

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

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>37</b>
 <b>Parte I    Servicios de red (temas) .....</b>	 <b>43</b>
 <b>1    Servicio de red (descripción general) .....</b>	 <b>45</b>
Temas para la Versión de actualización 10 de Oracle Solaris 10 .....	45
Perl 5 .....	46
Acceso a la documentación de Perl .....	46
Problemas de compatibilidad de Perl .....	47
Cambios en la versión Solaris de Perl .....	47
 <b>2    Gestión de servidores de antememoria web .....</b>	 <b>49</b>
Acelerador y antememoria de red (descripción general) .....	49
Servidores web que usan el protocolo de capa de sockets seguros .....	50
Gestión de servidores de antememoria web (mapa de tareas) .....	51
Planificación del NCA .....	52
Requisitos del sistema para el NCA .....	52
Registro del NCA .....	52
Biblioteca de interposición para compatibilidad con daemon del servidor Door .....	52
Soporte de varias instancias .....	53
Administración del almacenamiento en antememoria de las páginas web (tareas) .....	53
▼ Cómo habilitar el almacenamiento en antememoria de páginas web .....	53
▼ Cómo deshabilitar el almacenamiento en la antememoria de las páginas web .....	56
▼ Cómo habilitar y deshabilitar el registro del NCA .....	56
Cómo cargar la biblioteca de utilidades del socket NCA .....	57
▼ Cómo agregar un nuevo puerto al servicio del NCA .....	57
▼ Cómo configurar un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del	

núcleo .....	58
▼ Cómo configurar un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo .....	60
Uso del proxy SSL en el nivel del núcleo en zonas .....	62
Almacenamiento en antememoria de páginas web (referencia) .....	62
Archivos del NCA .....	62
Arquitectura del NCA .....	64
<b>3 Servicios relacionados con el tiempo .....</b>	<b>67</b>
Sincronización del reloj (descripción general) .....	67
Gestión del protocolo de hora de red (tareas) .....	68
▼ Cómo configurar un servidor NTP .....	68
▼ Cómo configurar un cliente NTP .....	68
Uso de otros comandos relacionados con el tiempo (tareas) .....	69
▼ Cómo sincronizar la fecha y la hora desde otro sistema .....	69
Protocolo de hora de red (referencia) .....	69
<b>Parte II Acceso a los sistemas de archivos de red (temas) .....</b>	<b>71</b>
<b>4 Gestión de sistemas de archivos de red (descripción general) .....</b>	<b>73</b>
Novedades del servicio NFS .....	73
Cambios en la versión Solaris 10 11/06 .....	73
Cambios en la versión Solaris 10 .....	74
Terminología de NFS .....	75
Servidores y clientes NFS .....	75
Sistemas de archivos NFS .....	75
Sobre el servicio NFS .....	76
Sobre autofs .....	77
Funciones del servicio NFS .....	77
Protocolo NFS versión 2 .....	77
Protocolo NFS versión 3 .....	77
Protocolo NFS versión 4 .....	78
Control de las versiones de NFS .....	79
Compatibilidad con ACL NFS .....	80
NFS a través de TCP .....	80

NFS a través de UDP .....	80
Descripción general de NFS a través de RDMA .....	81
Administrador de bloqueo de red y NFS .....	81
Compatibilidad con archivos grandes de NFS .....	81
Conmutación por error de cliente NFS .....	81
Compatibilidad con Kerberos para el servicio NFS .....	82
Compatibilidad con WebNFS .....	82
Tipo de seguridad RPCSEC_GSS .....	82
Extensiones Solaris 7 para montaje NFS .....	83
Negociación de seguridad para el servicio WebNFS .....	83
Registro del servidor NFS .....	83
Funciones de autofs .....	83
<b>5 Administración de sistema de archivos de red (tareas) .....</b>	<b>85</b>
Uso compartido de sistema de archivos automático .....	86
▼ Cómo configurar el uso compartido de sistema de archivos automático .....	87
▼ Cómo habilitar acceso WebNFS .....	88
▼ Cómo habilitar el inicio de sesión de servidor NFS .....	89
Montaje de sistemas de archivos .....	90
▼ Cómo montar un sistema de archivos al momento del inicio .....	91
▼ Cómo montar un sistema de archivos desde la línea de comandos .....	92
Montaje con el montador automático .....	92
▼ Cómo deshabilitar archivos grandes en un servidor NFS .....	93
▼ Cómo utilizar conmutación por error del lado del cliente .....	94
▼ Cómo deshabilitar el acceso de montaje para un cliente .....	94
▼ Cómo montar un sistema de archivos NFS a través de un cortafuegos .....	95
▼ Cómo montar un sistema de archivos NFS utilizando una URL de NFS .....	95
Configuración de servicios NFS .....	96
▼ Cómo iniciar los servicios NFS .....	97
▼ Cómo detener los servicios NFS .....	97
▼ Cómo iniciar el montador automático .....	98
▼ Cómo detener el montador automático .....	98
▼ Cómo seleccionar diferentes versiones de NFS en un servidor .....	98
▼ Cómo seleccionar diferentes versiones de NFS en un cliente mediante la modificación del archivo <code>/etc/default/nfs</code> . ....	100

▼ Cómo utilizar el comando mount para seleccionar diferentes versiones de NFS en un cliente .....	101
Administración de sistema NFS seguro .....	101
▼ Cómo configurar un entorno NFS seguro con autenticación DH .....	102
Tareas de administración WebNFS .....	103
Planificación de acceso WebNFS .....	104
Cómo explorar utilizando una URL de NFS .....	105
Cómo habilitar acceso WebNFS a través de un cortafuegos .....	106
Descripción general de tareas para administración autofs .....	106
Mapa de tareas para administración autofs .....	106
Uso del archivo /etc/default/autofs para configurar su entorno autofs .....	108
▼ Cómo configurar su entorno autofs con el archivo /etc/default/autofs .....	108
Tareas administrativas que incluyen mapas .....	109
Modificación de los mapas .....	110
▼ Cómo modificar el mapa maestro .....	110
▼ Cómo modificar mapas indirectos .....	111
▼ Cómo modificar mapas directos .....	111
Cómo evitar conflictos de punto de montaje .....	111
Acceso a sistemas de archivos no NFS .....	112
▼ Cómo acceder a aplicaciones de CD-ROM con autofs .....	112
▼ Cómo acceder a disquetes de datos PC-DOS con autofs .....	113
Acceso a sistemas de archivos NFS utilizando CacheFS .....	113
▼ Cómo acceder a sistemas de archivos NFS utilizando CacheFS .....	114
Personalización del montador automático .....	114
Configuración de una vista común de /home .....	114
▼ Cómo configurar /home con varios sistemas de archivos de directorio principal .....	115
▼ Cómo consolidar archivos relacionados con el proyecto en /ws .....	116
▼ Cómo configurar arquitecturas diferentes para acceder a un espacio de nombres compartido .....	118
▼ Cómo admitir versiones del sistema operativo de cliente incompatibles .....	119
▼ Cómo replicar archivos compartidos entre varios servidores .....	119
▼ Cómo aplicar restricciones de seguridad autofs .....	120
▼ Cómo utilizar un identificador de archivos público con autofs .....	120
▼ Cómo utilizar direcciones URL de NFS con autofs .....	121
Deshabilitación de la capacidad de explorar autofs .....	121
▼ Cómo deshabilitar por completo la capacidad de explorar autofs en un único cliente .....	

NFS .....	121
▼ Cómo deshabilitar la capacidad de explorar autofs para todos los clientes .....	122
▼ Cómo deshabilitar la capacidad de explorar autofs en un sistema de archivos seleccionado .....	122
Estrategias para resolución de problemas de NFS .....	123
Procedimientos de resolución de problemas NFS .....	124
▼ Cómo comprobar la conectividad en un cliente NFS .....	124
▼ Cómo comprobar el servidor NFS remotamente .....	125
▼ Cómo verificar el servicio NFS en el servidor .....	127
▼ Cómo reiniciar servicios NFS .....	128
Identifique qué host proporciona servicio de archivos NFS .....	128
▼ Cómo verificar las opciones que se utilizan con el comando mount .....	129
Resolución de problemas autofs .....	129
Mensajes de error generados por automount - v .....	130
Diversos mensajes de error .....	131
Otros errores con autofs .....	133
Mensajes de error NFS .....	133
<b>6 Acceso a los sistemas de archivos de red (referencia) .....</b>	<b>139</b>
Archivos NFS .....	139
Archivo /etc/default/autofs .....	141
Palabras clave para el archivo /etc/default/nfs .....	142
Archivo /etc/default/nfslogd .....	142
Archivo /etc/nfs/nfslog.conf .....	143
Daemons NFS .....	145
Daemon automountd .....	145
Daemon lockd .....	146
Daemon mountd .....	147
Daemon nfs4cbd .....	147
Daemon nfsd .....	147
Daemon nfslogd .....	148
Daemon nfsmapid .....	148
Daemon statd .....	156
Comandos NFS .....	157
Comando automount .....	158

Comando clear_locks .....	158
Comando fsstat .....	159
Comando mount .....	159
Comando umount .....	165
Comando mountall .....	166
Comando umountall .....	167
Comando share .....	167
Comando unshare .....	172
Comando shareall .....	173
Comando unshareall .....	173
Comando showmount .....	174
Comando setmnt .....	175
Comandos para resolución de problemas de NFS .....	175
Comando nfsstat .....	175
Comando pstack .....	177
Comando rpcinfo .....	177
Comando snoop .....	179
Comando truss .....	180
NFS a través RDMA .....	181
Cómo funciona el servicio NFS .....	182
Negociación de versión en NFS .....	182
Funciones en NFS versión 4 .....	183
Negociación UDP y TCP .....	194
Negociación de tamaño de transferencia de archivos .....	194
Cómo se montan los sistemas de archivos .....	195
Efectos de la opción -public y direcciones URL NFS al montar .....	196
Conmutación por error por parte del cliente .....	196
Archivos de gran tamaño .....	199
Cómo funciona el registro del servidor NFS .....	199
Cómo funciona el servicio WebNFS .....	200
Cómo funciona la negociación de seguridad WebNFS .....	201
Limitaciones WebNFS con uso de explorador web .....	202
Sistema NFS seguro .....	202
RPC segura .....	203
Mapas autofs .....	206
Mapa autofs maestro .....	206



Mapas autofs directos .....	208
Mapas autofs indirectos .....	210
Cómo funciona autofs .....	212
Cómo navega autofs por la red (mapas) .....	213
Cómo Autofs inicia el proceso de navegación (mapa maestro) .....	214
Proceso de montaje autofs .....	214
Cómo selecciona autofs los archivos de sólo lectura más cercanos para los clientes (ubicaciones múltiples) .....	216
Autofs y ponderación .....	219
Variables en una entrada de mapa .....	219
Mapas que hacen referencia a otros mapas .....	220
Mapas autofs ejecutables .....	222
Modificar cómo navega autofs por la red (modificación de mapas) .....	222
Comportamiento predeterminado de autofs con los servicios de nombres .....	222
Referencia de autofs .....	224
Autofs y metacaracteres .....	224
Autofs y caracteres especiales .....	225
 <b>Parte III Temas sobre el SLP .....</b>	 227
 <b>7 SLP (descripción general) .....</b>	 229
Arquitectura del SLP .....	229
Resumen del diseño del SLP .....	230
Agentes y procesos del SLP .....	230
Implementación del SLP .....	232
Otras fuentes de información del SLP .....	233
 <b>8 Planificación y habilitación del SLP (tareas) .....</b>	 235
Consideraciones para la configuración del SLP .....	235
Toma de decisiones con respecto a qué reconfigurar .....	236
Uso de snoop para supervisar la actividad del SLP .....	236
▼ Cómo utilizar snoop para ejecutar rastreos del SLP .....	237
Análisis de un rastreo de snoop s lp .....	237

<b>9 Administración del SLP (tareas)</b>	241
Configuración de propiedades del SLP	241
Archivo de configuración del SLP: elementos básicos	242
▼ Cómo cambiar la configuración del SLP	243
Modificación de frecuencia de detección y anuncios del DA	244
Limitación de UA y SA a DA configurados estáticamente	245
▼ Cómo limitar UA y SA a DA configurados estáticamente	245
Configuración de detección de DA para redes de acceso telefónico	246
▼ Cómo configurar la detección de DA para redes de acceso telefónico	246
Configuración del latido del DA para particiones frecuentes	247
▼ Cómo configurar latidos del DA para particiones frecuentes	248
Liberación de la congestión de la red	248
Adaptación de diferentes medios de red, topologías o configuraciones	249
Reducción de reregistros de SA	249
▼ Cómo reducir reregistros de SA	250
Configuración de la propiedad Time-to-Live de multidifusión	250
▼ Cómo configurar la propiedad Time-to-Live de multidifusión	251
Configuración del tamaño de paquete	252
▼ Cómo configurar el tamaño de paquete	252
Configuración de enrutamiento de sólo difusión	253
▼ Cómo configurar el enrutamiento de sólo difusión	253
Modificación de tiempos de espera en solicitudes de detección de SLP	254
Cambio de tiempos de espera predeterminados	254
▼ Cómo cambiar tiempos de espera predeterminados	255
Configuración del límite de espera aleatoria	256
▼ Cómo configurar el límite de espera aleatoria	257
Implementación de ámbitos	258
Cuándo configurar ámbitos	259
Consideraciones al configurar ámbitos	259
▼ Cómo configurar ámbitos	260
Implementación de DA	261
¿Por qué implementar un DA de SLP?	261
Cuándo implementar DA	263
▼ Cómo implementar DA	263
Dónde colocar DA	264
SLP y función de hosts múltiples	265

Configuración de la función de hosts múltiples para SLP .....	265
Cuándo realizar la configuración para múltiples interfaces de red no enrutadas .....	265
Configuración de múltiples interfaces de red no enrutadas (mapa de tareas) .....	266
Configuración de la propiedad <code>net.slp.interfaces</code> .....	266
Anuncios de proxy y hosts múltiples .....	268
Asignación de nombre de ámbito y colocación de DA .....	269
Consideraciones al configurar múltiples interfaces de red no enrutadas .....	269
<b>10 Incorporación de servicios antiguos</b> .....	271
Cuándo anunciar servicios antiguos .....	271
Anuncio de servicios antiguos .....	271
Modificación del servicio .....	272
Anuncio de un servicio que no está habilitado para SLP .....	272
Registro del proxy de SLP .....	272
▼ Cómo habilitar el registro del proxy de SLP .....	272
Uso del registro del proxy de SLP para anunciar .....	273
Consideraciones al anunciar servicios antiguos .....	275
<b>11 SLP (referencia)</b> .....	277
Códigos de estado del SLP .....	277
Tipos de mensaje del SLP .....	278
<b>Parte IV Servicios de correo (temas)</b> .....	281
<b>12 Servicios de correo (descripción general)</b> .....	283
Novedades de los servicios de correo .....	283
Cambios en esta versión .....	284
Cambios en la versión Solaris 10 1/06 .....	284
Cambios en la versión Solaris 10 .....	284
Otras fuentes de información de <code>sendmail</code> .....	285
Introducción a los componentes de los servicios de correo .....	285
Descripción general de los componentes de software .....	285
Descripción general de los componentes de hardware .....	286

<b>13 Servicios de correo (tareas)</b>	289
Mapa de tareas para servicios de correo	289
Planificación del sistema de correo	291
Sólo correo local	291
Correo local y una conexión remota	292
Configuración de los servicios de correo (mapa de tareas)	294
Configuración de los servicios de correo	294
▼ Cómo configurar un servidor de correo	295
▼ Cómo configurar un cliente de correo	297
▼ Cómo configurar un host de correo	298
▼ Cómo configurar una puerta de enlace de correo	300
▼ Cómo usar DNS con sendmail	302
Modificación de la configuración de sendmail (mapa de tareas)	303
Modificación de la configuración de sendmail	303
▼ Cómo generar un nuevo archivo <code>sendmail.cf</code>	304
Configuración de un host virtual	305
▼ Cómo volver a generar automáticamente un archivo de configuración	305
▼ Cómo usar sendmail en el modo abierto	306
▼ Cómo configurar SMTP para que utilice TLS	307
▼ Cómo gestionar la entrega de correo mediante una configuración alternativa de <code>sendmail.cf</code>	312
Administración de los archivos de alias de correo (mapa de tareas)	313
Administración de los archivos de alias de correo	314
▼ Cómo iniciar una tabla NIS+ <code>mail_aliases</code>	315
▼ Cómo mostrar el contenido de la tabla NIS+ <code>mail_aliases</code>	315
▼ Cómo agregar alias en la tabla NIS+ <code>mail_aliases</code> desde la línea de comandos	316
▼ Cómo agregar entradas mediante la edición de una tabla NIS+ <code>mail_aliases</code>	317
▼ Cómo editar entradas en una tabla NIS+ <code>mail_aliases</code>	318
▼ Cómo configurar un mapa NIS <code>mail_aliases</code>	319
▼ Cómo configurar un archivo de alias correo local	320
▼ Cómo crear un archivo de mapa con clave	321
Gestión del alias postmaster	322
Administración de los directorios de la cola (mapa de tareas)	324
Administración de los directorios de la cola	325
▼ Cómo mostrar el contenido de la cola de correo, <code>/var/spool/mqueue</code>	325
▼ Cómo forzar el procesamiento de la cola de correo, <code>/var/spool/mqueue</code>	326

▼ Cómo ejecutar un subconjunto de la cola de correo, /var/spool/mqueue .....	326
▼ Cómo mover la cola de correo, /var/spool/mqueue .....	327
▼ Cómo ejecutar la cola de correo antigua, /var/spool/omqueue .....	328
Administración de los archivos . forward (mapa de tareas) .....	328
Administración de los archivos . forward .....	329
▼ Cómo deshabilitar los archivos . forward .....	329
▼ Cómo cambiar la ruta de búsqueda de los archivos . forward .....	330
▼ Cómo crear y rellenar /etc/shells .....	330
Procedimientos y consejos para la resolución de problemas en servicios de correo (mapa de tareas) .....	331
Procedimientos y consejos para la resolución de problemas en servicios de correo .....	332
▼ Cómo probar la configuración de correo .....	332
Cómo comprobar los alias de correo .....	333
▼ Cómo probar los conjuntos de reglas de sendmail .....	333
Cómo verificar las conexiones con otros sistemas .....	334
Registro de los mensajes de error .....	335
Otras fuentes de información de diagnóstico de correo .....	336
Resolución de los mensajes de error .....	336
<b>14 Servicios de correo (referencia) .....</b>	<b>339</b>
La versión de Solaris de sendmail .....	340
Indicadores utilizados y no utilizados para compilar sendmail .....	340
MILTER, API de filtro de correo para sendmail .....	341
Comandos sendmail alternativos .....	342
Versiones del archivo de configuración .....	342
Componentes de software y hardware de servicios de correo .....	343
Componentes de software .....	343
Componentes de hardware .....	351
Archivos y programas de servicio de correo .....	354
Mejoras en la utilidad vacation .....	355
Contenido del directorio /usr/bin .....	355
Contenido del directorio /etc/mail .....	356
Contenido del directorio /etc/mail/cf .....	357
Contenido del directorio /usr/lib .....	360
Otros archivos utilizados para servicios de correo .....	360

Interacciones de programas de correo .....	361
Programa sendmail .....	362
Archivos de alias de correo .....	367
Archivos .forward .....	370
Archivo /etc/default/sendmail .....	372
Direcciones de correo y enrutamiento de correo .....	373
Interacciones de sendmail con servicios de nombres .....	374
sendmail.cf y dominios de correo .....	374
sendmail y servicios de nombres .....	374
Interacciones de NIS y sendmail .....	376
Interacciones de sendmail con NIS y DNS .....	377
Interacciones de NIS+ y sendmail .....	377
Interacciones de sendmail con NIS+ y DNS .....	378
Cambios en la versión 8.13 de sendmail .....	379
Compatibilidad para ejecutar SMTP con TLS en la versión 8.13 de sendmail .....	380
Opciones de línea de comandos adicionales en la versión 8.13 de sendmail .....	385
Opciones de archivo de configuración revisadas y adicionales en la versión 8.13 de sendmail .....	385
Declaraciones FEATURE() revisadas y adicionales en la versión 8.13 de sendmail .....	387
Cambios de la versión 8.12 de sendmail .....	388
Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail .....	388
Archivo de configuración submit.cf de la versión 8.12 de sendmail .....	389
Opciones de línea de comandos descartadas o adicionales de la versión 8.12 de sendmail .....	391
Argumentos adicionales para las opciones PidFile y ProcessTitlePrefix de la versión 8.12 de sendmail .....	392
Macros definidas adicionales de la versión 8.12 de sendmail .....	392
Macros adicionales de la versión 8.12 de sendmail .....	393
Macros MAX adicionales de la versión 8.12 de sendmail .....	394
Macros de configuración m4 revisadas y adicionales de la versión 8.12 de sendmail .....	395
Cambios en la declaración FEATURE() de la versión 8.12 de sendmail .....	395
Cambios en la declaración MAILER() de la versión 8.12 de sendmail .....	398
Indicadores de agente de entrega adicionales de la versión 8.12 de sendmail .....	399
Ecuaciones adicionales para agentes de entrega de la versión 8.12 de sendmail .....	400
Funciones de cola adicionales de la versión 8.12 de sendmail .....	401
Cambios en LDAP de la versión 8.12 de sendmail .....	401

Cambio en la aplicación de correo integrada de la versión 8.12 de sendmail .....	403
Conjuntos de reglas adicionales de la versión 8.12 de sendmail .....	403
Cambios en los archivos de la versión 8.12 de sendmail .....	404
Versión 8.12 de sendmail y direcciones IPv6 en configuración .....	405
 <b>Parte V Redes en serie (temas) .....</b>	 407
 <b>15 Solaris PPP 4.0 (descripción general) .....</b>	 409
Conceptos básicos de Solaris PPP 4.0 .....	409
Compatibilidad de Solaris PPP 4.0 .....	410
Cómo determinar qué versión de Solaris PPP se debe usar .....	410
Dónde ir para obtener más información acerca de PPP .....	411
Configuraciones y terminología de PPP .....	413
Descripción general de PPP de marcación telefónica .....	413
Descripción general de PPP de línea arrendada .....	417
Autenticación PPP .....	419
Autenticadores y autenticados .....	420
Protocolos de autenticación PPP .....	421
¿Por qué utilizar autenticación PPP? .....	421
Compatibilidad para usuarios de DSL a través de PPPoE .....	422
Descripción general de PPPoE .....	422
Partes de una configuración de PPPoE .....	422
Seguridad en un túnel PPPoE .....	424
 <b>16 Planificación del enlace de PPP (tareas) .....</b>	 425
Planificación de PPP general (mapa de tareas) .....	425
Planificación de un enlace de PPP por marcación telefónica .....	426
Antes de configurar el equipo de marcación de salida .....	426
Antes de configurar el servidor de marcación de entrada .....	427
Ejemplo de una configuración para PPP de marcación telefónica .....	428
Dónde ir para obtener más información sobre PPP de marcación telefónica .....	430
Planificación de un enlace de línea arrendada .....	430
Antes de configurar el enlace de línea arrendada .....	430
Ejemplo de una configuración para un enlace de línea arrendada .....	431

Donde ir para obtener más información sobre líneas arrendadas .....	433
Planificación para autenticación en un enlace .....	433
Antes de configurar la autenticación PPP .....	433
Ejemplos de configuraciones de autenticación PPP .....	434
Dónde ir para obtener más información sobre autenticación .....	437
Planificación de compatibilidad de DSL a través de un túnel PPPoE .....	438
Antes de configurar un túnel PPPoE .....	438
Ejemplo de una configuración para un túnel PPPoE .....	440
Dónde obtener más información sobre PPPoE .....	441
<b>17 Configuración de un enlace de PPP por marcación telefónica (tareas) .....</b>	<b>443</b>
Tareas principales para configuración de enlace de PPP por marcación telefónica (mapa de tareas) .....	443
Configuración del equipo de marcación de salida .....	444
Tareas para la configuración de un equipo de marcación de salida (mapa de tareas) .....	444
Archivos de plantilla de PPP de marcación telefónica .....	445
Configuración de dispositivos en el equipo de marcación de salida .....	445
▼ Cómo configurar el módem y el puerto de serie (equipo de marcación de salida) .....	446
Configuración de comunicaciones en el equipo de marcación de salida .....	447
▼ Cómo definir comunicaciones a través de la línea de serie .....	447
▼ Cómo crear las instrucciones para llamar a un igual .....	448
▼ Cómo definir la conexión con un igual individual .....	449
Configuración del servidor de marcación de entrada .....	451
Tareas para la configuración de un servidor de marcación de entrada (mapa de tareas) ..	451
Configuración de dispositivos en el servidor de marcación de entrada .....	452
▼ Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada) .....	452
▼ Cómo establecer la velocidad del módem .....	453
Configuración de usuarios del servidor de marcación de entrada .....	453
▼ Cómo configurar usuarios del servidor de marcación de entrada .....	454
Configuración de comunicaciones a través del servidor de marcación de entrada .....	455
▼ Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada) .....	456
Llamada al servidor de marcación de entrada .....	457
▼ Cómo llamar al servidor de marcación de entrada .....	457



<b>18 Configuración de un enlace de PPP de línea arrendada (tareas)</b>	459
Configuración de una línea arrendada (mapa de tareas)	459
Configuración de dispositivos síncronos en la línea arrendada	460
Requisitos previos para configuración de dispositivos síncronos	460
▼ Cómo configurar dispositivos síncronos	460
Configuración de un equipo en la línea arrendada	461
Requisitos previos para la configuración del equipo local en una línea arrendada	461
▼ Cómo configurar un equipo en una línea arrendada	462
<b>19 Configuración de autenticación PPP (tareas)</b>	465
Configuración de autenticación PPP (mapa de tareas)	465
Configuración de autenticación PAP	466
Configuración de autenticación PAP (mapas de tareas)	466
Configuración de autenticación PAP en el servidor de marcación de entrada	467
▼ Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada)	467
Modificación de archivos de configuración de PPP para PAP (servidor de marcación de entrada)	469
▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada)	469
Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)	470
▼ Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza	471
Modificación de archivos de configuración de PPP para PAP (equipo de marcación de salida)	472
▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida)	473
Configuración de autenticación CHAP	474
Configuración de autenticación CHAP (mapas de tareas)	474
Configuración de autenticación CHAP en el servidor de marcación de entrada	475
▼ Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)	476
Modificación de archivos de configuración de PPP para CHAP (servidor de marcación de entrada)	477
▼ Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada)	477

Configuración de autenticación CHAP para emisores de llamadas de confianza (equipos de marcación de salida) .....	478
▼ Cómo configurar credenciales de autenticación CHAP para los emisores de llamadas de confianza .....	478
Adición de CHAP para los archivos de configuración (equipo de marcación de salida) ..	479
▼ Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida) .....	480
<b>20 Configuración de un túnel PPPoE (tareas) .....</b>	<b>481</b>
Tareas principales para la configuración de un túnel PPPoE (mapas de tareas) .....	481
Configuración del cliente PPPoE .....	482
Requisitos previos para la configuración del cliente PPPoE .....	482
▼ Cómo configurar una interfaz para un cliente PPPoE .....	483
▼ Cómo definir un igual de servidor de acceso PPPoE .....	483
Configuración de un servidor de acceso PPPoE .....	485
▼ Cómo configurar un servidor de acceso PPPoE .....	485
▼ Cómo modificar un archivo /etc/ppp/pppoe existente .....	487
▼ Cómo restringir el uso de una interfaz a clientes específicos .....	487
<b>21 Resolución de problemas comunes de PPP (tareas) .....</b>	<b>489</b>
Resolución de problemas de PPP (mapa de tareas) .....	489
Herramientas para resolución de problemas de PPP .....	490
▼ Cómo obtener información de diagnóstico de pppd .....	491
▼ Cómo activar la depuración de PPP .....	492
Resolución de problemas relacionados con PPP y PPPoE .....	493
▼ Cómo diagnosticar problemas de red .....	494
Problemas de red comunes que afectan el PPP .....	495
▼ Cómo diagnosticar y solucionar problemas de comunicaciones .....	496
Problemas de comunicaciones generales que afectan PPP .....	497
▼ Cómo diagnosticar problemas con la configuración de PPP .....	498
Problemas de configuración de PPP comunes .....	498
▼ Cómo diagnosticar problemas del módem .....	498
▼ Cómo obtener información de depuración para secuencias de comandos de chat .....	500
Problemas de secuencia de comandos de chat comunes .....	500
▼ Cómo diagnosticar y solucionar problemas de velocidad de línea de serie .....	503

▼ Cómo obtener información de diagnóstico para PPPoE .....	504
Resolución de problemas de línea arrendada .....	506
Diagnóstico y resolución de problemas de autenticación .....	507
<b>22 Solaris PPP 4.0 (referencia) .....</b>	<b>509</b>
Uso de opciones de PPP en archivos y en la línea de comandos .....	509
Dónde definir opciones de PPP .....	509
Cómo se procesan las opciones de PPP .....	511
Cómo funcionan los privilegios de archivos de configuración de PPP .....	512
Archivo de configuración /etc/ppp/options .....	514
Archivo de configuración /etc/ppp/options. <i>nombre de tty</i> .....	515
Configuración de opciones específicas de usuarios .....	518
Configuración de \$HOME/.ppprc en un servidor de marcación de entrada .....	518
Configuración de \$HOME/.ppprc en un equipo de marcación de salida .....	518
Especificación de información para comunicación con el servidor de marcación de entrada .....	519
Archivo /etc/ppp/peers/ <i>nombre de igual</i> .....	519
Archivo de plantilla /etc/ppp/peers/myisp.tmpl .....	520
Dónde encontrar ejemplos de los archivos /etc/ppp/peers/ <i>nombre de igual</i> .....	521
Configuración de velocidad del módem para un enlace por marcación telefónica .....	522
Definición de la conversación en el enlace por marcación telefónica .....	522
Contenidos de la secuencia de comandos de chat .....	522
Ejemplos de secuencias de comandos de chat .....	523
Invocación de la secuencia de comandos de chat .....	530
▼ Cómo invocar una secuencia de comandos de chat (tarea) .....	530
Creación de un archivo de chat que es ejecutable .....	531
▼ Cómo crear un programa de chat ejecutable .....	532
Autenticación de emisores de llamadas en un enlace .....	532
Protocolo de autenticación de contraseña (PAP) .....	532
Protocolo de autenticación por desafío mutuo (CHAP) .....	535
Creación de un esquema de direccionamiento IP para emisores de llamadas .....	538
Asignación de direcciones IP dinámicas a emisores de llamadas .....	538
Asignación de direcciones IP estáticas a emisores de llamadas .....	539
Asignación de direcciones IP por número de unidad sPPP .....	540
Creación de túneles PPPoE para compatibilidad de DSL .....	541
Archivos para configuración de interfaces para PPPoE .....	541

Comandos y archivos de servidor de acceso PPPoE .....	543
Archivos y comandos de cliente PPPoE .....	548
<b>23 Migración de Solaris PPP asíncrono a Solaris PPP 4.0 (tareas) .....</b>	<b>551</b>
Antes de convertir archivos asppp .....	551
Ejemplo del archivo de configuración /etc/asppp.cf .....	551
Ejemplo del archivo /etc/uucp/Systems .....	552
Ejemplo del archivo /etc/uucp/Devices .....	553
Ejemplo del archivo /etc/uucp/Dialers .....	553
Ejecución de la secuencia de comandos de conversión asppp2pppd (tareas) .....	554
Requisitos previos de la tarea .....	554
▼ Cómo convertir de asppp a Solaris PPP 4.0 .....	555
▼ Cómo ver los resultados de la conversión .....	555
<b>24 UUCP (descripción general) .....</b>	<b>559</b>
Configuraciones de hardware del UUCP .....	559
Software del UUCP .....	560
Daemons del UUCP .....	560
Programas administrativos del UUCP .....	561
Programas de usuario del UUCP .....	562
Archivos de base de datos del UUCP .....	563
Configuración de archivos de base de datos del UUCP .....	564
<b>25 Administración del UUCP (tareas) .....</b>	<b>565</b>
Administración del UUCP (mapa de tareas) .....	565
Adición de inicios de sesión del UUCP .....	566
▼ Cómo agregar inicios de sesión del UUCP .....	566
Inicio del UUCP .....	567
▼ Cómo iniciar el UUCP .....	568
Secuencia de comandos de shell uudemond.poll .....	568
Secuencia de comandos de shell uudemond.hour .....	568
Secuencia de comandos de shell uudemond.admin .....	569
Secuencia de comandos de shell uudemond.cleanup .....	569
Ejecución del UUCP mediante TCP/IP .....	569

▼ Cómo activar el UUCP para TCP/IP .....	569
Seguridad y mantenimiento del UUCP .....	570
Configuración de la seguridad del UUCP .....	570
Mantenimiento regular del UUCP .....	571
Resolución de problemas del UUCP .....	572
▼ Cómo comprobar si existen módems o ACU con errores .....	572
▼ Cómo depurar transmisiones .....	572
Comprobación del archivo /etc/uucp/Systems del UUCP .....	574
Comprobación de mensajes de error del UUCP .....	574
Comprobación de información básica .....	574
<b>26 UUCP (referencia) .....</b>	<b>575</b>
Archivo /etc/uucp/Systems del UUCP .....	575
Campo System-Name en el archivo /etc/uucp/Systems .....	576
Campo Time en el archivo /etc/uucp/Systems .....	577
Campo Type en el archivo /etc/uucp/Systems .....	578
Campo Speed en el archivo /etc/uucp/Systems .....	578
Campo Phone en el archivo /etc/uucp/Systems .....	578
Campo Chat-Script en el archivo /etc/uucp/Systems .....	579
Habilitación de devolución de llamada por medio de la secuencia de comandos de chat .....	581
Control de flujo de hardware en el archivo /etc/uucp/Systems .....	582
Configuración de paridad en el archivo /etc/uucp/Systems .....	582
Archivo /etc/uucp/Devices del UUCP .....	583
Campo Type en el archivo /etc/uucp/Devices .....	583
Campo Line en el archivo /etc/uucp/Devices .....	585
Campo Line2 del archivo /etc/uucp/Devices .....	585
Campo Class en el archivo /etc/uucp/Devices .....	585
Campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices .....	586
Estructura del campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices .....	586
Definiciones de protocolo en el archivo /etc/uucp/Devices .....	588
Archivo /etc/uucp/Dialers del UUCP .....	589
Habilitación del control de flujo de hardware en el archivo /etc/uucp/Dialers .....	593
Configuración de paridad en el archivo /etc/uucp/Dialers .....	593
Otros archivos de configuración básica del UUCP .....	593
Archivo /etc/uucp/Dialcodes del UUCP .....	594

Archivo /etc/uucp/Sysfiles del UUCP .....	595
Archivo /etc/uucp/Sysname del UUCP .....	596
Archivo /etc/uucp/Permissions del UUCP .....	596
Entradas de estructuración del UUCP .....	596
Consideraciones del UUCP .....	597
Opción REQUEST del UUCP .....	597
Opción SENDFILES del UUCP .....	598
Opción MYNAME del UUCP .....	598
Opciones READ y WRITE del UUCP .....	599
Opciones NOREAD y NOWRITE del UUCP .....	600
Opción CALLBACK del UUCP .....	600
Opción COMMANDS del UUCP .....	600
Opción VALIDATE del UUCP .....	602
Entrada MACHINE para OTHER del UUCP .....	603
Combinación de entradas MACHINE y LOGNAME para el UUCP .....	604
Reenvío del UUCP .....	604
Archivo /etc/uucp/Poll del UUCP .....	605
Archivo /etc/uucp/Config del UUCP .....	605
Archivo /etc/uucp/Grades del UUCP .....	605
Campo User-job-grade del UUCP .....	606
Campo System-job-grade del UUCP .....	606
Campo Job-size del UUCP .....	607
Campo Permit-type del UUCP .....	607
Campo ID-list del UUCP .....	608
Otros archivos de configuración del UUCP .....	608
Archivo /etc/uucp/Devconfig del UUCP .....	608
Archivo /etc/uucp/Limits del UUCP .....	609
Archivo remote.unknown del UUCP .....	609
Archivos administrativos del UUCP .....	610
Mensajes de error del UUCP .....	612
Mensajes de error ASSERT del UUCP .....	612
Mensajes de error STATUS del UUCP .....	613
Mensajes de error numéricos del UUCP .....	615

<b>Parte VI Trabajo con sistemas remotos (temas)</b>	617
<b>27 Trabajo con sistemas remotos (descripción general)</b>	619
¿Qué es el servidor FTP?	619
¿Qué es un sistema remoto?	619
Cambios recientes realizados en el servicio de FTP	620
<b>28 Administración del servidor FTP (tareas)</b>	623
Administración del servidor FTP (mapa de tareas)	624
Control del acceso al servidor FTP	625
▼ Cómo definir clases de servidor FTP	626
▼ Cómo establecer límites de inicio de sesión de usuarios	627
▼ Cómo controlar el número de intentos de inicio de sesión no válidos	628
▼ Cómo impedir a determinados usuarios el acceso al servidor FTP	629
▼ Cómo restringir el acceso al servidor FTP predeterminado	630
Configuración de inicios de sesión del servidor FTP	631
▼ Cómo configurar usuarios reales del FTP	631
▼ Cómo configurar usuarios invitados del FTP	632
▼ Cómo configurar usuarios anónimos del FTP	633
▼ Cómo crear el archivo <code>/etc/shells</code>	634
Personalización de archivos de mensaje	634
▼ Cómo personalizar archivos de mensaje	635
▼ Cómo crear mensajes que se van a enviar a los usuarios	636
▼ Cómo configurar la opción README	636
Control del acceso a los archivos en el servidor FTP	638
▼ Cómo controlar comandos de acceso a archivos	638
Control de cargas y descargas en el servidor FTP	639
▼ Cómo controlar las cargas al servidor FTP	639
▼ Cómo controlar descargas al servidor FTP	641
Hospedaje virtual	642
▼ Cómo permitir el hospedaje virtual limitado	643
▼ Cómo habilitar el hospedaje virtual completo	644
Inicio del servidor FTP automáticamente	646
▼ Cómo iniciar un servidor FTP mediante SMF	646
▼ Cómo iniciar un servidor FTP independiente en segundo plano	647

▼ Cómo iniciar un servidor FTP independiente en primer plano .....	647
Cierre del servidor FTP .....	648
▼ Cómo cerrar el servidor FTP .....	648
Depuración del servidor FTP .....	649
▼ Cómo comprobar syslogd en busca de mensajes del servidor FTP .....	649
▼ Cómo utilizar greeting text para verificar ftpaccess .....	650
▼ Cómo comprobar los comandos ejecutados por usuarios del FTP .....	650
Ayuda de configuración para sitios ocupados .....	651
<b>29 Acceso a sistemas remotos (tareas) .....</b>	<b>653</b>
Acceso a sistemas remotos (mapa de tareas) .....	653
Inicio de sesión en un sistema remoto (rlogin) .....	654
Autenticación para inicios de sesión remotos (rlogin) .....	654
Vinculación de inicios de sesión remotos .....	657
Inicios de sesión remotos directos o indirectos .....	657
Qué sucede después iniciar sesión de manera remota .....	658
▼ Cómo buscar y eliminar archivos .rhosts .....	659
Cómo saber si un sistema remoto es operativo .....	659
Cómo buscar quién ha iniciado sesión en un sistema remoto .....	660
Cómo iniciar sesión en un sistema remoto (rlogin) .....	661
Cómo cerrar sesión desde un sistema remoto (exit) .....	661
Inicio de sesión en un sistema remoto (ftp) .....	662
Autenticación para inicios de sesión remotos (ftp) .....	662
Comandos ftp esenciales .....	662
▼ Cómo abrir una conexión ftp a un sistema remoto .....	663
Cómo cerrar una conexión ftp a un sistema remoto .....	664
▼ Cómo copiar archivos de un sistema remoto (ftp) .....	664
▼ Cómo copiar archivos a un sistema remoto (ftp) .....	666
Copia remota con rcp .....	668
Consideraciones de seguridad para operaciones de copia .....	669
Especificación de origen y destino .....	669
▼ Cómo copiar archivos entre un sistema local y un sistema remoto (rcp) .....	671



**Parte VII Supervisión de servicios de red (temas) ..... 675**

**30 Supervisión del rendimiento de la red (tareas) ..... 677**

Supervisión del rendimiento de la red ..... 677

    Cómo comprobar la respuesta de los hosts en la red ..... 678

    Cómo enviar paquetes a los hosts en la red ..... 678

    Cómo capturar paquetes de la red ..... 679

    Cómo comprobar el estado de la red ..... 679

    Cómo mostrar estadísticas de servidor y cliente NFS ..... 682

**Glosario ..... 687**

**Índice ..... 693**



# Lista de figuras

---

FIGURA 2-1	Flujo de datos con el servicio NCA .....	65
FIGURA 6-1	Relación de RDMA con otros protocolos .....	181
FIGURA 6-2	Vistas del sistema de archivos del servidor y del sistema de archivos del cliente .....	185
FIGURA 6-3	El servicio svc:/system/filesystem/autofs inicia automount .....	213
FIGURA 6-4	Navegación por el mapa maestro .....	214
FIGURA 6-5	Proximidad de servidor .....	217
FIGURA 6-6	Cómo utiliza autofs el servicio de nombres .....	223
FIGURA 7-1	Agentes y procesos básicos del SLP .....	231
FIGURA 7-2	Agentes y procesos arquitectónicos del SLP implementados con un DA .....	231
FIGURA 7-3	Implementación del SLP .....	233
FIGURA 12-1	Configuración típica de correo electrónico .....	287
FIGURA 13-1	Configuración de correo local .....	292
FIGURA 13-2	Configuración de correo local con una conexión UUCP .....	293
FIGURA 14-1	Puerta de enlace entre diferentes protocolos de comunicaciones .....	354
FIGURA 14-2	Interacciones de programas de correo .....	362
FIGURA 15-1	Partes del enlace de PPP .....	413
FIGURA 15-2	Enlace de PPP por marcación telefónica analógico básico .....	415
FIGURA 15-3	Configuración de línea arrendada básica .....	418
FIGURA 15-4	Los participantes de un túnel PPPoE .....	423
FIGURA 16-1	Enlace por marcación telefónica de ejemplo .....	429
FIGURA 16-2	Ejemplo de una configuración de línea arrendada .....	432
FIGURA 16-3	Ejemplo de un escenario de autenticación PAP (al trabajar desde casa) .....	435
FIGURA 16-4	Ejemplo de un escenario de autenticación CHAP (llamada a una red privada) .....	437
FIGURA 16-5	Ejemplo de un túnel PPPoE .....	440
FIGURA 22-1	Proceso de autenticación PAP .....	534
FIGURA 22-2	Autenticación CHAP secuencia .....	537



# Lista de tablas

---

TABLA 2-1	Archivos del NCA .....	62
TABLA 3-1	Archivos NTP .....	69
TABLA 5-1	Mapa de tareas de uso compartido de sistema de archivos .....	86
TABLA 5-2	Mapa de tareas para montar sistemas de archivos .....	90
TABLA 5-3	Mapa de tareas para servicios NFS .....	96
TABLA 5-4	Mapa de tareas para la administración WebNFS .....	104
TABLA 5-5	Mapa de tareas para administración autofs .....	106
TABLA 5-6	Tipos de mapas autofs y sus usos .....	109
TABLA 5-7	Mantenimiento de mapas .....	109
TABLA 5-8	Cuándo se debe ejecutar el comando automount .....	110
TABLA 6-1	Archivos NFS .....	139
TABLA 6-2	Variables de mapa predefinidas .....	219
TABLA 7-1	Agentes del SLP .....	230
TABLA 9-1	Operaciones de configuración del SLP .....	242
TABLA 9-2	Propiedades de solicitud de detección e intervalo de anuncios del DA .....	244
TABLA 9-3	Propiedades de rendimiento del SLP .....	249
TABLA 9-4	Propiedades de tiempo de espera .....	254
TABLA 9-5	Configuración de múltiples interfaces de red no enrutadas .....	266
TABLA 10-1	Descripción del archivo de registro de proxy de SLP .....	274
TABLA 11-1	Códigos de estado del SLP .....	277
TABLA 11-2	Tipos de mensaje del SLP .....	278
TABLA 14-1	Indicadores generales de sendmail .....	340
TABLA 14-2	Mapas y tipos de base de datos .....	340
TABLA 14-3	Indicadores del sistema operativo .....	341
TABLA 14-4	Indicadores genéricos que no se utilizan en esta versión de sendmail .....	341
TABLA 14-5	Comandos sendmail alternativos .....	342
TABLA 14-6	Valores de versión para el archivo de configuración .....	342
TABLA 14-7	Dominios de nivel superior .....	346

