archivos de auditoría

- reducción, 643–645, 667
- reducción de requisitos de espacio de almacenamiento, 610

## TCP

- direcciones, 696
- Secure Shell y, 361, 377

tecnologías de clave pública, *Ver* PKI

## terminología

- específica de Kerberos, 569
- específica de la autenticación, 569–570
- Kerberos, 569–575

## TGS, obtención de credencial para, 575–576

## TGT, en Kerberos, 395–397

ticket de otorgamiento de tickets, *Ver* TGT

## ticket inicial, definición, 571

## ticket no válido, definición, 571



- ticket posfechado
  - definición, 571
  - descripción, 395
- ticket proxy, definición, 571
- ticket que admite proxy, definición, 571
- ticket renovable, definición, 572
- tickets
  - advertencia sobre caducidad, 460
  - archivo
    - Ver antememoria de credenciales
  - comando klist, 551–552
  - creación, 549–550
  - creación con kinit, 550
  - definición, 394
  - definición en Kerberos, 570
  - destrucción, 552
  - duración, 572–573
  - duración máxima renovable, 573
  - inicial, 571
  - no válido, 571
  - o credenciales, 395
  - obtención, 549–550
  - opción -F u opción -f, 560
  - opción -k, 560
  - posfechados, 395, 571
  - proxy, 571
  - que admite proxy, 571
  - reenviables, 395, 550, 561–562, 570
  - renovables, 572
  - solicitud para dominios específicos, 560
  - tipos de, 570–575
  - visualización, 551–552
- tickets reenviables
  - con la opción -F, 560, 561–562
  - con la opción -f, 559, 561–562
  - definición, 570
  - descripción, 395
  - ejemplo, 550
- TIMEOUT en Secure Shell, 383
- tipos de tickets, 570–575
- todo, en campos de auditoría de usuario, 675
- todos (RBAC), perfil de derechos, 241
- token, definición en la estructura criptográfica, 282
- token de auditoría acl, formato, 688
- token de auditoría arbitrary
  - campo de formato de impresión, 689
  - campo de tamaño de elemento, 688
  - formato, 688–689
- token de auditoría arg, formato, 689
- token de auditoría attribute, 690
- token de auditoría cmd, 597, 690–691
- token de auditoría exec\_args
  - formato, 691
  - política argv, 691
- token de auditoría exec\_envn, formato, 691–692
- token de auditoría exit, formato, 692
- token de auditoría file, formato, 692
- token de auditoría group, sustituido por token groups, 692–693
- token de auditoría groups, 693
- token de auditoría header, orden en registro de auditoría, 693–694
- token de auditoría ip, formato, 694
- token de auditoría ip\_addr, formato, 694
- token de auditoría ipc, 694–695
  - formato, 694–695
- token de auditoría ipc\_perm, formato, 695–696
- token de auditoría ipport, formato, 696
- token de auditoría opaque, formato, 696
- token de auditoría path, formato, 696–697
- token de auditoría path\_attr, 598, 697
- token de auditoría privilege, 598, 697–698
- token de auditoría process, formato, 698–699
- token de auditoría return, formato, 700
- token de auditoría sequence
  - formato, 700–701
  - y política de auditoría seqy, 701
- token de auditoría socket, 701–702
- token de auditoría subject, formato, 702–703
- token de auditoría text, formato, 704
- token de auditoría trailer
  - formato, 704–705
  - orden en registro de auditoría, 704–705
  - visualización praudit, 705
- token de auditoría uauth, 598, 705
- token de auditoría upriv, 705
- token de auditoría vnode, formato, 690
- token de auditoría vnode de archivo, 690