TABLA 14-8	Convenciones para el formato de nombres de buzón .....	349
TABLA 14-9	Contenido del directorio /etc/mail/cf utilizado para servicios de correo ....	358
TABLA 14-10	Contenido del directorio /usr/lib .....	360
TABLA 14-11	Otros archivos utilizados para servicios de correo .....	360
TABLA 14-12	Columnas en la tabla mail_aliases NIS+ .....	369
TABLA 14-13	Opciones de archivo de configuración para ejecutar SMTP con TLS .....	381
TABLA 14-14	Macros para ejecutar SMTP con TLS .....	383
TABLA 14-15	Conjuntos de reglas para ejecutar SMTP con TLS .....	384
TABLA 14-16	Opciones de línea de comandos disponibles en la versión 8.13 de sendmail ..	385
TABLA 14-17	Opciones de archivo de configuración disponibles en la versión 8.13 de sendmail .....	386
TABLA 14-18	Declaraciones FEATURE() disponibles en la versión 8.13 de sendmail .....	387
TABLA 14-19	Opciones de línea de comandos descartadas o adicionales de la versión 8.12 de sendmail .....	391
TABLA 14-20	Argumentos para las opciones PidFile y ProcessTitlePrefix .....	392
TABLA 14-21	Macros definidas adicionales para sendmail .....	392
TABLA 14-22	Macros adicionales utilizadas para crear el archivo de configuración de sendmail .....	394
TABLA 14-23	Macros MAX adicionales .....	394
TABLA 14-24	Macros de configuración m4 revisadas y adicionales para sendmail .....	395
TABLA 14-25	Declaraciones FEATURE() revisadas y adicionales .....	396
TABLA 14-26	Declaraciones FEATURE() no admitidas .....	398
TABLA 14-27	Indicadores de aplicación de correo adicionales .....	399
TABLA 14-28	Ecuaciones adicionales para agentes de entrega .....	400
TABLA 14-29	Comparación de tokens .....	402
TABLA 14-30	Indicadores de mapa LDAP adicionales .....	402
TABLA 14-31	Valores posibles para el primer argumento de aplicación de correo .....	403
TABLA 14-32	Conjuntos de reglas nuevos .....	404
TABLA 16-1	Mapa de tareas para planificación de PPP .....	425
TABLA 16-2	Información para un equipo de marcación de salida .....	426
TABLA 16-3	Información para un servidor de marcación de entrada .....	427
TABLA 16-4	Planificación para un enlace de línea arrendada .....	431
TABLA 16-5	Requisitos previos antes de configurar la autenticación .....	434
TABLA 16-6	Planificación de clientes PPPoE .....	439
TABLA 16-7	Planificación de un servidor de acceso PPPoE .....	439
TABLA 17-1	Mapa de tareas para configuración de enlace de PPP por marcación telefónica	

	.....	443
TABLA 17-2	Mapa de tareas para configuración de equipo de marcación de salida .....	444
TABLA 17-3	Mapa de tareas para configuración de servidor de marcación de entrada .....	451
TABLA 18-1	Mapa de tareas para configuración del enlace de línea arrendada .....	459
TABLA 19-1	Mapa de tareas para autenticación general de PPP .....	465
TABLA 19-2	Mapa de tareas para autenticación PAP (servidor de marcación de entrada) ..	466
TABLA 19-3	Mapa de tareas para autenticación PAP (equipo de marcación de salida) .....	467
TABLA 19-4	Mapa de tareas para autenticación CHAP (servidor de marcación de entrada) .....	474
TABLA 19-5	Mapa de tareas para autenticación CHAP (equipo de marcación de salida) ....	475
TABLA 20-1	Mapa de tareas para configuración de un cliente PPPoE .....	481
TABLA 20-2	Mapa de tareas para configuración de un servidor de acceso PPPoE .....	482
TABLA 21-1	Mapa de tareas para resolución de problemas de PPP .....	489
TABLA 21-2	Problemas de red comunes que afectan el PPP .....	496
TABLA 21-3	Problemas de comunicaciones generales que afectan PPP .....	497
TABLA 21-4	Problemas de configuración de PPP comunes .....	498
TABLA 21-5	Problemas de secuencia de comandos de chat comunes .....	501
TABLA 21-6	Problemas comunes de línea arrendada .....	507
TABLA 21-7	Problemas de autenticación generales .....	507
TABLA 22-1	Resumen de comandos y archivos de configuración de PPP .....	510
TABLA 22-2	Comandos y archivos de configuración de PPPoE .....	541
TABLA 25-1	Mapa de tareas para la administración del UUCP .....	565
TABLA 26-1	Caracteres de escape utilizados en el campo Chat-Script del archivo Systems	580
TABLA 26-2	Protocolos que se utilizan en /etc/uucp/Devices .....	588
TABLA 26-3	Caracteres de barra diagonal inversa para /etc/uucp/Dialers .....	591
TABLA 26-4	Entradas en el archivo Dialcodes .....	594
TABLA 26-5	Campo Permit-type .....	607
TABLA 26-6	Archivos de bloqueo del UUCP .....	610
TABLA 26-7	Mensajes de error ASSERT .....	612
TABLA 26-8	Mensajes STATUS del UUCP .....	613
TABLA 26-9	Mensajes de error por número del UUCP .....	615
TABLA 28-1	Mapa de tareas: administración del servidor FTP .....	624
TABLA 29-1	Mapa de tareas: acceso a sistemas remotos .....	653
TABLA 29-2	Dependencias entre método de inicio de sesión y método de autenticación (rlogin) .....	657
TABLA 29-3	Comandos ftp esenciales .....	662

TABLA 29-4	Sintaxis permitidas para nombres de archivo y directorio .....	670
TABLA 30-1	Comandos para supervisión de la red .....	677
TABLA 30-2	Salida del comando netstat - r .....	682
TABLA 30-3	Comandos para mostrar estadísticas de cliente/servidor .....	683
TABLA 30-4	Salida del comando nfsstat - c .....	684
TABLA 30-5	Salida del comando nfsstat - m .....	684



# Lista de ejemplos

---

EJEMPLO 2-1	Uso de un dispositivo sin formato como archivo de registro del NCA .....	55
EJEMPLO 2-2	Uso de varios archivos de registro del NCA .....	55
EJEMPLO 2-3	Configuración de un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del núcleo .....	60
EJEMPLO 2-4	Configuración de un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo .....	61
EJEMPLO 2-5	Configuración de un servidor web Apache en una zona local para utilizar proxy SSL en el nivel del núcleo .....	62
EJEMPLO 3-1	Sincronización de fecha y hora desde otro sistema .....	69
EJEMPLO 5-1	Entrada en el archivo <code>vfstab</code> del cliente .....	91
EJEMPLO 6-1	Desmontaje de un sistema de archivos .....	166
EJEMPLO 6-2	Uso de las opciones con <code>umount</code> .....	166
EJEMPLO 6-3	Archivo de muestra <code>/etc/auto_master</code> .....	206
EJEMPLO 9-1	Configuración de <code>slpd</code> para funcionar como servidor de DA .....	244
EJEMPLO 13-1	Cómo establecer la nueva generación automática de <code>submit.cf</code> .....	306
EJEMPLO 13-2	Encabezado de correo Received: .....	311
EJEMPLO 13-3	Cómo mostrar una entrada individual en la tabla NIS+ <code>mail_aliases</code> .....	316
EJEMPLO 13-4	Cómo mostrar coincidencias parciales en la tabla NIS+ <code>mail_aliases</code> .....	316
EJEMPLO 13-5	Eliminación de entradas de una tabla NIS+ <code>mail_aliases</code> .....	319
EJEMPLO 13-6	Salida del modo de prueba de direcciones .....	334
EJEMPLO 21-1	Resultado de un enlace por marcación telefónica que funciona correctamente .....	491
EJEMPLO 21-2	Resultado de un enlace de línea arrendada que funciona correctamente .....	492
EJEMPLO 22-1	Secuencia de comandos de chat en línea .....	531
EJEMPLO 22-2	Archivo <code>/etc/ppp/pppoe</code> básico .....	545
EJEMPLO 22-3	Archivo para un servidor de acceso <code>/etc/ppp/pppoe</code> .....	547
EJEMPLO 22-4	Archivo para un servidor de acceso <code>/etc/ppp/options</code> .....	547
EJEMPLO 22-5	Archivo para un servidor de acceso <code>/etc/hosts</code> .....	548
EJEMPLO 22-6	Archivo para un servidor de acceso <code>/etc/ppp/pap-secrets</code> .....	548

EJEMPLO 22-7	Archivo para un servidor de acceso /etc/ppp/chap-secrets .....	548
EJEMPLO 22-8	/etc/ppp/peers/ <i>nombre de igual</i> para definir un servidor de acceso remoto	550
EJEMPLO 26-1	Entrada en /etc/uucp/Systems .....	576
EJEMPLO 26-2	Palabra clave con el campo Type .....	578
EJEMPLO 26-3	Entrada en el campo Speed .....	578
EJEMPLO 26-4	Entrada en el campo Phone .....	579
EJEMPLO 26-5	Comparación de los campos Type en el archivo Devices y en el archivo Systems .....	584
EJEMPLO 26-6	Campo Class en el archivo Devices .....	585
EJEMPLO 26-7	Campo Dialers para módems conectados directamente .....	587
EJEMPLO 26-8	Campo Dialers del UUCP para equipos en el mismo selector de puerto .....	587
EJEMPLO 26-9	Campo Dialers del UUCP para módems conectados al selector de puerto .....	587
EJEMPLO 26-10	Entrada en el archivo /etc/uucp/Dialers .....	590
EJEMPLO 26-11	Segmentos de /etc/uucp/Dialers .....	590
EJEMPLO 28-1	Definición de clases de servidor FTP .....	626
EJEMPLO 28-2	Configuración de límites de inicio de sesión de usuarios .....	627
EJEMPLO 28-3	Control del número de intentos de inicio de sesión no válidos .....	628
EJEMPLO 28-4	Prohibición del acceso al servidor FTP .....	629
EJEMPLO 28-5	Restricción de acceso al servidor FTP predeterminado .....	630
EJEMPLO 28-6	Configuración de un servidor FTP invitado .....	633
EJEMPLO 28-7	Configuración de usuarios anónimos del FTP .....	634
EJEMPLO 28-8	Creación del archivo /etc/shells .....	634
EJEMPLO 28-9	Personalización de archivos de mensaje .....	635
EJEMPLO 28-10	Creación de mensajes que se van a enviar a los usuarios .....	636
EJEMPLO 28-11	Configuración de la opción README .....	637
EJEMPLO 28-12	Control de comandos de acceso a archivos .....	639
EJEMPLO 28-13	Control de cargas al servidor FTP .....	641
EJEMPLO 28-14	Control de descargas al servidor FTP .....	642
EJEMPLO 28-15	Habilitación del hospedaje virtual limitado en el archivo ftpaccess .....	644
EJEMPLO 28-16	Habilitación del hospedaje virtual limitado en la línea de comandos .....	644
EJEMPLO 28-17	Habilitación del hospedaje virtual completo en el archivo ftpservers .....	645
EJEMPLO 28-18	Habilitación del hospedaje virtual completo en la línea de comandos .....	645
EJEMPLO 29-1	Búsqueda y eliminación de archivos . rhosts .....	659
EJEMPLO 29-2	Búsqueda de quién ha iniciado sesión en un sistema remoto .....	660
EJEMPLO 29-3	Inicio de sesión en un sistema remoto (rlogin) .....	661
EJEMPLO 29-4	Cierre de sesión desde un sistema remoto (exit) .....	662

EJEMPLO 29-5	Apertura de una conexión ftp a un sistema remoto .....	664
EJEMPLO 29-6	Copia de archivos de un sistema remoto (ftp) .....	665
EJEMPLO 29-7	Copia de archivos a un sistema remoto (ftp) .....	667
EJEMPLO 29-8	Uso de rcp para copiar un archivo remoto a un sistema local .....	671
EJEMPLO 29-9	Uso de rlogin y rcp para copiar un archivo remoto a un sistema local .....	672
EJEMPLO 29-10	Uso de rcp para copiar un archivo local a un sistema remoto .....	672
EJEMPLO 29-11	Uso de rlogin y rcp para copiar un archivo local a un sistema remoto .....	672
EJEMPLO 30-1	Comprobación de la respuesta de los hosts en la red .....	678
EJEMPLO 30-2	Envío de paquetes a los hosts en la red .....	679



# Prefacio

---

La *Guía de administración del sistema: servicios de red* forma parte de un conjunto de varios volúmenes que tratan de manera exhaustiva la administración de sistemas Oracle Solaris. En esta guía, se da por sentado que ya instaló el sistema operativo Oracle Solaris 10 y que configuró el software de red que tiene previsto usar.

---

**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.
- "x86 de 32 bits" destaca información específica de 32 bits acerca de sistemas basados en x86.

Para conocer cuáles son los sistemas admitidos, consulte las [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 Solaris 10. Para utilizar esta guía, se debe tener entre uno y dos años de experiencia en la administración de sistemas UNIX. Puede resultar útil participar en cursos de formación para 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, administración de servicios y administración de software (paquetes y parches)
<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 de Solaris, IP para móviles, multirruta IP de Solaris (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 Solaris, privilegios, RBAC, SASL y 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 administración 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

## Manuales relacionados

A continuación, se muestra una lista de la documentación relacionada a la que se hace referencia en esta guía.

- *Guía de administración del sistema: Administración avanzada*
- *Guía de administración del sistema: administración básica*
- *Guía de administración del sistema: servicios IP*
- *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*
- *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris*
- *Guía de administración del sistema: servicios de seguridad*
- Anderson, Bart, Bryan Costales y Harry Henderson. *UNIX Communications* (Comunicaciones UNIX). Howard W. Sams & Company, 1987.
- Costales, Bryan. *sendmail, Third Edition* (sendmail, tercera edición). O'Reilly & Associates, Inc., 2002.
- Frey, Donnalyn y Rick Adams. *!%@:: A Directory of Electronic Mail Addressing and Networks* (!%@:: Un directorio de direcciones y redes de correo electrónico). O'Reilly & Associates, Inc., 1993.
- Krol, Ed. *The Whole Internet User's Guide and Catalog* (Conéctate al mundo de Internet. Guía y catálogo). O'Reilly & Associates, Inc., 1993.
- O'Reilly, Tim y Grace Todino. *Managing UUCP and Usenet* (Gestión de UUCP y Usenet). O'Reilly & Associates, Inc., 1992.

# Información relacionada

Para obtener información sobre las condiciones de licencia PPPoE, consulte el material incluido en las siguientes ubicaciones:

```
/var/sadm/pkg/SUNWpppd/install/copyright
```

```
/var/sadm/pkg/SUNWpppdu/install/copyright
```

```
/var/sadm/pkg/SUNWpppg/install/copyright
```

# 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 visite <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si tiene alguna discapacidad auditiva.

# 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.
AaBbCc123	Lo que se escribe, en contraposición con la salida del equipo en pantalla	<code>nombre_sistema% su</code>  Contraseña:
aabbcc123	Marcador de posición: sustituir por un valor o nombre real	El comando necesario para eliminar un archivo es <code>rm nombrearchivo</code> .
AaBbCc123	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**

### **Servicios de red (temas)**

Esta sección proporciona una descripción general de la guía, además de información sobre la descripción general, las tareas y la referencia de los servicios NCA y NTP.



## Servicio de red (descripción general)

---

Este capítulo proporciona una lista de los principales temas que se tratan en esta guía. Además, brinda una descripción del servicio PERL que se incluye en esta versión.

- [“Temas para la Versión de actualización 10 de Oracle Solaris 10” en la página 45](#)
- [“Perl 5” en la página 46](#)

## Temas para la Versión de actualización 10 de Oracle Solaris 10

En esta guía, se tratan los siguientes servicios o utilidades:

### [“Perl 5” en la página 46](#)

Practical Extraction and Report Language (Perl) es una herramienta que se puede utilizar para generar secuencias de comandos que ayuden con las tareas de administración del sistema.

### [Capítulo 2, “Gestión de servidores de antememoria web”](#)

NCA proporciona un mejor rendimiento de los servidores web mediante el almacenamiento en caché de páginas web.

### [Capítulo 3, “Servicios relacionados con el tiempo”](#)

NTP y las utilidades relacionadas con el tiempo se pueden emplear para sincronizar la hora de varios sistemas.

### [Capítulo 4, “Gestión de sistemas de archivos de red \(descripción general\)”](#)

NFS es un protocolo que permite acceder a sistemas de archivos desde un host remoto.

### [Capítulo 7, “SLP \(descripción general\)”](#)

SLP es un protocolo de detección de servicios dinámico.

### [Capítulo 12, “Servicios de correo \(descripción general\)”](#)

Los servicios de correo permiten enviar un mensaje a una o varias personas mediante el enrutamiento del mensaje a través de las redes necesarias.

### Capítulo 15, “Solaris PPP 4.0 (descripción general)”

PPP es un protocolo que proporciona enlaces punto a punto entre hosts remotos.

### Capítulo 24, “UUCP (descripción general)”

UUCP permite a los hosts intercambiar archivos.

### Capítulo 27, “Trabajo con sistemas remotos (descripción general)”

Estos comandos se utilizan para acceder a archivos en sistemas remotos. Los comandos incluyen ftp, rlogin y rcp.

## Perl 5

Esta versión de Solaris incluye Practical Extraction and Report Language (Perl) 5.8.4, un eficaz lenguaje de programación de uso general que habitualmente está disponible como software gratuito. Perl ha surgido como la herramienta de desarrollo estándar para la compleja tarea de administración de sistemas debido a sus excelentes capacidades de manipulación de textos, procesos y archivos.

Perl 5 incluye una estructura de módulo cargable de manera dinámica, que permite la adición de nuevas capacidades para tareas específicas. Existen varios módulos disponibles de forma gratuita en Comprehensive Perl Archive Network (CPAN), en <http://www.cpan.org>. Si desea generar e instalar módulos adicionales desde CPAN mediante gcc, puede hacerlo por medio de la secuencia de comandos `/usr/perl5/5.8.4/bin/perl gcc`. Consulte la página del comando `man perl gcc(1)` para obtener detalles.

## Acceso a la documentación de Perl

En esta versión de Solaris, se incluyen varias fuentes de información sobre Perl. Encontrará la misma información disponible mediante estos dos mecanismos.

Puede agregar `/usr/perl5/man` a la variable de entorno `MANPATH` para acceder a las páginas del comando `man`. En este ejemplo, se muestra la descripción general de Perl.

```
% setenv MANPATH ${MANPATH}:/usr/perl5/man
% man perl
```

Puede usar la utilidad `perldoc` para acceder a documentación adicional. En este ejemplo, se muestra la misma información general.

```
% /usr/perl5/bin/perldoc perl
```

La página de descripción general de `perl` muestra toda la documentación que se incluye con la versión.

## Problemas de compatibilidad de Perl

En general, la versión 5.8.4 de Perl es compatible con la versión anterior. No es necesario volver a generar ni compilar las secuencias de comandos para que funcionen. Sin embargo, los módulos basados en XSUB (.xs) requieren una nueva compilación e instalación.

## Cambios en la versión Solaris de Perl

La versión Solaris de Perl se compiló para incluir compatibilidad con archivos grandes, valores enteros de 64 bits y asignación de memoria del sistema. Además, se aplicaron los parches apropiados. Para obtener una lista completa de toda la información de configuración, revise los resultados de este comando.

```
% /usr/perl5/bin/perlbug -dv
---
Flags:
    category=
    severity=
---
Site configuration information for perl v5.8.4:
.
.
```

Puede generar una lista más corta por medio de `perl -V`.





## Gestión de servidores de antememoria web

---

En este capítulo se proporciona una descripción general del Acelerador y antememoria de red (NCA) de Solaris. Se incluyen los procedimientos para utilizar el NCA y material de referencia sobre el NCA. Además, para Solaris 10 6/06, se agregan una introducción al uso del protocolo de capa de sockets seguros (SSL) y los procedimientos para utilizar el proxy SSL en el nivel del núcleo para mejorar el rendimiento del procesamiento de paquetes de SSL.

- “Acelerador y antememoria de red (descripción general)” en la página 49
- “Gestión de servidores de antememoria web (mapa de tareas)” en la página 51
- “Administración del almacenamiento en antememoria de las páginas web (tareas)” en la página 53
- “Almacenamiento en antememoria de páginas web (referencia)” en la página 62

### Acelerador y antememoria de red (descripción general)

El Acelerador y antememoria de red (NCA) de Solaris aumenta el rendimiento del servidor web y mantiene una antememoria en el núcleo de las páginas web a las que se accede durante las solicitudes de HTTP. Esta antememoria en el núcleo utiliza la memoria del sistema para aumentar significativamente el rendimiento de las solicitudes HTTP que normalmente manejan los servidores web. El uso de memoria de sistema para mantener las páginas web para las solicitudes HTTP aumenta el rendimiento del servidor web y reduce la carga entre el núcleo y el servidor web. El NCA proporciona una interfaz de socket a través de la cual cualquier servidor web se puede comunicar con el NCA con modificaciones mínimas.

En situaciones en las que la página solicitada se recupera de la antememoria en el núcleo (acierto de antememoria), el rendimiento mejora sustancialmente. En situaciones en las que la página solicitada no está en la antememoria (error de antememoria) y se debe recuperar del servidor web, el rendimiento también se ve mejorado significativamente.

Este producto está destinado a ejecutarse en un servidor web dedicado. Si ejecuta otros procesos grandes en un servidor que ejecuta el NCA, pueden producirse problemas.

El NCA proporciona compatibilidad de registro en cuanto el NCA registra todos los aciertos de la antememoria. Este registro se almacena en formato binario para mejorar el rendimiento. El comando `ncab2clf` se puede utilizar para convertir el archivo de registro de un formato binario a un formato de registro común (CLF).

La versión de Solaris incluye las siguientes mejoras:

- Interfaz de sockets.
- Compatibilidad con `sendfile` vectorizado, que proporciona compatibilidad con `AF_NCA`. Para obtener más información, consulte la página del comando `man sendfilev(3EXT)`.
- Nuevas opciones para el comando `ncab2clf` compatible con la capacidad omitir registros antes de una fecha seleccionada (`-s`) y para procesar un número especificado de registros (`-n`).
- `logd_path_name` en `ncalogd.conf` puede especificar un dispositivo sin formato, un archivo o una combinación de ambos.
- Compatibilidad con un servidor web para abrir varios sockets `AF_NCA`. Con varios sockets, se pueden tener diferentes servidores web que se ejecutan en un servidor.
- Un nuevo archivo de configuración que se llama `/etc/nca/ncaport.conf`. El archivo se puede utilizar para gestionar las direcciones IP y los puertos que el NCA utiliza. El servidor web no puede proporcionar compatibilidad nativa del socket `AF_NCA`. Si el servidor carece de esta compatibilidad, utilice este archivo y la biblioteca de utilidades del socket NCA para convertir un socket `AF_INET` en un socket `AF_NCA`.

## Servidores web que usan el protocolo de capa de sockets seguros

En la versión Solaris 10 6/06, un servidor Apache 2.0 y un Sun Java System Web Server podían configurarse para utilizar el protocolo de capa de sockets seguros (SSL). El protocolo ofrece confidencialidad, integridad de mensajes y autenticación de punto final entre dos aplicaciones. El núcleo se ha cambiado para acelerar el tráfico SSL.

El proxy SSL en el nivel del núcleo implementa la parte del servidor del protocolo SSL. El proxy ofrece un mejor rendimiento de SSL para las aplicaciones de servidor, como servidores web, en comparación con las aplicaciones que usan bibliotecas SSL de nivel de usuario. La mejora del rendimiento puede llegar a ser de hasta +35% según la carga de trabajo de la aplicación.

El proxy SSL en el nivel del núcleo admite los protocolos SSL 3.0 y TLS 1.0, así como la mayoría de los conjuntos de cifrado comunes. Consulte la página del comando `man ksslcfg(1M)` para ver una lista completa. El servidor proxy se puede configurar para que recurra al servidor SSL en el nivel de usuario para cualquier conjunto de cifrado no admitido.

Los procedimientos siguientes muestran cómo configurar los servidores para utilizar el proxy SSL en el nivel del núcleo:

- “Cómo configurar un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del núcleo” en la página 58
- “Cómo configurar un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo” en la página 60
- “Uso del proxy SSL en el nivel del núcleo en zonas” en la página 62

## Gestión de servidores de antememoria web (mapa de tareas)

La siguiente tabla describe los procedimientos necesarios para utilizar el NCA o SSL.

Tarea	Descripción	Para obtener instrucciones
Planificación del NCA	Una lista de problemas que deben estar resueltos antes de habilitar el uso de NCA.	“Planificación del NCA” en la página 52
Habilitación del NCA	Pasos para habilitar el almacenamiento en antememoria en núcleo de páginas web en un servidor web.	“Cómo habilitar el almacenamiento en antememoria de páginas web” en la página 53
Deshabilitación del NCA	Pasos para deshabilitar el almacenamiento en antememoria en núcleo de páginas web en un servidor web.	“Cómo deshabilitar el almacenamiento en la antememoria de las páginas web” en la página 56
Administración del registro del NCA	Pasos para habilitar o deshabilitar el proceso de registro del NCA.	“Cómo habilitar y deshabilitar el registro del NCA” en la página 56
Carga de la biblioteca del socket NCA	Pasos para utilizar el NCA si el socket AF_NCA no es compatible.	“Cómo cargar la biblioteca de utilidades del socket NCA” en la página 57
Uso del proxy SSL en el nivel del núcleo con un servidor web Apache 2.0	Pasos para utilizar el proxy SSL en el nivel del núcleo con un servidor web para mejorar el procesamiento de paquetes SSL.	“Cómo configurar un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del núcleo” en la página 58
Uso del proxy SSL en el nivel del núcleo con un Sun Java System Web Server	Pasos para utilizar el proxy SSL en el nivel del núcleo con un servidor web para mejorar el procesamiento de paquetes SSL.	“Cómo configurar un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo” en la página 60
Uso del proxy SSL en el nivel del núcleo con un servidor web en una zona local	Pasos para utilizar el proxy SSL en el nivel del núcleo con un servidor web en una zona local.	“Uso del proxy SSL en el nivel del núcleo en zonas” en la página 62

## Planificación del NCA

Las siguientes secciones incluyen los problemas que se deben resolver antes de iniciar el servicio del NCA.

### Requisitos del sistema para el NCA

Para admitir el NCA, el sistema debe cumplir con los siguientes requisitos:

- Debe contar con 256 Mbytes de memoria RAM instalados.
- Debe contar con Solaris versión 10 o 9, o una de las actualizaciones de Solaris 8.
- Compatibilidad con un servidor web que ofrezca soporte nativo para el NCA o un servidor web cuya secuencia de comandos de inicio se haya modificado para utilizar la biblioteca de utilidades del socket para el NCA:
  - Servidor web Apache, se envía con la actualización de Solaris 8 y con Solaris 9 y Oracle Solaris 10
  - Servidor web de Sun Java System
  - Servidor web Zeus disponible de Zeus Technology, [Http://www.zeus.com](http://www.zeus.com)

Este producto está destinado a ejecutarse en un servidor web dedicado. La ejecución de procesos grandes en un servidor que ejecuta el NCA puede causar problemas.

### Registro del NCA

El servicio del NCA se puede configurar para que registre la actividad web. Por lo general, el registro del NCA debe estar habilitado si está habilitado el registro del servidor web.

### Biblioteca de interposición para compatibilidad con daemon del servidor Door

Muchos servidores web utilizan sockets AF\_INET. De manera predeterminada, el NCA utiliza sockets AF\_NCA. Para corregir esta situación, se proporciona una biblioteca de interposición. La nueva biblioteca se carga en frente de la biblioteca de socket estándar, `libsocket.so`. La llamada de biblioteca `bind()` es interpuesta por la nueva biblioteca, `ncad_addr.so`. Por ejemplo, si el estado está habilitado en `/etc/nca/ncakmod.conf`. La versión de Apache que se incluye con las versiones Solaris 9 y Solaris 10 ya está configurada para invocar esta biblioteca. Si está utilizando IWS o los servidores Netscape, consulte “[Cómo cargar la biblioteca de utilidades del socket NCA](#)” en la [página 57](#) para utilizar la biblioteca nueva.

## Soporte de varias instancias

Los sistemas que tienen el NCA instalado a menudo necesitan ejecutar varias instancias de un servidor web. Por ejemplo, es posible que un servidor individual necesite admitir un servidor web para acceso exterior, así como un servidor de administración web. Para separar estos servidores, debe configurar cada servidor para utilizar un puerto independiente.

## Administración del almacenamiento en antememoria de las páginas web (tareas)

Las siguientes secciones incluyen los procedimientos para habilitar o deshabilitar las partes del servicio.

### ▼ Cómo habilitar el almacenamiento en antememoria de páginas web

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Registre las interfaces.

Escriba los nombres de cada una de las interfaces físicas en el archivo `/etc/nca/nca.if`. Consulte la página del comando `man nca.if(4)` para obtener más información.

```
# cat /etc/nca/nca.if
hme0
hme1
```

Cada interfaz debe estar junto con un archivo `nombre_interfaz hostname.` y una entrada en el archivo `/etc/hosts` para los contenidos de `nombre_interfazhostname.`. Para iniciar la función NCA en todas las interfaces, coloque un asterisco, `*`, en el archivo `nca.si`.

#### 3 Habilite el módulo de núcleo `ncakmod`.

Cambie la entrada `status` en `/etc/nca/ncakmod.conf` a `enabled`.

```
# cat /etc/nca/ncakmod.conf
#
# NCA Kernel Module Configuration File
#
status=enabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

Consulte la página del comando `man ncakmod.conf(4)` para obtener más información.

#### 4 (Opcional) Habilite el registro del NCA.

Cambie la entrada `status` en `/etc/nca/nalogd.conf` a `enabled`.

```
# cat /etc/nca/nalogd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

Puede cambiar la ubicación del archivo de registro si cambia la ruta indicada por la entrada `logd_path_name`. El archivo de registro puede ser un dispositivo sin formato o un archivo. Consulte los siguientes ejemplos para ver muestras de rutas de archivos de registro del NCA. Consulte la página del comando `man nalogd.conf(4)` para obtener más información sobre el archivo de configuración.

#### 5 (Opcional) Defina puertos para soporte de varias instancias.

Agregue los números de puerto en el archivo `/etc/nca/ncaport.conf`. Esta entrada hace que el NCA supervise el puerto 80 en todas las direcciones IP configuradas.

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
.
.
ncaport=*/80
```

#### 6 Sólo para x86: aumente el tamaño de memoria virtual.

Utilice el comando `eeeprom` para definir la `kernelbase` del sistema.

```
# eeeprom kernelbase=0x90000000
# eeeprom kernelbase
kernelbase=0x90000000
```

El segundo comando verifica que el parámetro se haya configurado.

---

**Nota** – Al configurar `kernelbase`, reduce la cantidad de memoria virtual que pueden usar los procesos de usuario a menos de 3 Gbytes. Esta restricción significa que el sistema no es compatible con ABI. Cuando el sistema se inicia, la consola muestra un mensaje que advierte acerca del incumplimiento. La mayoría de los programas no necesitan todo el espacio de dirección virtual de 3 GB. Si tiene un programa que requiere más de 3 Gbytes, debe ejecutar el programa en un sistema que no tenga el NCA habilitado.

---

#### 7 Reinicie el servidor.

**Ejemplo 2-1** Uso de un dispositivo sin formato como archivo de registro del NCA

La cadena `logd_path_name` en `nca logd.conf` puede definir un dispositivo sin formato como el lugar para almacenar el archivo de registro NCA. La ventaja de utilizar un dispositivo sin formato es que el servicio puede ejecutarse más rápido debido a que se disminuye la sobrecarga al acceder a un dispositivo sin formato.

El servicio del NCA prueba los dispositivos sin formato que aparecen en el archivo para garantizar que no haya ningún sistema de archivos en el lugar. Esta prueba garantiza que no se sobrescriban accidentalmente sistemas de archivos.

Para evitar que esta prueba encuentre un sistema de archivos, ejecute el siguiente comando. Este comando destruye parte del sistema de archivos en cualquier partición de disco que se haya configurado como sistema de archivos. En este ejemplo, `/dev/rdisk/c0t0d0s7` es el dispositivo sin formato que tiene un sistema de archivos antiguo.

```
# dd if=/dev/zero of=/dev/rdisk/c0t0d0s7 bs=1024 count=1
```

Después de ejecutar `dd`, puede agregar el dispositivo sin formato al archivo `nca logd.conf`.

```
# cat /etc/nca/nca logd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/dev/rdisk/c0t0d0s7"
logd_file_size=1000000
```

**Ejemplo 2-2** Uso de varios archivos de registro del NCA

La cadena `logd_path_name` en `nca logd.conf` puede definir varios destinos como el lugar para almacenar el archivo de registro del NCA. El segundo archivo se utiliza cuando el primer archivo está lleno. El siguiente ejemplo muestra cómo seleccionar escribir en el archivo `/var/nca/log` primero y luego usar la partición sin formato.

```
# cat /etc/nca/nca logd.conf
#
# NCA Logging Configuration File
#
status=enabled
logd_path_name="/var/nca/log /dev/rdisk/c0t0d0s7"
logd_file_size=1000000
```

## ▼ Cómo deshabilitar el almacenamiento en la antememoria de las páginas web

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Deshabilite el módulo de núcleo ncakmod.

Cambie la entrada status en `/etc/nca/ncakmod.conf` a disabled.

```
# cat /etc/nca/ncakmod.conf
# NCA Kernel Module Configuration File
#
status=disabled
httpd_door_path=/var/run/nca_httpd_1.door
nca_active=disabled
```

Consulte la página del comando `man ncakmod.conf(4)` para obtener más información.

### 3 Deshabilite el registro del NCA.

Cambie la entrada status en `/etc/nca/ncaologd.conf` a disabled.

```
# cat /etc/nca/ncaologd.conf
#
# NCA Logging Configuration File
#
status=disabled
logd_path_name="/var/nca/log"
logd_file_size=1000000
```

Consulte la página del comando `man ncaologd.conf(4)` para obtener más información.

### 4 Reinicie el servidor.

## ▼ Cómo habilitar y deshabilitar el registro del NCA

El registro del NCA puede habilitarse o deshabilitarse según sea necesario, una vez que se haya habilitado el NCA. Consulte [“Cómo habilitar el almacenamiento en antememoria de páginas web” en la página 53](#) para obtener más información.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).



## 2 Cambie el registro del NCA.

Para deshabilitar permanentemente el registro, debe cambiar el estado en `/etc/nca/ncaLogd.conf` a `disabled` y reiniciar el sistema. Consulte la página del comando `man ncaLogd.conf(4)` para obtener más información.

### a. Detenga el registro.

```
# /etc/init.d/ncaLogd stop
```

### b. Inicie el registro.

```
# /etc/init.d/ncaLogd start
```

## Cómo cargar la biblioteca de utilidades del socket NCA

Siga este proceso sólo si el servidor web no proporciona soporte nativo del socket `AF_NCA`.

En la secuencia de comandos de inicio para el servidor web, agregue una línea que haga que la biblioteca se precargue. La línea que obtendrá debe ser similar a la siguiente:

```
LD_PRELOAD=/usr/lib/ncad_addr.so /usr/bin/httpd
```

## ▼ Cómo agregar un nuevo puerto al servicio del NCA

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue un nuevo puerto.

Agregue una nueva entrada de puerto a `/etc/nca/ncaport.conf`. Este ejemplo agrega el puerto 8888 a la dirección IP 192.168.84.71. Consulte `ncaport.conf(4)` para obtener más información.

```
# cat /etc/nca/ncaport.conf
#
# NCA Kernel Module Port Configuration File
#
.
.
ncaport=*/80
ncaport=192.168.84.71/8888
```

### 3 Inicie una nueva instancia de web.

Una dirección debe estar en el archivo que contiene las configuraciones de puerto del NCA antes de que un servidor web pueda utilizar la dirección del NCA. Si el servidor web se ejecuta, debe reiniciarse después de que se defina la nueva dirección.

## ▼ Cómo configurar un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del núcleo

Este procedimiento se debe utilizar para mejorar el rendimiento del proceso de paquetes SSL en un servidor web Apache 2.0.

### Antes de empezar

El siguiente procedimiento requiere que se instale y configure un servidor web Apache 2.0. El servidor web Apache 2.0 se incluye en la versión.

Para utilizar el proxy SSL en el nivel del núcleo, la clave privada del servidor y el certificado de servidor tienen que existir en un único archivo. Si sólo los parámetros `SSLCertificateFile` se especifican en el archivo `ssl.conf`, el archivo especificado se puede utilizar directamente para el SSL del núcleo. Si el parámetro `SSLCertificateKeyFile` también se especifica, el archivo de certificado y el archivo de clave privada deben combinarse. Una forma de combinar el certificado y el archivo de clave es ejecutar el siguiente comando:

```
# cat cert.pem key.pem >cert-and-key.pem
```

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#). El comando `ksslcfg` se incluye en el perfil `Network Security`.

### 2 Detenga el servidor web.

Este comando detendrá el servidor web en un sistema en el que el servidor esté configurado para ejecutarse con SMF.

```
# svcadm disable svc:/network/http:apache2
```

Si el servicio no se ha convertido aún, deténgalo con esta sintaxis de comando:

```
/usr/apache2/bin/apachectl stop
```

### 3 Determine qué parámetros desea utilizar con el comando `ksslcfg`.

Todas las opciones se muestran en la página del comando `man ksslcfg(1M)`. Los parámetros para los que debe tener información son:

- `key-format`: se usa con la opción `-f` para definir el certificado y el formato de clave. Para el proxy SSL en el nivel del núcleo, el valor debería ser `pem` o `pkcs12`.
- `key-and-certificate-file`: se usa con la opción `-i` para establecer la ubicación del archivo que almacena la clave del servidor y el certificado.
- `password-file`: se utiliza con la opción `-p` para seleccionar la ubicación del archivo que incluye la contraseña utilizada para cifrar la clave privada. Esta contraseña se utiliza para permitir inicios sin vigilancia. Los permisos en el archivo deben ser `0400`.

- `proxy-port`: se usa con la opción `-x` para configurar el puerto proxy SSL. Seleccione un puerto diferente que el puerto estándar 80. El servidor web recibe el puerto proxy SSL.
- `ssl-port`: selecciona el puerto del que debe recibir el proxy SSL en el nivel del núcleo. Normalmente esto se establece en 443.

---

**Nota** – Los valores `ssl-port` y `proxy-port` no se pueden configurar para el NCA, ya que estos puertos son utilizados exclusivamente por el proxy SSL en el nivel del núcleo. Normalmente, el puerto 80 se utiliza para el NCA, el puerto 8443 para `proxy-port` y el 443 para `ssl-port`.

---

#### 4 Cree la instancia de servicio.

El comando `ksslcfg` para especificar el puerto proxy SSL y los parámetros asociados.

```
ksslcfg create -f key-format -i key-and-certificate-file -p password-file -x proxy-port ssl-port
```

#### 5 Verifique que la instancia se haya creado correctamente.

El servicio de estado informado por el siguiente comando debe ser “en línea”.

```
# svcs svc:/network/ssl/proxy
```

#### 6 Configure el servidor web para recibir el puerto proxy SSL.

Edite el archivo `/etc/apache2/http.conf` y agregue una línea para definir el puerto proxy SSL. Si utiliza las direcciones de los servidores IP, el servidor web sólo recibirá en dicha interfaz. La línea debe ser como esta:

```
Listen 0.0.0.0:proxy-port
```

#### 7 Defina una dependencia SMF para el servidor web.

El servidor web sólo debe iniciarse después de la instancia de proxy de núcleo SSL. Los siguientes comandos establecen la dependencia.

```
# svccfg -s svc:/network/http:apache2
svc:/network/http:apache2> addpg kssl dependency
svc:/network/http:apache2> setprop kssl/entities = fmri:svc:/network/ssl/proxy:kssl-INADDR_ANY-443
svc:/network/http:apache2> setprop kssl/grouping = astring: require_all
svc:/network/http:apache2> setprop kssl/restart_on = astring: refresh
svc:/network/http:apache2> setprop kssl/type = astring: service
svc:/network/http:apache2> end
```

#### 8 Habilite el servidor web.

```
# svcadm enable svc:/network/http:apache2
```

Si el servicio no se inicia mediante SMF, utilice el siguiente comando:

```
/usr/apache2/bin/apachectl startssl
```

**Ejemplo 2-3 Configuración de un servidor web Apache 2.0 para utilizar el proxy SSL en el nivel del núcleo**

El siguiente comando crea una instancia con el formato de clave pem.

```
# ksslcfg create -f pem -i cert-and-key.pem -p file -x 8443 443
```

**▼ Cómo configurar un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo**

Este procedimiento se debe utilizar para mejorar el rendimiento del proceso de paquete SSL en un Sun Java System Web Server. Consulte la [Sun Java System Web Server 6.1 SP4 Administrator's Guide](#) para obtener información acerca de este servidor web.

**Antes de empezar** El siguiente procedimiento requiere que se haya instalado y configurado un Sun Java System Web Server.

**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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*. El comando `kslcfg` se incluye en el perfil Network Security.

**2 Detenga el servidor web.**

Utilice la interfaz web del administrador para detener el servidor. Consulte *Starting and Stopping the Server* en la [Sun Java System Web Server 6.1 SP4 Administrator's Guide](#) para obtener más información.

**3 Deshabilite la metarranura de la estructura criptográfica.**

Este paso es necesario para asegurarse de que la metarranura esté deshabilitada al momento de crear la instancia de servicio SSL del núcleo.

```
# cryptoadm disable metaslot
```

**4 Determine qué parámetros desea utilizar con el comando `kslcfg`.**

Todas las opciones se muestran en la página del comando `man ksslcfg(1M)`. Los parámetros para los que debe tener información son:

- `key-format`: se usa con la opción `-f` para definir el certificado y el formato de clave.
- `token-label`: se usa con la opción `-T` para especificar el token PKCS#11.
- `certificate-label`: se usa con la opción `-C` para seleccionar la etiqueta en el objeto de certificado en el token PKCS#11.

- `password-file`: se usa con la opción `-p` para seleccionar la ubicación del archivo que incluye la contraseña usada para iniciar sesión con el usuario para el token PKCS#11 usado por el servidor web. Esta contraseña se utiliza para permitir inicios sin vigilancia. Los permisos en el archivo deben ser `0400`.
- `proxy-port`: se usa con la opción `-x` para configurar el puerto proxy SSL. Seleccione un puerto diferente que el puerto estándar `80`. El servidor web recibe el puerto proxy SSL.
- `ssl-port`: define el puerto del que debe recibir el proxy SSL en el nivel del núcleo. Normalmente este valor se establece en `443`.

---

**Nota** – Los valores `ssl-port` y `proxy-port` no se pueden configurar para el NCA, ya que estos puertos son utilizados exclusivamente por el proxy SSL en el nivel del núcleo. Normalmente, el puerto `80` se utiliza para el NCA, el puerto `8443` para `proxy-port` y el `443` para `ssl-port`.

---

## 5 Cree la instancia de servicio.

El comando `ksslcfg` para especificar el puerto proxy SSL y los parámetros asociados.

```
ksslcfg create -f key-format -T PKCS#11-token -C certificate-label -p password-file -x proxy-port ssl-port
```

## 6 Habilite la metarranura de la estructura criptográfica.

```
# cryptoadm enable metaslot
```

## 7 Verifique que la instancia se haya creado correctamente.

El servicio de estado informado por el siguiente comando debe ser “en línea”.

```
# svcs svc:/network/ssl/proxy
```

## 8 Configure el servidor web para recibir el puerto proxy SSL.

Consulte *Agregar y editar sockets de escucha* en la [Sun Java System Web Server 6.1 SP4 Administrator's Guide](#) para obtener más información.

## 9 Inicie el servidor web.

### Ejemplo 2–4 Configuración de un Sun Java System Web Server para utilizar el proxy SSL en el nivel del núcleo

El siguiente comando crea una instancia con el formato de clave pkcs11.

```
# ksslcfg create -f pkcs11 -T "Sun Software PKCS#11 softtoken" -C "Server-Cert" -p file -x 8443 443
```

# Uso del proxy SSL en el nivel del núcleo en zonas

El proxy SSL en el nivel del núcleo funciona en zonas con las siguientes limitaciones:

- Toda la administración del SSL del núcleo se debe realizar desde la zona global. El administrador de la zona global necesita acceder al certificado de la zona local y los archivos de claves. El servidor web de la zona local se puede iniciar una vez que la instancia de servicio se configure mediante el comando `ksslcfg` en la zona global.
- Debe especificarse un nombre de host específico o dirección IP al ejecutar el comando `ksslcfg` para configurar la instancia. En particular, la instancia no puede usar `INADDR_ANY`.

**EJEMPLO 2-5** Configuración de un servidor web Apache en una zona local para utilizar proxy SSL en el nivel del núcleo

En la zona local, primero detenga el servidor web. En la zona global, realice todos los pasos para configurar el servicio. Para crear una instancia para una zona local denominada `apache-zone`, utilice el siguiente comando:

```
# ksslcfg create -f pem -i /zone/apache-zone/root/keypair.pem -p /zone/apache-zone/root/pass \  
-x 8443 apache-zone 443
```

En la zona local, ejecute el siguiente comando para habilitar la instancia de servicio:

```
# svcadm enable svc:/network/http:apache2
```

# Almacenamiento en antememoria de páginas web (referencia)

Las siguientes secciones incluyen los archivos y los componentes necesarios para utilizar el NCA. Además, se incluyen especificaciones sobre cómo el NCA interacciona con el servidor web.

## Archivos del NCA

Necesita varios archivos para admitir la función del NCA. Muchos de estos archivos son ASCII, pero algunos de ellos son binarios. La siguiente tabla muestra todos los archivos.

TABLA 2-1 Archivos del NCA

Nombre de archivo	Función
/dev/nca	El nombre de la ruta del dispositivo del NCA.

TABLA 2-1 Archivos del NCA (Continuación)

Nombre de archivo	Función
/etc/hostname.*	Archivo que muestra todas las interfaces físicas configuradas en el servidor.
/etc/hosts	Archivo que muestra todos los nombres de host asociados con el servidor. Las entradas de este archivo deben coincidir con las entradas en los archivos /etc/hostname.* para que funcione el NCA.
/etc/init.d/ncakmod	Secuencia de comandos que inicia el servidor del NCA. Esta secuencia de comandos se ejecuta cuando se inicia un servidor.
/etc/init.d/ncalogd	Secuencia de comandos que inicia el registro del NCA. Esta secuencia de comandos se ejecuta cuando se inicia un servidor.
/etc/nca/nca.if	Archivo que muestra las interfaces en las que se ejecuta el NCA. Consulte la página del comando <a href="#">man nca.if(4)</a> para obtener más información.
/etc/nca/ncakmod.conf	Archivo que muestra los parámetros de configuración para el NCA. Consulte la página del comando <a href="#">man ncakmod.conf(4)</a> para obtener más información.
/etc/nca/ncalogd.conf	Archivo que muestra los parámetros de configuración para el registro del NCA. Consulte la página del comando <a href="#">man ncalogd.conf(4)</a> para obtener más información.
/etc/nca/ncaport.conf	Archivo que muestra las direcciones IP y los puertos para el NCA. Consulte la página del comando <a href="#">man ncaport.conf(4)</a> para obtener más información.
/usr/bin/ncab2clf	Comando que se utiliza para convertir los datos en el archivo de registro al formato de registro común. Consulte la página del comando <a href="#">man ncab2clf(1)</a> para obtener más información.
/usr/lib/net/ncaconfd	Comando que se utiliza para configurar que el NCA se ejecute en varias interfaces durante el inicio. Consulte la página del comando <a href="#">man ncaconfd(1M)</a> para obtener más información.
/usr/lib/nca_addr.so	Biblioteca que utiliza sockets AF_NCA en lugar de sockets AF_INET. Esta biblioteca se debe utilizar en los servidores web que utilizan sockets AF_INET. Consulte la página del comando <a href="#">man ncad_addr(4)</a> para obtener más información.

TABLA 2-1 Archivos del NCA (Continuación)

Nombre de archivo	Función
/var/nca/log	Archivo que contiene los datos del archivo de registro. El archivo se encuentra en formato binario, por lo que no debe editarlo.
/var/run/nca_httpd_1.door	El nombre de ruta de la puerta.

## Arquitectura del NCA

La función del NCA incluye los siguientes componentes.

- Módulo de núcleo, ncakmod
- Servidor web, httpd

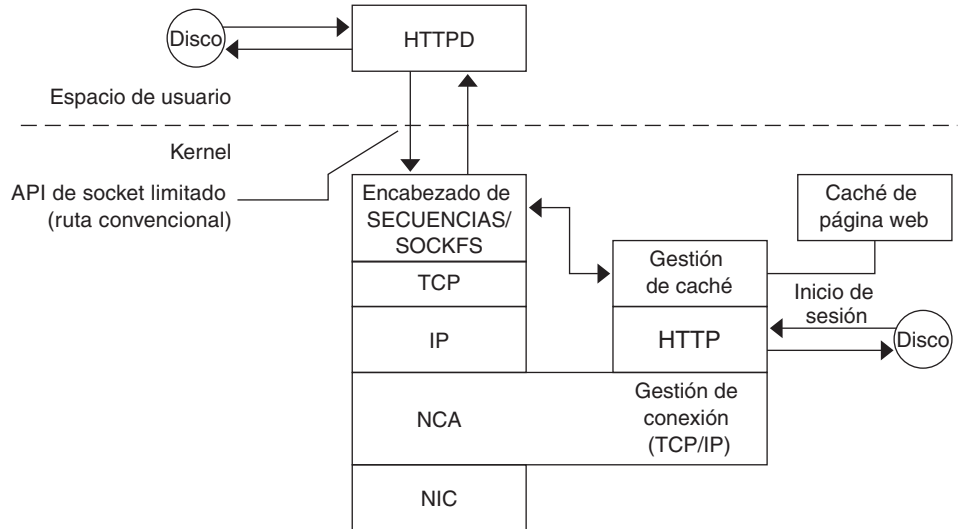
El módulo de núcleo ncakmod mantiene la antememoria de las páginas web en la memoria del sistema. El módulo se comunica con un servidor web, httpd , a través de una interfaz de sockets. El tipo de familia es PF\_NCA.

El módulo de núcleo también proporciona una utilidad de registro que registra todos los aciertos de la antememoria HTTP. El registro del NCA escribe los datos de HTTP en el disco en formato binario. El NCA proporciona una utilidad de conversión para convertir archivos de registro binarios al formato de registro común (CLF).

La siguiente figura muestra el flujo de datos de la ruta de acceso convencional y la ruta que se utiliza cuando el NCA está habilitado.



FIGURA 2-1 Flujo de datos con el servicio NCA



## Flujo de solicitud del NCA a httpd

La siguiente lista muestra el flujo de solicitud entre el cliente y el servidor web.

1. Una solicitud HTTP se creará desde cliente hasta el servidor web.
2. Si la página está en la antememoria, se devuelve la página web de la antememoria en el núcleo.
3. Si la página no está en la antememoria, la solicitud va al servidor web para recuperar o actualizar la página.
4. Según la semántica del protocolo HTTP que se utilice en la respuesta, la página se almacena o no en la antememoria. A continuación, se devuelve la página al cliente. Si se incluye el encabezado Pragma: No-cache en la solicitud de HTTP, la página no se almacena en la antememoria.



## Servicios relacionados con el tiempo

---

Mantener los relojes del sistema sincronizados dentro de una red es necesario para muchas bases de datos y servicios de autenticación. En este capítulo se cubren los temas siguientes.

- “Sincronización del reloj (descripción general)” en la página 67
- “Gestión del protocolo de hora de red (tareas)” en la página 68
- “Uso de otros comandos relacionados con el tiempo (tareas)” en la página 69
- “Protocolo de hora de red (referencia)” en la página 69

### Sincronización del reloj (descripción general)

El software de dominio público de protocolo de hora de red (NTP) de la Universidad de Delaware se incluye en el software de Solaris. El daemon `xntpd` establece y mantiene la hora del día del sistema. El daemon `xntpd` es una implementación completa de la versión 3 estándar, como se define en la RFC 1305.

El daemon `xntpd` lee el archivo `/etc/inet/ntp.conf` al iniciar el sistema. Consulte [xntpd\(1M\)](#) para obtener información sobre opciones de configuración.

Recuerde lo siguiente cuando se utiliza el NTP en su red:

- El daemon `xntpd` utiliza pocos recursos del sistema.
- Un cliente NTP se sincroniza automáticamente con un servidor NTP cuando se inicia. Si el cliente deja de estar sincronizado, el cliente se sincroniza de nuevo cuando el cliente se pone en contacto con un servidor de tiempo.

Otra manera de sincronizar los relojes es ejecutar `rdate` mientras se usa `cron`.

## Gestión del protocolo de hora de red (tareas)

Los procedimientos siguientes muestran cómo configurar y utilizar el servicio NTP.

### ▼ Cómo configurar un servidor NTP

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**2 Cree el archivo `ntp.conf`.**

Para garantizar la ejecución correcta del daemon `xntpd`, el archivo `ntp.conf` se debe crear primero. El archivo `ntp.server` se puede utilizar como plantilla.

```
# cd /etc/inet
# cp ntp.server ntp.conf
```

**3 Inicie el daemon `xntpd`.**

```
# svcadm enable network/ntp
```

### ▼ Cómo configurar un cliente NTP

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**2 Cree el archivo `ntp.conf`.**

Para activar el daemon `xntpd`, el archivo `ntp.conf` se debe crear primero.

```
# cd /etc/inet
# cp ntp.client ntp.conf
```

**3 Inicie el daemon `xntpd`.**

```
# svcadm enable network/ntp
```

# Uso de otros comandos relacionados con el tiempo (tareas)

El siguiente procedimiento se puede utilizar para actualizar la hora actual cada vez que se necesita, sin tener que configurar el NTP.

## ▼ Cómo sincronizar la fecha y la hora desde otro sistema

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)
- 2

**Restablezca la fecha y la hora de sincronización con otro sistema mediante el comando `rdate`.**

```
# rdate another-system  
otro-sistema      Nombre del otro sistema
```
- 3

**Verifique si ha restablecido la fecha del sistema correctamente mediante el comando `date`.**

La salida debe mostrar una fecha y una hora que coinciden con las del otro sistema.

### Ejemplo 3–1 Sincronización de fecha y hora desde otro sistema

El ejemplo siguiente muestra cómo usar `rdate` para sincronizar la fecha y la hora de un sistema con otro. En este ejemplo, el sistema `earth`, que se ejecuta varias horas más atrás, se restablece para que coincida con la fecha y la hora del servidor `starbug`.

```
earth# date  
Tue Jun 5 11:08:27 MDT 2001  
earth# rdate starbug  
Tue Jun 5 14:06:37 2001  
earth# date  
Tue Jun 5 14:06:40 MDT 2001
```

# Protocolo de hora de red (referencia)

Los siguientes archivos son necesarios para que el servicio NTP se ejecute.

TABLA 3–1 Archivos NTP

Nombre de archivo	Función
<code>/etc/inet/ntp.conf</code>	Enumera opciones de configuración para el NTP.

TABLA 3-1 Archivos NTP (Continuación)	
Nombre de archivo	Función
/etc/inet/ntp.client	Archivo de configuración de ejemplo para clientes NTP.
/etc/inet/ntp.server	Archivo de configuración de ejemplo para servidores NTP.
/etc/inet/ntp.keys	Contiene las claves de autenticación del NTP.
/usr/lib/inet/xntpd	Daemon NTP. Consulte <a href="#">xntpd(1M)</a> para obtener más información.
/usr/sbin/ntpdate	Utilidad para establecer la fecha y hora locales en función del NTP. Consulte <a href="#">ntpdate(1M)</a> para obtener más información.
/usr/sbin/ntpq	Programa de consulta NTP. Consulte <a href="#">ntpq(1M)</a> para obtener más información.
/usr/sbin/ntptrace	Programa para rastrear hosts NTP hasta el servidor NTP maestro. Consulte <a href="#">ntptrace(1M)</a> para obtener más información.
/usr/sbin/xntpd	Programa de consulta NTP para el daemon xntpd. Consulte <a href="#">xntpd(1M)</a> para obtener más información.
/var/ntp/ntpstats	Directorio para conservar estadísticas del NTP.
/var/ntp/ntp.drift	Establece el desplazamiento de frecuencia inicial en servidores NTP.

## P A R T E I I

# Acceso a los sistemas de archivos de red (temas)

En esta sección, se proporciona información general e información de referencia y tareas para el servicio NFS.





## Gestión de sistemas de archivos de red (descripción general)

---

En este capítulo se proporciona una descripción general del servicio NFS, que se puede utilizar para acceder a sistemas de archivos a través de la red. El capítulo incluye un análisis de los conceptos necesarios para comprender el servicio NFS y una descripción de las últimas funciones en NFS y autofs.

- “Novedades del servicio NFS” en la página 73
- “Terminología de NFS” en la página 75
- “Sobre el servicio NFS” en la página 76
- “Sobre autofs” en la página 77
- “Funciones del servicio NFS” en la página 77

---

**Nota** – Si el sistema tiene zonas habilitadas y desea utilizar esta función en una zona no global, consulte la *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris* para obtener más información.

---

## Novedades del servicio NFS

Esta sección proporciona información acerca de las nuevas funciones en las versiones del SO Solaris.

### Cambios en la versión Solaris 10 11/06

Solaris 10 11/06 proporciona compatibilidad con una herramienta de supervisión de sistemas de archivos. Consulte lo siguiente:

- “Comando `fsstat`” en la página 159 para obtener una descripción y ejemplos
- La página del comando `man fsstat(1M)` para obtener más información

Además, esta guía proporciona una descripción más detallada del daemon `nfsmapid`. Para obtener más información sobre `nfsmapid`, consulte lo siguiente:

- “Daemon `nfsmapid`” en la página 148
- Página del comando `man nfsmapid(1M)`

Para ver una lista completa de las funciones nuevas, consulte *Novedades de Oracle Solaris 10 8/11*.

## Cambios en la versión Solaris 10

A partir de Solaris 10, se usa de forma predeterminada la versión 4 de NFS. Para obtener información acerca de las nuevas funciones de la versión 4 de NFS y acerca de otros cambios, consulte lo siguiente:

- “Protocolo NFS versión 4” en la página 78
- “Archivo `/etc/default/autofs`” en la página 141
- “Palabras clave para el archivo `/etc/default/nfs`” en la página 142
- “Daemon `lockd`” en la página 146
- “Daemon `nfs4cbd`” en la página 147
- “Daemon `nfsmapid`” en la página 148
- “Opciones `mount` para sistemas de archivos NFS” en la página 160
- “NFS a través RDMA” en la página 181
- “Negociación de versión en NFS” en la página 182
- “Funciones en NFS versión 4” en la página 183
- “Cómo selecciona `autofs` los archivos de sólo lectura más cercanos para los clientes (ubicaciones múltiples)” en la página 216

Asimismo, consulte lo siguiente:

- “Configuración de servicios NFS” en la página 96 para obtener información sobre las tareas
- *Novedades de Oracle Solaris 10 8/11* para obtener una lista completa de las funciones nuevas

Además, el servicio NFS está gestionado por la utilidad de gestión de servicios. Las acciones administrativas de este servicio, como la habilitación, la deshabilitación o el reinicio, pueden realizarse con el comando `svcadm`. Utilice el comando `svcs` para consultar el estado del servicio. Para obtener más información sobre la utilidad de gestión de servicios, consulte la página del comando `man smf(5)` y el Capítulo 18, “Gestión de servicios (descripción general)” de *Guía de administración del sistema: administración básica*.

# Terminología de NFS

Esta sección presenta parte de la terminología básica que se debe comprender para trabajar con el servicio NFS. La cobertura expandida del servicio NFS se incluye en el [Capítulo 6, “Acceso a los sistemas de archivos de red \(referencia\)”](#).

## Servidores y clientes NFS

Los términos *cliente* y *servidor* se usan para describir los roles que un equipo asume al compartir sistemas de archivos. Los equipos que comparten sus sistemas de archivos a través de una red actúan como servidores. Se dice que los equipos que acceden a los sistemas de archivos son clientes. El servicio NFS habilita a cualquier equipo para que tenga acceso a los sistemas de archivos de cualquier otro equipo. Al mismo tiempo, el servicio NFS proporciona acceso a sus propios sistemas de archivos. Un equipo puede asumir el rol de cliente, servidor o de cliente y servidor en cualquier momento específico en una red.

Los clientes acceden a los archivos en el servidor montando los sistemas de archivos compartidos del servidor. Cuando un cliente monta un sistema de archivos remoto, el cliente no realiza una copia del sistema de archivos. En su lugar, el proceso de montaje utiliza una serie de llamadas de procedimiento remoto que permiten que el cliente acceda al sistema de archivos de manera transparente en el disco del servidor. El montaje se asemeja a un montaje local. Los usuarios escriben comandos como si los sistemas de archivos fueran locales. Consulte [“Montaje de sistemas de archivos” en la página 90](#) para obtener información sobre las tareas que montan los sistemas de archivos.

Después de que se haya compartido un sistema de archivos en un servidor a través de una operación NFS, se puede acceder al sistema de archivos desde un cliente. Puede montar un sistema de archivos NFS automáticamente con autofs. Consulte [“Uso compartido de sistema de archivos automático” en la página 86](#) y [“Descripción general de tareas para administración autofs” en la página 106](#) para las tareas que implican el comando `compartir` y autofs.

## Sistemas de archivos NFS

Los objetos que se pueden compartir con el servicio NFS incluyen cualquier árbol de directorios total o parcial o una jerarquía de archivos, incluido un único archivo. Un equipo no puede compartir una jerarquía de archivos que se superponga con otra jerarquía de archivos que ya esté compartida. Los dispositivos periféricos, como módems e impresoras, no se pueden compartir.

En la mayoría de los entornos de sistemas UNIX, una jerarquía de archivos que se pueden compartir corresponde a un sistema de archivos o a una parte de un sistema de archivos. Sin embargo, la compatibilidad con NFS funciona en distintos sistemas operativos, y el concepto de

un sistema de archivos puede no tener sentido en otros entornos que no sean de UNIX. Por lo tanto, el término *archivo* hace referencia a un archivo o una jerarquía de archivos que se puede compartir y montar con NFS.

## Sobre el servicio NFS

El servicio NFS habilita equipos de diferentes arquitecturas que ejecutan sistemas operativos diferentes para que compartan sistemas de archivos a través de una red. La compatibilidad con NFS se ha implementado en muchas plataformas que van desde el sistema operativo MS-DOS hasta el VMS.

El entorno NFS se puede implementar en diferentes sistemas operativos dado que NFS define un modelo abstracto de un sistema de archivos, en lugar de una especificación de arquitectura. Cada sistema operativo aplica el modelo NFS a su semántica de sistema de archivos. Este modelo significa que las operaciones del sistema de archivos, como la lectura y la escritura, funcionan como si las operaciones accedieran a un archivo local.

El servicio NFS tiene las siguientes ventajas:

- Permite que varios equipos utilicen los mismos archivos para que todos en la red puedan acceder a los mismos datos.
- Reduce los costos de almacenamiento, ya que los equipos comparten las aplicaciones y no necesitan espacio en el disco local para cada aplicación de usuario.
- Proporciona coherencia de datos y fiabilidad, ya que todos los usuarios pueden leer el mismo conjunto de archivos.
- Hace que el montaje de sistemas de archivos sea transparente para los usuarios.
- Hace que el acceso a los archivos remotos sea transparente para los usuarios.
- Admite entornos heterogéneos.
- Reduce los gastos generales de la administración del sistema.

El servicio NFS hace que la ubicación física del sistema de archivos sea irrelevante para el usuario. Puede utilizar la implementación NFS para habilitar a los usuarios para que vean todos los archivos relevantes independientemente de la ubicación. En lugar de colocar copias de los archivos más utilizados en cada sistema, el servicio NFS lo habilita a colocar una copia en el disco de un equipo. Todos los demás sistemas acceden a los archivos por la red. En la operación NFS, los sistemas de archivos remotos casi no se pueden distinguir de los sistemas de archivos locales.

## Sobre autofs

Los sistemas de archivos que se comparten a través del servicio NFS se pueden montar mediante montaje automático. Autofs, un servicio por parte del cliente, es una estructura de sistema de archivos que proporciona montaje automático. El sistema de archivos autofs es inicializado por automount, que se ejecuta automáticamente cuando se inicia un sistema. El daemon de automount, automountd, se ejecuta de forma continua, realizando el montaje y desmontaje de los directorios remotos según sea necesario.

Cada vez que un equipo de un cliente que está ejecutando automountd intenta acceder a un archivo o directorio remoto, el daemon monta el sistema de archivos remoto. Este sistema de archivos remoto permanece montado durante el tiempo necesario. Si no se accede al sistema de archivos remoto durante un determinado período, el sistema de archivos se desmonta automáticamente.

No es necesario que el montaje se realice al inicio, y ya no hace falta que el usuario deba conocer la contraseña de superusuario para montar un directorio. Los usuarios no necesitan utilizar los comandos mount y umount. El servicio autofs monta y desmonta sistemas de archivos según sea necesario sin la intervención del usuario.

El montaje de algunas jerarquías de archivos con automountd no excluye la posibilidad de montar otras jerarquías con mount. Un equipo sin disco *debe* montar / (root), /usr y /usr/kvm mediante el comando mount y el archivo /etc/vfstab.

[“Descripción general de tareas para administración autofs” en la página 106](#) y [“Cómo funciona autofs” en la página 212](#) proporcionan más información específica sobre el servicio autofs.

## Funciones del servicio NFS

En esta sección se describen las funciones importantes que se incluyen en el servicio NFS.

### Protocolo NFS versión 2

La versión 2 fue la primera versión del protocolo NFS de uso generalizado. La versión 2 sigue estando disponible en una gran variedad de plataformas. Todas las versiones de Solaris admiten la versión 2 del protocolo NFS, pero las versiones de Solaris anteriores a Solaris 2.5 sólo admiten la versión 2.

### Protocolo NFS versión 3

Una nueva función de la versión Solaris 2.5 fue una implementación del protocolo NFS versión 3. Se han efectuado varios cambios para mejorar la interoperabilidad y el rendimiento. Para un uso óptimo, el protocolo versión 3 debe estar en ejecución tanto en los servidores como en los clientes NFS.

A diferencia del protocolo NFS versión 2, el protocolo NFS versión 3 puede manejar archivos con tamaño superior a 2 Gbytes. Se ha eliminado la limitación anterior. Consulte [“Compatibilidad con archivos grandes de NFS” en la página 81](#).

El protocolo NFS versión 3 habilita la escritura asíncrona segura en el servidor, lo que mejora el rendimiento al permitir que el servidor almacene en la antememoria las solicitudes de escritura del cliente en la memoria. El cliente no necesita esperar a que el servidor valide los cambios en el disco, por lo que el tiempo de respuesta es más rápido. Además, el servidor puede lotear las solicitudes, lo que mejora el tiempo de respuesta en el servidor.

Muchas operaciones de Solaris NFS versión 3 devuelven los atributos del archivo, que se almacenan en la antememoria local. Debido a que la antememoria se actualiza con más frecuencia, la necesidad de realizar una operación separada para actualizar estos datos surge con menos frecuencia. Por lo tanto, el número de llamadas RPC al servidor se reduce, lo que mejora el rendimiento.

Se ha mejorado el proceso para verificar los permisos de acceso a archivos. La versión 2 generaba un mensaje de “error de escritura” o un mensaje de “error de lectura” si los usuarios intentaban copiar un archivo remoto sin los permisos adecuados. En la versión 3, los permisos se comprueban antes de abrir el archivo, por lo que el error se notifica como un “error de apertura”.

El protocolo NFS versión 3 ha eliminado el límite de tamaño de transferencia de 8 Kbytes. Los clientes y los servidores pueden negociar cualquier tamaño de transferencia para admitir, en lugar de ajustarse al límite de 8 Kbytes que imponía la versión 2. Tenga en cuenta que en la implementación de Solaris 2.5, el protocolo establecía por defecto un tamaño de transferencia de 32 Kbytes. A partir de la versión Solaris 10, las restricciones en los tamaños de las transferencias por cable se relajaron. Los tamaños de las transferencias se basan en la capacidad del medio de transporte subyacente.

## Protocolo NFS versión 4

La versión 4 de NFS tiene funciones que no están disponibles en las versiones anteriores.

El protocolo NFS versión 4 representa el ID de usuario y el ID de grupo como cadenas. El cliente y el servidor utilizan `nfsmapid` para realizar lo siguiente:

- Para asignar estas cadenas de ID de la versión 4 a un ID numérico local
- Para asignar los ID numéricos locales a cadenas de ID de la versión 4

Para obtener más información, consulte [“Daemon nfsmapid” en la página 148](#).

Tenga en cuenta que en la versión 4 de NFS, el asignador de ID `nfsmapid` se utiliza para asignar un ID de usuario o de grupo en entradas de la ACL de un servidor a un ID de usuario o de grupo en las entradas de la ACL en un cliente. Lo contrario también es cierto. Para obtener más información, consulte [“ACL y nfsmapid en NFS versión 4” en la página 192](#).

Con la versión 4 de NFS, cuando anula la compartición de un sistema de archivos, se destruye todo el estado de todos los archivos abiertos o bloqueos de archivos en ese sistema de archivos. En la versión 3 de NFS, el servidor mantenía cualquier bloqueo que los clientes hubieran obtenido antes de anular la compartición del sistema de archivos. Para obtener más información, consulte [“Anular el uso compartido y volver a compartir un sistema de archivos en NFS versión 4” en la página 184.](#)

Los servidores de la versión 4 de NFS utilizan un sistema de pseudoarchivos para ofrecer a los clientes acceso a los objetos exportados en el servidor. Antes de la versión 4 de NFS, no existía ningún sistema de pseudoarchivos. Para obtener más información, consulte [“Espacio de nombre de sistema de archivos en NFS versión 4” en la página 184.](#)

En las versiones 2 y 3 de NFS, el servidor devolvía identificadores de archivos persistentes. La versión 4 de NFS admite identificadores de archivos volátiles. Para obtener más información, consulte [“Identificadores de archivos volátiles en NFS versión 4” en la página 186.](#)

La delegación, una técnica mediante la cual el servidor delega la gestión de un archivo a un cliente, se admite tanto en el cliente como en el servidor. Por ejemplo, el servidor puede conceder una delegación de lectura o una delegación de escritura a un cliente. Para obtener más información, consulte [“Delegación en NFS versión 4” en la página 190.](#)

A partir de la versión Solaris 10, la versión 4 de NFS no admite el tipo de seguridad LIPKEY/SPKM.

Además, la versión 4 de NFS no utiliza los siguientes daemons:

- mountd
- nfslogd
- statd

Para obtener una lista completa de las funciones en la versión 4 de NFS, consulte [“Funciones en NFS versión 4” en la página 183.](#)

Para obtener información de procedimiento relacionada con el uso de la versión 4 de NFS, consulte [“Configuración de servicios NFS” en la página 96.](#)

## Control de las versiones de NFS

El archivo `/etc/default/nfs` tiene las palabras clave para controlar los protocolos NFS que utilizan tanto el cliente como el servidor. Por ejemplo, puede utilizar palabras clave para gestionar la negociación de la versión. Para obtener más información, consulte [“Palabras clave para el archivo `/etc/default/nfs`” en la página 142](#) o la página del comando `man nfs(4)`.

## Compatibilidad con ACL NFS

La compatibilidad con listas de control de acceso (ACL) se agregó en la versión Solaris 2.5. Las ACL proporcionan un mecanismo más detallado para definir permisos de acceso de archivos que el mecanismo disponible a través los permisos de archivos de UNIX estándar. La compatibilidad con ACL NFS ofrece un método de cambio y visualización de las entradas de ACL desde un cliente Solaris NFS hasta un servidor Solaris NFS.

Los protocolos NFS versión 2 y 3 admiten las antiguas ACL basadas en borrador POSIX. UFS admite las ACL basadas en borrador POSIX de manera nativa. Consulte [“Uso de listas de control de acceso para proteger archivos UFS” de Guía de administración del sistema: servicios de seguridad](#) para obtener más información sobre las ACL de UFS.

El protocolo NFS versión 4 admite las nuevas ACL basadas en NFSv4. ZFS admite las ACL NFSv4 de manera nativa. Para obtener las funciones completas de ACL NFSv4, ZFS debe usarse como sistema de archivos subyacente en el servidor NFSv4. Las ACL NFSv4 tienen un amplio conjunto de propiedades de herencia, así como un conjunto de bits de permiso más allá de la lectura, la escritura y la ejecución estándar. 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](#) para obtener una descripción general de las ACL nuevas. Para obtener más información sobre la compatibilidad con las ACL en la versión 4 de NFS, consulte [“ACL y nfsmapid en NFS versión 4” en la página 192](#).

## NFS a través de TCP

El protocolo de transporte predeterminado para el protocolo NFS se cambió por el protocolo TCP (protocolo de control de transporte) en la versión Solaris 2.5. El TCP mejora el rendimiento en redes lentas y redes de área amplia. El TCP también proporciona control de congestión y recuperación de errores. NFS a través de TCP funciona con las versiones 2, 3 y 4. Antes de la versión Solaris 2.5, el protocolo predeterminado de NFS era el protocolo de datagramas de usuario (UDP).

## NFS a través de UDP

A partir de la versión Solaris 10, el cliente NFS ya no utiliza un número excesivo de puertos UDP. Anteriormente las transferencias NFS a través de UDP utilizaban un puerto UDP independiente para cada solicitud pendiente. Ahora, de manera predeterminada, el cliente NFS utiliza únicamente un puerto UDP reservado. No obstante, esta admisión se puede configurar. Si el uso simultáneo de varios puertos aumenta el rendimiento del sistema debido a la mayor escalabilidad, el sistema puede configurarse para que utilice más puertos. Esta capacidad es idéntica también a la admisión de NFS a través de TCP, que dispone de esta posibilidad de configuración desde su introducción. Para obtener más información, consulte el [Oracle Solaris Tunable Parameters Reference Manual](#).



---

**Nota** – La versión 4 de NFS no utiliza UDP. Si monta un sistema de archivos con la opción `proto=udp`, se utiliza la versión 3 de NFS en lugar de la versión 4.

---

## Descripción general de NFS a través de RDMA

La versión Solaris 10 incluye el protocolo Remote Direct Memory Access (RDMA), que es una tecnología de transferencia de datos de memoria a memoria a través de redes de alta velocidad. En concreto, RDMA proporciona transferencia de datos remota directamente hacia la memoria y desde ella sin la intervención de una CPU. Para proporcionar esta capacidad, RDMA combina la tecnología de interconexión de E/S de InfiniBand en plataformas SPARC con el SO Solaris. Para obtener más información, consulte [“NFS a través RDMA” en la página 181](#).

## Administrador de bloqueo de red y NFS

La versión Solaris 2.5 también incluye una versión mejorada del administrador de bloqueo de red. El administrador de bloqueo de red proporcionaba bloqueo de registro UNIX y uso compartido de archivos de PC para archivos NFS. El mecanismo de bloqueo es ahora más fiable para los archivos NFS, de manera que es menos probable que se cuelguen los comandos que utilizan el bloqueo.

---

**Nota** – El administrador de bloqueo de red se utiliza sólo para los montajes de la versión 2 y 3 de NFS. El bloqueo de archivos está integrado en el protocolo NFS versión 4.

---

## Compatibilidad con archivos grandes de NFS

La implementación Solaris 2.6 del protocolo NFS versión 3 se cambió a fin de manipular correctamente los archivos de más de 2 Gbytes. La versión 2 del protocolo NFS y la implementación Solaris 2.5 de la versión 3 del protocolo no podían manejar archivos de más de 2 Gbytes.

## Conmutación por error de cliente NFS

Con la versión Solaris 2.6, se agregó la conmutación por error dinámica de sistemas de archivos de sólo lectura. La conmutación por error proporciona un alto nivel de disponibilidad de recursos de sólo lectura que ya se han replicado, como páginas del comando `man`, otra documentación y archivos binarios compartidos. La conmutación por error puede producirse en cualquier momento después de que se haya montado el sistema de archivos. Los montajes manuales ahora pueden presentar varias réplicas, de forma muy similar al montador

automático de las versiones anteriores. El montador automático no ha cambiado, excepto que la conmutación por error no necesita esperar hasta que el sistema de archivos se vuelva a montar. Consulte [“Cómo utilizar conmutación por error del lado del cliente” en la página 94](#) y [“Conmutación por error por parte del cliente” en la página 196](#) para obtener más información.

## Compatibilidad con Kerberos para el servicio NFS

La compatibilidad con clientes Kerberos V4 estaba incluida en la versión Solaris 2.0. En la versión 2.6, los comandos `mount` y `share` se modificaron para admitir los montajes de la versión 3 de NFS que usan autenticación Kerberos V5. Además, el comando `share` se ha cambiado para habilitar varios tipos de autenticación para clientes diferentes. Consulte [“Tipo de seguridad RPCSEC\\_GSS” en la página 82](#) para obtener más información acerca de los cambios que implican los tipos de seguridad. Consulte [“Configuración de servidores NFS con Kerberos” de Guía de administración del sistema: servicios de seguridad](#) para obtener información acerca de la autenticación Kerberos V5.

## Compatibilidad con WebNFS

La versión Solaris 2.6 también incluye la capacidad de poder acceder a un sistema de archivos en Internet a través de cortafuegos. Esta capacidad ha sido proporcionada mediante una extensión del protocolo NFS. Una de las ventajas de utilizar el protocolo WebNFS para el acceso a Internet es su fiabilidad. El servicio se incorpora como una extensión del protocolo NFS versión 3 y versión 2. Además, la implementación de WebNFS proporciona la posibilidad de compartir estos archivos sin los gastos generales administrativos de un sitio `ftp` anónimo. Consulte [“Negociación de seguridad para el servicio WebNFS” en la página 83](#) para obtener una descripción de otros cambios que están relacionadas con el servicio WebNFS. Consulte [“Tareas de administración WebNFS” en la página 103](#) para obtener más información de la tarea.

---

**Nota** – El protocolo NFS versión 4 se prefiere frente al servicio WebNFS. La versión 4 de NFS integra completamente toda la negociación de seguridad agregada al protocolo `MOUNT` y al servicio WebNFS.

---

## Tipo de seguridad RPCSEC\_GSS

Un tipo de seguridad, denominado `RPCSEC_GSS`, es compatible con la versión Solaris 7. Este tipo utiliza interfaces GSS-API estándar para proporcionar la información de autenticación, integridad y privacidad, así como para habilitar la admisión de varios mecanismos de seguridad. Consulte [“Compatibilidad con Kerberos para el servicio NFS” en la página 82](#) para obtener más información sobre compatibilidad de la autenticación de Kerberos V5. Consulte la [Developer's Guide to Oracle Solaris Security](#) para obtener más información sobre GSS-API.

## Extensiones Solaris 7 para montaje NFS

La versión Solaris 7 incluye extensiones de los comandos `mount` y `automountd`. Las extensiones habilitan la solicitud de montaje para utilizar el identificador de archivos público en lugar del protocolo MOUNT. El protocolo MOUNT es el mismo método de acceso que utiliza el servicio WebNFS. Al eludir el protocolo MOUNT, el montaje se puede producir a través de un cortafuegos. Además, dado que deben producirse menos transacciones entre el servidor y el cliente, el montaje debería producirse con mayor rapidez.

Las extensiones también habilitan el uso de las URL de NFS URL en lugar del nombre de ruta estándar. Además, puede utilizar la opción `public` con el comando `mount`, y el montador automático fuerza el uso del identificador de archivos público. Consulte [“Compatibilidad con WebNFS” en la página 82](#) para obtener más información acerca de los cambios en el servicio WebNFS.

## Negociación de seguridad para el servicio WebNFS

En la versión Solaris 8, se agregó un nuevo protocolo a fin de habilitar que un cliente WebNFS negocie un mecanismo de seguridad con un servidor NFS. Este protocolo proporciona la posibilidad de usar transacciones seguras cuando se utiliza el servicio WebNFS. Consulte [“Cómo funciona la negociación de seguridad WebNFS” en la página 201](#) para obtener más información.

## Registro del servidor NFS

En la versión Solaris 8, el registro del servidor NFS habilita que un servidor NFS proporcione un registro de las operaciones de archivos que se han realizado en sus sistemas de archivos. El registro incluye información acerca de a qué archivo se accedió, cuándo se accedió a él y quién lo hizo. Puede especificar la ubicación de los registros que contengan esta información a través de un conjunto de opciones de configuración. También puede utilizar estas opciones para seleccionar las operaciones que deben registrarse. Esta función resulta particularmente útil para sitios que ponen a disposición archivos FTP anónimos para clientes NFS y WebNFS. Consulte [“Cómo habilitar el inicio de sesión de servidor NFS” en la página 89](#) para obtener más información.

---

**Nota** – La versión 4 de NFS no admite el registro del servidor.

---

## Funciones de autofs

Autofs funciona con sistemas de archivos que se especifican en el espacio de nombres local. Esta información se puede mantener en archivos locales, NIS o NIS+.

En la versión Solaris 2.6, se incluye una versión completamente multiproceso de automountd. Esta mejora hace que autofs sea más fiable y habilita el servicio simultáneo de varios montajes, lo que impide que el servicio se bloquee si un servidor no está disponible.

El nuevo comando automountd también proporciona un mejor montaje a petición. Las versiones anteriores montaban un conjunto completo de sistemas de archivos si los sistemas de archivos estaban relacionados jerárquicamente. Ahora, sólo se monta el sistema de archivos superior. Los otros sistemas de archivos que están relacionados con este punto de montaje se montan cuando es necesario.

El servicio autofs admite la capacidad de exploración de mapas indirectos. Esta compatibilidad permite al usuario ver los directorios que pueden montarse sin necesidad de montar realmente cada sistema de archivos. Se ha agregado una opción -nobrowse a los mapas autofs a fin de que los sistemas de archivos grandes, como /net y /home no puedan explorarse automáticamente. También, puede desactivar la capacidad de exploración autofs en cada cliente mediante la opción -n con automount. Consulte [“Deshabilitación de la capacidad de explorar autofs” en la página 121](#) para obtener más información.

## Administración de sistema de archivos de red (tareas)

---

En este capítulo se proporciona información sobre cómo realizar tareas de administración NFS como la configuración de servicios NFS, la adición de nuevos sistemas de archivos para compartir y el montaje de sistemas de archivos. El capítulo también abarca el uso del sistema NFS seguro y el uso de la funcionalidad WebNFS. La última parte del capítulo incluye los procedimientos de resolución de problemas y una lista de algunos mensajes de error de NFS y sus significados.

- “Uso compartido de sistema de archivos automático” en la página 86
- “Montaje de sistemas de archivos” en la página 90
- “Configuración de servicios NFS” en la página 96
- “Administración de sistema NFS seguro” en la página 101
- “Tareas de administración WebNFS” en la página 103
- “Descripción general de tareas para administración autofs” en la página 106
- “Estrategias para resolución de problemas de NFS” en la página 123
- “Procedimientos de resolución de problemas NFS” en la página 124
- “Mensajes de error NFS” en la página 133

Sus responsabilidades como administrador NFS dependen de los requisitos del sitio y del rol de su equipo en la red. Es posible que sea responsable de todos los equipos en la red local, en cuyo caso sería responsable de determinar los siguientes elementos de configuración:

- Qué equipos deberían ser servidores dedicados
- Qué equipos deberían actuar como servidores y clientes
- Qué equipos deberían ser clientes solamente

Mantener un servidor después de haber sido configurado implica las siguientes tareas:

- Compartir y no compartir sistemas de archivos según sea necesario
- Modificar los archivos administrativos para actualizar las listas de sistemas de archivos que el equipo comparte o monta automáticamente
- Comprobar el estado de la red
- Diagnosticar y solucionar problemas relacionados con NFS cuando se produzcan

■ Configurar mapas para autofs

Recuerde que un equipo puede ser tanto un servidor como un cliente. Por lo tanto, un equipo se puede utilizar para compartir sistemas de archivos locales con equipos remotos y para montar sistemas de archivos remotos.

**Nota** – Si el sistema tiene zonas habilitadas y desea utilizar esta función en una zona no global, consulte la [Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris](#) para obtener más información.

# Uso compartido de sistema de archivos automático

Los servidores proporcionan acceso a sus sistemas de archivos mediante el uso compartido de sistemas de archivos a través del entorno NFS. Puede especificar qué sistemas de archivos se van a compartir con el comando `share` o con el archivo `/etc/dfs/dfstab`.

Las entradas del archivo `/etc/dfs/dfstab` se comparten automáticamente siempre que inicie una operación del servidor NFS. Debe configurar un uso compartido automático si necesita compartir el mismo conjunto de sistemas de archivos de forma regular. Por ejemplo, si su equipo es un servidor que admite directorios principales, deberá hacer que los directorios principales estén disponibles todo el tiempo. La mayor parte del uso compartido del sistema de archivos se debería realizar de manera automática. La única vez que el uso compartido manual debería ocurrir es durante la prueba o la resolución de problemas.

El archivo `dfstab` enumera todos los sistemas de archivos que el servidor comparte con los clientes. Este archivo controla también qué clientes pueden montar un sistema de archivos. Puede modificar `dfstab` para agregar o eliminar un sistema de archivos o para cambiar la manera en que se comparte. Simplemente edite el archivo con cualquier editor de texto que sea compatible (como `vi`). La próxima vez que el equipo entre en un nivel de ejecución 3, el sistema lee el `dfstab` actualizado para determinar qué sistemas de archivos deberían compartirse automáticamente.

Cada línea del archivo `dfstab` tiene un comando `share`, el mismo comando que escribe en el indicador de línea de comandos para compartir el sistema de archivos. El comando `share` se ubica en `/usr/sbin`.

TABLA 5–1 Mapa de tareas de uso compartido de sistema de archivos

Tarea	Descripción	Para obtener instrucciones
Establecer uso compartido de sistema de archivos automático	Pasos para configurar un servidor para que los sistemas de archivos se compartan automáticamente cuando el servidor se reinicia	<a href="#">“Cómo configurar el uso compartido de sistema de archivos automático” en la página 87</a>

TABLA 5-1 Mapa de tareas de uso compartido de sistema de archivos (Continuación)

Tarea	Descripción	Para obtener instrucciones
Habilitar WebNFS	Pasos para configurar un servidor para que los usuarios puedan acceder a archivos utilizando WebNFS	<a href="#">“Cómo habilitar acceso WebNFS” en la página 88</a>
Habilitar el inicio de sesión de servidor NFS	Pasos para configurar un servidor para que el inicio de sesión NFS se ejecute en los sistemas de archivos seleccionados	<a href="#">“Cómo habilitar el inicio de sesión de servidor NFS” en la página 89</a>

## ▼ Cómo configurar el uso compartido de sistema de archivos automático

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Agregue entradas para cada sistema de archivos que se compartirá.

Edite `/etc/dfs/dfstab`. Agregue una entrada al archivo para cada sistema de archivos que desee que se comparta automáticamente. Cada entrada debe estar en una línea por sí misma en el archivo y utilizar esta sintaxis:

```
share [-F nfs] [-o specific-options] [-d description] pathname
```

Consulte la página del comando `man dfstab(4)` para obtener una descripción de `/etc/dfs/dfstab` y la página del comando `man share_nfs(1M)` para obtener una lista completa de opciones.

### 3 Comparta el sistema de archivos.

Una vez que la entrada está en `/etc/dfs/dfstab`, puede compartir el sistema de archivos ya sea reiniciando el sistema o utilizando el comando `shareall`.

```
# shareall
```

### 4 Verifique que la información es correcta.

Ejecute el comando `share` para comprobar que se muestran las opciones correctas:

```
# share
-      /export/share/man    ro    ""
-      /usr/src             rw=eng ""
-      /export/ftp          ro,public ""
```

**Véase también** El siguiente paso es para configurar mapas `autofs` para que los clientes puedan acceder a los sistemas de archivos que haya compartido en el servidor. Consulte [“Descripción general de tareas para administración `autofs`” en la página 106](#).

## ▼ Cómo habilitar acceso WebNFS

A partir de la versión Solaris 2.6, de manera predeterminada, todos los sistemas de archivos que están disponibles para el montaje NFS están disponibles automáticamente para el acceso WebNFS. La única condición que requiere el uso de este procedimiento es una de las siguientes:

- Para permitir el montaje NFS en un servidor que aún no admite el montaje NFS
- Para restablecer el identificador de archivos público para acortar las URL de NFS mediante la opción `public`
- Para forzar la carga de un archivo HTML específico mediante la opción `index`

Consulte [“Planificación de acceso WebNFS” en la página 104](#) para una lista de cuestiones a considerar antes de iniciar el servicio WebNFS.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Agregue entradas para cada sistema de archivos que se va a compartir mediante el servicio WebNFS.

Edita `/etc/dfs/dfstab`. Agregue una entrada al archivo para cada sistema de archivos. Las etiquetas `public` e `index` que se muestran en el siguiente ejemplo son opcionales.

```
share -F nfs -o ro,public,index=index.html /export/ftp
```

Consulte la página del comando `man dfstab(4)` para obtener una descripción de `/etc/dfs/dfstab` y la página del comando `man share_nfs(1M)` para obtener una lista completa de opciones.

### 3 Comparta el sistema de archivos.

Una vez que la entrada está en `/etc/dfs/dfstab`, puede compartir el sistema de archivos ya sea reiniciando el sistema o utilizando el comando `shareall`.

```
# shareall
```

### 4 Verifique que la información es correcta.

Ejecute el comando `share` para comprobar que se muestran las opciones correctas:

```
# share
-      /export/share/man    ro      ""
-      /usr/src             rw=eng  ""
-      /export/ftp          ro,public,index=index.html  ""
```



## ▼ Cómo habilitar el inicio de sesión de servidor NFS

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 (Opcional) Cambie los valores de configuración del sistema de archivos.

En `/etc/nfs/nfslog.conf`, puede modificar la configuración de una o dos maneras. Puede editar los valores predeterminados de todos los sistemas de archivos si cambia los datos que están asociados a la etiqueta `global`. Como alternativa, puede agregar una etiqueta nueva para este sistema de archivos. Si estos cambios no son necesarios, no necesita modificar este archivo. El formato de `/etc/nfs/nfslog.conf` se describe en [nfslog.conf\(4\)](#).

### 3 Agregue entradas para cada sistema de archivos que se va a compartir mediante el inicio de sesión de servidor NFS

Edite `/etc/dfs/dfstab`. Agregue una entrada al archivo para el sistema de archivos en el que habilita el inicio de sesión de servidor NFS. La etiqueta que se utiliza con la opción `log=etiqueta` se debe introducir en `/etc/nfs/nfslog.conf`. En este ejemplo se utiliza la configuración predeterminada en la etiqueta `global`.

```
share -F nfs -o ro,log=global /export/ftp
```

Consulte la página del comando `man dfstab(4)` para obtener una descripción de `/etc/dfs/dfstab` y la página del comando `man share_nfs(1M)` para obtener una lista completa de opciones.

### 4 Comparta el sistema de archivos.

Una vez que la entrada está en `/etc/dfs/dfstab`, puede compartir el sistema de archivos ya sea reiniciando el sistema o utilizando el comando `shareall`.

```
# shareall
```

### 5 Verifique que la información es correcta.

Ejecute el comando `share` para comprobar que se muestran las opciones correctas:

```
# share
-      /export/share/man    ro      ""
-      /usr/src             rw=eng   ""
-      /export/ftp          ro,log=global  ""
```

### 6 Compruebe si `nfslogd`, el daemon NFS, está en ejecución.

```
# ps -ef | grep nfslogd
```

7 (Opcional) Inicie `nfslogd`, si aún no está en ejecución.

- (Opcional) Si `/etc/nfs/nfslogtab` está presente, inicie el daemon de registro NFS escribiendo lo siguiente:  

```
# svcadm restart network/nfs/server:default
```
- (Opcional) Si `/etc/nfs/nfslogtab` no está presente, ejecute cualquiera de los comandos `share` para crear el archivo y, a continuación, iniciar el daemon.  