- token de auditoría zonename, 598, 705
  - token de auditoríaheader
    - formato, 693–694
    - indicadores de campo de modificador de evento, 693
  - tokens de auditoría
    - Ver también* nombres de token de auditoría individuales
    - agregados por política de auditoría, 682
    - descripción, 589, 592
    - formato, 686
    - formato de registros de auditoría, 685
    - listas de, 686
    - nuevo en la versión actual, 597
  - tokens relacionados con Internet
    - token ip, 694
    - token ip\_addr, 694
    - token ipport, 696
    - token socket, 701–702
  - transacciones reproducidas, 327
  - transferencia de paquetes, seguridad de cortafuegos, 60
  - transferencias de archivos, auditoría, 662–663
  - transferencias de paquetes, interceptación de paquetes, 61
  - transparencia, definición en Kerberos, 394
  - TZ en Secure Shell, 383
- U**
- opción -U
    - comando allocate, 98
    - comando list\_devices, 98
  - UDP
    - direcciones, 696
    - reenvío del puerto y, 361
    - Secure Shell y, 361
    - uso para registros de auditoría remotos, 593
  - umbral de auditoría, 673
  - unidades de CD-ROM
    - asignación, 94
    - seguridad, 102
  - unidades de cinta
    - asignación, 92
    - secuencias de comandos device-clean, 101
  - unidades de cintas, limpieza de datos, 102
  - unidades de disquete
    - asignación, 93–94
    - secuencias de comandos device-clean, 102
  - URL para ayuda en pantalla, herramienta gráfica de Kerberos, 419–420
  - usar
    - comando ppriv, 257
    - comando smrole, 261
    - comando truss, 258
    - comando usermod, 261
    - mapa de tareas de privilegios, 264
    - mapa de tareas de RBAC, 203–204
    - mapa de tareas de roles, 219
    - privilegios, 264
    - roles, 219
  - uso
    - ASET, 171–175
    - asignación de dispositivos, 91
    - BART, 109
    - comando allocate, 91–92
    - comando cryptoadm, 299
    - comando dd, 288–290
    - comando deallocate, 95
    - comando digest, 293–294
    - comando encrypt, 296–298
    - comando mac, 295–296
    - comando mount, 93
    - comando pktool, 290–293
    - comando ssh-add, 367–368
    - comando umount, 95
    - daemon ssh-agent, 367–368
    - mapa de tareas de estructura criptográfica, 287
    - mapa de tareas de Secure Shell, 362–363
    - nuevo algoritmo de contraseña, 73
  - uso compartido de archivos
    - con autenticación DH, 333–334
    - y seguridad de red, 56
  - uso de la estructura de gestión de claves (mapa de tareas), 315–316
  - /usr/sbin/gsscred comando, descripción, 567
  - usuario de Solaris básico (RBAC), contenido de perfil de derechos, 240
  - usuario nobody, 56–57

## usuario root

- cambiar a rol root, 215–219
- cambiar de rol root, 218
- reemplazar en RBAC, 191
- restricción de acceso, 56–57
- restricción de acceso remoto, 77–78
- seguimiento de inicios de sesión, 50
- supervisión de intentos de comando su, 76–77
- supervisión de intentos del comando su, 50
- visualización de intentos de acceso en consola, 77–78

## usuarios

- agregar usuario local, 216
  - asignación de autorización para, 87
  - asignación de dispositivos, 91–92
  - asignar privilegios a, 260–261
  - asignar valores predeterminados de RBAC, 250–251
  - auditoría de todos sus comandos, 656–658
  - cálculo de MAC de archivos, 295–296
  - cálculo de resumen de archivos, 293–294
  - cambiar propiedades desde línea de comandos, 233
  - cifrado de archivos, 296–298
  - conjunto básico de privilegios, 198
  - crear usuario local, 216
  - desasignación de dispositivos, 94–95
  - deshabilitación de inicio de sesión, 66–67
  - desmontaje de dispositivos asignados, 95
  - determinar comandos con privilegios propios, 266–267
  - determinar privilegios asignados directamente, 265–266
  - generación de una clave simétrica, 290–293
  - modificar máscara de preselección de auditoría de, 620–621
  - modificar propiedades (RBAC), 231–233
  - montaje de dispositivos asignados, 92–94
  - privilegios heredables iniciales, 198
  - resolución de problemas de ejecución de comandos con privilegios, 266–267
  - restringir privilegios básicos, 262
  - sin contraseñas, 66
  - visualización de estado de inicio de sesión, 64–65
- utilidad de gestión de servicios
- actualización de la estructura criptográfica, 303

utilidad de gestión de servicios (*Continuación*)

- habilitación de servidor de claves, 329
  - reinicio de la estructura criptográfica, 310–311
  - reinicio de Secure Shell, 362
- Utilidad de gestión de servicios (SMF), Ver SMF

**V**

- valor `max_life`, descripción, 572
- valor `max_renewable_life`, descripción, 573
- valor `umask`
  - valores típicos, 131
  - y creación de archivos, 131–132
- valores de campo de tipo `ipc` (token `ipc`), 694–695
- valores predeterminados
  - auditoría en todo el sistema, 679
  - configuración de privilegios en archivo `policy.conf`, 272
  - de todo el sistema en el archivo `policy.conf`, 43
  - entradas de ACL para directorios, 136
  - formato de salida `praudit`, 670
  - secuencia de comandos `audit_startup`, 674–675
  - valor `umask`, 131–132
- variable `CKLISTPATH_level` (ASET), 169
- variable de sistema `KEYBOARD_ABORT`, 80
- variable del entorno `PATH`
  - configuración, 51
  - y seguridad, 51
- variable del sistema `CRYPT_DEFAULT`, 72
- variable del sistema `rstchown`, 140
- variable `noexec_user_stack`, 137, 151
- variable `noexec_user_stack_log`, 137, 152
- variable `PERIODIC_SCHEDULE` (ASET), 164, 168
- variable `TASKS` (ASET), 163, 169
- variable `UID_ALIASES` (ASET), 161, 164, 169
- variable `YPCHECK` (ASET), 164, 169
- variables
  - agregar a registro de auditoría, 605, 691–692
  - auditoría de las asociadas con un comando, 690–691
  - configuración en Secure Shell, 383
  - `KEYBOARD_ABORT`, 80
  - login y Secure Shell, 382–383
  - `noexec_user_stack`, 137