```
# shareall  
# svcadm restart network/nfs/server:default
```

# Montaje de sistemas de archivos

Puede montar sistemas de archivos de distintas maneras. Los sistemas de archivos se pueden montar automáticamente cuando se inicia el sistema a petición desde la línea de comandos o a través del montador automático. El montador automático proporciona muchas ventajas para realizar un montaje al momento del inicio o desde la línea de comandos. Sin embargo, muchas situaciones exigen una combinación de los tres métodos. Además, existen varias formas de habilitación o deshabilitación de procesos, en función de las opciones que utiliza al montar el sistema de archivos. Consulte la siguiente tabla para obtener una lista completa de las tareas asociadas al montaje del sistema de archivos.

TABLA 5-2 Mapa de tareas para montar sistemas de archivos

Tarea	Descripción	Para obtener instrucciones
Montar un sistema de archivos el momento del inicio	Pasos para que un sistema de archivos se monte siempre que se inicia un sistema.	<a href="#">“Cómo montar un sistema de archivos al momento del inicio” en la página 91.</a>
Montar un sistema de archivos mediante un comando	Pasos para montar un sistema de archivos cuando un sistema está en ejecución. Este procedimiento resulta útil durante la prueba.	<a href="#">“Cómo montar un sistema de archivos desde la línea de comandos” en la página 92.</a>
Montar con el montador automático	Pasos para acceder a un sistema de archivos a petición sin utilizar la línea de comandos.	<a href="#">“Montaje con el montador automático” en la página 92.</a>
Evitar archivos grandes	Pasos para evitar se creen archivos grandes en un sistema de archivos.	<a href="#">“Cómo deshabilitar archivos grandes en un servidor NFS” en la página 93.</a>
Iniciar conmutación por error del lado del cliente	Pasos para habilitar el cambio automático a un sistema de archivos de trabajo si un servidor falla.	<a href="#">“Cómo utilizar conmutación por error del lado del cliente” en la página 94.</a>
Deshabilitar el acceso de montaje para un cliente	Pasos para deshabilitar la capacidad de un cliente de acceder a un sistema de archivos remoto.	<a href="#">“Cómo deshabilitar el acceso de montaje para un cliente” en la página 94.</a>

TABLA 5-2 Mapa de tareas para montar sistemas de archivos (Continuación)

Tarea	Descripción	Para obtener instrucciones
Proporcionar acceso a un sistema de archivos a través de un cortafuegos	Pasos para permitir el acceso a un sistema de archivos a través de un cortafuegos utilizando el protocolo WebNFS.	<a href="#">“Cómo montar un sistema de archivos NFS a través de un cortafuegos” en la página 95.</a>
Montar un sistema de archivos utilizando una URL de NFS	Pasos para permitir el acceso a un sistema de archivos utilizando una URL de NFS. Este proceso permite el acceso al sistema de archivos sin utilizar el protocolo MOUNT.	<a href="#">“Cómo montar un sistema de archivos NFS utilizando una URL de NFS” en la página 95.</a>

## ▼ Cómo montar un sistema de archivos al momento del inicio

Si desea montar sistemas de archivos al momento del inicio en lugar de utilizar mapas autofs, siga este procedimiento. Este procedimiento se debe completar en cada cliente que debe tener acceso a sistemas de archivos remotos.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

### 2 Agregue una entrada para el sistema de archivos a `/etc/vfstab`.

Las entradas en el archivo `/etc/vfstab` tienen la siguiente sintaxis:

```
special fsckdev mountp fstype fsckpass mount-at-boot mntopts
```

Consulte la página del comando `man vfstab(4)` para obtener más información.



**Precaución** – Los servidores NFS que también poseen entradas `vfstab` de clientes NFS deben especificar siempre la opción `bg` para evitar un cuelgue del sistema durante el reinicio. Para obtener más información, consulte [“Opciones mount para sistemas de archivos NFS” en la página 160.](#)

### Ejemplo 5-1 Entrada en el archivo `vfstab` del cliente

Desea que un equipo cliente monte el directorio `/var/mail` desde el servidor `wasp`. Desea montar el sistema de archivos como `/var/mail` en el cliente y desea que el cliente tenga acceso de lectura y escritura. Agregue la siguiente entrada al archivo `vfstab` del cliente.

```
wasp:/var/mail - /var/mail nfs - yes rw
```

## ▼ Cómo montar un sistema de archivos desde la línea de comandos

El montaje de un sistema de archivos desde la línea de comandos se realiza generalmente para probar un nuevo punto de montaje. Este tipo de montaje permite el acceso temporal a un sistema de archivos que no está disponible a través del montador automático.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Monte el sistema de archivos.

Escriba el siguiente comando:

```
# mount -F nfs -o ro bee:/export/share/local /mnt
```

En esta instancia, el sistema de archivos `/export/share/local` del servidor `bee` se monta para sólo lectura en `/mnt` en el sistema local. El montaje desde la línea de comandos permite una visualización temporal del sistema de archivos. Puede desmontar un sistema de archivos con `umount` reiniciando el host local.



---

**Precaución** – Ninguna versión del comando `mount` advierte acerca de opciones no válidas. El comando ignora sin notificación las opciones que no es posible interpretar. Para evitar un comportamiento inesperado, asegúrese de verificar todas las opciones que se han utilizado.

---

## Montaje con el montador automático

“[Descripción general de tareas para administración autofs](#)” en la [página 106](#) incluye instrucciones específicas para establecer y admitir montajes con el montador automático. Sin realizar ninguna modificación en el sistema genérico, los clientes deberían poder acceder a sistemas de archivos remotos a través del punto de montaje `/net`. Para montar el sistema de archivos `/export/share/local` del ejemplo anterior, escriba lo siguiente:

```
% cd /net/bee/export/share/local
```

Debido a que el montador automático permite a todos los usuarios montar sistemas de archivos, no se requiere acceso `root`. El montador automático también permite el desmontaje automático de sistemas de archivos, para que no tenga que desmontar sistemas de archivos después de haber terminado.

## ▼ Cómo deshabilitar archivos grandes en un servidor NFS

Para los servidores que admiten clientes que no pueden gestionar un archivo más grande que 2 GB, es posible que tenga que deshabilitar la función de crear archivos grandes.

---

**Nota** – Las versiones anteriores a la versión 2.6 de Solaris no pueden utilizar archivos de gran tamaño. Si los clientes necesitan acceder a archivos de gran tamaño, compruebe que los clientes del servidor NFS ejecuten, como mínimo, la versión 2.6.

---

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Compruebe que no existan archivos de gran tamaño en el sistema de archivos.

Por ejemplo:

```
# cd /export/home1
# find . -xdev -size +2000000 -exec ls -l {} \;
```

Si hay archivos grandes en el sistema de archivos, debe eliminarlos o moverlos a otro sistema de archivos.

### 3 Desmonte el sistema de archivos.

```
# umount /export/home1
```

### 4 Restablezca el estado del sistema de archivos si el sistema de archivos se ha montado utilizando **largefiles**.

fsck restablece el estado del sistema de archivos si no existen archivos de gran tamaño en el sistema de archivos:

```
# fsck /export/home1
```

### 5 Monte el sistema de archivos utilizando **noLargefiles**.

```
# mount -F ufs -o noLargefiles /export/home1
```

Puede realizar el montaje desde la línea de comandos, pero para que la opción sea más permanente, agregue una entrada que se asemeje a lo siguiente en `/etc/vfstab`:

```
/dev/dsk/c0t3d0s1 /dev/rdisk/c0t3d0s1 /export/home1 ufs 2 yes noLargefiles
```

## ▼ Cómo utilizar conmutación por error del lado del cliente

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 En el cliente NFS, monte el sistema de archivos utilizando la opción `ro`.

Puede realizar el montaje desde la línea de comandos, mediante el montador automático o agregando una entrada para `/etc/vfstab` que se asemeje a lo siguiente:

```
bee,wasp:/export/share/local - /usr/local nfs - no ro
```

El montador automático ha permitido esta sintaxis. Sin embargo, la conmutación por error no estaba disponible mientras el sistema de archivos estaba montado, sólo cuando se seleccionaba un servidor.

---

**Nota** – Los servidores que ejecutan diferentes versiones del protocolo NFS no se pueden mezclar utilizando una línea de comandos o en una entrada `vfstab`. La mezcla de servidores que admite protocolos versión 2, versión 3 o versión 4 de NFS sólo se puede realizar con `autofs`. En `autofs`, se utiliza el mejor subconjunto de las versiones 2, 3 o 4.

---

## ▼ Cómo deshabilitar el acceso de montaje para un cliente

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue una entrada en `/etc/dfs/dfstab`.

En el primer ejemplo se permite el acceso de montaje para todos los clientes del grupo de red `eng` a excepción del host denominado `rose`. En el segundo ejemplo se permite el acceso de montaje a todos los clientes en el dominio DNS `eng.example.com` a excepción de `rose`.

```
share -F nfs -o ro=-rose:eng /export/share/man
share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

Para obtener información adicional sobre las listas de acceso, consulte “[Configuración de listas de acceso con el comando `share`](#)” en la [página 170](#). Para obtener una descripción de `/etc/dfs/dfstab`, consulte [dfstab\(4\)](#).

### 3 Comparta el sistema de archivos.

El servidor NFS no utiliza modificaciones para `/etc/dfs/dfstab` hasta que los sistemas de archivos se compartan nuevamente o hasta que el servidor se reinicie.

```
# shareall
```

## ▼ Cómo montar un sistema de archivos NFS a través de un cortafuegos

Para acceder a sistemas de archivos a través de un cortafuegos, utilice el siguiente procedimiento.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Monte manualmente el sistema de archivos utilizando un comando como el siguiente:

```
# mount -F nfs bee:/export/share/local /mnt
```

En este ejemplo, el sistema de archivos `/export/share/local` está montado en el cliente local mediante el identificador de archivos público. Una URL de NFS puede utilizarse en lugar del nombre de ruta estándar. Si el identificador de archivos público no es admitido por el servidor `bee`, la operación de montaje falla.

---

**Nota** – Este procedimiento requiere que el sistema de archivos en el servidor NFS se pueda compartir mediante la opción `public`. Además, cualquier cortafuegos entre el cliente y el servidor debe permitir conexiones TCP en el puerto 2049. Todos los sistemas de archivos que se comparten permiten acceso de identificador de archivos público, para que la opción `public` se aplique de manera predeterminada.

---

## ▼ Cómo montar un sistema de archivos NFS utilizando una URL de NFS

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

2 (Opcional) Si usa una versión 2 o 3 de NFS, monte manualmente el sistema de archivos mediante un comando como el siguiente:

```
# mount -F nfs nfs://bee:3000/export/share/local /mnt
```

En este ejemplo, el sistema de archivos /export/share/local se monta desde el servidor bee utilizando un número de puerto NFS 3000. El número de puerto no es necesario y de manera predeterminada se utiliza el número de puerto NFS estándar de 2049. Puede elegir incluir la opción public con una URL de NFS. Sin la opción public, el protocolo MOUNT se utiliza si el identificador de archivos público no es admitido por el servidor. La opción public fuerza el uso del identificador de archivos público y el montaje falla si el identificador de archivos público no se admite.

3 (Opcional) Si usa una versión 4 de NFS, monte manualmente el sistema de archivos mediante un comando como el siguiente:

```
# mount -F nfs -o vers=4 nfs://bee:3000/export/share/local /mnt
```

# Configuración de servicios NFS

Esta sección describe algunas de las tareas necesarias para realizar lo siguiente:

- Iniciar y detener el servidor NFS
- Iniciar y detener el montador automático
- Seleccionar una versión diferente de NFS

**Nota** – A partir de Solaris 10, se usa de manera predeterminada la versión 4 de NFS.

TABLA 5–3 Mapa de tareas para servicios NFS

Tarea	Descripción	Para obtener instrucciones
Iniciar el servidor NFS	Pasos para iniciar el servicio NFS si no se ha iniciado automáticamente.	<a href="#">“Cómo iniciar los servicios NFS” en la página 97</a>
Detener el servidor NFS	Pasos para detener el servicio NFS. Normalmente, el servicio no debería requerir que se lo detenga.	<a href="#">“Cómo detener los servicios NFS” en la página 97</a>
Iniciar el montador automático	Pasos para iniciar el montador automático. Este procedimiento es necesario cuando algunos de los mapas del montador automático se modifican.	<a href="#">“Cómo iniciar el montador automático” en la página 98</a>
Detener el montador automático	Pasos para detener el montador automático. Este procedimiento es necesario cuando algunos de los mapas del montador automático se modifican.	<a href="#">“Cómo detener el montador automático” en la página 98</a>
Seleccionar una versión diferente de NFS en el servidor	Pasos para seleccionar una versión diferente de NFS en el servidor. Si decide no utilizar la versión 4 de NFS, utilice este procedimiento.	<a href="#">“Cómo seleccionar diferentes versiones de NFS en un servidor” en la página 98</a>



TABLA 5-3 Mapa de tareas para servicios NFS (Continuación)

Tarea	Descripción	Para obtener instrucciones
Seleccionar una versión diferente de NFS en el cliente	Pasos para seleccionar una versión diferente de NFS en el cliente mediante la modificación del archivo <code>/etc/default/nfs</code> . Si decide no utilizar la versión 4 de NFS, utilice este procedimiento.	<a href="#">“Cómo seleccionar diferentes versiones de NFS en un cliente mediante la modificación del archivo <code>/etc/default/nfs</code>” en la página 100</a>
	Pasos alternativos para seleccionar una versión diferente de NFS en el cliente utilizando la línea de comandos. Si decide no utilizar la versión 4 de NFS, utilice este procedimiento alternativo.	<a href="#">“Cómo utilizar el comando <code>mount</code> para seleccionar diferentes versiones de NFS en un cliente” en la página 101</a>

## ▼ Cómo iniciar los servicios NFS

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Habilite el servicio NFS en el servidor.

Escriba el siguiente comando.

```
# svcadm enable network/nfs/server
```

Este comando habilita el servicio NFS.

---

**Nota** – El servidor NFS se inicia automáticamente al iniciar el sistema. Además, en cualquier momento después de que el sistema se ha iniciado, los daemons de servicio NFS se pueden habilitar automáticamente mediante el uso compartido del sistema de archivos NFS. Consulte [“Cómo configurar el uso compartido de sistema de archivos automático” en la página 87](#).

---

## ▼ Cómo detener los servicios NFS

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Deshabilite el servicio NFS en el servidor.

Escriba el siguiente comando.

```
# svcadm disable network/nfs/server
```

## ▼ Cómo iniciar el montador automático

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Habilite el daemon autofs.

Escriba el siguiente comando:

```
# svcadm enable system/filesystem/autofs
```

## ▼ Cómo detener el montador automático

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Deshabilite el daemon autofs.

Escriba el siguiente comando:

```
# svcadm disable system/filesystem/autofs
```

## ▼ Cómo seleccionar diferentes versiones de NFS en un servidor

Si decide no utilizar la versión 4 de NFS, utilice este procedimiento.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Edite el archivo `/etc/default/nfs`.

Por ejemplo, si desea que el servidor proporcione sólo la versión 3, establezca los valores para `NFS_SERVER_VERSMAX` y `NFS_SERVER_VERSMIN` a 3. Para obtener una lista de las palabras clave y sus valores, consulte [“Palabras clave para el archivo `/etc/default/nfs`” en la página 142](#).

```
NFS_SERVER_VERSMAX=value  
NFS_SERVER_VERSMIN=value
```

*valor*      Proporcione el número de versión.

---

**Nota** – De manera predeterminada, estas líneas tienen comentarios. Recuerde eliminar el signo de almohadilla (#) también.

---

**3 (Opcional) Si desea deshabilitar la delegación de servidor, incluya esta línea en el archivo `/etc/default/nfs`.**

`NFS_SERVER_DELEGATION=off`

---

**Nota** – En la versión 4 de NFS, la delegación de servidor está habilitada de manera predeterminada. Para obtener más información, consulte [“Delegación en NFS versión 4” en la página 190](#).

---

**4 (Opcional) Si desea definir un dominio común para clientes y servidores, incluya esta línea en el archivo `/etc/default/nfs`.**

`NFSMAPID_DOMAIN=my.comany.com`

`my.comany.com`      Proporcione el dominio común

Para obtener más información, consulte [“Daemon nfsmapid” en la página 148](#).

**5 Compruebe si el servicio NFS está en ejecución en el servidor.**

Escriba el siguiente comando:

`# svcs network/nfs/server`

Este comando informa si el servicio del servidor NFS está en línea o deshabilitado.

**6 (Opcional) Si es necesario, deshabilite el servicio NFS.**

Si detectó en el paso anterior que el servicio NFS está en línea, escriba el siguiente comando para deshabilitar el servicio.

`# svcadm disable network/nfs/server`

---

**Nota** – Si necesita configurar el servicio NFS, consulte [“Cómo configurar el uso compartido de sistema de archivos automático” en la página 87](#).

---

**7 Habilite el servicio NFS.**

Escriba el siguiente comando para habilitar el servicio.

`# svcadm enable network/nfs/server`

**Véase también**      [“Negociación de versión en NFS” en la página 182](#)

## ▼ **Cómo seleccionar diferentes versiones de NFS en un cliente mediante la modificación del archivo `/etc/default/nfs`.**

El siguiente procedimiento le muestra cómo controlar qué versión de NFS se utiliza en el cliente mediante la modificación del archivo `/etc/default/nfs`. Si prefiere utilizar la línea de comandos, consulte [“Cómo utilizar el comando `mount` para seleccionar diferentes versiones de NFS en un cliente” en la página 101](#).

### **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 \(mapa de tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#).

### **2 Edite el archivo `/etc/default/nfs`.**

Por ejemplo, si sólo desea la versión 3 en el cliente, establezca los valores para `NFS_CLIENT_VERSMAX` y `NFS_CLIENT_VERSMIN` a 3. Para obtener una lista de las palabras clave y sus valores, consulte [“Palabras clave para el archivo `/etc/default/nfs`” en la página 142](#).

```
NFS_CLIENT_VERSMAX=value
NFS_CLIENT_VERSMIN=value
```

*valor*      Proporcione el número de versión.

---

**Nota** – De manera predeterminada, estas líneas tienen comentarios. Recuerde eliminar el signo de almohadilla (#) también.

---

### **3 Monte NFS en el cliente.**

Escriba el siguiente comando:

```
# mount server-name:/share-point /local-dir
```

*nombre\_servidor*      Proporcione el nombre del servidor.

*/punto\_compartir*      Proporcione la ruta del directorio remoto que se compartirá.

*/directorio\_local*      Proporcione la ruta del punto de montaje local.

**Véase también**      [“Negociación de versión en NFS” en la página 182](#)

## ▼ Cómo utilizar el comando `mount` para seleccionar diferentes versiones de NFS en un cliente

El siguiente procedimiento muestra cómo utilizar el comando `mount` para controlar la versión de NFS que se utiliza en un cliente para un montaje específico. Si prefiere modificar la versión de NFS para todos los sistema de archivos que monta el cliente, consulte [“Cómo seleccionar diferentes versiones de NFS en un cliente mediante la modificación del archivo `/etc/default/nfs`”](#) en la página 100.

### 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 \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

### 2 Monte la versión deseada de NFS en el cliente.

Escriba el siguiente comando:

```
# mount -o vers=value server-name:/share-point /local-dir
valor                Proporcione el número de versión.
nombre_servidor      Proporcione el nombre del servidor.
/punto_compartir     Proporcione la ruta del directorio remoto que se compartirá.
/directorio_local    Proporcione la ruta del punto de montaje local.
```

---

**Nota** – Este comando utiliza el protocolo NFS para montar el directorio remoto y sustituye la configuración de cliente en el archivo `/etc/default/nfs`.

---

**Véase también** [“Negociación de versión en NFS”](#) en la página 182

## Administración de sistema NFS seguro

Para utilizar el sistema NFS seguro, todos lo equipos de los que es responsable deben tener un nombre de dominio. Normalmente, un dominio es una entidad administrativa de varios equipos que forma parte de una red más grande. Si ejecuta un servicio de nombres, también debe establecer el nombre de servicio para el dominio. Consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#).

El servicio NFS admite la autenticación Kerberos V5. El [Capítulo 21, “Introducción al servicio Kerberos”](#) de *Guía de administración del sistema: servicios de seguridad* trata sobre el servicio Kerberos.

También puede configurar el entorno NFS seguro para utilizar autenticación Diffie-Hellman. El [Capítulo 16, “Uso de servicios de autenticación \(tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#) trata sobre este servicio de autenticación.

## ▼ Cómo configurar un entorno NFS seguro con autenticación DH

- 1 **Asigne a su dominio un nombre de dominio y haga que el nombre de dominio sea conocido por cada equipo del dominio.**

Consulte la [Guía de administración del sistema: Servicios de nombres y directorios \(DNS, NIS y LDAP\)](#) si utiliza NIS+ como su servicio de nombres.

- 2 **Establezca claves públicas y claves secretas para los usuarios de clientes utilizando el comando `newkey` o `nisaddcred`. Haga que cada usuario establezca su propia contraseña de RPC segura mediante el comando `chkey`.**

---

**Nota** – Para obtener más información acerca de estos comandos, consulte las páginas del comando `man newkey(1M)`, `nisaddcred(1M)` y `chkey(1)`.

---

Cuando se han generado claves públicas y claves secretas, las claves públicas y las claves secretas encriptadas se almacenan en la base de datos `publickey`.

- 3 **Verifique que el servicio de nombres responda.**

Si está ejecutando NIS+, escriba lo siguiente:

```
# nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
      Last update occurred at Mon Jun  5 11:16:10 1995
```

```
Replica server is eng1-replica-replica-58.acme.com.
      Last Update seen was Mon Jun  5 11:16:10 1995
```

Si ejecuta NIS, verifique que el daemon `yplibind` esté en ejecución.

- 4 **Verifique que el daemon `keyserv` del servidor clave esté en ejecución.**

Escriba el siguiente comando.

```
# ps -ef | grep keyserv
root    100      1  16   Apr 11 ?        0:00 /usr/sbin/keyserv
root    2215    2211  5 09:57:28 pts/0    0:00 grep keyserv
```

Si el daemon no está en ejecución, inicie el servidor de claves introduciendo lo siguiente:

```
# /usr/sbin/keyserv
```

## 5 Descifre y almacene la clave secreta.

Normalmente, la contraseña de inicio de sesión es idéntica a la contraseña de red. En esta situación, `keylogin` no es necesario. Si las contraseñas son distintas, los usuarios tienen que iniciar sesión y, a continuación, ejecutar `keylogin`. Aún necesita utilizar el comando `keylogin -r` como `root` para almacenar la clave secreta descifrada en `/etc/.rootkey`.

---

**Nota** – Debe ejecutar `keylogin -r` si la clave secreta raíz cambia o si `/etc/.rootkey` se pierde.

---

## 6 Actualice las opciones de montaje para el sistema de archivos.

Para autenticación Diffie-Hellman, edite el archivo `/etc/dfs/dfstab` y agregue la opción `sec=dh` a las entradas apropiadas.

```
share -F nfs -o sec=dh /export/home
```

Consulte la página del comando `man dfstab(4)` para obtener una descripción de `/etc/dfs/dfstab`.

## 7 Actualice los mapas de montador automático para el sistema de archivos.

Edite los datos `auto_master` para incluir `sec=dh` como opción de montaje en las entradas apropiadas para autenticación Diffie-Hellman:

```
/home      auto_home      -nosuid,sec=dh
```

---

**Nota** – Las versiones hasta Solaris 2.5 tienen una limitación. Si un cliente no monta de manera segura un sistema de archivos compartido que es seguro, los usuarios tienen acceso como `nobody` en lugar de como ellos mismos. Para versiones posteriores que utilizan la versión 2, el servidor NFS niega el acceso si los modos de seguridad no coinciden, a menos que `-sec=ninguno` se incluya en la línea de comandos `share`. Con la versión 3, el modo se hereda del servidor NFS, para que los clientes no necesiten especificar `sec=dh`. Los usuarios tienen acceso a los archivos como ellos mismos.

---

Cuando reinstala, mueve o actualiza un equipo, acuérdesse de guardar `/etc/.rootkey` si no establece nuevas claves o modifica las claves para `root`. Si elimina `/etc/.rootkey`, siempre puede escribir lo siguiente:

```
# keylogin -r
```

# Tareas de administración WebNFS

Esta sección proporciona instrucciones para administrar el sistema WebNFS. Tareas relacionadas.

TABLA 5-4 Mapa de tareas para la administración WebNFS

Tarea	Descripción	Para obtener instrucciones
Planificar para WebNFS	Algunas cuestiones que debe tener en cuenta antes de habilitar el servicio WebNFS.	<a href="#">“Planificación de acceso WebNFS” en la página 104</a>
Habilitar WebNFS	Pasos para habilitar el montaje de un sistema de archivos NFS mediante el protocolo WebNFS.	<a href="#">“Cómo habilitar acceso WebNFS” en la página 88</a>
Habilitar WebNFS a través de un cortafuegos	Pasos para permitir el acceso a archivos a través de un cortafuegos utilizando el protocolo WebNFS.	<a href="#">“Cómo habilitar acceso WebNFS a través de un cortafuegos” en la página 106</a>
Explorar utilizando una URL de NFS	Instrucciones para el uso de una URL de NFS en un explorador web.	<a href="#">“Cómo explorar utilizando una URL de NFS” en la página 105</a>
Utilizar un identificador de archivos público con autofs	Pasos para forzar el uso del identificador de archivos público al montar un sistema de archivos con el montador automático.	<a href="#">“Cómo utilizar un identificador de archivos público con autofs” en la página 120</a>
Utilizar una URL de NFS con autofs	Pasos para agregar una URL de NFS para los mapas del montador automático.	<a href="#">“Cómo utilizar direcciones URL de NFS con autofs” en la página 121</a>
Proporcionar acceso a un sistema de archivos a través de un cortafuegos	Pasos para permitir el acceso a un sistema de archivos a través de un cortafuegos utilizando el protocolo WebNFS.	<a href="#">“Cómo montar un sistema de archivos NFS a través de un cortafuegos” en la página 95</a>
Montar un sistema de archivos utilizando una URL de NFS	Pasos para permitir el acceso a un sistema de archivos utilizando una URL de NFS. Este proceso permite el acceso al sistema de archivos sin utilizar el protocolo MOUNT.	<a href="#">“Cómo montar un sistema de archivos NFS utilizando una URL de NFS” en la página 95</a>

## Planificación de acceso WebNFS

Para utilizar WebNFS, primero necesita una aplicación capaz de ejecutar y cargar una URL de NFS (por ejemplo, `nfs://server/path`). El siguiente paso es elegir el sistema de archivos que puede exportarse para acceso WebNFS. Si la aplicación es para navegar por Internet, se utiliza con frecuencia la raíz del documento para el servidor web. Debe tener en cuenta varios factores al elegir un sistema de archivos a exportar para acceso WebNFS.

1. Cada servidor tiene un identificador de archivos público que, de manera predeterminada, está asociado con el sistema de archivos raíz del servidor. La ruta de acceso en una URL de NFS se evalúa según el directorio con el que el identificador de archivos público está asociado. Si la ruta conduce a un archivo o a un directorio dentro de un sistema de archivos exportado, el servidor proporciona acceso. Puede utilizar la opción `public` del comando `share` para asociar el identificador de archivos público con un directorio exportado específico. Con esta opción permite que las URL sean relativas al sistema de archivos



compartido en lugar de ser relativas al sistema de archivos raíz del servidor. El sistema de archivos raíz no permite acceso a Internet a menos que el sistema de archivos raíz esté compartido.

2. El entorno WebNFS habilita a los usuarios que ya poseen privilegios de montaje para acceder a archivos a través de un explorador. Esta función está habilitada independientemente de si el sistema de archivos se exporta utilizando la opción `public`. Debido a que los usuarios ya tienen acceso a estos archivos a través de la configuración NFS, este acceso no debe crear ningún riesgo de seguridad adicional. Sólo necesita compartir un sistema de archivos utilizando la opción `public` si los usuarios que no pueden montar el sistema de archivos necesitan utilizar acceso WebNFS.
3. Los sistemas de archivos que ya están abiertos al público son buenos candidatos para utilizar la opción `public`. Algunos ejemplos son: el directorio superior en un archivo ftp o el directorio URL principal para un sitio web.
4. Puede utilizar la opción `index` con el comando `share` para forzar la carga de un archivo HTML. De lo contrario, puede mencionar el directorio cuando se accede a una URL de NFS. Después de elegir un sistema de archivos, revise los archivos y establezca permisos de acceso para restringir la visualización de archivos o directorios, según sea necesario. Establezca permisos, según sea necesario, para cualquier sistema de archivos NFS que se comparta. Para muchos sitios, los permisos 755 para directorios y los permisos 644 para archivos proporcionan el nivel correcto de acceso.

Es necesario considerar factores adicionales si las URL de NFS y HTTP se utilizarán para acceder a un sitio web. Estos factores se describen en [“Limitaciones WebNFS con uso de explorador web” en la página 202](#).

## Cómo explorar utilizando una URL de NFS

Los exploradores capaces de admitir el servicio WebNFS deberían proporcionar acceso a una URL de NFS que se asemeje a lo siguiente:

`nfs://server[:port]/path`

*servidor*      Nombre del servidor de archivos

*puerto*      Número de puerto que se va a utilizar (2049, valor predeterminado)

*ruta*          Ruta al archivo, que puede ser relativa al identificador de archivos público o al sistema de archivos raíz

**Nota** – En la mayoría de los exploradores, el tipo de servicio URL (por ejemplo, `nfs` o `http`) se recuerda de una transacción a la siguiente. La excepción se produce cuando se carga una URL que incluye un tipo de servicio distinto. Después de utilizar una URL de NFS, es posible cargar una referencia a una URL de HTTP. Si se carga dicha referencia, las páginas siguientes se cargan mediante el protocolo HTTP en lugar del protocolo NFS.

## Cómo habilitar acceso WebNFS a través de un cortafuegos

Puede habilitar acceso WebNFS para clientes que no son parte de la subred local si configura el cortafuegos para que permita una conexión TCP en el puerto 2049. Permitir acceso para `httpd` no permite que las URL de NFS se utilicen.

## Descripción general de tareas para administración autofs

En esta sección se describen algunas de las tareas más comunes que posiblemente encuentre en su propio entorno. Se incluyen procedimientos recomendados para cada escenario para ayudarlo a configurar autofs para satisfacer las necesidades de los clientes de la mejor manera.

**Nota** – A partir de la versión Solaris 10, puede utilizar también el archivo `/etc/default/autofs` para configurar su entorno autofs. Para obtener información sobre las tareas, consulte [“Uso del archivo /etc/default/autofs para configurar su entorno autofs”](#) en la página 108.

## Mapa de tareas para administración autofs

La siguiente tabla proporciona una descripción y un puntero a muchas de las tareas que están relacionadas con autofs.

TABLA 5-5 Mapa de tareas para administración autofs

Tarea	Descripción	Para obtener instrucciones
Iniciar autofs	Iniciar el servicio de montador automático sin necesidad de reiniciar el sistema	<a href="#">“Cómo iniciar el montador automático”</a> en la página 98
Detener autofs	Detener el servicio de montador automático sin deshabilitar otros servicios de red	<a href="#">“Cómo detener el montador automático”</a> en la página 98

TABLA 5-5 Mapa de tareas para administración autofs (Continuación)

Tarea	Descripción	Para obtener instrucciones
Configurar su entorno autofs utilizando el archivo <code>/etc/default/autofs</code>	Asignar valores a palabras clave en el archivo <code>/etc/default/autofs</code>	“Uso del archivo <code>/etc/default/autofs</code> para configurar su entorno autofs” en la página 108
Acceder a sistemas de archivos utilizando autofs	Acceder a sistemas de archivos utilizando el servicio de montador automático	“Montaje con el montador automático” en la página 92
Modificar mapas autofs	Pasos para modificar el mapa maestro, que debería utilizarse para mencionar otros mapas	“Cómo modificar el mapa maestro” en la página 110
	Pasos para modificar un mapa indirecto, el cual se debería utilizar para la mayoría de los mapas	“Cómo modificar mapas indirectos” en la página 111
	Pasos para modificar un mapa directo, que debería utilizarse cuando se requiere una asociación directa entre un punto de montaje en un cliente y un servidor	“Cómo modificar mapas directos” en la página 111
Modificar los mapas autofs para acceder a sistemas de archivos NFS	Pasos para configurar un mapa autofs con una entrada para una aplicación de CD-ROM	“Cómo acceder a aplicaciones de CD-ROM con autofs” en la página 112
	Pasos para configurar un mapa autofs con una entrada para un disquete PC-DOS	“Cómo acceder a disquetes de datos PC-DOS con autofs” en la página 113
	Pasos para utilizar autofs para acceder a un sistema de archivos CacheFS	“Cómo acceder a sistemas de archivos NFS utilizando CacheFS” en la página 114
Utilizar <code>/home</code>	Ejemplo de cómo configurar un mapa <code>/home</code> común	“Configuración de una vista común de <code>/home</code> ” en la página 114
	Pasos para configurar un mapa <code>/home</code> que haga referencia a varios sistemas de archivos	“Cómo configurar <code>/home</code> con varios sistemas de archivos de directorio principal” en la página 115
Usar un nuevo punto de montaje autofs	Pasos para configurar un mapa autofs relacionado con el proyecto	“Cómo consolidar archivos relacionados con el proyecto en <code>/ws</code> ” en la página 116
	Pasos para configurar un mapa autofs que admita diferentes arquitecturas de cliente	“Cómo configurar arquitecturas diferentes para acceder a un espacio de nombres compartido” en la página 118
	Pasos para configurar un mapa autofs que admita diferentes sistemas operativos	“Cómo admitir versiones del sistema operativo de cliente incompatibles” en la página 119
Replicar sistemas de archivos con autofs	Proporcionar acceso a los sistemas de archivos que se conmutan por error	“Cómo replicar archivos compartidos entre varios servidores” en la página 119

TABLA 5-5 Mapa de tareas para administración autofs (Continuación)

Tarea	Descripción	Para obtener instrucciones
Utilizar restricciones de seguridad con autofs	Proporcionar acceso a sistemas de archivos al restringir acceso root remoto a los archivos	<a href="#">“Cómo aplicar restricciones de seguridad autofs” en la página 120</a>
Utilizar un identificador de archivos público con autofs	Forzar el uso del identificador de archivos público al montar un sistema de archivos	<a href="#">“Cómo utilizar un identificador de archivos público con autofs” en la página 120</a>
Utilizar una URL de NFS con autofs	Agregar una URL de NFS de forma que el montador automático pueda utilizarla	<a href="#">“Cómo utilizar direcciones URL de NFS con autofs” en la página 121</a>
Deshabilitar capacidad de explorar autofs	Pasos para deshabilitar la capacidad de explorar para que los puntos de montaje autofs no se rellenen automáticamente en un solo cliente	<a href="#">“Cómo deshabilitar por completo la capacidad de explorar autofs en un único cliente NFS” en la página 121</a>
	Pasos para deshabilitar la capacidad de explorar para que los puntos de montaje autofs no se rellenen automáticamente en todos los clientes	<a href="#">“Cómo deshabilitar la capacidad de explorar autofs para todos los clientes” en la página 122</a>
	Pasos para deshabilitar la capacidad de explorar para que un punto de montaje autofs específico no se rellene automáticamente en un solo cliente	<a href="#">“Cómo deshabilitar la capacidad de explorar autofs en un sistema de archivos seleccionado” en la página 122</a>

## Uso del archivo `/etc/default/autofs` para configurar su entorno autofs

A partir de la versión Solaris 10, puede utilizar el archivo `/etc/default/autofs` para configurar su entorno autofs. En concreto, este archivo proporciona una manera adicional de configurar los comandos autofs y los daemons autofs. Las mismas especificaciones que se harían en la línea de comandos pueden hacerse en este archivo de configuración. Puede establecer sus especificaciones proporcionando valores para palabras clave. Para obtener más información, consulte [“Archivo `/etc/default/autofs`” en la página 141](#).

El procedimiento siguiente muestra cómo utilizar el archivo `/etc/default/autofs`.

### ▼ Cómo configurar su entorno autofs con el archivo `/etc/default/autofs`

#### 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 \(mapa de tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#).

2 **Agregue o modifique una entrada en el archivo `/etc/default/autofs`.**

Por ejemplo, si desea desactivar la exploración para todos los puntos de montaje autofs, puede añadir la siguiente línea.

**AUTOMOUNTD\_NOBROWSE=ON**

La palabra clave equivale al argumento `-n` de `automountd`. Para obtener una lista de palabras clave, consulte [“Archivo `/etc/default/autofs`” en la página 141](#).

3 **Reinicie el daemon autofs.**

Escriba el siguiente comando:

**# `svcadm restart system/filesystem/autofs`**

**Tareas administrativas que incluyen mapas**

La siguiente tabla describe varios de los factores que necesita tener en cuenta al administrar mapas autofs. La elección de mapa y servicio de nombres afectan el mecanismo que necesita utilizar para realizar cambios en los mapas autofs.

La siguiente tabla describe los tipos de mapas y sus usos.

**TABLA 5-6** Tipos de mapas autofs y sus usos

Tipo de mapa	Uso
Maestro	Asocia un directorio con un mapa
Directo	Dirige autofs a sistemas de archivos específicos
Indirecto	Dirige autofs a sistemas de archivos orientados a la referencia

La siguiente tabla describe cómo realizar cambios en su entorno autofs basado en su servicio de nombres.

**TABLA 5-7** Mantenimiento de mapas

Servicio de nombres	Método
Archivos locales	Editor de texto
NIS	<code>archivos make</code>
NIS+	<code>nistbladm</code>

La siguiente tabla le dice cuándo ejecutar el comando `automount`, según la modificación que haya realizado en el tipo de mapa. Por ejemplo, si ha realizado una adición o una eliminación en un mapa directo, debe ejecutar el comando `automount` en el sistema local. Mediante la ejecución

del comando, hace que la modificación entre en vigor. Sin embargo, si ha modificado una entrada existente, no necesita ejecutar el comando automount para que la modificación entre en vigor.

TABLA 5-8 Cuándo se debe ejecutar el comando automount

Tipo de mapa	¿Reiniciar automount?	
	Adición o eliminación	Modificación
auto_master	Y	Y
direct	Y	N
indirect	N	N

## Modificación de los mapas

Los siguientes procedimientos requieren que se use NIS+ como servicio de nombres.

### ▼ Cómo modificar el mapa maestro

- 1 **Inicie sesión como un usuario que tiene permisos para cambiar los mapas.**
- 2 **Realice sus modificaciones en el mapa maestro utilizando el comando `nistbladm`.**  
Consulte la *System Administration Guide: Naming and Directory Services (NIS+)*.
- 3 **Para cada cliente, conviértase en superusuario o adopte un rol equivalente.**  
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “*Configuración de RBAC (mapa de tareas)*” de *Guía de administración del sistema: servicios de seguridad*.
- 4 **Para cada cliente, ejecute el comando `automount` para asegurarse que sus modificaciones entren en vigor.**
- 5 **Notifique a los usuarios de las modificaciones.**  
La notificación es necesaria para que los usuarios también puedan ejecutar el comando `automount` como superusuarios en sus propios equipos. Tenga en cuenta que el comando `automount` recopila información del mapa maestro siempre que se ejecute.

## ▼ Cómo modificar mapas indirectos

- 1 Inicie sesión como un usuario que tiene permisos para cambiar los mapas.

- 2 Realice sus modificaciones en el mapa indirecto utilizando el comando `nistbladm`.

Consulte la [System Administration Guide: Naming and Directory Services \(NIS+\)](#). Tenga en cuenta que la modificación entra en vigor la próxima vez que se utiliza el mapa, que es la próxima vez que se realiza un montaje.

## ▼ Cómo modificar mapas directos

- 1 Inicie sesión como un usuario que tiene permisos para cambiar los mapas.

- 2 Agregue o elimine modificaciones en el mapa directo utilizando el comando `nistbladm`.

Consulte la [System Administration Guide: Naming and Directory Services \(NIS+\)](#).

- 3 Notifique a los usuarios de las modificaciones.

La notificación es necesaria para que los usuarios puedan ejecutar el comando `automount` como superusuarios en sus propios equipos, si es necesario.

---

**Nota** – Si sólo modifica o cambia los contextos de una entrada de mapa directo existente, no necesita ejecutar el comando `automount`.

---

Por ejemplo, supongamos que modifica el mapa `auto_direct` para que el directorio `/usr/src` se monte desde un servidor diferente. Si `/usr/src` no está montado en ese momento, la nueva entrada entra en vigor inmediatamente cuando intenta acceder a `/usr/src`. Si `/usr/src` está montado, puede esperar hasta que se produzca el desmontaje automático y, luego, acceder al archivo.

---

**Nota** – Utilice mapas indirectos siempre que sea posible. Los mapas indirectos son más fáciles de construir y menos exigentes en los sistemas de archivos de los equipos. También, los mapas indirectos no ocupan tanto espacio en la tabla de montaje como los mapas directos.

---

## Cómo evitar conflictos de punto de montaje

Si tiene una partición de disco local montada en `/src` y planea utilizar el servicio autofs para montar otros directorios de origen, es posible que encuentre un problema. Si especifica el punto de montaje `/src`, el servicio NFS oculta la partición local cada vez que intenta acceder a ella.

Debe montar la partición en otra ubicación, por ejemplo, en `/export/src`. Luego necesita una entrada en `/etc/vfstab` como la siguiente:

```
/dev/dsk/d0t3d0s5 /dev/rdisk/c0t3d0s5 /export/src ufs 3 yes -
```

También necesita esta entrada en `auto_src`:

```
terra          terra:/export/src
```

terra es el nombre del equipo.

## Acceso a sistemas de archivos no NFS

Autofs puede también montar archivos que no sean archivos NFS. Autofs monta archivos en medios extraíbles, como disquetes o CD-ROM. Normalmente, montaría archivos en medios extraíbles mediante Volume Manager. Los siguientes ejemplos muestran cómo este montaje se puede lograr mediante autofs. Volume Manager y autofs no trabajan conjuntamente, por lo tanto, esas entradas no se utilizarían sin antes desactivar Volume Manager.

En lugar de montar un sistema de archivos desde un servidor, coloca el medio en la unidad y hace referencia al sistema de archivos desde el mapa. Si piensa acceder a sistemas de archivos no NFS y utiliza autofs, consulte los siguientes procedimientos.

### ▼ Cómo acceder a aplicaciones de CD-ROM con autofs

---

**Nota** – Utilice este procedimiento si *no* utiliza Volume Manager.

---

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Actualice los mapas autofs.

Agregue una entrada para el sistema de archivos de CD-ROM, que debería ser similar a lo siguiente:

```
hsfs          -fstype=hsfs,ro          :/dev/sr0
```

El dispositivo de CD-ROM que intenta montar debe aparecer como un nombre después de los dos puntos.



## ▼ Cómo acceder a disquetes de datos PC-DOS con autofs

---

**Nota** – Utilice este procedimiento si *no* utiliza Volume Manager.

---

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Actualice los mapas autofs.

Agregue una entrada para el sistema de archivos de disquete como la siguiente:

```
pcfs      -fstype=pcfs      :/dev/diskette
```

## Acceso a sistemas de archivos NFS utilizando CacheFS

El sistema de archivos de antememoria (CacheFS) es un mecanismo de almacenamiento no volátil genérico. CacheFS mejora el rendimiento de ciertos sistemas de archivos, ya que utiliza un disco local más pequeño y rápido. Por ejemplo, puede mejorar el rendimiento del entorno NFS utilizando CacheFS.

CacheFS funciona de manera distinta con las diversas versiones de NFS. Por ejemplo, si el cliente y el sistema de archivos secundario (back file system) están ejecutando la versión 2 o 3 de NFS, los archivos se almacenan en la antememoria en el sistema de archivos principal (front file system) para que pueda acceder el cliente. No obstante, si el cliente y el servidor ejecutan la versión 4 de NFS, el funcionamiento es el siguiente. Cuando el cliente realiza la solicitud inicial para acceder a un archivo desde un sistema de archivos CacheFS, la solicitud evita el sistema de archivos principal (o almacenado en la antememoria) y accede directamente al sistema de archivos secundario. Con la versión 4 de NFS, los archivos ya no se almacenan en el sistema de archivos principal. Todo el acceso a los archivos lo proporciona el sistema de archivos secundario. También, como ningún archivo se almacena en la antememoria en el sistema de archivos principal, se hace caso omiso de las opciones de montaje específicas de CacheFS, que afectan al sistema de archivos principal. Las opciones de montaje específicas de CacheFS no son aplicables al sistema de archivos secundario.

---

**Nota** – La primera vez que configure el sistema para la versión 4 de NFS, aparecerá un mensaje de advertencia en la consola que indica que ya no se realiza el almacenamiento en la antememoria.

---

## ▼ Cómo acceder a sistemas de archivos NFS utilizando CacheFS

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Ejecute el comando `cfsadmin` para crear un directorio de antememoria en el disco local.

```
# cfsadmin -c /var/cache
```

### 3 Agregue la entrada `cacheafs` al mapa de montador automático apropiado.

Por ejemplo, agregar esta entrada al mapa maestro almacena todos los directorios principales:

```
/home auto_home -fstype=cacheafs,cachedir=/var/cache,backfstype=nfs
```

Agregar esta entrada al mapa `auto_home` sólo almacena el directorio principal para el usuario denominado `rich`:

```
rich -fstype=cacheafs,cachedir=/var/cache,backfstype=nfs dragon:/export/home1/rich
```

---

**Nota** – Las opciones incluidas en mapas que se buscan posteriormente reemplazan las opciones establecidas en mapas que se buscan anteriormente. Las últimas opciones que se encuentran son las que se utilizan. En el ejemplo anterior, una entrada adicional al mapa `auto_home` sólo debe incluir las opciones en los mapas maestros si algunas opciones requerían modificaciones.

---

## Personalización del montador automático

Puede configurar los mapas del montador automático de diferentes maneras. Las siguientes tareas proporcionan detalles sobre cómo personalizar los mapas de montador automático para proporcionar una estructura de directorios fácil de usar.

## Configuración de una vista común de `/home`

Lo ideal es que todos los usuarios de red puedan ubicar sus propios directorios principales, o los de cualquiera, en `/home`. Esta vista debería ser común entre todos los equipos, ya sean cliente o servidor.

Cada instalación de Solaris incluye un mapa maestro: `/etc/auto_master`.

```
# Master map for autofs
#
```

```
+auto_master
/net      -hosts      -nosuid,nobrowse
/home     auto_home    -nobrowse
```

Un mapa para `auto_home` también se instala en `/etc`.

```
# Home directory map for autofs
#
+auto_home
```

Excepto para una referencia a un mapa `auto_home` externo, este mapa está vacío. Si los directorios en `/home` deben ser comunes a todos los equipos, no modifique este mapa `/etc/auto_home`. Todas las entradas de directorio principal deberían aparecer en los archivos del servicio de nombres, ya sea NIS o NIS+.

---

**Nota** – No se debería permitir a los usuarios ejecutar `setuid` desde sus directorios principales. Sin esta restricción, cualquier usuario podría tener privilegios de superusuario en cualquier equipo.

---

## ▼ **Cómo configurar `/home` con varios sistemas de archivos de directorio principal**

### **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 \(mapa de tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#).

### **2 Instale particiones de directorio principal en `/export/home`.**

Si el sistema tiene varias particiones, instale las particiones en directorios independientes, por ejemplo, `/export/home1` y `/export/home2`.

### **3 Utilice las herramientas de Solaris Management Console para crear y mantener el mapa `auto_home`.**

Cada vez que cree una nueva cuenta de usuario, escriba la ubicación del directorio principal del usuario en el mapa `auto_home`. Las entradas de mapa pueden ser simples, por ejemplo:

```
rusty      dragon:/export/home1/&
gwenda     dragon:/export/home1/&
charles    sundog:/export/home2/&
rich       dragon:/export/home3/&
```

Observe el uso de `&` ("y" comercial) para sustituir la clave de mapa. El símbolo `&` es una abreviatura para la segunda instancia de `rusty` en el siguiente ejemplo.

```
rusty      dragon:/export/home1/rusty
```

Con el mapa `auto_home` en su lugar, los usuarios pueden hacer referencia a cualquier directorio principal (incluidos sus propios directorios) con la ruta `/home/usuario.usuario` es el nombre de inicio de sesión y la clave en el mapa. Esta vista común de todos los directorios principales resulta muy útil al iniciar sesión en el equipo de otro usuario. Autofs monta su directorio principal por usted. De igual manera, si ejecuta un cliente de sistema de ventanas remoto en otro equipo, el programa cliente tiene la misma vista que el directorio `/home`.

Esta vista común se extiende también al servidor. Con el ejemplo anterior, si `rusty` inicia sesión en el servidor `dragon`, autofs proporciona acceso directo al disco local mediante montaje en bucle de retorno `/export/home1/rusty` en `/home/rusty`.

Los usuarios no necesitan conocer la ubicación real de sus directorios principales. Si `rusty` necesita más espacio en disco y necesita tener su directorio principal reubicado en otro servidor, un simple cambio es suficiente. Sólo necesita cambiar la entrada de `rusty` en el mapa `auto_home` para reflejar la nueva ubicación. Otros usuarios pueden seguir utilizando la ruta `/home/rusty`.

## ▼ **Cómo consolidar archivos relacionados con el proyecto en `/ws`**

Piense que es el administrador de un proyecto de desarrollo de software grande. Desea que todos los archivos relacionados con el proyecto estén disponibles en un directorio denominado `/ws`. Este directorio debe ser común para todas las estaciones de trabajo del sitio.

### **1 Agregue una entrada para el directorio `/ws` para el mapa `auto_master` de sitio, ya sea NIS o NIS+.**

```
/ws      auto_ws      -nosuid
```

El mapa `auto_ws` determina los contenidos del directorio `/ws`.

### **2 Agregue la opción `-nosuid` como precaución.**

Esta opción impide que los usuarios ejecuten programas `setuid` que posiblemente se encuentren en cualquier espacio de trabajo.

### **3 Agregue entradas al mapa `auto_ws`.**

El mapa `auto_ws` se organiza de manera que cada entrada describe un subproyecto. Su primer intento proporciona un mapa similar a lo siguiente:

```
compiler  alpha:/export/ws/&
windows   alpha:/export/ws/&
files     bravo:/export/ws/&
drivers   alpha:/export/ws/&
man       bravo:/export/ws/&
tools     delta:/export/ws/&
```

El símbolo de "y" comercial (&) al final de cada entrada es una abreviatura para la clave de entrada. Por ejemplo, la primera entrada es equivalente a lo siguiente:

```
compiler      alpha:/export/ws/compiler
```

Este primer intento proporciona un mapa que se muestra simple, pero el mapa es inadecuado. El organizador del proyecto decide que la documentación en la entrada `man` debería proporcionarse como un subdirectorio en cada subproyecto. Además, cada subproyecto requiere subdirectorios para describir varias versiones del software. Debe asignar cada uno de estos subdirectorios a toda una partición de disco en el servidor.

Modifique las entradas en el mapa como se indica a continuación:

```
compiler \
  /vers1.0  alpha:/export/ws/&/vers1.0 \
  /vers2.0  bravo:/export/ws/&/vers2.0 \
  /man      bravo:/export/ws/&/man
windows \
  /vers1.0  alpha:/export/ws/&/vers1.0 \
  /man      bravo:/export/ws/&/man
files \
  /vers1.0  alpha:/export/ws/&/vers1.0 \
  /vers2.0  bravo:/export/ws/&/vers2.0 \
  /vers3.0  bravo:/export/ws/&/vers3.0 \
  /man      bravo:/export/ws/&/man
drivers \
  /vers1.0  alpha:/export/ws/&/vers1.0 \
  /man      bravo:/export/ws/&/man
tools \
  /          delta:/export/ws/&
```

Aunque el mapa ahora parece ser mucho más grande, el mapa aún contiene sólo las cinco entradas. Cada entrada es más grande porque cada entrada contiene varios montajes. Por ejemplo, una referencia a `/ws/compiler` necesita tres montajes para los directorios `vers1.0`, `vers2.0` y `man`. La barra diagonal inversa situada al final de cada línea informa a `autofs` que la entrada sigue en la siguiente línea. La entrada es una línea larga, aunque se hayan utilizado espacios o sangrías para que la entrada fuese más legible. El directorio `tools` contiene herramientas de desarrollo de software para todos los subproyectos, de modo que este directorio no está sujeto a la misma estructura de subdirectorio. El directorio `tools` sigue siendo un solo montaje.

Este acuerdo proporciona al administrador mucha flexibilidad. Los proyectos de software normalmente abarcan grandes cantidades de espacio en disco. A lo largo del proyecto, es posible que necesite reubicar y ampliar varias particiones de disco. Si estas modificaciones se reflejan en el mapa `auto_ws`, no es necesario notificar a los usuarios, ya que la jerarquía de directorio en `/ws` no cambia.

Debido a que los servidores `alpha` y `bravo` visualizan los mismos mapas `autofs`, cualquier usuario que inicie sesión en estos equipos puede encontrar el espacio de nombres `/ws` como se espera. Se les proporciona a los usuarios acceso directo a archivos locales a través de montajes de bucle de retorno en lugar de montajes NFS.

## ▼ **Cómo configurar arquitecturas diferentes para acceder a un espacio de nombres compartido**

Necesita establecer un espacio de nombres compartido para ejecutables locales y aplicaciones, como aplicaciones de hoja de cálculo y paquetes de procesamiento de textos. Los clientes de este espacio usan diversas arquitecturas de estaciones de trabajo que necesitan distintos formatos ejecutables. Asimismo, algunas estaciones de trabajo ejecutan diversas versiones en el sistema operativo.

### **1 Cree el mapa `auto_local`.**

Consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.

### **2 Seleccione un único nombre específico de sitio para el espacio de nombres compartidos.**

Este nombre hace que los archivos y directorios que pertenecen a este espacio sean fácilmente identificables. Por ejemplo, si selecciona `/usr/local` como el nombre, la ruta `/usr/local/bin` es obviamente una parte de este espacio de nombres.

### **3 Para facilitar el reconocimiento de comunidad de usuarios, cree un mapa indirecto autofs.**

Monte este mapa en `/usr/local`. Configure la siguiente entrada en el mapa `auto_master` NIS:

```
/usr/local    auto_local    -ro
```

Tenga en cuenta que la opción de montaje `-ro` implica que los clientes no pueden escribir en ningún archivo o directorio.

### **4 Exporte el directorio adecuado en el servidor.**

### **5 Incluya una entrada `bin` en el mapa `auto_local`.**

La estructura de directorios es similar a lo siguiente:

```
bin    aa:/export/local/bin
```

### **6 (Opcional) Para servir a clientes de arquitecturas diferentes, cambie la entrada agregando la variable `CPU` autofs.**

```
bin    aa:/export/local/bin/$CPU
```

- Para clientes SPARC – Ubique ejecutables en `/export/local/bin/sparc`.
- Para clientes x86 – Ubique ejecutables en `/export/local/bin/i386`.

## ▼ Cómo admitir versiones del sistema operativo de cliente incompatibles

- 1 **Combine el tipo de arquitectura con una variable que determine el tipo de sistema operativo del cliente.**

Puede combinar la variable OSREL con la variable CPU autofs para formar un nombre que determine el tipo de CPU y la versión del sistema operativo.

- 2 **Cree la siguiente entrada de mapa.**

```
bin    aa:/export/local/bin/$CPU$OSREL
```

Para los clientes que ejecutan la versión 5.6 del sistema operativo, exporte los siguientes sistemas de archivos:

- Para clientes SPARC – Exporte /export/local/bin/sparc5.6.
- Para clientes x86 – Ubique ejecutables en /export/local/bin/i3865.6.

## ▼ Cómo replicar archivos compartidos entre varios servidores

La mejor manera de compartir sistemas de archivos replicados de sólo lectura es utilizar conmutación por error. Consulte [“Conmutación por error por parte del cliente” en la página 196](#) para una discusión de conmutación por error.

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Modifique la entrada en los mapas autofs.**

Cree la lista de todos los servidores réplica como una lista separada por comas, como la siguiente:

```
bin    aa,bb,cc,dd:/export/local/bin/$CPU
```

Autofs elige el servidor más cercano. Si un servidor tiene varias interfaces de red, enumere cada interfaz. Autofs elige la interfaz más cercana al cliente, evitando enrutamiento innecesario de tráfico NFS.

## ▼ Cómo aplicar restricciones de seguridad autofs

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Cree la siguiente entrada en el archivo `auto_master` de servicio de nombres, ya sea NIS o NIS+:

```
/home      auto_home      -nosuid
```

La opción `nosuid` evita que los usuarios creen archivos con el conjunto de bits `setuid` o `setgid`.

Esta entrada sustituye la entrada para `/home` en un archivo `/etc/auto_master` local genérico. Consulte el ejemplo anterior. La sustitución se produce porque la referencia `+auto_master` al mapa de servicio de nombres externo sucede antes que la entrada `/home` en el archivo. Si las entradas del mapa `auto_home` incluyen opciones de montaje, la opción `nosuid` se sustituye. Por lo tanto, no se deben utilizar opciones en el mapa `auto_home` o se debe incluir la opción `nosuid` con cada entrada.

---

**Nota** – No monte las particiones de disco de directorio principal en `/home` en el servidor.

---

## ▼ Cómo utilizar un identificador de archivos público con autofs

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Cree una entrada en los mapas autofs como la siguiente:

```
/usr/local      -ro,public      bee:/export/share/local
```

La opción `public` obliga a que se utilice el identificador de archivos público. Si el servidor NFS no admite un identificador de archivos público, el montaje falla.



## ▼ Cómo utilizar direcciones URL de NFS con autofs

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Cree una entrada autofs como la siguiente:

```
/usr/local      -ro      nfs://bee/export/share/local
```

El servicio intenta utilizar el identificador de archivos público en el servidor NFS. Sin embargo, si el servidor no admite un identificador de archivos público, se utiliza el protocolo MOUNT.

## Deshabilitación de la capacidad de explorar autofs

La versión predeterminada de `/etc/auto_master` que está instalada tiene la opción `-nobrowse` agregada a las entradas para `/home` y `/net`. Además, el procedimiento de actualización agrega la opción `-nobrowse` a las entradas `/home` y `/net` en `/etc/auto_master` si esas entradas no se han modificado. Sin embargo, es posible realizar estas modificaciones manualmente o desactivar la capacidad de explorar para puntos de montaje autofs específicos del sitio después de la instalación.

Puede desactivar la capacidad de explorar de diferentes maneras. Puede deshabilitar la función mediante una opción de línea de comandos para el daemon `automountd`, que deshabilita completamente la capacidad de explorar autofs para el cliente. O puede deshabilitar la capacidad de explorar para cada entrada de mapa en todos los clientes mediante mapas autofs en un espacio de nombres NIS o NIS+. También puede deshabilitar la función de cada entrada de mapa en cada cliente, mediante mapas autofs locales si ningún espacio de nombres en toda la red está en uso.

## ▼ Cómo deshabilitar por completo la capacidad de explorar autofs en un único cliente NFS

### 1 Conviértase en superusuario o asuma un rol equivalente en el cliente NFS.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Edite el archivo `/etc/default/autofs` para incluir el valor y palabra clave siguientes.

```
AUTOMOUNTD_NOBROWSE=TRUE
```

### 3 Reinicie el servicio autofs.

```
# svcadm restart system/filesystem/autofs
```

## ▼ Cómo deshabilitar la capacidad de explorar autofs para todos los clientes

Para deshabilitar la capacidad de explorar autofs para todos los clientes, debe emplear un servicio de nombres como NIS o NIS+. De lo contrario, tendrá que editar manualmente los mapas de montador automático en cada cliente. En este ejemplo, la capacidad de explorar el directorio /home está deshabilitada. Debe seguir este procedimiento para cada nodo autofs indirecto que necesite deshabilitar.

### 1 Agregue la opción -nobrowse a la entrada /home en el archivo auto\_master de servicio de nombres.

```
/home      auto_home      -nobrowse
```

### 2 Ejecute el comando automount en todos los clientes.

El nuevo comportamiento entra en vigor después de ejecutar el comando automount en los sistemas cliente o después de un reinicio.

```
# /usr/sbin/automount
```

## ▼ Cómo deshabilitar la capacidad de explorar autofs en un sistema de archivos seleccionado

En este ejemplo, la capacidad de explorar del directorio /net está deshabilitada. Puede utilizar el mismo procedimiento para /home o cualquier otro punto de montaje autofs.

### 1 Compruebe la entrada automount en /etc/nsswitch.conf.

Para que entradas de archivos locales tengan precedencia, la entrada en el archivo de cambio del servicio de nombres debería enumerar files antes del servicio de nombres. Por ejemplo:

```
automount:  files nis
```

Esta entrada muestra la configuración predeterminada en una instalación estándar de Solaris.

### 2 Compruebe la posición de la entrada +auto\_master en /etc/auto\_master.

Para que las adiciones a los archivos locales tengan precedencia sobre las entradas en el espacio de nombres, la entrada +auto\_master se debe mover después de /net:

```
# Master map for automounter
#
/net      -hosts      -nosuid
/home     auto_home
/xfn      -xfn
+auto_master
```

Una configuración estándar ubica la entrada `+auto_master` en la parte superior del archivo. Esto evita que se utilicen modificaciones locales.

**3 Agregue la opción `nobrowse` a la entrada `/net` en el archivo `/etc/auto_master`.**

```
/net      -hosts      -nosuid,nobrowse
```

**4 En todos los clientes, ejecute el comando `automount`.**

El nuevo comportamiento entra en vigor después de ejecutar el comando `automount` en los sistemas cliente o después de un reinicio.

```
# /usr/sbin/automount
```

## Estrategias para resolución de problemas de NFS

Al rastrear un problema NFS, tenga presente los puntos principales de posible fallo: el servidor, el cliente y la red. La estrategia que se describe en esta sección intenta aislar cada componente individual para encontrar cuál es el que no funciona. En todas las situaciones, los daemons `mountd` y `nfsd` deben estar en ejecución en el servidor para que los montajes remotos se realicen correctamente.

La opción `-intr` se establece de manera predeterminada para todos los montajes. Si un programa se bloquea con un mensaje `server not responding` puede cerrar el programa con la interrupción de teclado `Control-c`.

Cuando la red o el servidor tienen problemas, los programas que acceden a archivos remotos con montaje forzado fallan de modo distinto de aquellos programas que acceden a archivos remotos montados con montaje flexible. Los sistemas de archivos remotos con montaje forzado hacen que el núcleo del cliente vuelva a intentar las solicitudes hasta que el servidor responda nuevamente. Los sistemas de archivos remotos con montaje flexible hacen que las llamadas del sistema del cliente devuelvan un error después de intentar durante un tiempo. Debido a que estos errores pueden dar como resultado errores de aplicación inesperados y daños en los datos, evite el montaje flexible.

Cuando un sistema de archivos tiene un montaje forzado, un programa que intenta acceder al sistema de archivos se bloquea si el servidor no puede responder. En esta situación, el sistema NFS muestra el siguiente mensaje en la consola:

```
NFS server hostname not responding still trying
```

Cuando el servidor finalmente responde, aparece el siguiente mensaje en la consola:

```
NFS server hostname ok
```

Un programa que accede a un sistema de archivos con montaje flexible cuyo servidor no responde genera el siguiente mensaje:

```
NFS operation failed for server hostname: error # (error-message)
```

---

**Nota** – Debido a los posibles errores, no utilice el montaje flexible en sistemas de archivos con datos de lectura-escritura o en sistemas de archivos desde los cuales se ejecutan archivos ejecutables. Los datos en los que se puede escribir podrían resultar dañados si la aplicación ignora los errores. Es posible que los ejecutables montados no se carguen correctamente y tengan errores.

---

## Procedimientos de resolución de problemas NFS

Para determinar dónde el servicio NFS ha fallado, debe seguir varios procedimientos para aislar el fallo. Compruebe los siguientes elementos:

- ¿Puede el cliente acceder al servidor?
- ¿Puede el cliente ponerse en contacto con los servicios NFS en el servidor?
- ¿Los servicios NFS están en ejecución en el servidor?

En el proceso de verificar esos elementos, es posible que otros sectores de la red no funcionen. Por ejemplo, es posible que no funcionen el servicio de nombres o el hardware de red física. La *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* contiene procedimientos de depuración para varios servicios de nombres. Además, durante el proceso, es posible que note que el problema no se encuentra en el extremo del cliente. Un ejemplo es si obtiene al menos una llamada de problemas de cada subred en su área de trabajo. En esta situación, puede suponer que el problema es del servidor o el hardware de red cerca del servidor. Por lo tanto, debe iniciar el proceso de depuración en el servidor, no en el cliente.

### ▼ Cómo comprobar la conectividad en un cliente NFS

- 1 **Compruebe que se pueda alcanzar el servidor NFS desde el cliente. En el cliente, escriba el siguiente comando.**

```
% /usr/sbin/ping bee
bee is alive
```

Si el comando informa que el servidor está activo, compruebe de forma remota el servidor NFS. Consulte [“Cómo comprobar el servidor NFS remotamente” en la página 125](#).

- 2 **Si no se puede acceder al servidor desde el cliente, asegúrese de que el servicio de nombres local esté en ejecución.**

Para clientes NIS+, escriba lo siguiente:

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
      Last update occurred at Mon Jun  5 11:16:10 1995
```

```
Replica server is engl-replica-58.acme.com.
Last Update seen was Mon Jun  5 11:16:10 1995
```

- 3 Si el servicio de nombres está en ejecución, asegúrese de que el cliente haya recibido la información de host correcta escribiendo lo siguiente:

```
% /usr/bin/getent hosts bee
129.144.83.117    bee.eng.acme.com
```

- 4 Si la información de host es correcta, pero no se puede acceder al servidor desde el cliente, ejecute el comando `ping` desde otro cliente.

Si el comando que se ejecuta desde un segundo cliente falla, consulte [“Cómo verificar el servicio NFS en el servidor” en la página 127](#).

- 5 Si se puede acceder al servidor desde el segundo cliente, utilice `ping` para comprobar la conectividad del primer cliente en otros sistemas de la red local.

Si este comando falla, compruebe la configuración de software de red en el cliente, por ejemplo, `/etc/netmasks` y `/etc/nsswitch.conf`.

- 6 (Opcional) Compruebe el resultado del comando `rpcinfo`.

Si el comando `rpcinfo` no muestra `program 100003 version 4 ready and waiting`, la versión 4 de NFS no está habilitada en el servidor. Consulte la [Tabla 5-3](#) para obtener información sobre la habilitación de la versión 4 de NFS.

- 7 Si el software es correcto, compruebe el hardware de red.

Intente mover el cliente en un segundo descarte de red.

## ▼ Cómo comprobar el servidor NFS remotamente

Tenga en cuenta que no es necesaria la compatibilidad para los protocolos UDP y MOUNT si utiliza un servidor versión 4 de NFS.

- 1 Compruebe que los servicios NFS se hayan iniciado en el servidor NFS. Para ello escriba el siguiente comando:

```
% rpcinfo -s bee | egrep 'nfs|mountd'
100003 3,2 tcp,udp,tcp6,udp6 nfs superuser
100005 3,2,1 ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 mountd superuser
```

Si los daemons no se han iniciado, consulte [“Cómo reiniciar servicios NFS” en la página 128](#).

## 2 Compruebe que los procesos de `nfsd` del servidor estén activos.

En el cliente, escriba el siguiente comando para probar las conexiones UDP NFS desde el servidor.

```
% /usr/bin/rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

---

**Nota** – La versión 4 de NFS no admite UDP.

---

Si el servidor está en ejecución, se imprime una lista de programas y números de versión. Con la opción `-t` se prueba la conexión TCP. Si este comando falla, continúe con [“Cómo verificar el servicio NFS en el servidor” en la página 127](#).

## 3 Compruebe que `mountd` del servidor esté activo. Para ello escriba el siguiente comando.

```
% /usr/bin/rpcinfo -u bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
```

Si el servidor está en ejecución, se imprime una lista de programas y números de versión asociados con el protocolo UDP. Con la opción `-t` se prueba la conexión TCP. Si este intento falla, continúe con [“Cómo verificar el servicio NFS en el servidor” en la página 127](#).

## 4 Compruebe el servicio `autofs` local si está en uso:

```
% cd /net/wasp
```

Seleccione un punto de montaje `/net` o `/home` si sabe que debería funcionar correctamente. Si este comando falla, como `root` en el cliente, escriba lo siguiente para reiniciar el servicio `autofs`:

```
# svcadm restart system/filesystem/autofs
```

## 5 Verifique que el sistema de archivos se comparte como se espera en el servidor.

```
% /usr/sbin/showmount -e bee
/usr/src                               eng
/export/share/man                      (everyone)
```

Compruebe la entrada en el servidor y la entrada de montaje local en busca de errores. Compruebe también el espacio de nombres. En esta instancia, si el primer cliente no está en el grupo de red `eng`, ese cliente no puede montar el sistema de archivos `/usr/src`.

Compruebe todas las entradas que incluyan información de montaje en todos los archivos locales. La lista incluye `/etc/vfstab` y todos los archivos `/etc/auto_*`.

## ▼ Cómo verificar el servicio NFS en el servidor

### 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 \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

### 2 Compruebe que el servidor pueda acceder a los clientes.

```
# ping lilac
lilac is alive
```

### 3 Si no se puede acceder al cliente desde el servidor, asegúrese de que el servicio de nombres local esté en ejecución.

Para clientes NIS+, escriba lo siguiente:

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
Master server is eng-master.acme.com.
      Last update occurred at Mon Jun  5 11:16:10 1995

Replica server is eng1-replica-58.acme.com.
      Last Update seen was Mon Jun  5 11:16:10 1995
```

### 4 Si el servicio de nombres está en ejecución, compruebe la configuración de software de red en el servidor, por ejemplo, /etc/netmasks y /etc/nsswitch.conf.

### 5 Escriba el siguiente comando para comprobar si el daemon rpcbind está en ejecución.

```
# /usr/bin/rpcinfo -u localhost rpcbind
program 100000 version 1 ready and waiting
program 100000 version 2 ready and waiting
program 100000 version 3 ready and waiting
```

Si el servidor está en ejecución, se imprime una lista de programas y números de versión asociados con el protocolo UDP. Si parece que rpcbind se va a colgar, reinicie el servidor.

### 6 Escriba el siguiente comando para comprobar si el daemon nfsd está en ejecución.

```
# rpcinfo -u localhost nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
# ps -ef | grep nfsd
root    232      1  0 Apr 07      ?        0:01 /usr/lib/nfs/nfsd -a 16
root    3127    2462  1 09:32:57 pts/3    0:00 grep nfsd
```

---

**Nota** – La versión 4 de NFS no admite UDP.

---

Si el servidor está en ejecución, se imprime una lista de programas y números de versión asociados con el protocolo UDP. También utilice la opción `-t` con `rpcinfo` para comprobar la conexión TCP. Si estos comandos fallan, reinicie el servicio NFS. Consulte [“Cómo reiniciar servicios NFS” en la página 128](#).

**7 Escriba el siguiente comando para comprobar si el daemon `mountd` está en ejecución.**

```
# /usr/bin/rpcinfo -u localhost mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
# ps -ef | grep mountd
root    145      1 0 Apr 07 ?        21:57 /usr/lib/autofs/automountd
root    234      1 0 Apr 07 ?          0:04 /usr/lib/nfs/mountd
root   3084 2462 1 09:30:20 pts/3    0:00 grep mountd
```

Si el servidor está en ejecución, se imprime una lista de programas y números de versión asociados con el protocolo UDP. También utilice la opción `-t` con `rpcinfo` para comprobar la conexión TCP. Si estos comandos fallan, reinicie el servicio NFS. Consulte [“Cómo reiniciar servicios NFS” en la página 128](#).

## ▼ Cómo reiniciar servicios NFS

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Reinicie el servicio NFS en el servidor.**

Escriba el siguiente comando.

```
# svcadm restart network/nfs/server
```

## Identifique qué host proporciona servicio de archivos NFS

Ejecute el comando `nfsstat` con la opción `-m` para recopilar información NFS actual. El nombre del servidor actual se imprime después de `"currserver="`.

```
% nfsstat -m
/usr/local from bee,waspi:/export/share/local
Flags: vers=3,proto=tcp,sec=sys,hard,intr,llock,link,synlink,
      acl,rsize=32768,wsiz=32678,retrans=5
Failover: noresponse=0, failover=0, remap=0, currserver=bee
```



## ▼ Cómo verificar las opciones que se utilizan con el comando mount

No se emite ningún mensaje de advertencia para opciones no válidas. El siguiente procedimiento ayuda a determinar si las opciones que se suministraron en la línea de comandos o mediante `/etc/vfstab` eran válidas.

Para este ejemplo, suponga que el siguiente comando se ha ejecutado:

```
# mount -F nfs -o ro,vers=2 bee:/export/share/local /mnt
```

### 1 Verifique las opciones ejecutando el siguiente comando.

```
% nfsstat -m
/mnt from bee:/export/share/local
Flags: vers=2,proto=tcp,sec=sys,hard,intr,dynamic,acl,rsize=8192,wsiz=8192,
      retrans=5
```

El sistema de archivos de bee se ha montado con la versión de protocolo establecida en 2. Desafortunadamente, el comando `nfsstat` no muestra información de todas las opciones. Sin embargo, el uso del comando `nfsstat` es la manera más precisa de verificar las opciones.

### 2 Compruebe la entrada en `/etc/mnttab`.

El comando `mount` no permite que se agreguen opciones no válidas a la tabla de montaje. Por lo tanto, compruebe que las opciones que aparecen en el archivo coincidan con las opciones enumeradas en la línea de comandos. De este modo, puede comprobar las opciones que el comando `nfsstat` no informa.

```
# grep bee /etc/mnttab
bee:/export/share/local /mnt nfs ro,vers=2,dev=2b0005e 859934818
```

## Resolución de problemas autofs

Es posible que alguna vez encuentre problemas con autofs. Esta sección debería mejorar el proceso de resolución de problemas. La sección se divide en dos subsecciones.

En esta sección se presenta una lista de los mensajes de error que autofs genera. La lista se divide en dos partes:

- Mensajes de error generados por la opción (-v) detallada de automount
- Mensajes de error que pueden aparecer en cualquier momento

Cada mensaje de error va seguido de una descripción y posible causa del mensaje.

Al solucionar problemas, inicie los programas con la opción (-v) detallada. De lo contrario, es posible que encuentre problemas sin conocer la causa.

Los siguientes párrafos están etiquetados con el mensaje de error que posiblemente vea si autofs falla y una descripción del posible problema.

## Mensajes de error generados por automount - v

clave incorrecta *clave* en mapa directo *nombre de mapa*

**Descripción:** Mientras se exploraba un mapa directo, autofs encontró una clave de entrada sin un prefijo /.

**Solución:** Las claves en los mapas directos deben ser nombres de ruta completos.

clave incorrecta *clave* en mapa indirecto *nombre de mapa*

**Descripción:** Mientras se exploraba un mapa indirecto, autofs encontró una clave de entrada que contenía una /.

**Solución:** Las claves de mapas indirectos deben ser nombres simples, no nombres de ruta.

can't mount *servidor*: *nombre de ruta*: *motivo*

**Descripción:** El daemon de montaje en el servidor se rehúsa a proporcionar un identificador de archivos para *servidor*: *nombre de ruta*.

**Solución:** Compruebe la tabla de exportación en el servidor.

no ha sido posible crear un punto de montaje *punto de montaje*: *motivo*

**Descripción:** Autofs no ha podido crear un punto de montaje necesario para un montaje. Este problema se produce con más frecuencia cuando se intenta montar jerárquicamente todo de un sistema de archivos exportado del servidor.

**Solución:** Un punto de montaje necesario sólo puede existir en un sistema de archivos que no se puede montar, lo que significa que el sistema de archivos no se puede exportar. El punto de montaje no se puede crear porque el sistema de archivos principal exportado se exporta de sólo lectura.

leading space in map entry *entrada* texto en *nombre de mapa*

**Descripción:** Autofs ha detectado una entrada en un mapa de montador automático que contiene espacios iniciales. Este problema generalmente indica una entrada de mapa continuada de manera incorrecta. Por ejemplo:

```
fake
/blat          frobz:/usr/frotz
```

**Solución:** En este ejemplo, la advertencia se genera cuando autofs encuentra la segunda línea porque la primera línea debería terminar con una barra diagonal inversa (\).

*nombre de mapa*: no encontrado

**Descripción:** El mapa requerido no se puede ubicar. Este mensaje se produce sólo cuando se utiliza la opción -v.

**Solución:** Compruebe el nombre de ruta del nombre de mapa y que el nombre de mapa esté bien escrito.

*remount servidor: nombre de ruta en punto de montaje:* el servidor no responde

**Descripción:** Autofs no ha podido volver a montar un sistema de archivos que ha desmontado previamente.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

**ADVERTENCIA:** *punto de montaje* ya montado en

**Descripción:** Autofs intenta realizar un montaje sobre un punto de montaje existente. Este mensaje significa que se ha producido un error interno en autofs (una anomalía).

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

## Diversos mensajes de error

*dir punto de montaje* debe empezar con '/'

**Solución:** El punto de montaje del montador automático se debe proporcionar como un nombre de ruta completo. Compruebe el nombre de ruta del punto de montaje y que el punto de montaje esté bien escrito.

*hierarchical mountpoints: nombre de ruta 1 y nombre de ruta 2*

**Solución:** Autofs no permite que sus puntos de montaje tengan una relación jerárquica. Un punto de montaje autofs no debe estar contenido dentro de otro sistema de archivos montado automáticamente.

*el sistema servidor* no responde

**Descripción:** Autofs intentó ponerse en contacto con el *servidor*, pero no se recibió respuesta.

**Solución:** Compruebe el estado del servidor NFS.

*nombre de host: exportaciones: rpc-err*

**Descripción:** Se ha producido un error al obtener la lista de exportación desde *nombre de host*. Este mensaje indica un problema de red o de servidor.

**Solución:** Compruebe el estado del servidor NFS.

*mapa nombre de mapa, clave clave:* incorrecta

**Descripción:** La entrada de mapa está mal construida y autofs no puede interpretar la entrada.

**Solución:** Vuelva a revisar la entrada. Posiblemente la entrada tenga caracteres que deben escapar.

*nombre de mapa: nis err*

**Descripción:** Se ha producido un error al buscar una entrada en un mapa NIS. Este mensaje puede indicar problemas NIS.

**Solución:** Compruebe el estado del servidor NIS.

*montaje de servidor: nombre de ruta en punto de montaje: motivo*

**Descripción:** Autofs no se ha podido realizar un montaje. Esto puede indicar un problema de red o de servidor. La cadena *motivo* define el problema.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

*punto de montaje: no es un directorio*

**Descripción:** Autofs no se puede montarse a sí mismo en *punto de montaje* porque no es un directorio.

**Solución:** Compruebe el nombre de ruta del punto de montaje y que el punto de montaje esté bien escrito.

*nfscast: cannot send packet: motivo*

**Descripción:** Autofs no puede enviar un paquete de consulta a un servidor en una lista de ubicaciones de sistemas de archivos replicados. La cadena *motivo* define el problema.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

*nfscast: cannot receive reply: motivo*

**Descripción:** Autofs no puede recibir respuestas de ningún servidor de la lista de ubicaciones de sistemas de archivos replicados. La cadena *motivo* define el problema.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

*nfscast: select: motivo*

**Descripción:** Todos estos mensajes de error indican problemas cuando se intenta comprobar los servidores en busca de sistemas de archivos replicados. Este mensaje puede indicar problemas de red. La cadena *motivo* define el problema.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es extremadamente raro y no es sencillo solucionarlo.

pathconf: no info para *servidor: nombre de ruta*

**Descripción:** Autofs no ha podido obtener información pathconf para el nombre de ruta.

**Solución:** Consulte la página del comando man `fpathconf(2)`.

pathconf: *servidor*: el servidor no responde

**Descripción:** Autofs no puede ponerse en contacto con el daemon de montaje en *servidor* que proporciona la información a pathconf( ).

**Solución:** Evite utilizar la opción de montaje POSIX con este servidor.

## Otros errores con autofs

Si los archivos `/etc/auto*` tienen el conjunto de bits ejecutable, el montador automático intenta ejecutar los mapas, los cuales crean mensajes como los siguientes:

```
/etc/auto_home: +auto_home: not found
```

En esta situación, el archivo `auto_home` tiene permisos incorrectos. Cada entrada en el archivo genera un mensaje de error que es similar a este mensaje. Los permisos para el archivo se deberían restablecer escribiendo el siguiente comando:

```
# chmod 644 /etc/auto_home
```

## Mensajes de error NFS

En esta sección se muestra un mensaje de error seguido de una descripción de las condiciones que deberían provocar el error y al menos una solución.

Argumento incorrecto especificado con opción `index` - debe ser un archivo

**Solución:** Debe incluir un nombre de archivo con la opción `index`. No puede utilizar nombres de directorio.

No se puede establecer servicio NFS sobre `/dev/tcp`: problema de configuración de transporte

**Descripción:** Este mensaje se crea generalmente cuando la información de servicios en el espacio de nombres se ha actualizado. El mensaje también se puede informar para UDP.

**Solución:** Para solucionar este problema, debe actualizar los datos de servicios en el espacio de nombres.

Para NIS+, las entradas deberían aparecer de la siguiente manera:

```
nfsd nfsd tcp 2049 NFS server daemon
nfsd nfsd udp 2049 NFS server daemon
```

Para NIS y `/etc/services`, las entradas deberían aparecer de la siguiente manera:

```
nfsd    2049/tcp    nfs      # NFS server daemon
nfsd    2049/udp    nfs      # NFS server daemon
```

La opción `index` no se puede usar sin la opción `public`

**Solución:** Incluya la opción `public` con la opción `index` en el comando de uso compartido. Debe definir el identificador de archivos público para que la opción `index` funcione.

---

**Nota** – La versión Solaris 2.5.1 requería que el identificador de archivos público se estableciera mediante el uso del comando `share`. Una modificación en la versión Solaris 2.6 establece el identificador de archivos público para que sea `root ( / )` de manera predeterminada. Este mensaje de error ya no es relevante.

---

No se ha podido iniciar *daemon*: *error*

**Descripción:** Se muestra este mensaje si el daemon termina de forma anormal o si se produce un error de llamada del sistema. La cadena *error* define el problema.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es raro y no es sencillo solucionarlo.

No ha sido posible usar una gestión de archivos pública en respuesta a la solicitud del *servidor*

**Descripción:** Este mensaje se muestra si se especifica la opción `public` pero el servidor NFS no admite el identificador de archivos público. En esta situación, el montaje falla.

**Solución:** Para solucionar esta situación, intente la solicitud de montaje sin utilizar el identificador de archivos público o vuelva a configurar el servidor NFS para admitir el identificador de archivos público.

*daemon* ya está en ejecución con pid *pid*

**Descripción:** El daemon ya está en ejecución.

**Solución:** Si desea ejecutar una nueva copia, cierre la versión actual e inicie una nueva versión.

error de bloqueo *archivo de bloqueo*

**Descripción:** Este mensaje se muestra cuando el *archivo de bloqueo* que está asociado con un daemon no se puede bloquear correctamente.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es raro y no es sencillo solucionarlo.

error de comprobación *archivo de bloqueo: error*

**Descripción:** Este mensaje se muestra cuando el *archivo de bloqueo* que está asociado con un daemon no se puede abrir correctamente.

**Solución:** Póngase en contacto con Sun para obtener ayuda. Este mensaje de error es raro y no es sencillo solucionarlo.

AVISO: NFS3: conmutación por error de *host 1* a *host 2*

**Descripción:** Este mensaje se muestra en la consola cuando se produce una conmutación por error. El mensaje sólo tiene el fin de avisar.

**Solución:** No se necesita ninguna acción.

*nombre de archivo:* archivo demasiado grande

**Descripción:** Un cliente versión 2 de NFS intenta acceder a un archivo de más de 2 Gbytes.

**Solución:** Evite utilizar la versión 2 de NFS. Monte el sistema de archivos con la versión 3 o la versión 4. Además, consulte la descripción de la opción `no largefiles` en [“Opciones mount para sistemas de archivos NFS” en la página 160](#).

montaje: ... el servidor no responde: `RPC_PMAP_FAILURE - RPC_TIMED_OUT`

**Descripción:** El servidor que comparte el sistema de archivos que intenta montar está caído o no se puede acceder al mismo, en el nivel de ejecución equivocado, o su `rpcbind` está inactivo o colgado.

**Solución:** Espere que se reinicie el servidor. Si el servidor está colgado, reinicie el servidor.

montaje: ... el servidor no responde: `RPC_PROG_NOT_REGISTERED`

**Descripción:** La solicitud de montaje está registrada con `rpcbind`, pero el daemon de montaje NFS `mountd` no está registrado.

**Solución:** Espere que se reinicie el servidor. Si el servidor está colgado, reinicie el servidor.

montaje: ...no existe tal archivo o directorio

**Descripción:** El directorio remoto o el directorio local no existen.

**Solución:** Compruebe que los nombres de directorio estén bien escritos. Ejecute `ls` en ambos directorios.

montaje: ...: permiso denegado

**Descripción:** Es posible que el nombre de su equipo no esté en la lista de clientes o en el grupo de red que tiene permiso para acceder al sistema de archivos que intenta montar.

**Solución:** Use `showmount -e` para verificar la lista de acceso.

archivo NFS temporalmente no disponible en el servidor, reintentando ...

**Descripción:** Un servidor versión 4 de NFS puede delegar la gestión de un archivo a un cliente. Este mensaje indica que el servidor solicita una delegación para otro cliente que entra en conflicto con una solicitud de su cliente.

**Solución:** Esto se debe realizar antes de que el servidor pueda procesar la solicitud del cliente. Para obtener más información sobre delegación, consulte [“Delegación en NFS versión 4” en la página 190](#).

NFS fsstat no satisfactorio para servidor *nombre de host*: RPC: error de autenticación

**Descripción:** Este error puede ser provocado por muchas situaciones. Una de las situaciones más difíciles para la depuración es cuando este problema se produce porque un usuario está en demasiados grupos. Actualmente, un usuario no puede estar en más de 16 grupos si el usuario accede a los archivos mediante montajes NFS.

**Solución:** Existe una alternativa para los usuarios que necesitan estar en más de 16 grupos. Puede utilizar las listas de control de acceso a fin de proporcionar los privilegios de acceso necesarios.

montaje nfs: ignorando opción “-opción” no válida

**Descripción:** El indicador -opción no es válido.

**Solución:** Consulte la página del comando `man mount_nfs(1M)` para verificar la sintaxis requerida.

---

**Nota** – Este mensaje de error no aparece cuando ejecuta cualquier versión del comando `mount` que se incluye en una versión de Solaris 2.6 o posterior, o versiones anteriores con parches.

---

montaje nfs: NFS can't support “nolargefiles”

**Descripción:** Un cliente NFS intentó montar un sistema de archivos desde un servidor NFS mediante la opción -nolargefiles.

**Solución:** Los tipos de sistemas de archivos NFS no admiten esta opción.

montaje nfs: NFS V2 can't support “largefiles”

**Descripción:** El protocolo versión 2 de NFS no puede gestionar archivos de gran tamaño.

**Solución:** Debe utilizar la versión 3 o la versión 4 si se requiere acceso a archivos de gran tamaño.



servidor NFS *nombre de host* no responde, aún intentando

**Descripción:** Si los programas se cuelgan durante trabajos relacionados con los archivos, es posible que se haya producido un fallo en el servidor NFS. Este mensaje indica que el servidor NFS *nombre de host* está caído o que se ha producido un problema en el servidor o en la red.

**Solución:** Si se utiliza la conmutación por error, *nombre de host* es una lista de servidores. Comience con la resolución de problemas con [“Cómo comprobar la conectividad en un cliente NFS” en la página 124](#).

servidor NFS recuperándose

**Descripción:** Durante una parte del reinicio del servidor versión 4 de NFS, algunas operaciones no estaban permitidas. Este mensaje indica que el cliente espera que el servidor permita esta operación para continuar.

**Solución:** No se necesita ninguna acción. Espere que el servidor permita esta operación.

Permiso denegado

**Descripción:** Los comandos `ls -l`, `getfacl` y `setfacl` muestran este mensaje por los siguientes motivos:

- Si el usuario o grupo que existe en una entrada de lista de control de acceso (ACL) en un servidor versión 4 de NFS no puede asignarse a un usuario o grupo válido en un cliente versión 4 de NFS, el usuario no tiene autorización para leer la lista de control de acceso en el cliente.
- Si el usuario o grupo que existe en una entrada de lista de control de acceso que se establece en un cliente versión 4 de NFS no puede asignarse a un usuario o grupo válido en un servidor versión 4 de NFS, el usuario no tiene autorización para escribir o modificar una lista de control de acceso en el cliente.
- Si un cliente y un servidor versión 4 de NFS tienen valores NFSMAPID\_DOMAIN que no coinciden, la asignación de ID falla.

Para obtener más información, consulte [“ACL y nfsmapid en NFS versión 4” en la página 192](#).

**Solución:** Realice lo siguiente:

- Asegúrese de que todos los ID de usuario y de grupo en las entradas de ACL estén presentes en el cliente y en el servidor.
- Asegúrese de que el valor para NFSMAPID\_DOMAIN esté establecido correctamente en el archivo `/etc/default/nfs`. Para obtener más información, consulte [“Palabras clave para el archivo /etc/default/nfs” en la página 142](#).

Para determinar si algún usuario o grupo no se puede asignar en el servidor o en el cliente, utilice la secuencia de comandos que se proporciona en [“Comprobación de ID de usuario o de grupo sin asignar” en la página 193](#).

el puerto *número* en la URL de nfs no es el mismo que el puerto *número* en la opción de puerto

**Descripción:** El número de puerto que se incluye en la URL de NFS debe coincidir con el número de puerto que se incluye con la opción `-port` para montar. Si los números de puerto no coinciden, el montaje falla.

**Solución:** Cambie el comando para que los números de puerto sean idénticos o no especifique el número de puerto incorrecto. Normalmente, no es necesario especificar el número de puerto con la URL de NFS y también con la opción `-port`.

las réplicas deben tener la misma versión

**Descripción:** Para que la conmutación por error NFS funcione correctamente, los servidores NFS que son réplicas deben admitir la misma versión del protocolo NFS.

**Solución:** La ejecución de varias versiones no está permitida.

los montajes replicados deben ser de sólo lectura

**Descripción:** La conmutación por error no funciona en sistemas de archivos montados de sólo lectura. Montar el sistema de archivos de lectura-escritura aumenta la probabilidad de que un archivo cambie.

**Solución:** La conmutación por error NFS depende de si los sistemas de archivos son idénticos.

los montajes replicados no pueden ser soft

**Descripción:** Los montajes replicados requieren que espere antes de que se produzca la conmutación por error.

**Solución:** La opción `soft` requiere que el montaje falle inmediatamente cuando se inicia un tiempo de espera, para que no pueda incluir la opción `-soft` con un montaje replicado.

`share_nfs`: no es posible compartir más de un sistema de archivos con la opción `'public'`

**Solución:** Compruebe que el archivo `/etc/dfs/dfstab` tenga un solo sistema de archivos seleccionado para compartir con la opción `-public`. Sólo se puede establecer un identificador de archivos público por servidor, por lo tanto, sólo un sistema de archivos por servidor se puede compartir con esta opción.

**ADVERTENCIA:** no hay bloqueo de red en *nombre de host*: *ruta*: póngase en contacto con el administrador para instalar el cambio de servidor

**Descripción:** Un cliente NFS ha intentado sin éxito establecer una conexión con el administrador de bloqueo de red en un servidor NFS. En lugar de mostrar un error en el montaje, esta advertencia se genera para advertirle que el bloqueo no funciona.

**Solución:** Actualizar el servidor con una nueva versión del sistema operativo que proporciona soporte completo de administrador de bloqueo.

## Acceso a los sistemas de archivos de red (referencia)

---

En este capítulo se describen los comandos NFS, así como las distintas partes del entorno NFS y cómo estas partes trabajen juntas.

- “Archivos NFS” en la página 139
- “Daemons NFS” en la página 145
- “Comandos NFS” en la página 157
- “Comandos para resolución de problemas de NFS” en la página 175
- “NFS a través RDMA” en la página 181
- “Cómo funciona el servicio NFS” en la página 182
- “Mapas autofs” en la página 206
- “Cómo funciona autofs” en la página 212
- “Referencia de autofs” en la página 224

---

**Nota** – Si el sistema tiene zonas habilitadas y desea utilizar esta función en una zona no global, consulte la *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris* para obtener más información.

---

## Archivos NFS

Necesita varios archivos a fin de admitir actividades NFS en cualquier equipo. Muchos de estos archivos son ASCII, pero algunos de ellos son archivos de datos. La [Tabla 6–1](#) muestra estos archivos y sus funciones.

TABLA 6–1 Archivos NFS

Nombre de archivo	Función
/etc/default/autofs	Muestra información de configuración para el entorno autofs.
/etc/default/fs	Muestra el tipo de sistema de archivos predeterminado para sistemas de archivos locales.

TABLA 6-1 Archivos NFS (Continuación)

Nombre de archivo	Función
/etc/default/nfs	Muestra la información de configuración para <code>lockd</code> y <code>nfsd</code> . Para obtener más información, consulte “Palabras clave para el archivo <code>/etc/default/nfs</code> ” en la página 142 y la página del comando <code>man nfs(4)</code> .
/etc/default/nfslogd	Muestra la información de configuración para el daemon de registro del servidor NFS <code>nfslogd</code> .
/etc/dfs/dfstab	Muestra los recursos locales que se compartirán.
/etc/dfs/fstypes	Muestra los tipos de sistemas de archivos predeterminados para sistemas de archivos remotos.
/etc/dfs/sharetab	Muestra los recursos locales y remotos que se van a compartir. Consulte la página del comando <code>man sharetab(4)</code> . No edite este archivo.
/etc/mnttab	Muestra los sistemas de archivos montados actualmente, incluidos los directorios de montaje automático. Consulte la página del comando <code>man mnttab(4)</code> . No edite este archivo.
/etc/netconfig	Muestra los protocolos de transporte. No edite este archivo.
/etc/nfs/nfslog.conf	Muestra la información de configuración general para el registro del servidor NFS.
/etc/nfs/nfslogtab	Muestra información para el posprocesamiento del registro de <code>nfslogd</code> . No edite este archivo.
/etc/nfssec.conf	Muestra los servicios de seguridad de NFS.
/etc/rmtab	Muestra los sistemas de archivos montados remotamente por los clientes NFS. Consulte la página del comando <code>man rmtab(4)</code> . No edite este archivo.
/etc/vfstab	Define los sistemas de archivos que se montarán localmente. Consulte la página del comando <code>man vfstab(4)</code> .

La primera entrada en `/etc/dfs/fstypes` se suele utilizar como sistema de archivos predeterminado para sistemas de archivos remotos. Esta entrada define el sistema de archivos tipo NFS como valor predeterminado.

Sólo hay una entrada en `/etc/default/fs`: el tipo de sistema de archivos predeterminado para discos locales. Puede determinar los tipos de sistemas de archivos admitidos en un cliente o servidor comprobando los archivos en `/kernel/fs`.

## Archivo `/etc/default/autofs`

A partir de la versión Solaris 10, puede utilizar el archivo `/etc/default/autofs` para configurar su entorno autofs. En concreto, este archivo proporciona una manera adicional de configurar los comandos autofs y los daemons autofs. Las mismas especificaciones que se harían en la línea de comandos pueden hacerse en este archivo de configuración. No obstante, a diferencia de las especificaciones que se harían en la línea de comandos, este archivo conserva sus especificaciones, incluso si realiza una actualización del sistema operativo. Además, ya no es necesario que actualice los archivos de arranque críticos para garantizar que se conserve el comportamiento existente de su entorno autofs. Puede realizar sus especificaciones si proporciona valores para las siguientes palabras clave:

### `AUTOMOUNT_TIMEOUT`

Establece el tiempo durante el cual debe permanecer inactivo un sistema de archivos antes de que se desmonte el sistema en cuestión. Esta palabra clave equivale al argumento `-t` del comando `automount`. El valor predeterminado es 600.

### `AUTOMOUNT_VERBOSE`

Proporciona información acerca de los montajes y desmontajes de autofs, y otros eventos que no son esenciales. Esta palabra clave equivale al argumento `-v` de `automount`. El valor predeterminado es `FALSE`.

### `AUTOMOUNTD_VERBOSE`

Registra los mensajes de estado en la consola y es equivalente al argumento `-v` del daemon `automountd`. El valor predeterminado es `FALSE`.

### `AUTOMOUNTD_NOBROWSE`

Activa o desactiva la exploración en todos los puntos de montaje de autofs y es el equivalente del argumento `-n` para `automountd`. El valor predeterminado es `FALSE`.

### `AUTOMOUNTD_TRACE`

Amplía cada llamada de procedimiento remoto (RPC) y la muestra como una RPC ampliada o salida estándar. Esta palabra clave equivale al argumento `-T` de `automountd`. El valor predeterminado es 0. Los valores pueden oscilar entre 0 y 5.

### `AUTOMOUNTD_ENV`

Permite asignar diferentes valores a diversos entornos. Esta palabra clave equivale al argumento `-D` de `automountd`. La palabra clave `AUTOMOUNTD_ENV` se puede utilizar varias veces. No obstante, debe utilizar líneas independientes para cada asignación de entorno.

Para obtener más información, consulte las páginas del comando `man` para [automount\(1M\)](#) y [automountd\(1M\)](#). Para obtener información de procedimiento, consulte “[Cómo configurar su entorno autofs con el archivo `/etc/default/autofs`](#)” en la página 108.

## Palabras clave para el archivo `/etc/default/nfs`

En NFS versión 4, se pueden establecer las siguientes palabras clave en el archivo `/etc/default/nfs`. Estas palabras clave controlan los protocolos NFS utilizados por el cliente y el servidor.

### NFS\_SERVER\_VERSMIN

Establece la versión mínima del protocolo NFS que debe registrar y ofrecer el servidor. A partir de la versión Solaris 10, la versión predeterminada es 2. Otros valores válidos incluyen 3 o 4. Consulte [“Configuración de servicios NFS” en la página 96](#).

### NFS\_SERVER\_VERSMAX

Establece la versión máxima del protocolo NFS que debe registrar y ofrecer el servidor. A partir de la versión Solaris 10, la versión predeterminada es 4. Otros valores válidos incluyen 2 o 3. Consulte [“Configuración de servicios NFS” en la página 96](#).

### NFS\_CLIENT\_VERSMIN

Establece la versión mínima del protocolo NFS que debe utilizar el cliente NFS. A partir de la versión Solaris 10, la versión predeterminada es 2. Otros valores válidos incluyen 3 o 4. Consulte [“Configuración de servicios NFS” en la página 96](#).

### NFS\_CLIENT\_VERSMAX

Establece la versión máxima del protocolo NFS que debe utilizar el cliente NFS. A partir de la versión Solaris 10, la versión predeterminada es 4. Otros valores válidos incluyen 2 o 3. Consulte [“Configuración de servicios NFS” en la página 96](#).

### NFS\_SERVER\_DELEGATION

Controla si la función de delegación de la versión 4 de NFS está habilitada para el servidor. Si esta función está habilitada, el servidor intenta proporcionar delegaciones al cliente con NFS versión 4. De manera predeterminada, la delegación de servidor está habilitada. Para deshabilitar la delegación del servidor, consulte [“Cómo seleccionar diferentes versiones de NFS en un servidor” en la página 98](#). Para obtener más información, consulte [“Delegación en NFS versión 4” en la página 190](#).

### NFSMAPID\_DOMAIN

Establece un dominio común para clientes y servidores. Sustituye el comportamiento predeterminado de utilizar el nombre de dominio DNS local. Para obtener información sobre las tareas, consulte [“Configuración de servicios NFS” en la página 96](#). Asimismo, consulte [“Daemon nfsmapid” en la página 148](#).

## Archivo `/etc/default/nfslogd`

Este archivo define algunos de los parámetros que se utilizan al usar el registro del servidor NFS. Los siguientes parámetros se pueden definir.

**CYCLE\_FREQUENCY**

Determina el número de horas que deben transcurrir antes de que se realice el ciclo de los archivos de registro. El valor predeterminado es 24 h. Esta opción se utiliza para impedir que los archivos de registro alcancen un tamaño excesivo.

**IDLE\_TIME**

Define el número de segundos que el comando `nfslogd` debe estar suspendido antes de comprobar si hay más información en el archivo de memoria intermedia. Este parámetro también determina la frecuencia con que el archivo de configuración se comprueba. Este parámetro, junto con `MIN_PROCESSING_SIZE`, determina la frecuencia con la que el archivo de memoria intermedia se procesa. El valor predeterminado es de 300 s. El aumento de este número puede mejorar el rendimiento al reducir el número de comprobaciones.

**MAPPING\_UPDATE\_INTERVAL**

Especifica el número de segundos entre las actualizaciones de los registros de las tablas de asignación de identificador de archivo a ruta. El valor predeterminado es 86400 s o 1 d. Este parámetro ayuda a mantener las tablas de asignación de identificador de archivo a ruta actualizadas sin tener que actualizar continuamente las tablas.

**MAX\_LOGS\_PRESERVE**

Determina el número de archivos de registro que se van a guardar. El valor predeterminado es 10.

**MIN\_PROCESSING\_SIZE**

Establece el número mínimo de bytes que el archivo de memoria intermedia debe alcanzar antes de realizar el procesamiento y escribir en el archivo de registro. Este parámetro, junto con `IDLE_TIME`, determina la frecuencia en la que el archivo de memoria intermedia se procesa. El valor predeterminado es 524288 bytes. Al aumentar este número, puede mejorar el rendimiento ya que reduce el número de veces que el archivo de memoria intermedia se procesa.

**PRUNE\_TIMEOUT**

Selecciona el número de horas que deben transcurrir antes de que un registro de asignación de identificador de archivo a ruta caduque y pueda reducirse. El valor predeterminado es 168 h o 7 d.

**UMASK**

Especifica la máscara de creación del modo de archivo para los archivos de registro que se crean mediante `nfslogd`. El valor predeterminado es 0137.

## Archivo `/etc/nfs/nfslog.conf`

Este archivo define la ruta de acceso, los nombres de archivo y el tipo de registro que va a utilizar `nfslogd`. Cada definición se asocia a una *etiqueta*. Para iniciar el registro del servidor NFS, es necesario que identifique la *etiqueta* para cada sistema de archivos. La etiqueta global define los valores predeterminados. Puede utilizar los siguientes parámetros con cada etiqueta según sea necesario.

`defaultdir=ruta`

Especifica la ruta de acceso de directorio predeterminada para los archivos de registro. A menos que lo especifique de una forma diferente, el directorio predeterminado es `/var/nfs`.

`log=ruta/nombre de archivo`

Establece la ruta y el nombre de archivo para los archivos de registro. El valor predeterminado es `/var/nfs/nfslog`.

`fh table=ruta/nombre de archivo`

Selecciona la ruta de acceso y el nombre de archivo para los archivos de la base de datos de identificador de archivo a ruta. El valor predeterminado es `/var/nfs/fhtable`.

`buffer=ruta/nombre de archivo`

Determina la ruta de acceso y el nombre de archivo para los archivos de la memoria intermedia. El valor predeterminado es `/var/nfs/nfslog_workbuffer`.

`logformat=básico|ampliado`

Selecciona el formato que se debe utilizar al crear archivos de registro que pueda leer el usuario. El formato básico genera un archivo de registro que es similar a algunos daemons `ftpd`. El formato ampliado proporciona una vista más detallada.

Si la ruta de acceso no está especificada, se utiliza la ruta definida por `defaultdir`. También, puede sustituir `defaultdir` con una ruta absoluta.

Para identificar los archivos más fácilmente, colóquelos en directorios independientes. A continuación se muestra un ejemplo de los cambios que se necesitan.

```
% cat /etc/nfs/nfslog.conf
#ident "@(#)nfslog.conf      1.5      99/02/21 SMI"
#
.
.
# NFS server log configuration file.
#

global defaultdir=/var/nfs \
      log=nfslog fh table=fhtable buffer=nfslog_workbuffer

publicftp log=logs/nfslog fh table=fh/fhtables buffer=buffers/workbuffer
```

En este ejemplo, cualquier sistema de archivos que se comparte con `log=publicftp` utiliza los siguientes valores:

- El directorio por defecto es `/var/nfs`.
- Los archivos de registro se almacenan en `/var/nfs/logs/nfslog*`.
- Las tablas de la base de datos de identificador de archivo a ruta se almacenan en `/var/nfs/fh/fhtables`.
- Los archivos de memoria intermedia se almacenan en `/var/nfs/buffers/workbuffer`.



Para obtener información de procedimiento, consulte [“Cómo habilitar el inicio de sesión de servidor NFS” en la página 89](#).

## Daemons NFS

Para admitir las actividades NFS, varios daemons se inician cuando un sistema entra en el nivel de ejecución 3 o el modo multiusuario. Los daemons `mountd` y `nfsd` se ejecutan en sistemas que son servidores. El inicio automático de los daemons del servidor depende de la existencia de entradas etiquetadas con el tipo de sistema de archivos NFS en `/etc/dfs/sharetab`. Para admitir el bloqueo de archivos NFS, los daemons `lockd` y `statd` se ejecutan en los clientes y servidores NFS. Sin embargo, a diferencia de las versiones anteriores de NFS, en NFS versión 4, los daemons `lockd`, `statd`, `mountd` y `nfslogd` no se utilizan.

Esta sección describe los siguientes daemons.

- [“Daemon automountd” en la página 145](#)
- [“Daemon lockd” en la página 146](#)
- [“Daemon mountd” en la página 147](#)
- [“Daemon nfs4cbd” en la página 147](#)
- [“Daemon nfsd” en la página 147](#)
- [“Daemon nfslogd” en la página 148](#)
- [“Daemon nfsmapid” en la página 148](#)
- [“Daemon statd” en la página 156](#)

### Daemon automountd

Este daemon gestiona el montaje y desmontaje de las solicitudes del servicio autofs. La sintaxis del comando es la siguiente:

```
automountd [ -Tnv ] [ -D name= valor ]
```

El comando se comporta de las siguientes formas:

- `-T` habilita el seguimiento.
- `-n` deshabilita la exploración en todos los nodos de autofs.
- `-v` selecciona registrar todos los mensajes de estado en la consola.
- `-D nombre=valor` sustituye el *valor* por la variable de mapa de montaje automático que se indica mediante *nombre*.

El valor por defecto para el mapa de montaje automático es `/etc/auto_master`. Utilice la opción `-T` para la resolución de problemas.

## Daemon lockd

Este daemon admite las operaciones de bloqueo de registro en archivos NFS. El daemon lockd administra las conexiones RPC entre el cliente y el servidor para el protocolo de administrador de bloqueo de red (NLM). Normalmente, el daemon se inicia sin opciones. Con este comando puede utilizar tres opciones. Consulte la página del comando [man lockd\(1M\)](#). Estas opciones pueden utilizarse desde la línea de comandos o editando la cadena correspondiente en `/etc/default/nfs`. A continuación, se muestran descripciones de palabras clave que se pueden establecer en el archivo `/etc/default/nfs`.

---

**Nota** – A partir de la versión Solaris 10, la palabra clave `LOCKD_GRACE_PERIOD` y la opción `-g` se descartaron. La palabra clave descartada se sustituyó con la nueva palabra clave `GRACE_PERIOD`. Si se establecen ambas palabras clave, el valor para `GRACE_PERIOD` sustituirá el valor de `LOCKD_GRACE_PERIOD`. Consulte la descripción de `GRACE_PERIOD` que aparece a continuación.

---

Como `LOCKD_GRACE_PERIOD`, `GRACE_PERIOD=período_gracia` en `/etc/default/nfs` establece la cantidad de segundos que deben transcurrir después del reinicio de un servidor para que el cliente reclame los bloqueos de NFS versión 3, proporcionados por NLM, y los bloqueos de la versión 4. Por lo tanto, el valor para `GRACE_PERIOD` controla la duración del período de gracia para la recuperación del bloqueo, para las versiones 3 y 4 de NFS.

El parámetro `LOCKD_RETRANSMIT_TIMEOUT=tiempo_espera` en `/etc/default/nfs` selecciona la cantidad de segundos que se debe esperar antes de retransmitir una solicitud de bloqueo al servidor remoto. Esta opción afecta al servicio NFS por parte del cliente. El valor predeterminado para `tiempo_espera` es 15 s. Si disminuye el valor de `tiempo_espera`, puede mejorar el tiempo de respuesta para los clientes NFS en una red “con ruido”. Sin embargo, este cambio puede provocar una carga adicional del servidor al aumentar la frecuencia de solicitudes de bloqueo. El mismo parámetro se puede utilizar desde la línea de comandos iniciando el daemon con la opción `-t tiempo_espera`.

El parámetro `LOCKD_SERVERS=nthreads` en `/etc/default/nfs` especifica el número máximo de subprocesos simultáneos que el servidor maneja por conexión. Base el valor para `nthreads` en la carga que se espera para el servidor NFS. El valor predeterminado es 20. Cada cliente NFS que utiliza TCP utiliza una sola conexión con el servidor NFS. Por lo tanto, cada cliente puede utilizar un máximo de 20 subprocesos simultáneos en el servidor.

Todos los clientes NFS que utilizan UDP comparten una única conexión con el servidor NFS. En estas condiciones, puede que tenga que aumentar el número de subprocesos que están disponibles para la conexión UDP. Un cálculo mínimo sería permitir dos subprocesos para cada cliente UDP. Sin embargo, este número es específico para la carga de trabajo en el cliente, por lo que dos subprocesos por cliente podría no ser suficiente. La desventaja frente al uso de más subprocesos es que cuando se usan los subprocesos, se usa más memoria en el servidor NFS. Sin

embargo, si nunca se utilizan los subprocesos, aumentar *nthreads* no tiene ningún efecto. Se puede utilizar el mismo parámetro desde la línea de comandos al iniciar el daemon con la opción *nthreads*.

## Daemon mountd

Este daemon gestiona solicitudes de montaje de sistema de archivos desde sistemas remotos y proporciona control de acceso. El daemon *mountd* comprueba */etc/dfs/sharetab* para determinar qué sistemas de archivos están disponibles para el montaje remoto y qué sistemas están autorizados a hacer el montaje remoto. Puede utilizar la opción *-v* y la opción *-r* con este comando. Consulte la página del comando [man mountd\(1M\)](#).

La opción *-v* ejecuta el comando en modo detallado. Cada vez que un servidor NFS determina el acceso que se debe otorgar a un cliente, se imprime un mensaje en la consola. La información que se genera puede ser útil al intentar determinar por qué un cliente no puede acceder a un sistema de archivos.

La opción *-r* rechaza todas las solicitudes de montaje futuras de los clientes. Esta opción no afecta a los clientes que ya tienen un sistema de archivos montado.

---

**Nota** – La versión 4 de NFS no utiliza este daemon.

---

## Daemon nfs4cbd

*nfs4cbd*, que es para el uso exclusivo del cliente NFS versión 4, gestiona los puntos finales de comunicación para el programa de devolución de llamadas de NFS versión 4. El daemon no tiene ninguna interfaz accesible para el usuario. Para obtener más información, consulte la página del comando [man nfs4cbd\(1M\)](#).

## Daemon nfsd

Este daemon gestiona otras solicitudes de sistema de archivos de cliente. Con este comando puede utilizar varias opciones. Consulte la página del comando [man nfsd\(1M\)](#) para ver una lista completa. Estas opciones pueden utilizarse desde la línea de comandos o editando la cadena correspondiente en */etc/default/nfs*.

El parámetro *NFSD\_LISTEN\_BACKLOG=longitud* en */etc/default/nfs* ajusta la duración de la cola de conexión sobre transportes orientados a la conexión para NFS y TCP. El valor predeterminado es de 32 entradas. La misma selección se puede realizar desde la línea de comandos al iniciar *nfsd* con la opción *-l*.

El parámetro `NFSD_MAX_CONNECTIONS=#-conn` en `/etc/default/nfs` selecciona el número máximo de conexiones por transporte orientado a la conexión. El valor por defecto para `#-conn` es ilimitado. El mismo parámetro se puede utilizar desde la línea de comandos al iniciar el daemon con la opción `-c #-conn`.

El parámetro `NFSD_SERVER=nservers` en `/etc/default/nfs` selecciona el número máximo de solicitudes simultáneas que un servidor puede manejar. El valor predeterminado para `nservers` es 16. La misma selección se puede realizar desde la línea de comandos al iniciar `nfsd` con la opción `nservers`.

A diferencia de las versiones anteriores de este daemon, `nfsd` no reproduce varias copias para manejar solicitudes simultáneas. Al comprobar la tabla de procesos con `ps`, sólo se muestra una copia del daemon en ejecución.

## Daemon `nfslogd`

Este daemon proporciona el registro operativo. Las operaciones de NFS que se registran con un servidor están basadas en las opciones de configuración que se definen en `/etc/default/nfslogd`. Cuando el registro del servidor NFS está habilitado, el núcleo escribe en un archivo de memoria intermedia los registros de todas las operaciones de RPC en un sistema de archivos seleccionado. A continuación `nfslogd` realiza el posprocesamiento de estas solicitudes. El cambio de servicio de nombres se utiliza para ayudar a asignar UID a inicios de sesión y direcciones IP a nombres de host. Si no se puede encontrar ninguna coincidencia a través de los servicios de nombres identificados, el número se registra.

El comando `nfslogd` también se encarga de la asignación de los identificadores de archivo para los nombres de ruta. El daemon realiza un seguimiento de estas asignaciones en una tabla de asignaciones de identificador de archivo a ruta. Existe una tabla de asignaciones para cada etiqueta identificada en `/etc/nfs/nfslogd`. Después del procesamiento posterior, los registros se escriben en archivos de registro ASCII.

---

**Nota** – La versión 4 de NFS no utiliza este daemon.

---

## Daemon `nfsmapid`

La versión 4 del protocolo NFS (RFC3530) ha cambiado la forma en que los identificadores de usuarios o grupos (UID o GID) son intercambiados entre el cliente y el servidor. El protocolo exige que el cliente NFS versión 4 y el servidor NFS versión 4 intercambien los atributos de grupo y propietario de archivo como cadenas con el formato `usuario@nfsv4_domain` o `grupo@nfsv4_domain` respectivamente.

Por ejemplo, el usuario `known_user` tiene el UID 123456 en un cliente NFS versión 4 cuyo nombre de host completo es `system.example.com`. Para que el cliente pueda realizar solicitudes al servidor NFS versión 4, el cliente debe asignar el UID 123456 a `known_user@example.com` y, a

continuación, enviar este atributo al servidor NFS versión 4. El servidor NFS versión 4 espera recibir los atributos de archivo de grupo y usuario en el formato `user_or_group@nfsv4_domain`. Después de que el servidor recibe `known_user@example.com` desde el cliente, el servidor asigna la cadena al UID 123456 local, que es entendida por el sistema de archivos subyacente. Esta funcionalidad asume que cada UID y GID en la red es único y que los dominios NFS versión 4 en el cliente coinciden con los dominios NFS versión 4 en el servidor.

---

**Nota** – Si el servidor no reconoce el usuario o nombre de grupo determinado, incluso si el dominio NFS versión 4 coincide, el servidor no puede asignar el nombre de usuario o grupo con su ID exclusivo, un valor entero. En estas circunstancias, el servidor asigna el nombre de usuario o grupo entrante al usuario `nobody`. Para evitarlo, los administradores deben evitar la creación de cuentas especiales que sólo existan en el cliente NFS versión 4.

---

El cliente y el servidor NFS versión 4 son capaces de realizar conversiones de entero a cadena y de cadena a entero. Por ejemplo, en respuesta a una operación `GETATTR`, el servidor NFS versión 4 asigna los UID y GID obtenidos del sistema de archivos subyacente en sus respectivas representaciones en una cadena y envía esta información al cliente. Asimismo, el cliente debe también asignar los UID y GID a representaciones de cadenas. Por ejemplo, en respuesta al comando `chown`, el cliente asigna los nuevos UID o GID a una representación de cadena antes de enviar una operación `SETATTR` al servidor.

Tenga en cuenta, sin embargo, que el cliente y el servidor responden diferente ante cadenas no reconocidas:

- Si el usuario no existe en el servidor, incluso dentro de la misma configuración de dominio NFS versión 4, el servidor rechaza la llamada de procedimiento remoto (RPC) y devuelve un mensaje de error al cliente. Esta situación limita las operaciones que puede realizar el usuario remoto.
- Si el usuario existe en el cliente y en el servidor, pero los dominios no coinciden, el servidor rechaza las operaciones de modificación de atributo (por ejemplo, `SETATTR`) que necesitan que el servidor asigne la cadena de usuario entrante en un valor entero que el sistema de archivos subyacente pueda comprender. Para que los clientes y servidores NFS versión 4 funcionen adecuadamente, sus dominios NFS versión 4, la parte de la cadena después del signo @, deben coincidir.
- Si el cliente NFS versión 4 no reconoce un usuario o nombre de grupo obtenido del servidor, el cliente no puede asignar la cadena a su ID exclusivo, un valor de entero. En estas circunstancias, el cliente asigna la cadena de usuario o grupo entrante al usuario `nobody`. Esta asignación a `nobody` crea distintos problemas para aplicaciones diferentes. Para la funcionalidad NFS versión 4, fallarán las operaciones que modifican los atributos de archivo.

Puede cambiar el nombre de dominio de los clientes y servidores mediante el comando `sharectl` con la opción siguiente.

### `nfsmapid_domain`

Establece un dominio común para clientes y servidores. Sustituye el comportamiento predeterminado de utilizar el nombre de dominio DNS local. Para obtener información sobre las tareas, consulte [“Configuración de servicios NFS” en la página 96](#).

## Archivos de configuración y `nfsmapid`

A continuación se describe cómo el daemon `nfsmapid` utiliza los archivos `/etc/nsswitch.conf` y `/etc/resolv.conf`:

- `nfsmapid` utiliza funciones de biblioteca estándar de C para solicitar contraseña e información de grupo desde servicios de nombres en segundo plano. Estos servicios de nombres están controlados por los valores del archivo `/etc/nsswitch.conf`. Los cambios en el archivo `nsswitch.conf` afectan las operaciones `nfsmapid`. Para obtener más información acerca del archivo `nsswitch.conf`, consulte la página del comando `man nsswitch.conf(4)`.
- Para asegurarse de que los clientes NFS versión 4 sean capaces de montar sistemas de archivos de diferentes dominios, `nfsmapid` se basa en la configuración del registro de recursos DNS TXT (RR), `_nfsv4idmapdomain`. Para obtener más información sobre la configuración del registro de recursos `_nfsv4idmapdomain`, consulte [“Comando `nfsmapid` y registros DNS TXT” en la página 152](#). También, tenga en cuenta lo siguiente:
  - El DNS TXT RR debe estar configurado explícitamente en el servidor DNS con la información de dominio deseada.
  - El archivo `/etc/resolv.conf` debe estar configurado con los parámetros deseados a fin de habilitar el comando `resolver` para que encuentre el servidor DNS y busque en los registros TXT los dominios NFS versión 4 para el cliente y el servidor.

Para obtener más información, consulte lo siguiente:

- [“Reglas de precedencia” en la página 151](#)
- [“Configuración del dominio predeterminado NFS versión 4” en la página 153](#)
- Página del comando `man resolv.conf(4)`

## Reglas de precedencia

Para que `nfsmapid` funcione correctamente, los clientes y servidores NFS versión 4 deben tener el mismo dominio. Para garantizar la coincidencia de los dominios NFS versión 4, `nfsmapid` sigue estas estrictas reglas de precedencia:

1. El daemon primero comprueba el archivo `/etc/default/nfs` para ver si contiene un valor que se haya asignado a la palabra clave `NFSMAPID_DOMAIN`. Si se encuentra un valor, dicho valor asignado cobra importancia con respecto a cualquier otra preferencia. El valor asignado se anexa a las cadenas de atributos salientes y se compara con las cadenas de atributos entrantes. Para obtener más información sobre las palabras clave en el archivo `/etc/default/nfs`, consulte [“Palabras clave para el archivo `/etc/default/nfs`” en la página 142](#). Para obtener información de procedimiento, consulte [“Configuración de servicios NFS” en la página 96](#).

---

**Nota** – El uso de la configuración `NFSMAPID_DOMAIN` no es ampliable y no se recomienda para grandes implementaciones.

---

2. Si no se asignó ningún valor a `NFSMAPID_DOMAIN`, el daemon busca un nombre de dominio desde un DNS TXT RR. `nfsmapid` se basa en directivas en el archivo `/etc/resolv.conf` que son utilizadas por el conjunto de rutinas en el comando `resolver`. El comando `resolver` busca el TXT RR `_nfsv4idmapdomain` a través de los servidores DNS configurados. Tenga en cuenta que el uso de registros DNS TXT es más ampliable. Por este motivo, el uso continuo de los registros TXT se prefiere más que la definición de la palabra clave en el archivo `/etc/default/nfs`.

3. Si ningún registro DNS TXT se ha configurado para proporcionar un nombre de dominio, el daemon `nfsmapid` utiliza el valor especificado por las directivas `domain` o `search` en el archivo `/etc/resolv.conf`, y la directiva se especifica como la última precedencia.

En el ejemplo siguiente, donde se utilizan las directivas `domain` y `search`, el daemon `nfsmapid` utiliza el primer dominio que se muestra después de la directiva `search`, que es `company.com`.

```
domain example.company.com
search company.com foo.bar.com
```

4. Si el archivo `/etc/resolv.conf` no existe, `nfsmapid` obtiene el nombre del dominio NFS versión 4 siguiendo el comportamiento del comando `domainname`. En concreto, si el archivo `/etc/defaultdomain` existe, `nfsmapid` utiliza el contenido de dicho archivo para el dominio NFS versión 4. Si el archivo `/etc/defaultdomain` no existe, `nfsmapid` utiliza el nombre de dominio que ofrece el servicio de nombres configurado de la red. Para obtener más información, consulte la página del comando `man domainname(1M)`.

## Comando `nfsmapid` y registros DNS TXT

La naturaleza ubicua de DNS proporciona un almacenamiento eficiente y un mecanismo de distribución para el nombre de dominio NFS versión 4. Además, debido a la inherente escalabilidad de DNS, el uso de registros de recursos DNS TXT es el método preferido para configurar el nombre de dominio NFS versión 4 para grandes implementaciones. Debe configurar el registro TXT `_nfsv4idmapdomain` en los servidores DNS del nivel de la empresa. Dichas configuraciones aseguran que cualquier cliente o servidor NFS versión 4 pueda encontrar su dominio NFS versión 4 al atravesar el árbol DNS.

El siguiente es un ejemplo de una entrada preferida para habilitar el servidor DNS a fin de proporcionar el nombre de dominio NFS versión 4:

```
_nfsv4idmapdomain      IN      TXT      "foo.bar"
```

En este ejemplo, el nombre de dominio para configurar es el valor entre comillas dobles. Tenga en cuenta que no se especifica ningún campo `tTL` y que no se anexa ningún dominio a `_nfsv4idmapdomain`, que es el valor en el campo `owner`. Esta configuración permite que el registro TXT utilice la entrada `{ORIGEN}` de la zona del registro de inicio de autoridad (SOA). Por ejemplo, en diferentes niveles del espacio de nombres de dominio, el registro puede ser el siguiente:

```
_nfsv4idmapdomain.subnet.yourcorp.com.  IN      TXT      "foo.bar"
_nfsv4idmapdomain.yourcorp.com.         IN      TXT      "foo.bar"
```

Esta configuración proporciona a los clientes DNS la flexibilidad de utilizar el archivo `resolv.conf` para buscar hacia arriba en la jerarquía del árbol DNS. Consulte la página del comando `man resolv.conf(4)`. Esta capacidad proporciona una mayor probabilidad de encontrar el registro TXT. Para más flexibilidad, los subdominios de DNS de nivel inferior pueden definir sus propios registros de recursos DNS TXT (RR). Esta capacidad le permite a los subdominios DNS de nivel inferior sustituir el registro TXT definido por el dominio DNS de nivel superior.

---

**Nota** – El dominio que se especifica en el registro TXT puede ser una cadena arbitraria que no coincida necesariamente con el dominio DNS para los clientes y servidores que utilicen NFS versión 4. Tiene la opción de no compartir los datos de NFS versión 4 con otros dominios DNS.

---

## Comprobación del dominio NFS versión 4

Antes de asignar un valor para el dominio NFS versión 4 de la red, compruebe si un dominio NFS versión 4 ya se ha configurado para su red. Los siguientes ejemplos proporcionan formas de identificar los dominios NFS versión 4.

- Para identificar el dominio NFS versión 4 desde un DNS TXT RR, utilice los comandos `nslookup` o `dig`.

A continuación se proporciona un ejemplo de resultado del comando `nslookup`:



```
# nslookup -q=txt _nfsv4idmapdomain
Server:      10.255.255.255
Address:     10.255.255.255#53
```

```
_nfsv4idmapdomain.example.company.com text = "company.com"
```

Consulte este ejemplo de resultado para el comando dig:

```
# dig +domain=example.company.com -t TXT _nfsv4idmapdomain
...
;; QUESTION SECTION:
;_nfsv4idmapdomain.example.company.com. IN      TXT

;; ANSWER SECTION:
_nfsv4idmapdomain.example.company.com. 21600 IN TXT    "company.com"

;; AUTHORITY SECTION:
...
```

Para obtener información sobre la configuración de un DNS TXT RR, consulte [“Comando nsmapid y registros DNS TXT” en la página 152](#).

- Si la red no está configurada con un DNS TXT RR de NFS versión 4, utilice el siguiente comando para identificar el dominio NFS versión 4 del nombre de dominio DNS:

```
# egrep domain /etc/resolv.conf
domain example.company.com
```

- Si el archivo `/etc/resolv.conf` no está configurado para proporcionar un nombre de dominio DNS para el cliente, utilice el siguiente comando para identificar el dominio desde la configuración de dominio NFS versión 4 de la red:

```
# cat /var/run/nfs4_domain
company.com
```

- Si utiliza otro servicio de nombres, como NIS, utilice el siguiente comando para identificar el dominio para el servicio de asignación de nombres configurado para su red:

```
# domainname
it.example.company.com
```

Para obtener más información, consulte las páginas del comando man:

- [nslookup\(1M\)](#)
- [dig\(1M\)](#)
- [resolv.conf\(4\)](#)
- [domainname\(1M\)](#)

## Configuración del dominio predeterminado NFS versión 4

En esta sección se describe cómo la red obtiene el dominio predeterminado que desee:

- Para la mayoría de las versiones actuales, consulte [“Configuración de un dominio predeterminado NFS versión 4” en la página 154](#).
- Para la primera versión de Solaris 10, consulte [“Configuración de un dominio predeterminado NFS versión 4 en la versión Solaris 10” en la página 155](#).

## Configuración de un dominio predeterminado NFS versión 4

En la primera versión de Solaris 10, el dominio se definía durante el primer reinicio del sistema, después de instalar el SO. En versiones posteriores, el dominio NFS versión 4 se define durante la instalación del SO. Para proporcionar esta funcionalidad, se han agregado las siguientes funciones:

- El comando `sysidtool` incluye el programa `sysidnfs4`. Este programa se ejecuta durante el proceso de instalación para establecer si la red tiene configurado un dominio NFS versión 4. Consulte las páginas del comando `man sysidtool(1M)` y `sysidnfs4(1M)`.
- El archivo `sysidcfg` tiene una nueva palabra clave, `nfs4_domain`. Esta palabra clave se puede utilizar para definir el dominio NFS versión 4. Tenga en cuenta que otras palabras clave también se pueden definir en el archivo `sysidcfg`. Consulte la página del comando `man sysidcfg(4)`.

A continuación se describe cómo opera la funcionalidad:

1. El programa `sysidnfs4` comprueba el archivo `/etc/.sysIDtool.state` para determinar si se ha identificado un dominio NFS versión 4.
  - Si el archivo `.sysIDtool.state` muestra que un dominio NFS versión 4 se ha configurado para la red, el programa `sysidnfs4` no realiza controles complementarios. Vea el siguiente ejemplo de un archivo `.sysIDtool.state`:

```
1      # System previously configured?
1      # Bootparams succeeded?
1      # System is on a network?
1      # Extended network information gathered?
1      # Autobinder succeeded?
1      # Network has subnets?
1      # root password prompted for?
1      # locale and term prompted for?
1      # security policy in place
1      # NFSv4 domain configured
xterms
```

El 1 que aparece antes de `# NFSv4 domain configured` confirma que el dominio NFS versión 4 se ha configurado.

- Si el archivo `.sysIDtool.state` muestra que no se ha configurado ningún dominio NFS versión 4 para la red, el programa `sysidnfs4` debe hacer más comprobaciones. Vea el siguiente ejemplo de un archivo `.sysIDtool.state`:

```
1      # System previously configured?
1      # Bootparams succeeded?
1      # System is on a network?
1      # Extended network information gathered?
1      # Autobinder succeeded?
1      # Network has subnets?
1      # root password prompted for?
1      # locale and term prompted for?
1      # security policy in place
0      # NFSv4 domain configured
xterms
```

El 0 que aparece antes de # NFSv4 domain configured confirma que el dominio NFS versión 4 no se ha configurado.

2. Si no hay ningún dominio NFS versión 4 identificado, el programa sysidnfs4 comprueba la palabra clave nfs4\_domain en el archivo sysidcfg.
  - Si un valor para nfs4\_domain existe, ese valor se asigna a la palabra clave NFSMAPID\_DOMAIN en el archivo /etc/default/nfs. Tenga en cuenta que cualquier valor asignado a NFSMAPID\_DOMAIN sustituye la capacidad de selección de dominios dinámica del daemon nfsmapid. Para obtener más información sobre la capacidad de selección de dominios dinámica de nfsmapid, consulte [“Reglas de precedencia” en la página 151](#).
  - Si no hay ningún valor para nfs4\_domain, el programa sysidnfs4 identifica el dominio que nfsmapid deriva de los servicios de nombres configurados del sistema operativo. Este valor derivado se presenta como un dominio predeterminado en una solicitud interactiva que le ofrece la opción de aceptar el valor predeterminado o asignar otro dominio NFS versión 4.

Esta funcionalidad hace que lo siguiente sea obsoleto:

- La secuencia de comandos de ejemplo JumpStart, set\_nfs4\_domain, que se proporcionó en la distribución de medios inicial de Solaris 10 ya no es necesaria y se desaconseja.
- El archivo /etc/.NFS4inst\_state.domain, creado por la implementación anterior del programa sysidnfs4, ya no es necesario.

---

**Nota** – Debido a la inherente naturaleza ubicua y ampliable de DNS, el uso de registros DNS TXT para configurar el dominio de grandes implementaciones de NFS versión 4 sigue siendo la opción preferida y se recomienda encarecidamente. Consulte [“Comando nfsmapid y registros DNS TXT” en la página 152](#).

---

Para obtener información específica sobre el proceso de instalación de Solaris, consulte lo siguiente:

- [Guía de instalación de Oracle Solaris 10 9/10: instalaciones básicas](#)
- [Guía de instalación de Oracle Solaris 10 9/10: instalaciones basadas en red](#)

## Configuración de un dominio predeterminado NFS versión 4 en la versión Solaris 10

En la primera versión de Solaris 10 de NFS versión 4, si la red incluye varios dominios DNS, pero sólo tiene un solo espacio de nombre UID y GID, todos los clientes deben utilizar un valor para NFSMAPID\_DOMAIN. Para los sitios que usen DNS, nfsmapid resuelve este problema al obtener el nombre del dominio a partir del valor asignado a \_nfsv4idmapdomain. Para obtener más información, consulte [“Comando nfsmapid y registros DNS TXT” en la página 152](#). Si la

red no está configurada para usar DNS, durante el primer inicio del sistema, el SO usa la utilidad [sysidconfig\(1M\)](#) para proporcionar las siguientes solicitudes para un nombre de dominio de NFS versión 4:

```
This system is configured with NFS version 4, which uses a
domain name that is automatically derived from the system's
name services. The derived domain name is sufficient for most
configurations. In a few cases, mounts that cross different
domains might cause files to be owned by nobody due to the
lack of a common domain name.
```

```
Do you need to override the system's default NFS version 4 domain
name (yes/no)? [no]
```

La respuesta predeterminada es [no]. Si selecciona [no], puede ver lo siguiente:

For more information about how the NFS version 4 default domain name is derived and its impact, refer to the man pages for [nfsmapid\(1M\)](#) and [nfs\(4\)](#), and the System Administration Guide: Network Services.

Si selecciona [sí], verá esta solicitud:

```
Enter the domain to be used as the NFS version 4 domain name.
NFS version 4 domain name []:
```

---

**Nota** – Si un valor para NFSMAPID\_DOMAIN existe en `/etc/default/nfs`, el `[domain_name]` que proporcione sustituye ese valor.

---

## Información adicional sobre `nfsmapid`

Para obtener más información sobre `nfsmapid`, consulte lo siguiente:

- Página del comando `man nfsmapid(1M)`
- Página del comando `man nfs(4)`
- <http://www.ietf.org/rfc/rfc1464.txt>
- “ACL y `nfsmapid` en NFS versión 4” en la página 192

## Daemon `statd`

Este daemon trabaja con `lockd` para proporcionar funciones de bloqueo y recuperación para el administrador de bloqueo. El daemon `statd` realiza un seguimiento de los clientes que mantienen bloqueos en un servidor NFS. Si un servidor se bloquea, al reiniciar `statd` en el servidor, se contacta `statd` en el cliente. El cliente `statd` entonces puede intentar reclamar cualquier bloqueo en el servidor. El cliente `statd` también informa al servidor `statd` cuando un cliente se ha bloqueado a fin de que se puedan borrar los bloqueos del cliente en el servidor. No tiene opciones para seleccionar con este daemon. Para obtener más información, consulte la página del comando `man statd(1M)`.

En la versión 7 de Solaris, se ha mejorado la forma en la que `statd` realiza un seguimiento de los clientes. En todas las versiones anteriores de Solaris, `statd` creaba archivos en `/var/statmon/sm` para cada cliente mediante el nombre de host no completo del cliente. Esta nomenclatura de archivos causaba problemas si disponía de dos clientes en diferentes dominios que compartían un nombre de host o si los clientes no residían en el mismo dominio que el servidor NFS. Como el nombre de host no completo sólo contiene el nombre de host, sin ningún dominio ni información de dirección IP, la versión anterior de `statd` no tenía forma de diferenciar entre estos tipos de clientes. Para solucionar este problema, `statd` de Solaris 7 crea un enlace simbólico en `/var/statmon/sm` al nombre de host no completo mediante la dirección IP del cliente. El nuevo enlace se parece a lo siguiente:

```
# ls -l /var/statmon/sm
lrwxrwxrwx 1 daemon      11 Apr 29 16:32 ipv4.192.168.255.255 -> myhost
lrwxrwxrwx 1 daemon      11 Apr 29 16:32 ipv6.fec0::56:a00:20ff:feb9:2734 -> v6host
--w----- 1 daemon      11 Apr 29 16:32 myhost
--w----- 1 daemon      11 Apr 29 16:32 v6host
```

En este ejemplo, el nombre del host del cliente es `myhost` y la dirección IP del cliente es `192.168.255.255`. Si otro host con el nombre `myhost` estaba montando un sistema de archivos, dos enlaces simbólicos darían lugar al nombre del host.

---

**Nota** – La versión 4 de NFS no utiliza este daemon.

---

## Comandos NFS

Para ser completamente eficaces, estos comandos se deben ejecutar como `root`, aunque las solicitudes para obtener información pueden ser realizadas por todos los usuarios:

- “Comando `automount`” en la página 158
- “Comando `clear_locks`” en la página 158
- “Comando `fsstat`” en la página 159
- “Comando `mount`” en la página 159
- “Comando `mountall`” en la página 166
- “Comando `setmnt`” en la página 175
- “Comando `share`” en la página 167
- “Comando `shareall`” en la página 173
- “Comando `showmount`” en la página 174
- “Comando `umount`” en la página 165
- “Comando `umountall`” en la página 167
- “Comando `unshare`” en la página 172
- “Comando `unshareall`” en la página 173

## Comando automount

Este comando instala puntos de montaje autofs y asocia la información de los archivos automaster con cada punto de montaje. La sintaxis del comando es la siguiente:

```
automount [ -t duración ] [ -v ]
```

-t *duración* establece el tiempo, en segundos, que un sistema de archivos permanece montado, y -v selecciona el modo detallado. La ejecución de este comando en modo detallado facilita la resolución de problemas.

Si no se ha definido específicamente, el valor de duración se define en 5 minutos. En la mayoría de los casos, este valor es bueno. Sin embargo, en los sistemas que tienen varios sistemas de montaje automático, es posible que necesite aumentar el valor de duración. En concreto, si un servidor tiene muchos usuarios activos, la comprobación de los sistemas de archivos de montaje automático cada 5 minutos puede ser ineficaz. Comprobar los sistemas de archivos autofs cada 1800 s, es decir, cada 30 min, puede ser mejor. Si no se desmontan los sistemas de archivos cada 5 m, /etc/mnttab puede llegar a ser grande. Para reducir la salida cuando df comprueba cada entrada de /etc/mnttab, puede filtrar la salida de df mediante la opción -F (consulte la página del comando [man df\(1M\)](#)) o mediante egrep.

Debe tener en cuenta que al ajustar la duración también cambia la rapidez con que se reflejan los cambios en los mapas del montador automático. Los cambios no se pueden ver hasta que se desmonte el sistema de archivos. Consulte [“Modificación de los mapas” en la página 110](#) para obtener instrucciones sobre cómo modificar los mapas del montador automático.

## Comando clear\_locks

Este comando permite eliminar todos los bloqueos compartidos, de archivos y de registros de un cliente NFS. Debe ser root para ejecutar este comando. Desde un servidor NFS, puede borrar los bloqueos de un cliente específico. Desde un cliente NFS, puede borrar los bloqueos para ese cliente en un servidor específico. El ejemplo siguiente borraría los bloqueos del cliente NFS que se denomina tulip en el sistema actual.