variables (*Continuación*)

- noexec\_user\_stack\_log, 137
- para puertos y servidores proxy, 372
- rstchown, 140
- variables de entorno de ASET
  - ASETDIR, 167
  - ASETSECLEVEL, 167
  - CKLISTPATH\_level, 162, 163, 169
  - PERIODIC\_SCHEDULE, 164, 168
  - resumen, 166
  - TASKS, 163, 169
  - UID\_ALIASES, 161, 164, 169
  - YPCHECK, 164, 169

## variables de entorno

- ASETDIR (ASET), 167
- ASETSECLEVEL (ASET), 167
- CKLISTPATH\_level (ASET), 163, 169
- PERIODIC\_SCHEDULE (ASET), 164, 168
- presencia en registros de auditoría, 605, 687
- resumen (ASET), 166
- Secure Shell y, 382–383
- sustitución de puertos y servidores proxy, 372
- TASKS (ASET), 163, 169
- UID\_ALIASES (ASET), 161, 164, 169
- uso con comando ssh-agent, 387
- YPCHECK (ASET), 164, 169

## variables de entorno login, Secure Shell y, 382–383

## variables de sistema

- CRYPT\_DEFAULT, 72
- KEYBOARD\_ABORT, 80
- noexec\_user\_stack, 151
- noexec\_user\_stack\_log, 152
- rstchown, 140
- SYSLOG\_FAILED\_LOGINS, 68

## variables del entorno

- Ver también* variables
- PATH, 51
- token de auditoría para, 691–692

## variables del sistema

- Ver también* variables

## ver

- contenido de perfiles de derechos, 242
- privilegios asignados directamente, 265
- privilegios en un proceso, 257

ver (*Continuación*)

- privilegios en un shell, 257, 265–266

## verificador de ventana, 326

## verificadores

- descripción, 326
- devuelto al cliente NFS, 327
- ventana, 326

## virus

- ataque de denegación de servicio, 54
- caballo de Troya, 51

## vista

- formato de registros de auditoría, 641–643
- usuarios sin contraseñas, 66

## visualización

- archivos de auditoría binarios, 647–649
- archivos e información relacionada, 128
- atributos de política, 531–533
- atributos de principal, 518–520
- dispositivos asignables, 88
- entradas de ACL, 136, 144–145, 148–149
- estado de inicio de sesión de usuario, 64–65, 65
- estado de tarea de ASET, 155, 158
- formato de registros de auditoría, 641–643
- formatos de registro de auditoría, 641–643
- información de archivos, 138–139
- información de asignación de dispositivos, 88
- intentos de acceso root, 77–78
- intentos de comando su, 77–78
- lista de políticas, 529–531
- lista de principales, 516–518
- MAC de un archivo, 296
- mecanismos criptográficos
  - disponibles, 301, 305
  - existentes, 300, 301, 305
- mecanismos criptográficos disponibles, 301, 305
- mecanismos criptográficos existentes, 301, 305
- memoria intermedia de lista de claves con el
  - comando list, 546, 547
- permisos de archivo, 138–139
- política de dispositivos, 82–83
- políticas de auditoría, 630
- proveedores de la estructura criptográfica, 300–302
- registro de auditoría en formato XML, 648
- registros de auditoría, 647–649

visualización (*Continuación*)

- registros de auditoría seleccionados, 643–645
- registros de auditoría XML, 648, 670
- resumen de un archivo, 294
- sublista de principales (Kerberos), 517
- tickets, 551–552
- usuarios sin contraseñas, 66

**X**

- opción -X, comandos Kerberizados, 560

**Z**

zonas

- auditoría y, 596, 678
  - dispositivos y, 48
  - estructura criptográfica y, 285
  - planificación de auditoría en, 600–601
  - política de auditoría perzone, 596, 601, 678
  - política de auditoría zonename, 601, 678
  - servicios criptográficos y, 310–311
- zones, configuración de auditoría en zona
- global, 630–631