```
# clear_locks tulip
```

Mediante la opción -s, puede especificar de qué host NFS eliminar los bloqueos. Debe ejecutar esta opción desde el cliente NFS que creó los bloqueos. En esta situación, los bloqueos del cliente se eliminarían del servidor NFS que se denomina bee.

```
# clear_locks -s bee
```



**Precaución** – Este comando sólo se debe ejecutar cuando un cliente se bloquea y no es posible eliminar sus bloqueos. Para evitar problemas de corrupción de datos, no borre los bloqueos de un cliente activo.

## Comando fsstat

A partir de Solaris 10 11/06, la utilidad `fsstat` le permite supervisar las operaciones de sistema de archivos por tipo de sistema de archivos y por punto de montaje. Diversas opciones le permiten personalizar la salida. Observe los ejemplos siguientes.

Este ejemplo muestra la salida para NFS versión 3, versión 4 y el punto de montaje `root`.

```
% fsstat nfs3 nfs4 /
new      name      name      attr      attr      lookup    rddir     read      read      write     write
file     remov  chng      get       set       ops       ops       ops      bytes     ops      bytes
3.81K    90      3.65K    5.89M    11.9K     35.5M    26.6K    109K    118M    35.0K    8.16G   nfs3
759      503     457     93.6K    1.44K     454K     8.82K    65.4K    827M    292     223K   nfs4
25.2K    18.1K   1.12K    54.7M    1017     259M     1.76M    22.4M    20.1G    1.43M    3.77G   /
```

En este ejemplo se utiliza la opción `-i` para proporcionar estadísticas sobre las operaciones de E/S de NFS versión 3, versión 4 y del punto de montaje `root`.

```
% fsstat -i nfs3 nfs4 /
read      read      write     write     rddir     rddir     rwlock    rwulock
ops      bytes     ops      bytes     ops      bytes     ops      ops
109K     118M     35.0K    8.16G    26.6K    4.45M     170K     170K    nfs3
65.4K    827M     292     223K     8.82K    2.62M     74.1K    74.1K   nfs4
22.4M    20.1G    1.43M    3.77G    1.76M    3.29G     25.5M    25.5M   /
```

En este ejemplo se utiliza la opción `-n` para proporcionar estadísticas sobre las operaciones de nomenclatura de NFS versión 3, versión 4 y del punto de montaje `root`.

```
% fsstat -n nfs3 nfs4 /
lookup    creat     remov    link      renam     mkdir     rmdir     rddir     symlink  rdlnk
35.5M     3.79K    90       2         3.64K     5         0         26.6K    11       136K   nfs3
454K      403     503      0         101       0         0         8.82K    356     1.20K   nfs4
259M      25.2K   18.1K    114      1017     10        2         1.76M    12      8.23M   /
```

Para obtener más información, consulte la página del comando `man fsstat(1M)`.

## Comando mount

Con este comando, se puede adjuntar un sistema de archivos con nombre, ya sea local o remoto, para un punto de montaje específico. Para obtener más información, consulte la página del comando `man mount(1M)`. Si se utiliza sin argumentos, `mount` muestra una lista de los sistemas de archivos montados actualmente en el equipo.

En la instalación estándar de Solaris, se incluyen muchos tipos de sistemas de archivos. Cada tipo de sistema de archivos tiene una página del comando `man` específica que muestra las opciones de `mount` adecuadas para ese tipo de sistema de archivos. La página del comando `man` para los sistemas de archivos NFS es `mount_nfs(1M)`. En los sistemas de archivos UFS, consulte `mount_ufs(1M)`.

La versión 7 de Solaris incluye la posibilidad de seleccionar un nombre de ruta para montar desde un servidor NFS utilizando una URL de NFS en lugar de la sintaxis `server:/pathname` estándar. Consulte “[Cómo montar un sistema de archivos NFS utilizando una URL de NFS](#)” en la [página 95](#) para obtener más información.



---

**Precaución** – La versión del comando `mount` no advierte acerca de opciones no válidas. El comando ignora sin notificación las opciones que no es posible interpretar. Asegúrese de verificar todas las opciones que se han utilizado a fin de poder prevenir comportamientos inesperados.

---

## Opciones `mount` para sistemas de archivos NFS

El siguiente texto muestra algunas de las opciones que puede seguir el indicador `-o` cuando está montando un sistema de archivos de NFS. Para obtener una lista completa de las opciones, consulte la página del comando `manmount_nfs(1M)`.

### `bg|fg`

Puede usar estas opciones para seleccionar el comportamiento de reintento en caso de que falle el montaje. La opción `bg` hace que los intentos de montaje se ejecuten en segundo plano. La opción `fg` hace que el intento de montaje se ejecute en primer plano. El valor predeterminado es `fg`, que es la mejor selección para los sistemas de archivos que deben estar disponibles. Esta opción impide otro procesamiento hasta que el montaje se haya completado. La opción `bg` es una buena selección para sistemas de archivos no críticos porque el cliente puede realizar otros procesos mientras espera que se complete la solicitud de montaje.

### `forcedirectio`

Esta opción mejora el rendimiento de las transferencias de datos secuenciales de gran tamaño. Los datos se copian directamente en la memoria intermedia de un usuario. No se realiza almacenamiento en antememoria en el núcleo del cliente. Esta opción está desactivada de manera predeterminada.

Anteriormente, todas las solicitudes de escritura se trataban en serie tanto en el cliente como en el servidor NFS. El cliente NFS se ha modificado para permitir que una aplicación emita escrituras simultáneas, así como escrituras y lecturas simultáneas, a un único archivo. Se puede habilitar esta funcionalidad en el cliente mediante la opción de montaje `forcedirectio`. Al utilizar esta opción, habilita la funcionalidad para todos los archivos dentro del sistema de archivos montado. También puede habilitar esta funcionalidad en un único archivo del cliente mediante la interfaz `directio()`. A menos que haya habilitado esta



funcionalidad, las escrituras a los archivos se serializan. Además, si hay escrituras o escrituras y lecturas simultáneas, la semántica de POSIX deja de admitirse en ese archivo.

Para ver un ejemplo de cómo utilizar esta opción, consulte [“Uso del comando mount” en la página 163](#).

largefiles

Con esta opción, puede acceder a los archivos que tienen un tamaño superior a 2 Gbytes. El hecho de que pueda accederse a un archivo grande sólo se puede controlar en el servidor, así que esta opción se ignora sin notificación en los montajes de NFS versión 3. De manera predeterminada, todos los sistemas de archivos UFS se montan con la opción `largefiles`. Para montajes que utilizan el protocolo NFS versión 2, la opción `largefiles` hace el montaje falle y se produzca un error.

nolargefiles

Esta opción para los montajes UFS garantiza que no haya archivos de gran tamaño en el sistema de archivos. Consulte la página del comando `man mount_ufs(1M)`. Como la existencia de archivos grandes sólo puede controlarse en el servidor NFS, ninguna opción para `nolargefiles` existe al utilizar montajes NFS. Los intentos de realizar un montaje NFS con un sistema de archivos mediante esta opción se rechazan y se produce un error.

nosuid|suid

A partir de la versión Solaris 10, la opción `nosuid` es el equivalente de especificar la opción `nodevices` con la opción `nosetuid`. Cuando la opción `nodevices` se especifica, no se permite la apertura de archivos especiales del dispositivo en el sistema de archivos montado. Cuando se especifica la opción `nosetuid`, se ignoran el bit `setuid` y el bit `setgid` en archivos binarios que se encuentran en el sistema de archivos. Los procesos se ejecutan con los privilegios del usuario que ejecuta el archivo binario.

La opción `suid` es el equivalente de especificar la opción `devices` con la opción `setuid`. Cuando la opción `devices` se especifica, se permite la apertura de archivos especiales del dispositivo en el sistema de archivos montado. Cuando la opción `setuid` se especifica, el núcleo respeta el bit `setuid` y el bit `setgid` en los archivos binarios que se encuentran en el sistema de archivos.

Si no se especifica ninguna opción, la opción predeterminada es `suid`, que proporciona el comportamiento predeterminado para especificar la opción `devices` con la opción `setuid`.

La tabla siguiente describe el efecto de combinar `nosuid` o `suid` con `devices` o `nodevices` y `setuid` o `nosetuid`. Tenga en cuenta que en cada combinación de opciones, la opción más restrictiva determina el comportamiento.

Comportamiento de opciones combinadas	Opción	Opción	Opción
El equivalente de <code>nosetuid</code> con <code>nodevices</code>	<code>nosuid</code>	<code>nosetuid</code>	<code>nodevices</code>

Comportamiento de opciones combinadas	Opción	Opción	Opción
El equivalente de nosetuid con nodevices	nosuid	nosetuid	devices
El equivalente de nosetuid con nodevices	nosuid	setuid	nodevices
El equivalente de nosetuid con nodevices	nosuid	setuid	devices
El equivalente de nosetuid con nodevices	suid	nosetuid	nodevices
El equivalente de nosetuid con devices	suid	nosetuid	devices
El equivalente de setuid con nodevices	suid	setuid	nodevices
El equivalente de setuid con devices	suid	setuid	devices

La opción `nosuid` proporciona seguridad adicional para clientes NFS que accedan a servidores potencialmente no confiables. El montaje de sistemas de archivos remotos con esta opción reduce las posibilidades de escalonamiento de privilegios a través de la importación de dispositivos no confiables o la importación de archivos binarios `setuid` no confiables. Todas estas opciones están disponibles en todos los sistemas de archivos de Solaris.

public

Esta opción fuerza el uso del identificador de archivos público para ponerse en contacto con el servidor NFS. Si el identificador de archivos público es admitido por el servidor, la operación de montaje es más rápida debido a que el protocolo MOUNT no se utiliza. Además, como el protocolo MOUNT no se utiliza, la opción `public` permite que el montaje se produzca a través de un cortafuegos.

rw|ro

Las opciones `-rw` y `-ro` indican si un sistema de archivos debe ser montado en el modo de sólo lectura o en el modo de lectura y escritura. La opción predeterminada es el modo de lectura y escritura, que es la opción apropiada para los directorios principales remotos, los directorios de correo y trabajos en cola, u otros sistemas de archivos que deben ser cambiados por los usuarios. La opción de sólo lectura es adecuada para los directorios que no deben ser cambiados por los usuarios. Por ejemplo, los usuarios no deben poder escribir en las copias compartidas de las páginas del comando `man`.

sec=modo

Puede utilizar esta opción para especificar el mecanismo de autenticación que se va a utilizar durante la transacción de montaje. El valor para *modo* puede ser uno de los siguientes.

- Use `krb5` para el servicio de autenticación de la versión 5 de Kerberos.
- Use `krb5i` para la versión 5 de Kerberos con integridad.
- Use `krb5p` para la versión 5 de Kerberos con privacidad.
- Use `none` para que no haya ninguna autenticación.
- Use `dh` para la autenticación Diffie-Hellman (DH).
- Use `sys` para la autenticación UNIX estándar.

Los modos también se definen en `/etc/nfssec.conf`.

#### `soft|hard`

Un sistema de archivos NFS montado con la opción `soft` devuelve un error si el servidor no responde. La opción `hard` hace que el montaje siga intentando hasta que el servidor responda. El valor predeterminado es `hard`, que debe ser utilizado por la mayoría de los sistemas de archivos. Las aplicaciones no comprueban con frecuencia los valores devueltos de los sistemas de archivos montados con `soft`, lo que puede hacer que la aplicación falle o puede ocasionar que se dañen archivos. Si la aplicación no comprueba los valores de devolución, los problemas de enrutamiento y otras condiciones pueden confundir a la aplicación o hacer que un archivo se dañe si se utiliza la opción `soft`. En la mayoría de las situaciones, la opción `soft` no debe utilizarse. Si un sistema de archivos se monta utilizando la opción `hard` y deja de estar disponible, las aplicaciones que utilizan este sistema de archivos se bloquean hasta que el sistema de archivos esté disponible.

## Uso del comando `mount`

Consulte los ejemplos siguientes.

- En NFS versión 2 o versión 3, estos dos comandos se montan en un sistema de archivos NFS desde el servidor `bee` de sólo lectura.

```
# mount -F nfs -r bee:/export/share/man /usr/man
```

```
# mount -F nfs -o ro bee:/export/share/man /usr/man
```

En la versión 4 de NFS, la siguiente línea de comandos lograría el mismo montaje.

```
# mount -F nfs -o vers=4 -r bee:/export/share/man /usr/man
```

- En NFS versión 2 o 3, este comando utiliza la opción `-O` para forzar las páginas del comando `man` desde el servidor `bee` para montar en el sistema local incluso si `/usr/man` ya se ha montado. Vea lo siguiente.

```
# mount -F nfs -O bee:/export/share/man /usr/man
```

En la versión 4 de NFS, la siguiente línea de comandos lograría el mismo montaje.

```
# mount -F nfs -o vers=4 -O bee:/export/share/man /usr/man
```

- En NFS versión 2 o 3, este comando utiliza la conmutación por error de cliente.

```
# mount -F nfs -r bee,waspl:/export/share/man /usr/man
```

En NFS versión 4, la siguiente línea de comandos utiliza la conmutación por error de cliente.

```
# mount -F nfs -o vers=4 -r bee:/export/share/man /usr/man
```

---

**Nota** – Cuando se utilizan desde la línea de comandos, los servidores que aparecen deben admitir la misma versión del protocolo NFS. No utilice al mismo tiempo servidores versión 2 y versión 3 cuando ejecute mount desde la línea de comandos. Puede utilizar los dos servidores con autofs. Autofs selecciona automáticamente el mejor subconjunto de servidores versión 2 o 3.

---

- A continuación se muestra un ejemplo del uso de una URL NFS con el comando mount en NFS versión 2 o versión 3.

```
# mount -F nfs nfs://bee//export/share/man /usr/man
```

A continuación se muestra un ejemplo del uso de una URL de NFS con el comando mount en NFS versión 4.

```
# mount -F nfs -o vers=4 nfs://bee//export/share/man /usr/man
```

- Utilice la opción de montaje `forcedirectio` a fin de habilitar al cliente para permitir escrituras simultáneas, así como escrituras y lecturas simultáneas, en un archivo. A continuación le mostramos un ejemplo.

```
# mount -F nfs -o forcedirectio bee:/home/somebody /mnt
```

En este ejemplo, el comando monta un sistema de archivos NFS desde el servidor bee y permite escrituras y lecturas simultáneas para cada archivo en el directorio `/mnt`. Cuando la compatibilidad con escrituras y lecturas simultáneas está habilitada, se produce lo siguiente.

- El cliente permite que las aplicaciones escriban en un archivo en paralelo.
- El almacenamiento en antememoria está deshabilitado en el cliente. Por lo tanto, los datos de las lecturas y escrituras se mantienen en el servidor. Más explícitamente, como el cliente no almacena en la antememoria los datos leídos o escritos, cualquier dato que la aplicación no haya almacenado en la antememoria para sí misma se lee desde el servidor. El sistema operativo del cliente no tiene una copia de estos datos. Normalmente, el cliente NFS almacena en la antememoria los datos en el núcleo para que utilicen las aplicaciones.

Como el almacenamiento en la antememoria está desactivado en el cliente, los procesos de lectura anticipada y escritura retrasada están deshabilitados. Un proceso de lectura avanzada se produce cuando el núcleo anticipa los datos que es posible que una aplicación solicite a continuación. Entonces, el núcleo inicia el proceso de recopilación de los datos anticipadamente. El objetivo del núcleo es tener los datos preparados antes de que la aplicación solicite los datos.

El cliente utiliza el proceso de escritura retrasada a fin de aumentar el rendimiento de escritura. En lugar de iniciar inmediatamente una operación de E/S cada vez que una aplicación escribe los datos en un archivo, los datos se almacenan en la antememoria. Más tarde, los datos se escriben en el disco.

Potencialmente, el proceso de escritura retrasada permite que los datos se escriban en fragmentos mayores o que se escriban de forma asíncrona desde la aplicación. Normalmente, el resultado de la utilización de fragmentos mayores es un mayor rendimiento. La escritura asíncrona permite la superposición de procesamiento de aplicaciones y procesamiento de E/S. Además, la escritura asíncrona permite que el subsistema de almacenamiento optimice la E/S al proporcionar una mejor secuenciación de la E/S. Las escrituras síncronas fuerzan una secuencia de E/S en el subsistema de almacenamiento que puede no ser es óptima.

- Puede ocurrir una degradación importante del rendimiento si la aplicación no está preparada para manejar la semántica de los datos que no se almacenan en la antememoria. Las aplicaciones multiprocesamiento evitan este problema.

---

**Nota** – Si no está habilitada la compatibilidad con escrituras simultáneas, todas las solicitudes de escritura se serializan. Cuando las solicitudes se serializan, se produce lo siguiente. Cuando una solicitud de escritura está en curso, si hay una segunda solicitud de escritura, ésta tiene que esperar a que finalice la primera antes de continuar.

---

- Utilice el comando `mount` sin argumentos para mostrar los sistemas de archivos montados en un cliente. Vea lo siguiente.

```
% mount
/ on /dev/dsk/c0t3d0s0 read/write/setuid on Wed Apr 7 13:20:47 2004
/usr on /dev/dsk/c0t3d0s6 read/write/setuid on Wed Apr 7 13:20:47 20041995
/proc on /proc read/write/setuid on Wed Apr 7 13:20:47 2004
/dev/fd on fd read/write/setuid on Wed Apr 7 13:20:47 2004
/tmp on swap read/write on Wed Apr 7 13:20:51 2004
/opt on /dev/dsk/c0t3d0s5 setuid/read/write on Wed Apr 7 13:20:51 20041995
/home/kathys on bee:/export/home/bee7/kathys
intr/nosuid/nosuid/remote on Wed Apr 24 13:22:13 2004
```

## Comando umount

Este comando le permite eliminar un sistema de archivos remoto que esté montando en la actualidad. El comando `umount` es compatible con la opción `-V` para permitir la realización de pruebas. También puede utilizar la opción `-a` para desmontar varios sistemas de archivos a la vez. Si se incluyen *puntos de montaje* con la opción `-a`, los sistemas de archivos se desmontan. Si no hay puntos de montaje incluidos, se realiza un intento de desmontar todos los sistemas de archivos que aparecen en `/etc/mnttab`, excepto los sistemas de archivos "necesarios", como `/`, `/usr`, `/var`, `/proc`, `/dev/fd` y `/tmp`. Como el sistema de archivos ya está montado y debe tener una entrada en `/etc/mnttab`, no tiene que incluir un indicador para el tipo de sistema de archivos.

La opción `-f` fuerza un sistema de archivos ocupado para que se desmonte. Puede utilizar esta opción para desbloquear un cliente bloqueado cuando intenta montar un sistema de archivos desmontable.



---

**Precaución** – Al forzar el desmontaje de un sistema de archivos, puede ocasionar una pérdida de datos si se está escribiendo en los archivos.

---

Observe los ejemplos siguientes.

**EJEMPLO 6-1** Desmontaje de un sistema de archivos

Este ejemplo desmonta un sistema de archivos montado en `/usr/man`:

```
# umount /usr/man
```

**EJEMPLO 6-2** Uso de las opciones con `umount`

Este ejemplo muestra los resultados de la ejecución de `umount -a -V`:

```
# umount -a -V
umount /home/kathys
umount /opt
umount /home
umount /net
```

Tenga en cuenta que este comando realmente no desmonta los sistemas de archivos.

## Comando `mountall`

Utilice este comando para montar todos los sistemas de archivos o un grupo de sistemas de archivos específico que aparezcan en una tabla del sistema de archivos. El comando proporciona una manera de hacer lo siguiente:

- Selección del tipo de sistema de archivos al que se tendrá acceso con la opción `-F FSType`
- Selección de todos los sistemas de archivos remotos que aparecen en una tabla del sistema de archivos con la opción `-r`
- Selección de todos los sistemas de archivos locales con la opción `-l`

Como todos los sistemas de archivos que están etiquetados como sistema de archivo NFS son sistemas de archivos remotos, algunas de estas opciones son redundantes. Para obtener más información, consulte la página del comando `man mountall(1M)`.

Tenga en cuenta que los dos ejemplos siguientes de entrada de usuario son equivalentes:

```
# mountall -F nfs
```

```
# mountall -F nfs -r
```

## Comando `umountall`

Utilice este comando para desmontar un grupo de sistemas de archivos. La opción `-k` ejecuta el comando `fuser -k punto_montaje` para cerrar todos los procesos asociados con *punto\_montaje*. La opción `-s` indica que no se va a realizar el desmontaje en paralelo. La opción `-l` especifica que sólo se deben usar los sistemas de archivos locales, y la opción `-r` especifica que sólo se deben usar los sistemas de archivos remotos. La opción `-h host` indica que se deben desmontar todos los sistemas de archivos desde el host nombrado. No se puede combinar la opción `-h` con las opciones `-l` o `-r`.

A continuación se muestra un ejemplo del desmontaje de todos los sistemas de archivos montados desde hosts remotos:

```
# umountall -r
```

A continuación se muestra un ejemplo de desmontaje de todos los sistemas de archivos que se encuentran actualmente montados desde el servidor `bee`:

```
# umountall -h bee
```

## Comando `share`

Con este comando, puede hacer que el sistema de archivos local en un servidor NFS esté disponible para el montaje. También puede utilizar el comando `share` para mostrar una lista de los sistemas de archivos en el sistema que se comparten actualmente. El servidor NFS debe estar en ejecución para que el comando `share` funcione. El software del servidor NFS se inicia automáticamente durante el inicio si una entrada es en `/etc/dfs/dfstab`. El comando no informa un error si el software del servidor NFS no se está ejecutando, por lo que debe verificar que el software se esté ejecutando.

Los objetos que se pueden compartirse incluyen cualquier árbol de directorios. Sin embargo, cada jerarquía del sistema de archivos está limitada por el segmento de disco o la partición en donde se encuentra el sistema de archivos. Por ejemplo, al compartir el sistemas de archivos root (`/`) no sólo comparte `/usr`, a menos que estos directorios estén en la misma partición de disco o en el mismo segmento. La instalación normal ubica root en el segmento 0 y `/usr` en el segmento 6. Además, si se comparte `/usr`, no se comparte cualquier otra partición local de disco montada en subdirectorios de `/usr`.

Un sistema de archivos no se puede compartir si ese sistema de archivos es parte de un sistema de archivos más grande que ya se está compartiendo. Por ejemplo, si `/usr` y `/usr/local` están en un segmento de disco, es posible compartir `/usr` o `/usr/local`. Sin embargo, si ambos directorios deben compartirse con diferentes opciones para compartir, `/usr/local` se debe mover a un segmento de disco separado.

Puede obtener acceso a un sistema de archivos de sólo lectura que esté compartido a través del identificador de archivos de un sistema de archivos compartido de lectura y escritura. Sin embargo, los dos sistemas de archivos tienen que estar en el mismo segmento de disco. Puede crear una situación más segura. Coloque los sistemas de archivos que deben ser de lectura y escritura en una partición distinta o en un segmento de disco independiente de los sistemas de archivos que necesita compartir como de sólo lectura.

---

**Nota** – Para obtener información acerca de cómo funciona NFS versión 4 cuando un sistema de archivos no se comparte y, luego, se vuelve a compartir, consulte [“Anular el uso compartido y volver a compartir un sistema de archivos en NFS versión 4”](#) en la página 184.

---

## Opciones share no específicas del sistema de archivos

Las siguientes son algunas de las opciones que puede incluir con el indicador -o.

`rw|ro`

El sistema de archivos *pathname* se comparte en modo de lectura y escritura y en modo de sólo lectura para todos los clientes.

`rw=lista_acceso`

El sistema de archivos se comparte en modo de lectura y escritura sólo para los clientes mostrados. Todas las demás solicitudes se deniegan. A partir de la versión Solaris 2.6, la lista de clientes que se definen en *lista\_acceso* se ha ampliado. Consulte [“Configuración de listas de acceso con el comando share”](#) en la página 170 para obtener más información. Puede utilizar esta opción para anular una opción -ro.

## Opciones share específicas de NFS

Las opciones que puede utilizar con sistemas de archivos NFS incluyen las siguientes.

`aclok`

Esta opción habilita que un servidor NFS que admite el protocolo NFS versión 2 sea configurado para controlar el acceso de los clientes NFS versión 2. Sin esta opción, todos los clientes obtienen acceso mínimo. Con esta opción, los clientes obtienen acceso máximo. Por ejemplo, en los sistemas de archivos que se comparten con la opción -aclok, si alguien cuenta con permisos de lectura, todos lo tienen. Sin embargo, sin esta opción, puede denegar el acceso a un cliente que debe tener los permisos de acceso. La decisión de permitir demasiado acceso o acceso muy limitado depende de los sistemas de seguridad en lugar. Consulte [“Uso de listas de control de acceso para proteger archivos UFS”](#) de *Guía de administración del sistema: servicios de seguridad* para obtener más información acerca de las listas de control de acceso (ACL).



---

**Nota** – Para utilizar las ACL, asegúrese de que los clientes y los servidores ejecuten software compatible con los protocolos NFS versión 3 y NFS\_ACL. Si el software sólo admite el protocolo NFS versión 3, los clientes obtienen acceso correcto pero no pueden manipular las ACL. Si el software admite el protocolo NFS\_ACL, los clientes obtienen acceso correcto y pueden manipular las ACL.

---

#### *anon=uid*

Utiliza *uid* para seleccionar el ID de usuario de los usuarios no autenticados. Si define *uid* en -1, el servidor niega el acceso a los usuarios no autenticados. Puede otorgar acceso root si configura *anon=0*, pero esta opción permite que los usuarios no autenticados tengan acceso root, por lo que debe utilizar la opción *root* en su lugar.

#### *index=nombre\_archivo*

Cuando un usuario accede a una URL de NFS, la opción *-index=nombre\_archivo* fuerza la carga del archivo HTML, en lugar de mostrar una lista del directorio. Esta opción imita la acción de los exploradores actuales si se encuentra un archivo *index.html* en el directorio al que la dirección URL de HTTP está accediendo. Esta opción es el equivalente a la configuración de la opción *DirectoryIndex* para *httpd*. Por ejemplo, supongamos que la entrada del archivo *dfstab* se parece a lo siguiente:

```
share -F nfs -o ro,public,index=index.html /export/web
```

Estas URL muestran la misma información:

```
nfs://<server>/<dir>
nfs://<server>/<dir>/index.html
nfs://<server>/export/web/<dir>
nfs://<server>/export/web/<dir>/index.html
http://<server>/<dir>
http://<server>/<dir>/index.html
```

#### *log=etiqueta*

Esta opción especifica la etiqueta en */etc/nfs/nfslog.conf* que contiene la información de configuración del registro del servidor NFS para un sistema de archivos. Esta opción debe estar seleccionada para habilitar el registro del servidor NFS.

#### *nosuid*

Esta opción señala que deben ignorarse todos los intentos de habilitar el modo *setuid* o *setgid*. Los clientes NFS no pueden crear archivos con los bits *setuid* o *setgid* activados.

#### *public*

La opción *-public* se ha agregado al comando *share* a fin de habilitar la exploración WebNFS. Sólo se puede compartir un sistema de archivos en un servidor con esta opción.

#### *root=lista\_acceso*

El servidor otorga acceso root a los hosts incluidos en la lista. De manera predeterminada, el servidor no otorga acceso root a ninguno de los hosts remotos. Si el modo de seguridad seleccionado es cualquier otro valor que no sea *-sec=sys*, sólo puede incluir los nombres de

host de cliente en *lista\_acceso*. A partir de la versión Solaris 2.6, la lista de clientes que se definen en *lista\_acceso* está ampliada. Consulte “[Configuración de listas de acceso con el comando share](#)” en la página 170 para obtener más información.



---

**Precaución** – El otorgamiento de acceso root a otros hosts tiene grandes consecuencias en la seguridad. Utilice la opción `-root=` con extrema precaución.

---

`root=nombre_cliente`

El valor *nombre\_cliente* se utiliza con la autenticación AUTH\_SYS para comprobar la dirección IP del cliente en comparación con una lista de direcciones proporcionada por [exportfs\(1B\)](#). Si se encuentra una coincidencia, se dará acceso root en los sistemas de archivos que se comparten.

`root=nombre_host`

Para los modos NFS seguros, como AUTH\_SYS o RPCSEC\_GSS, el servidor comprueba los nombres principales de los clientes frente a una lista de nombres principales basados en host que se derivan de una lista de acceso. La sintaxis genérica del nombre principal del cliente es `root@nombre_host`. Para Kerberos V la sintaxis es `root/nombre.host.completo@REALM`. Al utilizar el valor *nombre\_host*, los clientes en la lista de acceso deben tener las credenciales de un nombre principal. Para Kerberos V, el cliente debe tener una entrada de tabla de claves válida para su nombre principal `root/nombre.host.completo@REALM`. Para obtener más información, consulte “[Configuración de clientes Kerberos](#)” de *Guía de administración del sistema: servicios de seguridad*.

`sec=modo[:modo]`

*modo* selecciona los modos de seguridad que son necesarios para obtener acceso al sistema de archivos. De manera predeterminada, el modo de seguridad es la autenticación UNIX. Puede especificar varios modos, pero sólo puede utilizar cada modo de seguridad una vez por línea de comandos. Cada opción `-mode` se aplica a todas las opciones subsiguientes `-rw`, `-ro`, `-rw=`, `-ro=`, `-root=` y `-window=` hasta encontrar otra opción `-mode`. El uso de `-sec=none` asigna todos los usuarios al usuario nobody.

`window=valor`

*valor* selecciona la duración máxima en segundos de una credencial en el servidor NFS. El valor predeterminado es 30000 s o 8,3 h.

## Configuración de listas de acceso con el comando share

En versiones de Solaris anteriores a la 2.6, la *lista\_acceso* que estaba incluida con la opción `-ro=`, `-rw=` o `-root=` del comando `share` estaba restringida a una lista de nombres de host o nombres de grupo de red. A partir de la versión Solaris 2.6, la lista de acceso también puede incluir un nombre de dominio, un número de subred o una entrada para denegar el acceso. Estas extensiones deberían simplificar el control de acceso a archivos en un único servidor sin tener que cambiar el espacio de nombres o mantener largas listas de clientes.

Este comando proporciona acceso de sólo lectura para la mayoría de los sistemas pero permite el acceso de lectura y escritura para `rose` y `lilac`:

```
# share -F nfs -o ro,rw=rose:lilac /usr/src
```

En el ejemplo a continuación, se asigna acceso de sólo lectura a cualquier host en el grupo de red `eng`. Al cliente `rose` se le otorga específicamente acceso de lectura y escritura.

```
# share -F nfs -o ro=eng,rw=rose /usr/src
```

---

**Nota** – No puede especificar `rw` y `ro` sin argumentos. Si no se especifica una opción de lectura y escritura, el valor predeterminado para todos los clientes es de lectura y escritura.

---

Para compartir un sistema de archivos con varios clientes, debe escribir todas las opciones en la misma línea. Si se invoca el comando `share` varias veces en el mismo objeto, sólo se “recuerda” el último comando ejecutado. Este comando habilita el acceso de lectura y escritura a tres sistemas de cliente, pero sólo `rose` y `tulip` tienen acceso al sistema de archivos como `root`.

```
# share -F nfs -o rw=rose:lilac:tulip,root=rose:tulip /usr/src
```

Al compartir un sistema de archivos que utiliza varios mecanismos de autenticación, asegúrese de incluir las opciones `-ro`, `-ro=`, `-rw`, `-rw=`, `-root` y `-window` después de los modos de seguridad correctos. En este ejemplo, se selecciona la autenticación de UNIX para todos los hosts del grupo de red denominado `eng`. Estos hosts sólo pueden montar el sistema de archivos en modo de sólo lectura. Los hosts `tulip` y `lilac` pueden montar el sistema de archivos de lectura y escritura si utilizan autenticación Diffie-Hellman. Con estas opciones, `tulip` y `lilac` pueden montar el sistema de archivos de sólo lectura, incluso si estos hosts no utilizan autenticación DH. Sin embargo, los nombres de host deben estar incluidos en el grupo de red `eng`.

```
# share -F nfs -o sec=dh,rw=tulip:lilac,sec=sys,ro=eng /usr/src
```

Aunque la autenticación UNIX es el modo de seguridad predeterminado, la autenticación UNIX no se incluye si se utiliza la opción `-seg`. Por lo tanto, debe incluir una opción `-sec=sys` si la autenticación UNIX se utilizará con cualquier otro mecanismo de autenticación.

Puede utilizar el nombre de dominio DNS en la lista de acceso si antepone un punto al nombre de dominio actual. La cadena que continua después del punto es un nombre de dominio, no un nombre de host completo. La entrada siguiente permite el acceso de montaje a todos los hosts del dominio `eng.example.com`:

```
# share -F nfs -o ro=.:.eng.example.com /export/share/man
```

En este ejemplo, el único “.” coincide con todos los hosts confrontados mediante los espacio de nombres NIS o NIS+. Los resultados que se devuelven de estos servicios de nombres no incluyen el nombre de dominio. La entrada “`.eng.example.com`” coincide con todos los hosts

que usan DNS para la resolución de espacios de nombres. DNS siempre devuelve un nombre de host completo. Por lo tanto, se requiere la entrada más larga si debe usar una combinación de DNS y los otros espacios de nombres.

Puede utilizar un número de subred en una lista de acceso si antepone “@” al número de red real o el nombre de red. Este carácter diferencia el nombre de red de un grupo de red o un nombre de host completo. Debe identificar la subred en `/etc/networks` o en un espacio de nombres NIS o NIS+. Las entradas siguientes tienen el mismo efecto si la subred `192.168` se ha identificado como red `eng`:

```
# share -F nfs -o ro=@eng /export/share/man
# share -F nfs -o ro=@192.168 /export/share/man
# share -F nfs -o ro=@192.168.0.0 /export/share/man
```

Las últimas dos entradas muestran que no tiene que incluir las direcciones de red completas.

Si el prefijo de red no está alineado con el byte, como con el enrutamiento entre dominios sin clase (CIDR), la longitud de la máscara puede especificarse explícitamente en la línea de comandos. La longitud de la máscara se define siguiendo el nombre de red o el número de red con una barra diagonal y el número de bits significativos en el prefijo de la dirección. Por ejemplo:

```
# share -f nfs -o ro=@eng/17 /export/share/man
# share -F nfs -o ro=@192.168.0/17 /export/share/man
```

En estos ejemplos, “/17” indica que los primeros 17 bits de la dirección se utilizarán como máscara. Para obtener información adicional acerca de CIDR, consulte RFC 1519.

También puede seleccionar acceso negativo si coloca “-” antes de la entrada. Tenga en cuenta que las entradas se leen de izquierda a derecha. Por lo tanto, debe colocar el acceso negativo a las entradas antes de la entrada sobre la que se aplicará el acceso negativo:

```
# share -F nfs -o ro=-rose:.eng.example.com /export/share/man
```

Este ejemplo permite el acceso a cualquier host en el dominio `eng.example.com`, excepto el host que se denomina `rose`.

## Comando unshare

Este comando le permite hacer que los sistemas de archivos anteriormente disponibles pasen a estar no disponibles para el montaje de los clientes. Puede utilizar el comando `unshare` para dejar de compartir cualquier sistema de archivos, tanto si el sistema de archivos fue compartido explícitamente con el comando `share` o de forma automática mediante `/etc/dfs/dfstab`. Debe tener cuidado si utiliza el comando `unshare` para dejar de compartir un sistema de archivos que compartió mediante el archivo `dfstab`. Recuerde que el sistema de archivos se vuelve a compartir cuando sale y vuelve a ingresar en el nivel de ejecución 3. Debe eliminar la entrada de este sistema de archivos del archivo `dfstab` para que el cambio continúe.

Cuando deja de compartir un sistema de archivos NFS, se inhibe el acceso de los clientes con los montajes existentes. Puede que el sistema de archivos aún esté montado en el cliente, pero que no pueda accederse a los archivos.

---

**Nota** – Para obtener información acerca de cómo funciona NFS versión 4 cuando un sistema de archivos no se comparte y, luego, se vuelve a compartir, consulte [“Anular el uso compartido y volver a compartir un sistema de archivos en NFS versión 4”](#) en la página 184.

---

A continuación se muestra un ejemplo de cómo dejar de compartir un sistema de archivos específico:

```
# unshare /usr/src
```

## Comando shareall

Este comando permite compartir varios sistemas de archivos. Cuando se utiliza sin opciones, el comando comparte todas las entradas en `/etc/dfs/dfstab`. Puede incluir un nombre de archivo para especificar el nombre de un archivo que muestra las líneas de comandos `share`. Si no incluye un nombre de archivo, se activa `/etc/dfs/dfstab`. Si utiliza “-” para sustituir el nombre de archivo, puede escribir comandos `share` desde la entrada estándar.

A continuación se muestra un ejemplo del uso compartido de todos los sistemas de archivos que aparecen en un archivo local:

```
# shareall /etc/dfs/special_dfstab
```

## Comando unshareall

Este comando hace que todos los recursos compartidos dejen de estar disponibles. La opción `-F` *FSType* selecciona una lista de los tipos de sistemas de archivos que se definen en `/etc/dfs/fstypes`. Este indicador le permite seleccionar únicamente determinados tipos de sistemas de archivos que se van a dejar de compartir. El tipo de sistema de archivos predeterminado se define en `/etc/dfs/fstypes`. Para seleccionar sistemas de archivos específicos, utilice el comando `unshare`.

A continuación se muestra un ejemplo de cómo dejar de compartir todos los sistemas de archivos tipo NFS:

```
# unshareall -F nfs
```

## Comando showmount

Este comando muestra una de las siguientes opciones:

- Todos los clientes que tienen sistemas de archivos montados de forma remota y que se comparten desde un servidor NFS
- Sólo los sistemas de archivos que montan los clientes
- Los sistemas de archivos compartidos con la información de acceso de cliente

---

**Nota** – El comando showmount sólo muestra exportaciones de NFS versión 2 y versión 3. Este comando no muestra exportaciones NFS versión 4.

---

La sintaxis del comando es la siguiente:

showmount [ -ade ] [ *host* ]

- a Imprime una lista de todos los montajes remotos. Cada entrada incluye el nombre de cliente y el directorio.
- d Imprime una lista de los directorios montados de forma remota por los clientes.
- e Imprime una lista de los archivos compartidos o exportados.
- nombre\_host* Selecciona el servidor NFS del que se recopilará información.

Si no se especifica *nombre\_host*, se consulta al host local.

El siguiente comando muestra todos los clientes y los directorios locales que los clientes han montado:

```
# showmount -a bee
lilac:/export/share/man
lilac:/usr/src
rose:/usr/src
tulip:/export/share/man
```

El siguiente comando muestra una lista de los directorios que se han montado:

```
# showmount -d bee
/export/share/man
/usr/src
```

El siguiente comando muestra los sistemas de archivos que se han compartido:

```
# showmount -e bee
/usr/src                               (everyone)
/export/share/man                     eng
```

## Comando setmnt

Este comando crea una tabla `/etc/mnttab`. Los comandos `mount` y `umount` consultan la tabla. Por lo general, no tiene que ejecutar este comando manualmente, ya que se ejecuta automáticamente cuando se inicia un sistema.

## Comandos para resolución de problemas de NFS

Estos comandos pueden ser útiles al solucionar problemas de NFS.

### Comando nfsstat

Puede utilizar este comando para recopilar información estadística acerca de las conexiones RPC y NFS. La sintaxis del comando es la siguiente:

```
nfsstat [ -cmnrsz ]
```

- c Muestra información del lado del cliente
- m Muestra estadísticas para cada sistema de archivos montado en NFS
- n Especifica que la información de NFS se mostrará en el lado del cliente y en el del servidor
- r Muestra estadísticas de RPC
- s Muestra información del lado del servidor
- z Especifica que las estadísticas se deben establecer en cero

Si no hay opciones especificadas en la línea de comandos, se utilizan las opciones `-cnrs`.

Recopilar estadísticas del lado del servidor puede ser importante para depurar problemas cuando se agrega software o hardware nuevo al entorno informático. Si se ejecuta este comando por lo menos una vez a la semana y se almacenan los números, se obtiene un buen historial del rendimiento previo.

Consulte el siguiente ejemplo:

```
# nfsstat -s
```

```
Server rpc:
Connection oriented:
calls      badcalls  nullrecv  badlen    xdrCALL   dupchecks dupreqs
719949194  0         0         0         0         58478624  33
Connectionless:
calls      badcalls  nullrecv  badlen    xdrCALL   dupchecks dupreqs
```

```

73753609    0          0          0          0          987278    7254

Server nfs:
calls                badcalls
787783794          3516
Version 2: (746607 calls)
null      getattr      setattr      root      lookup      readlink      read
883 0%    60 0%      45 0%    0 0%    177446 23% 1489 0%    537366 71%
wrcache   write      create      remove    rename      link      symlink
0 0%      1105 0%    47 0%    59 0%    28 0%    10 0%    9 0%
mkdir     rmdir      readdir      statfs
26 0%      0 0%    27926 3%    108 0%
Version 3: (728863853 calls)
null      getattr      setattr      lookup      access
1365467 0%    496667075 68% 8864191 1%    66510206 9%    19131659 2%
readlink    read      write      create      mkdir
414705 0%    80123469 10% 18740690 2%    4135195 0%    327059 0%
symlink     mknod      remove      rmdir      rename
101415 0%    9605 0%    6533288 0%    111810 0%    366267 0%
link        readdir      readdirplus  fsstat      fsinfo
2572965 0%    519346 0%    2726631 0%    13320640 1%    60161 0%
pathconf    commit
13181 0%    6248828 0%
Version 4: (54871870 calls)
null      compound
266963 0%    54604907 99%
Version 4: (167573814 operations)
reserved      access      close      commit
0 0%          2663957 1%    2692328 1%    1166001 0%
create        delegpurge  delegreturn  getattr
167423 0%      0 0%        1802019 1%    26405254 15%
getfh         link        lock        lockt
11534581 6%    113212 0%    207723 0%    265 0%
locku         lookup      lookupp      nverify
230430 0%      11059722 6%    423514 0%    21386866 12%
open          openattr    open_confirm  open_downgrade
2835459 1%      4138 0%        18959 0%    3106 0%
putfh         putpubfh    putrootfh     read
52606920 31%    0 0%          35776 0%    4325432 2%
readdir       readlink    remove        rename
606651 0%      38043 0%      560797 0%    248990 0%
renew         restorefh   savefh        secinfo
2330092 1%      8711358 5%    11639329 6%    19384 0%
setattr       setclientid  setclientid_confirm  verify
453126 0%      16349 0%      16356 0%    2484 0%
write         release_lockowner  illegal
3247770 1%      0 0%          0 0%

Server nfs_acl:
Version 2: (694979 calls)
null      getacl      setacl      getattr      access      getxattrdir
0 0%      42358 6%    0 0%        584553 84%    68068 9%    0 0%
Version 3: (2465011 calls)
null      getacl      setacl      getxattrdir
0 0%      1293312 52% 1131 0%    1170568 47%

```



La lista anterior es un ejemplo de estadísticas de servidor NFS. Las primeras cinco líneas se relacionan con RPC y las líneas restantes informan actividades de NFS. En ambos conjuntos de estadísticas, conocer el número medio de `badcalls` o `calls` y el número de llamadas por semana puede ayudar a identificar un problema. El valor `badcalls` informa el número de mensajes incorrectos de un cliente. Este valor puede indicar problemas de hardware de red.

Algunas de las conexiones generan actividad de escritura en los discos. Un aumento repentino en estas estadísticas puede indicar problemas y debe ser investigado. Para las estadísticas NFS versión 2, las conexiones que se deben tener en cuenta son `setattr`, `write`, `create`, `remove`, `rename`, `link`, `symlink`, `mkdir` y `rmdir`. Para las estadísticas NFS versión 3 y versión 4, el valor que se debe observar es `commit`. Si el nivel de `commit` es alto en un servidor NFS, en comparación con otro servidor casi idéntico, compruebe que el cliente NFS tenga suficiente memoria. El número de operaciones `commit` en el servidor crece cuando los clientes no tienen recursos disponibles.

## Comando `pstack`

Este comando muestra un rastreo de la pila para cada proceso. El comando `pstack` debe ser ejecutado por el responsable del proceso o por `root`. Puede utilizar `pstack` para determinar dónde está bloqueado un proceso. La única opción que se permite con este comando es el PID del proceso que desea comprobar. Consulte la página del comando [man `proc\(1\)`](#).

El ejemplo siguiente está comprobando el proceso `nfsd` que se está ejecutando.

```
# /usr/bin/pgrep nfsd
243
# /usr/bin/pstack 243
243: /usr/lib/nfs/nfsd -a 16
ef675c04 poll (24d50, 2, ffffffff)
000115dc ???????? (24000, 132c4, 276d8, 1329c, 276d8, 0)
00011390 main (3, effffff14, 0, 0, ffffffff, 400) + 3c8
00010fb0 _start (0, 0, 0, 0, 0, 0) + 5c
```

El ejemplo muestra que el proceso está esperando una nueva solicitud de conexión, lo que es una respuesta normal. Si la pila muestra que el proceso todavía se encuentra en sondeo después de que se realiza una solicitud, es posible que el proceso se bloquee. Siga las instrucciones de “[Cómo reiniciar servicios NFS](#)” en la [página 128](#) para solucionar este problema. Revise las instrucciones en “[Procedimientos de resolución de problemas NFS](#)” en la [página 124](#) para verificar que su problema es un bloqueo de programa.

## Comando `rpcinfo`

Este comando genera información sobre el servicio de llamada de procedimiento remoto (RPC) que se está ejecutando en un sistema. También puede utilizar este comando para cambiar el

servicio RPC. Hay muchas opciones disponibles con este comando. Consulte la página del comando [man rpcinfo\(1M\)](#). La siguiente es una sinopsis de algunas de las opciones que puede utilizar con el comando.

```
rpcinfo [ -m | -s ] [ nombre_host ]
```

```
rpcinfo -T transporte nombre_host [ nombre_programa ]
```

```
rpcinfo [ -t | -u ] [ nombre_host ] [ nombre_programa ]
```

-m	Muestra una tabla de estadísticas de las operaciones rpcbind
-s	Muestra una lista concisa de todos los programas RPC registrados
-T	Muestra información sobre los servicios que usan transportes o protocolos específicos
-t	Examina los programas RPC que utilizan TCP
-u	Examina los programas RPC que utilizan UDP
<i>transporte</i>	Selecciona el transporte o el protocolo de los servicios
<i>nombre_host</i>	Selecciona el nombre de host del servidor del que necesita información
<i>nombre_programa</i>	Selecciona el programa RPC sobre el cual recopilar información

Si no se proporciona un valor para *nombre\_host*, se usan el nombre de host local. Puede sustituir *nombre\_programa* por el número de programa RPC, pero muchos usuarios pueden recordar el nombre y no el número. Puede utilizar la opción -p en lugar de la opción -s en los sistemas que no ejecutan el software NFS versión 3.

Los datos que se generan con este comando pueden incluir la siguiente información:

- El número de programa RPC
- El número de versión de un programa específico
- El protocolo de transporte que se está utilizando
- El nombre del servicio RPC
- El responsable del servicio RPC

El siguiente ejemplo recopila información sobre los servicios RPC que se están ejecutando en un servidor. El texto que genera el comando está filtrado por el comando sort para que la salida sea más legible. Se han eliminado del ejemplo varias líneas que muestran los servicios RPC.

```
% rpcinfo -s bee |sort -n
program version(s) netid(s) service owner
100000 2,3,4 udp6,tcp6,udp,tcp,ticlts,ticotsord,ticots rpcbind superuser
100001 4,3,2 ticlts,udp,udp6 rstatd superuser
100002 3,2 ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 rusersd superuser
100003 3,2 tcp,udp,tcp6,udp6 nfs superuser
100005 3,2,1 ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 mountd superuser
```

100007	1,2,3	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	ybind	superuser
100008	1	ticlts,udp,udp6	walld	superuser
100011	1	ticlts,udp,udp6	rquotad	superuser
100012	1	ticlts,udp,udp6	sprayd	superuser
100021	4,3,2,1	tcp,udp,tcp6,udp6	nlockmgr	superuser
100024	1	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	status	superuser
100029	3,2,1	ticots,ticotsord,ticlts	keyerv	superuser
100068	5	tcp,udp	cmsd	superuser
100083	1	tcp,tcp6	ttldbserverd	superuser
100099	3	ticotsord	autofs	superuser
100133	1	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	-	superuser
100134	1	ticotsord	tokenring	superuser
100155	1	ticots,ticotsord,tcp,tcp6	smserverd	superuser
100221	1	tcp,tcp6	-	superuser
100227	3,2	tcp,udp,tcp6,udp6	nfs_acl	superuser
100229	1	tcp,tcp6	metad	superuser
100230	1	tcp,tcp6	metamhd	superuser
100231	1	ticots,ticotsord,ticlts	-	superuser
100234	1	ticotsord	gssd	superuser
100235	1	tcp,tcp6	-	superuser
100242	1	tcp,tcp6	metamedd	superuser
100249	1	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	-	superuser
300326	4	tcp,tcp6	-	superuser
300598	1	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	-	superuser
390113	1	tcp	-	unknown
805306368	1	ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6	-	superuser
1289637086	1,5	tcp	-	26069

Los siguientes dos ejemplos muestran cómo obtener información sobre un servicio RPC particular al seleccionar un transporte particular en un servidor. El primer ejemplo comprueba el servicio mountd que se está ejecutando sobre TCP. El segundo ejemplo comprueba el servicio NFS que se está ejecutando sobre UDP.

```
% rpcinfo -t bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
% rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

## Comando snoop

Este comando se utiliza a menudo para controlar paquetes en la red. El comando snoop se debe ejecutar como root. El uso de este comando es una buena forma de asegurar que el hardware de red funciona en el cliente y el servidor. Hay muchas opciones disponibles. Consulte la página del comando [man snoop\(1M\)](#). A continuación sigue una sinopsis del comando:

```
snoop [ -d dispositivo ] [ -o nombre_archivo ] [ host nombre_host ]

-d dispositivo           Especifica la interfaz de red local
```

`-o nombre_archivo`      Almacena todos los paquetes capturados en el archivo con nombre `nombre_host`  
`nombre_host`              Muestra paquetes sólo hacia un host específico y desde él

La opción `-d dispositivo` es útil para los servidores que tienen varias interfaces de red. Puede utilizar varias expresiones además de configurar el host. Una combinación de expresiones de comando con `grep` a menudo puede generar datos lo suficientemente específicos para resultar útiles.

Al solucionar problemas, asegúrese de que los paquetes se dirijan al host correspondiente y provengan de él. También, busque los mensajes de error. Si guarda los paquetes en un archivo, puede simplificar la revisión de los datos.

## Comando `truss`

Puede utilizar este comando para comprobar si un proceso está bloqueado. El comando `truss` debe ser ejecutado por el responsable del proceso o por `root`. Con este comando puede utilizar muchas opciones. Consulte la página del comando `man truss(1)`. A continuación sigue una sintaxis abreviada del comando.

```
truss [ -t llamada_sistema ] -p pid
```

`-t llamada_sistema`      Selecciona las llamadas del sistema que se deben rastrear

`-p pid`                      Indica el PID del proceso que se rastreará

`llamada_sistema` puede ser una lista de las llamadas de sistema separadas por comas que se rastrearán. También, si precede `lista_llamada` con un `!`, excluye la lista las llamadas de sistema del rastreo.

En este ejemplo se muestra que el proceso está esperando otra solicitud de conexión de un nuevo cliente.

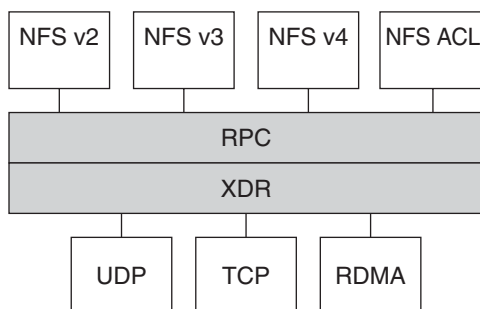
```
# /usr/bin/truss -p 243  
poll(0x00024D50, 2, -1)              (sleeping...)
```

El ejemplo anterior muestra una respuesta normal. Si la respuesta no cambia después de que se haya efectuado una nueva solicitud de conexión, es posible que el proceso esté bloqueado. Siga las instrucciones de [“Cómo reiniciar servicios NFS” en la página 128](#) para solucionar el bloqueo del programa. Revise las instrucciones en [“Procedimientos de resolución de problemas NFS” en la página 124](#) para verificar que su problema sea un bloqueo de programa.

## NFS a través RDMA

La versión Solaris 10 incluye el protocolo Remote Direct Memory Access (RDMA), que es una tecnología de transferencia de datos de memoria a memoria a través de redes de alta velocidad. En concreto, RDMA proporciona transferencia de datos remota directamente hacia la memoria y desde ella sin la intervención de una CPU. RDMA también proporciona ubicación directa de datos, lo que elimina las copias de datos y, por lo tanto, elimina la intervención de la CPU. Por lo tanto, RDMA alivia no sólo la CPU del host, sino que también reduce la contención de la memoria del host y los buses de E/S. Para proporcionar esta capacidad, RDMA combina la tecnología de interconexión de E/S de InfiniBand en plataformas SPARC con el sistema operativo Solaris. La siguiente figura muestra la relación de RDMA con otros protocolos, tales como UDP y TCP.

FIGURA 6-1 Relación de RDMA con otros protocolos



NFS es una familia de protocolos en capas a través de RPC. La capa de representación de datos externa (XDR, eXternal Data Representation) codifica argumentos de RPC y resultados de RPC en uno de los varios transportes de RPC, como UDP, TCP y RDMA.

Si el transporte RDMA no está disponible en el cliente y el servidor, el transporte TCP es el mecanismo de reserva inicial, seguido de UDP, en caso de que TCP no esté disponible. Tenga en cuenta, sin embargo, que, si utiliza la opción de montaje `proto=rDMA`, los montajes NFS son forzados a utilizar sólo RDMA.

Para obtener más información acerca de las opciones de montaje de NFS, consulte la página del comando `man mount_nfs(1M)` y “Comando `mount`” en la página 159.

---

**Nota** – RDMA para InfiniBand utiliza el formato de las direcciones IP y la infraestructura de consulta IP para especificar iguales. Sin embargo, como RDMA es una pila de protocolo independiente, no implementa completamente toda la semántica IP. Por ejemplo, RDMA no utiliza las direcciones IP para comunicarse con iguales. Por lo tanto, RDMA puede omitir las configuraciones de varias políticas de seguridad que se basan en direcciones IP. Sin embargo, las políticas administrativas de NFS y RPC, como las restricciones mount y RPC seguras, no se omiten.

---

## Cómo funciona el servicio NFS

En las siguientes secciones se describen algunas de las complejas funciones del software NFS. Tenga en cuenta que algunas de las descripciones de las funciones en esta sección son exclusivas de NFS versión 4.

- “Negociación de versión en NFS” en la página 182
- “Funciones en NFS versión 4” en la página 183
- “Negociación UDP y TCP” en la página 194
- “Negociación de tamaño de transferencia de archivos” en la página 194
- “Cómo se montan los sistemas de archivos” en la página 195
- “Efectos de la opción `-public` y direcciones URL NFS al montar” en la página 196
- “Conmutación por error por parte del cliente” en la página 196
- “Archivos de gran tamaño” en la página 199
- “Cómo funciona el registro del servidor NFS” en la página 199
- “Cómo funciona el servicio WebNFS” en la página 200
- “Limitaciones WebNFS con uso de explorador web” en la página 202
- “Sistema NFS seguro” en la página 202
- “RPC segura” en la página 203

---

**Nota** – Si el sistema tiene zonas habilitadas y desea utilizar esta función en una zona no global, consulte la *Guía de administración de sistemas: administración de recursos y contenedores de Oracle Solaris y zonas de Oracle Solaris* para obtener más información.

---

## Negociación de versión en NFS

El proceso de inicio de NFS incluye la negociación de los niveles de protocolo para servidores y clientes. Si no especifica el nivel de versión, se selecciona el mejor nivel de manera predeterminada. Por ejemplo, si el cliente y el servidor pueden admitir la versión 3, se utiliza la versión 3. Si el cliente o el servidor sólo pueden admitir la versión 2, se utiliza la versión 2.

A partir de Solaris 10, puede definir las palabras clave `NFS_CLIENT_VERSMIN`, `NFS_CLIENT_VERSMAX`, `NFS_SERVER_VERSMIN`, `NFS_SERVER_VERSMAX` en el archivo `/etc/default/nfs`. Los valores mínimos y máximos especificados para el servidor y el cliente sustituirían los valores predeterminados para estas palabras clave. Para el cliente y el servidor, el valor predeterminado mínimo es 2 y el valor predeterminado máximo es 4. Consulte [“Palabras clave para el archivo /etc/default/nfs” en la página 142](#). Para encontrar la versión que admite el servidor, el cliente NFS comienza con el valor para `NFS_CLIENT_VERSMAX` y prueba cada versión hasta que se alcance la configuración de versión de `NFS_CLIENT_VERSMIN`. Apenas se encuentra la versión compatible, finaliza el proceso. Por ejemplo, si `NFS_CLIENT_VERSMAX=4` y `NFS_CLIENT_VERSMIN=2`, el cliente prueba primero la versión 4, luego prueba la versión 3 y, por último, la versión 2. Si `NFS_CLIENT_VERSMIN` y `NFS_CLIENT_VERSMAX` están definidos con el mismo valor, el cliente siempre utiliza esta versión y no intenta ninguna otra versión. Si el servidor no ofrece esta versión, el montaje falla.

---

**Nota** – Puede sustituir los valores que están determinados por la negociación mediante la opción `vers` con el comando `mount`. Consulte la página del comando `man mount_nfs(1M)`.

---

Para obtener información de procedimiento, consulte [“Configuración de servicios NFS” en la página 96](#).

## Funciones en NFS versión 4

Se han realizado muchos cambios en NFS versión 4. En esta sección se proporcionan descripciones de estas nuevas funciones.

- “Anular el uso compartido y volver a compartir un sistema de archivos en NFS versión 4” en la página 184
- “Espacio de nombre de sistema de archivos en NFS versión 4” en la página 184
- “Identificadores de archivos volátiles en NFS versión 4” en la página 186
- “Recuperación de cliente en NFS versión 4” en la página 187
- “Compatibilidad de uso compartido `OPEN` en NFS versión 4” en la página 189
- “Delegación en NFS versión 4” en la página 190
- “`ACL` y `nfsmapid` en NFS versión 4” en la página 192
- “Conmutación por error por parte del cliente en NFS versión 4” en la página 198

---

**Nota** – A partir de la versión Solaris 10, la versión 4 de NFS no admite el tipo de seguridad `LIPKEY/SPKM`. Además, NFS versión 4 no utiliza los daemons `mountd`, `nfslogd` y `statd`.

---

Para obtener información de procedimiento relacionada con el uso de NFS versión 4, consulte [“Configuración de servicios NFS” en la página 96](#).

## **Anular el uso compartido y volver a compartir un sistema de archivos en NFS versión 4**

Con NFS versión 3 y versión 4, si un cliente intenta acceder a un sistema de archivos que se ha dejado de compartir, el servidor responde con un código de error. Sin embargo, con NFS versión 3 el servidor mantiene cualquier bloqueo que los clientes hayan obtenido antes de que se dejara de compartir el sistema de archivos. Por lo tanto, cuando el sistema de archivos se vuelve a compartir, los clientes NFS versión 3 pueden acceder al sistema de archivos como si éste nunca se hubiera dejado de compartir.

Con NFS versión 4, cuando anula la compartición de un sistema de archivos, se destruye todo el estado de todos los archivos abiertos o bloqueos de archivos en ese sistema de archivos. Si el cliente intenta acceder a estos archivos o bloqueos, el cliente recibe un error. Este error suele notificarse como un error I/O en la aplicación. Tenga en cuenta, sin embargo, que si vuelve a compartir un sistema de archivos que ya está compartido para cambiar las opciones no destruye ningún estado en el servidor.

Para obtener información relacionada, consulte [“Recuperación de cliente en NFS versión 4” en la página 187](#) o la página del comando `man unshare_nfs(1M)`.

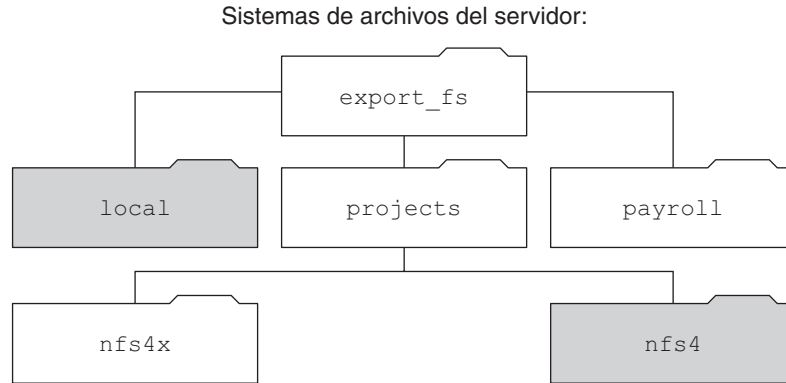
## **Espacio de nombre de sistema de archivos en NFS versión 4**

Los servidores NFS versión 4 crean y mantienen un pseudosistema de archivos que proporciona a los clientes un acceso ininterrumpido a todos los objetos exportados en el servidor. Antes de la versión 4 de NFS, el pseudosistema de archivos no existía. Los clientes estaban forzados a montar cada sistema de archivos de servidor compartido para el acceso. Considere el siguiente ejemplo.

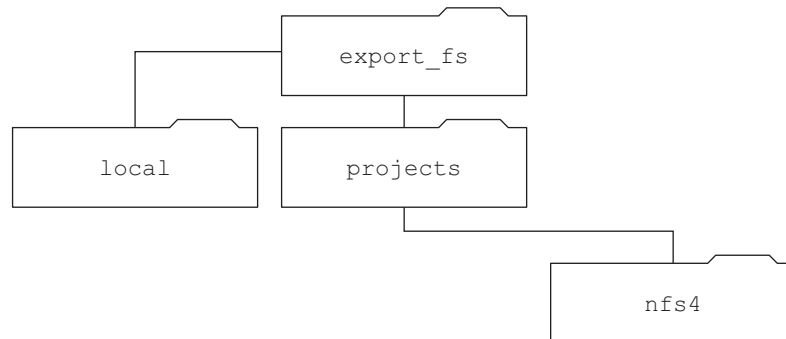


**FIGURA 6-2** Vistas del sistema de archivos del servidor y del sistema de archivos del cliente

<b>Exportaciones del servidor:</b>	<b>Sistemas de archivos del servidor:</b>
/export_fs/local	/
/export_fs/projects/nfs4	/export_fs



**Visión del cliente del directorio del servidor: export\_fs**



#### ■ Directorios exportados

Tenga en cuenta que el cliente no puede ver el directorio `payroll` ni el directorio `nfs4x`, ya que estos directorios no se exportan y no conducen a directorios exportados. Sin embargo, el directorio `local` está visible para el cliente, ya que `local` es un directorio exportado. El directorio `projects` es visible para los clientes, ya que `projects` conduce al directorio exportado `nfs4`. Por lo tanto, las partes del espacio de nombres del servidor que no están explícitamente exportadas se enlazan con un pseudosistema de archivos que visualiza sólo los directorios exportados y aquellos directorios que conducen a las exportaciones del servidor.

Un pseudosistema de archivos es una estructura que contiene sólo directorios y se crea mediante el servidor. El pseudosistema de archivos permite que un cliente examine la jerarquía

de sistemas de archivos exportados. Por lo tanto, la vista que tiene el cliente del pseudosistema de archivos se limita a rutas que conducen a sistemas de archivos exportados.

Las versiones anteriores de NFS no permitían que un cliente atravesara sistemas de archivos del servidor sin montar cada sistema de archivos. Sin embargo, en la versión 4 de NFS, el espacio de nombres del servidor hace lo siguiente:

- Restringe la vista del sistema de archivos a los directorios que conduzcan a exportaciones del servidor.
- Proporciona a los clientes un acceso ininterrumpido a las exportaciones del servidor sin necesidad de que el cliente monte cada sistema de archivos subyacente. Consulte el ejemplo anterior. Tenga en cuenta, sin embargo, que diferentes sistemas operativos pueden necesitar que el cliente monte cada sistema de archivos del servidor.

Por motivos relacionados con POSIX, el cliente NFS versión 4 de Solaris no cruza los límites del sistema de archivos del servidor. Cuando se realizan tales intentos, el cliente hace que el directorio parezca estar vacío. Para solucionar esta situación, debe realizar un montaje para cada uno de los sistemas de archivos del servidor.

## **Identificadores de archivos volátiles en NFS versión 4**

En el servidor se crean identificadores de archivos que contienen información que identifica de forma exclusiva archivos y directorios. En las versiones 2 y 3 de NFS, el servidor devolvía identificadores de archivos persistentes. Por lo tanto, el cliente podía garantizar que el servidor generara un identificador de archivo que siempre hiciera referencia al mismo archivo. Por ejemplo:

- Si un archivo se suprimía y sustituía por otro archivo con el mismo nombre, el servidor generaba un nuevo identificador de archivos para el archivo nuevo. Si el cliente utilizaba el identificador de archivos anterior, el servidor devolvía un error que indicaba que el identificador de archivos era obsoleto.
- Si se cambiaba el nombre de un archivo, el identificador de archivos seguía siendo el mismo.
- Si tenía que reiniciar el servidor, los identificadores de archivos seguían siendo los mismos.

Por lo tanto, cuando el servidor recibía una solicitud de un cliente que incluía un identificador de archivo, la resolución era sencilla y el identificador de archivos siempre hacía referencia al archivo correcto.

Este método de identificación de archivos y directorios para las operaciones de NFS era aceptable para la mayoría de los servidores basados en UNIX. Sin embargo, el método no podía ejecutarse en servidores que dependieran de otros métodos de identificación, como el nombre de ruta de un archivo. Para resolver este problema, el protocolo NFS versión 4 permite que un servidor declare que sus identificadores de archivos son volátiles. Por lo tanto, un identificador de archivos puede cambiar. Si el identificador de archivos cambia, el cliente debe encontrar el nuevo identificador de archivos.

Como en las versiones 2 y 3 de NFS, el servidor NFS versión 4 de Solaris siempre proporciona identificadores de archivos persistentes. Sin embargo, los clientes NFS versión 4 de Solaris que accedan a servidores que no sean de NFS versión 4 de Solaris deben admitir identificadores de archivos volátiles si el servidor los utiliza. Específicamente, cuando el servidor indica al cliente que el identificador de archivos es volátil, el cliente debe almacenar en la antememoria la asignación entre el nombre de la ruta de acceso y el identificador de archivos. El cliente utiliza este identificador de archivos volátil hasta que caduque. Cuando caduca, el cliente hace lo siguiente:

- Vacía la información almacenada en la antememoria que hace referencia a ese identificador de archivo
- Busca el identificador de archivos nuevo del archivo
- Vuelve a intentar la operación

---

**Nota** – El servidor siempre le indica al cliente qué identificadores de archivos son persistentes y qué identificadores de archivos son volátiles.

---

Los identificadores de archivos volátiles pueden caducar por cualquiera de estos motivos:

- Cuando cierra un archivo
- Cuando migra el sistema de archivos del identificador de archivos
- Cuando un cliente cambia el nombre de un archivo
- Cuando el servidor se reinicia

Tenga en cuenta que si el cliente no puede encontrar el nuevo identificador de archivos, se coloca un mensaje de error en el archivo `sys log`. Otros intentos de acceder a este archivo fallan con un error I/O.

## Recuperación de cliente en NFS versión 4

El protocolo NFS versión 4 es un protocolo con estado. Un protocolo es con estado cuando tanto el cliente como el servidor mantienen información actualizada sobre lo siguiente:

- Archivos abiertos
- Bloqueos de archivos

Cuando se produce un fallo, como un bloqueo del servidor, el cliente y el servidor trabajar juntos para restablecer los estados "abierto" y "bloqueado" que existían antes del error.

Cuando un servidor se bloquea y se reinicia, el servidor pierde su estado. El cliente detecta que el servidor se ha reiniciado y comienza el proceso de ayudar a que el servidor reconstruya su estado. Este proceso se denomina recuperación de cliente, ya que el cliente dirige el proceso.

Cuando el cliente detecta que el servidor se ha reiniciado, el cliente inmediatamente suspende su actividad actual e inicia el proceso de recuperación de cliente. Cuando el proceso de recuperación se inicia, se muestra un mensaje como el siguiente en registro de errores del sistema `/var/adm/messages`.

```
NOTICE: Starting recovery server basil.example.company.com
```

Durante el proceso de recuperación, el cliente envía información al servidor sobre el estado anterior del cliente. Tenga en cuenta, sin embargo, que durante este período, el cliente no envía las solicitudes nuevas al servidor. Las solicitudes nuevas para abrir archivos o establecer bloqueos de archivos deben esperar hasta que el servidor complete el período de recuperación antes de continuar.

Cuando se completa el proceso de recuperación de cliente, se muestra el siguiente mensaje en el registro de errores del sistema `/var/adm/messages`.

```
NOTICE: Recovery done for server basil.example.company.com
```

Ahora el cliente ha completado correctamente el envío de su información de estado al servidor. Sin embargo, aunque el cliente haya completado este proceso, es posible que otros clientes no hayan completado sus procesos de envío de información de estado al servidor. Por lo tanto, durante un período, el servidor no acepta ninguna solicitud de apertura o bloqueo. Este período, conocido como el período de gracia, se ha designado para permitir que todos los clientes completen su recuperación.

Durante el período de gracia, si el cliente intenta abrir archivos nuevos o establecer bloqueos nuevos, el servidor niega la solicitud con el código de error GRACE. Al recibir este error, el cliente debe esperar a que finalice el período de gracia y, a continuación, reenviar la solicitud al servidor. Durante el período de gracia aparece el siguiente mensaje.

```
NFS server recovering
```

Tenga en cuenta que durante el período de gracia los comandos que no abren archivos ni establecen bloqueos de archivos pueden continuar. Por ejemplo, los comandos `ls` y `cd` no abren ningún archivo ni establecen un bloqueo de archivo. Por lo tanto, estos comandos no se suspenden. Sin embargo, un comando como `cat`, que abre un archivo, se suspendería hasta que el período de gracia finalice.

Cuando el período de gracia termina, aparece el siguiente mensaje.

```
NFS server recovery ok.
```

El cliente ahora puede enviar nuevas solicitudes de apertura y de bloqueo al servidor.

La recuperación de cliente puede fallar por una serie de razones. Por ejemplo, si existe una partición de red después del reinicio del servidor, es posible que el cliente no pueda restablecer

su estado con el servidor antes de que finalice el período de gracia. Una vez que finaliza el período de gracia, el servidor no permite que el cliente restablezca su estado, ya que un nuevo estado de operaciones puede crear conflictos. Por ejemplo, un nuevo bloqueo de archivo puede entrar en conflicto con un bloqueo de archivo anterior que el cliente está intentando recuperar. Cuando ocurre este tipo de situaciones, el servidor devuelve el código de error `NO_GRACE` al cliente.

Si falla la recuperación de una operación de apertura de un archivo en particular, el cliente marca el archivo como no utilizable y aparece el siguiente mensaje.

```
WARNING: The following NFS file could not be recovered and was marked dead
(can't reopen:  NFS status 70):  file : filename
```

Tenga en cuenta que el número `70` es sólo un ejemplo.

Si falla el restablecimiento de un bloqueo de archivo durante la recuperación, se publica el siguiente mensaje de error.

```
NOTICE: nfs4_send_siglost:  pid PROCESS-ID lost
lock on server SERVER-NAME
```

En esta situación, se publica la señal `SIGLOST` en el proceso. La acción predeterminada para la señal `SIGLOST` es terminar el proceso.

Para que pueda recuperarse de este estado, debe reiniciar todas las aplicaciones que tengan archivos abiertos en el momento del fallo. Tenga en cuenta que puede ocurrir lo siguiente.

- Algunos procesos que no volvieron a abrir el archivo pudieron recibir errores I/O.
- Otros procesos que volvieron a abrir el archivo, o que realizaron la operación de apertura después del error de recuperación, pueden acceder al archivo sin problemas.

Por lo tanto, algunos procesos pueden acceder a un archivo determinado mientras que otros procesos no pueden hacerlo.

## Compatibilidad de uso compartido OPEN en NFS versión 4

El protocolo NFS versión 4 proporciona varios modos de uso compartido de archivos que el cliente puede utilizar para controlar el acceso de otros clientes. Un cliente puede especificar lo siguiente:

- El modo `DENY_NONE` permite que otros clientes tengan acceso de lectura y escritura para un archivo.
- El modo `DENY_READ` impide que otros clientes tengan acceso de lectura para un archivo.
- El modo `DENY_WRITE` impide que otros clientes tengan acceso de escritura para un archivo.
- El modo `DENY_BOTH` impide que otros clientes tengan acceso de lectura y escritura para un archivo.

El servidor NFS versión 4 de Solaris implementa todos estos modos de uso compartido de archivos. Por lo tanto, si un cliente intenta abrir un archivo de forma que entra en conflicto con el modo de uso compartido actual, el servidor impide el intento y hace fallar la operación. Cuando estos intentos fallan con el inicio de las operaciones de apertura o creación, el cliente NFS versión 4 recibe un error de protocolo. Este error se asigna al error de aplicación EACCES.

Aunque el protocolo proporciona varios modos de uso compartido, en la actualidad, la operación de apertura en Solaris no ofrece varios modos de uso compartido. Al abrir un archivo, un cliente NFS versión 4 de Solaris sólo puede utilizar el modo `DENY_NONE`.

Además, aunque la llamada de sistema `fcntl` tiene un comando `F_SHARE` para controlar el uso compartido de archivos, los comandos `fcntl` no pueden implementarse correctamente con la versión 4 de NFS. Si utiliza estos comandos `fcntl` para un cliente NFS versión 4, éste devuelve el error `EAGAIN` a la aplicación.

## Delegación en NFS versión 4

NFS versión 4 proporciona compatibilidad de cliente y servidor para la delegación. La delegación es una técnica mediante la cual el servidor delega la gestión de un archivo a un cliente. Por ejemplo, el servidor puede conceder una delegación de lectura o una delegación de escritura a un cliente. Las delegaciones de lectura se pueden otorgar a varios clientes al mismo tiempo, ya que estas delegaciones de lectura no entran en conflicto entre ellas. Es posible otorgar una delegación de escritura a un solo cliente, ya que la delegación de escritura entra en conflicto con cualquier acceso de archivo de cualquier otro cliente. En posesión de una delegación de escritura, el cliente no enviaría diversas operaciones al servidor porque el cliente tiene acceso exclusivo garantizado a un archivo. De forma similar, el cliente no enviaría diversas operaciones al servidor mientras posee una delegación de lectura. El motivo es que el servidor garantiza que ningún cliente pueda abrir el archivo en el modo de escritura. El efecto de la delegación es reducir en gran medida las interacciones entre el servidor y el cliente para los archivos delegados. Por lo tanto, se reduce el tráfico de la red, y se mejora el rendimiento en el cliente y el servidor. Tenga en cuenta, sin embargo, que el grado de mejora del rendimiento depende del tipo de interacción de archivo utilizada por una aplicación y la cantidad de congestión en la red y el servidor.

La decisión sobre si conceder una delegación la toma completamente el servidor. Un cliente no solicita una delegación. El servidor toma decisiones acerca de si se debe otorgar una delegación o no en función de los patrones de acceso para el archivo. Si varios clientes distintos han accedido recientemente a un archivo en el modo de escritura, es posible que el servidor no otorgue una delegación. El motivo es que este patrón de acceso indica la posibilidad de conflictos futuros.

Se produce un conflicto cuando un cliente accede a un archivo de una forma que sea incoherente con las delegaciones que se han otorgado para ese archivo. Por ejemplo, si un cliente posee una delegación de escritura sobre un archivo y un segundo cliente abre ese archivo para obtener acceso de lectura o escritura, el servidor recupera la primera delegación de

escritura del cliente. De manera similar, si un cliente posee una delegación de lectura y otro cliente abre el mismo archivo para escritura, el servidor recupera la delegación de lectura. Tenga en cuenta que en ambas situaciones, no se ha concedido una delegación al segundo cliente porque existe un conflicto. Cuando se produce un conflicto, el servidor utiliza un mecanismo de devolución de llamada para ponerse en contacto con el cliente que posee actualmente la delegación. Al recibir esta devolución de llamada, el cliente envía el estado actualizado del archivo al servidor y devuelve la delegación. Si el cliente no responde a la recuperación, el servidor revoca la delegación. En tales circunstancias, el servidor rechaza todas las operaciones del cliente para este archivo, y el cliente informa las operaciones solicitadas como fallos. Por lo general, estos fallos se notifican en la aplicación como errores de I/O. Para recuperarse de estos errores, el archivo se debe cerrar y, a continuación, volver a abrir. Pueden producirse fallos desde las delegaciones revocadas cuando existe una partición de red entre el cliente y el servidor mientras el cliente posee una delegación.

Tenga en cuenta que un servidor no resuelve los conflictos de acceso para un archivo almacenado en otro servidor. Por lo tanto, un servidor NFS sólo resuelve los conflictos para los archivos que almacena. Además, en respuesta a los conflictos provocados por los clientes que ejecutan varias versiones de NFS, un servidor NFS solamente puede iniciar recuperaciones para el cliente que está ejecutando NFS versión 4. Un servidor NFS no puede iniciar recuperaciones para los clientes que ejecutan versiones anteriores de NFS.

El proceso para detectar conflictos varía. Por ejemplo, a diferencia de la versión 4 de NFS, y como las versiones 2 y 3 no tienen un procedimiento abierto, el conflicto sólo se detecta después de que el cliente intenta leer, escribir o bloquear un archivo. La respuesta del servidor frente a estos conflictos también varía. Por ejemplo:

- Para NFS versión 3, el servidor devuelve el error JUKEBOX, que hace que el cliente detenga la solicitud de acceso y vuelva a intentarlo más tarde. El cliente imprime el mensaje `File unavailable`.
- Para NFS versión 2, como no existe un equivalente para el error JUKEBOX, el servidor no responde, lo que hace que el cliente deba esperar y volver a intentarlo. El cliente imprime el mensaje `NFS server not responding`.

Estas condiciones se eliminan una vez que se resuelve el conflicto de delegación.

De manera predeterminada, la delegación de servidor está habilitada. Puede desactivar la delegación si modifica el archivo `/etc/default/nfs`. Para obtener información de procedimiento, consulte [“Cómo seleccionar diferentes versiones de NFS en un servidor” en la página 98](#).

No se requieren palabras clave para la delegación de cliente. El daemon de devolución de llamadas NFS versión 4, `nfs4cbd`, proporciona el servicio en el cliente. El daemon se inicia automáticamente siempre que haya un montaje para la versión 4 de NFS habilitado. De manera predeterminada, el cliente ofrece la información de devolución de llamada necesaria al servidor para todos los transportes de Internet que se muestran en el archivo de sistema

/etc/netconfig. Tenga en cuenta que si el cliente está habilitado para IPv6 y la dirección IPv6 para el nombre del cliente se puede determinar, el daemon de devolución de llamadas acepta las conexiones IPv6.

El daemon de devolución de llamadas utiliza un número de programa transitorio y un número de puerto asignado de forma dinámica. Esta información se proporciona al servidor, y el servidor prueba la ruta de devolución de llamadas antes de conceder delegaciones. Si la ruta de devolución de llamadas no es correcta, el servidor no otorga las delegaciones, lo cual es el único comportamiento externamente visible.

Tenga en cuenta que, debido a la información de devolución de llamadas integrada en una solicitud de NFS versión 4, el servidor no puede establecer contacto con el cliente a través de un dispositivo que utiliza traducción de direcciones de red (NAT). Además, el daemon de devolución de llamadas utiliza un número de puerto dinámico. Por lo tanto, es posible que el servidor no pueda atravesar un cortafuegos, incluso si el cortafuegos permite el tráfico NFS normal en el puerto 2049. En tales situaciones, el servidor no otorga delegaciones.

## ACL y nfsmapid en NFS versión 4

Una lista de control de acceso (ACL) proporciona una mejor seguridad de archivos al habilitar al responsable de un archivo para que defina los permisos para el responsable del archivo, el grupo u otros usuarios o grupos específicos. Las ACL se establecen en el servidor y el cliente mediante el comando `setfacl`. Consulte la página del comando `man setfacl(1)`. En la versión 4 de NFS, el asignador de ID `nfsmapid` se utiliza para asignar los ID de usuario o de grupo en las entradas de la ACL de un servidor a los ID de usuario o de grupo en las entradas de ACL de un cliente. Lo contrario también es cierto. Los ID de grupo y de usuario en las entradas de la ACL deben existir en el cliente y el servidor.

## Motivos de falla de la asignación de ID

Las siguientes situaciones pueden originar una falla en la asignación de ID:

- Si el usuario o el grupo en una entrada de la ACL en el servidor no se pueden asignar a un usuario o grupo válidos en el cliente, el usuario no puede leer la ACL en el cliente.

Por ejemplo, cuando emite el comando `ls -lv` o `ls -lV`, y recibe el mensaje de error `Permission denied` para los archivos con entidades de ACL de ID de usuario o grupo que no se pueden asignar desde el servidor al cliente. El asignador de ID no ha podido asignar un usuario o grupo en la ACL. Si el asignador de ID ha podido asignar el usuario o grupo, tendría que haber aparecido un signo más (+) después los permisos en la lista de archivos producida por `ls -l`. Por ejemplo:

```
% ls -l
-rw-r--rw-+ 1 luis  staff    11968 Aug 12  2005 foobar
```



De forma similar, el comando `getfacl` puede devolver el mensaje de error `Permission denied` por la misma razón. Para obtener más información sobre este comando, consulte la página del comando `man getfacl(1)`.

- Si el ID de usuario o grupo en cualquier entrada de la ACL establecida en el cliente no se puede asignar a un ID de usuario o grupo válido en el servidor, el comando `setfacl` o `chmod` puede fallar y devolver el mensaje de error `Permission denied`.
- Si el cliente y el servidor no hacen coincidir correctamente los valores `NFSMAPID_DOMAIN`, la asignación de ID falla. Para obtener más información, consulte “Palabras clave para el archivo `/etc/default/nfs`” en la página 142.

## Cómo evitar problemas de asignación de ID con las ACL

Para evitar problemas de asignación de ID, realice lo siguiente:

- Asegúrese de que el valor para `NFSMAPID_DOMAIN` esté configurado correctamente en el archivo `/etc/default/nfs`.
- Asegúrese de que todos los ID de usuario y de grupo en las entradas de la ACL existan tanto en el cliente como en el servidor de NFS versión 4.

## Comprobación de ID de usuario o de grupo sin asignar

Para determinar si un usuario o grupo no se pueden asignar al servidor o el cliente, utilice la siguiente secuencia de comandos:

```
#!/usr/sbin/dtrace -Fs

sdt::nfs4-acl-nobody
{
    printf("validate_idmapping: (%s) in the ACL could not be mapped!",
    stringof(arg0));
}
```

---

**Nota** – El nombre de sondeo que se utiliza en esta secuencia de comandos es una interfaz que podría cambiar en el futuro. Para obtener más información, consulte “Niveles de estabilidad” de *Guía de seguimiento dinámico de Solaris*.

---

## Información adicional sobre las ACL o `nfsmapid`

Consulte lo siguiente:

- “Protección de archivos UFS con ACL (mapa de tareas)” de *Guía de administración del sistema: servicios de seguridad*
- 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*

- “[Daemon nfsmapid](#)” en la página 148

## Negociación UDP y TCP

Durante el inicio, también se negocia el protocolo de transporte. De manera predeterminada, se selecciona el primer transporte orientado a la conexión que se admite tanto en el cliente como en el servidor. Si esta selección no se realiza correctamente, se utiliza el primer protocolo de transporte sin conexión disponible. Los protocolos de transporte que se admiten en un sistema se muestran en `/etc/netconfig`. TCP es el protocolo de transporte orientado a la conexión que es compatible con la versión. UDP es el protocolo de transporte sin conexión.

Cuando la versión del protocolo NFS y el protocolo de transporte se determinan mediante negociación, la versión del protocolo NFS tiene prioridad sobre el protocolo de transporte. El protocolo NFS versión 3 que utiliza UDP tiene mayor prioridad que el protocolo NFS versión 2 que está utilizando TCP. Puede seleccionar de forma manual tanto la versión del protocolo NFS como el protocolo de transporte con el comando `mount`. Consulte la página del comando [man mount\\_nfs\(1M\)](#). En la mayoría de las condiciones, permita que la negociación seleccione las opciones más adecuadas.

## Negociación de tamaño de transferencia de archivos

El tamaño de transferencia del archivo establece el tamaño de las memorias intermedias que se utilizan al transferir datos entre el cliente y el servidor. En general, mientras mayor sea el tamaño de la transferencia, mejor. El protocolo NFS versión 3 tiene tamaño de transferencia ilimitado. Sin embargo, a partir de la versión Solaris 2.6, el software ofrece un tamaño de memoria intermedia predeterminado de 32 Kbytes. El cliente puede pedir un tamaño menor de transferencia en el momento del montaje si es necesario, pero en la mayoría de los casos esto no es necesario.

El tamaño de transferencia no se negocia con sistemas que utilizan el protocolo NFS versión 2. En este caso, el tamaño de transferencia máximo se establece en 8 Kbytes.

Puede utilizar las opciones `-rsize` y `-wsize` para establecer el tamaño de transferencia manualmente con el comando `mount`. Es posible que necesite reducir el tamaño de transferencia para algunos clientes de PC. Además, puede aumentar el tamaño de transferencia si el servidor NFS está configurado para utilizar tamaños de transferencias más grandes.

---

**Nota** – A partir de la versión Solaris 10, las restricciones en los tamaños de las transferencias por cable se relajaron. Los tamaños de las transferencias se basan en la capacidad del medio de transporte subyacente. Por ejemplo, el límite de transporte NFS para UDP sigue siendo de 32 Kbytes. No obstante, como TCP es un protocolo de flujo sin los límites de datagramas de UDP, los tamaños máximos de transferencia a través de TCP se han incrementado en 1 Mbyte.

---

## Cómo se montan los sistemas de archivos

La siguiente descripción se aplica a los montajes de NFS versión 3. El proceso de montaje de NFS versión 4 no incluye el servicio de asignación de puerto ni incluye el protocolo MOUNT.

Si un cliente necesita montar un sistema de archivos desde un servidor, el cliente debe obtener un identificador de archivos del servidor. El identificador de archivos debe corresponderse con el sistema de archivos. Este proceso exige que varias transacciones ocurran entre el cliente y el servidor. En este ejemplo, el cliente intenta montar /home/terry desde el servidor. A continuación sigue un rastreo snoop para esta transacción.

```
client -> server PORTMAP C GETPORT prog=100005 (MOUNT) vers=3 proto=UDP
server -> client PORTMAP R GETPORT port=33492
client -> server MOUNT3 C Null
server -> client MOUNT3 R Null
client -> server MOUNT3 C Mount /export/home9/terry
server -> client MOUNT3 R Mount OK FH=9000 Auth=unix
client -> server PORTMAP C GETPORT prog=100003 (NFS) vers=3 proto=TCP
server -> client PORTMAP R GETPORT port=2049
client -> server NFS C NULL3
server -> client NFS R NULL3
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

En este rastreo, el cliente primero solicita el número de montaje de puerto del servicio de asignación de puerto en el servidor NFS. Después de que el cliente recibe el número de puerto montaje (33492), el número se utiliza para probar la disponibilidad del servicio en el servidor. Después de que el cliente haya determinado que un servicio se está ejecutando en ese número de puerto, el cliente realiza una solicitud de montaje. Cuando el servidor responde a esta solicitud, el servidor incluye el identificador de archivo para el sistema de archivos (9000) que se está montando. A continuación, el cliente envía una solicitud para el número de puerto NFS. Cuando el cliente recibe el número del servidor, el cliente prueba la disponibilidad del servicio NFS (nfsd). También, el cliente solicita a NFS información sobre el sistema de archivos que utiliza el identificador de archivos.

En el siguiente rastreo, el cliente monta el sistema de archivos con la opción `public`.

```
client -> server NFS C LOOKUP3 FH=0000 /export/home9/terry
server -> client NFS R LOOKUP3 OK FH=9000
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

Al utilizar el identificador de archivos público predeterminado (que es `0000`), se omiten todas las transacciones para obtener información del servicio de asignación de puerto y para determinar el número de puerto NFS.

---

**Nota** – La versión 4 de NFS admite identificadores de archivos volátiles. Para obtener más información, consulte [“Identificadores de archivos volátiles en NFS versión 4” en la página 186](#).

---

## Efectos de la opción `-public` y direcciones URL NFS al montar

Mediante la opción `-public`, puede crear condiciones que hagan que falle un montaje. Si agrega una URL de NFS también puede confundir la situación. La siguiente lista describe los aspectos concretos de cómo se monta un sistema de archivos al utilizar estas opciones.

**Opción pública con URL de NFS:** fuerza el uso del identificador de archivos público. El montaje falla si el identificador de archivos público no es compatible.

**Opción pública con ruta de acceso regular:** fuerza el uso del identificador de archivos público. El montaje falla si el identificador de archivos público no es compatible.

**Sólo URL de NFS:** use el identificador de archivos público si el identificador de archivos está habilitado en el servidor NFS. Si el montaje falla cuando se utiliza el identificador de archivos público, pruebe el montaje con el protocolo MOUNT.

**Sólo ruta de acceso normal:** no utilice el identificador de archivos público. Se utiliza el protocolo MOUNT.

## Conmutación por error por parte del cliente

Mediante la conmutación por error por parte del cliente, un cliente NFS puede estar al tanto de varios servidores que hacen que los mismos datos estén disponibles y puede cambiar a un servidor alternativo cuando el servidor actual no está disponible. El sistema de archivos puede llegar a no estar disponible si se produce una de las siguientes opciones.

- Si el sistema de archivos está conectado a un servidor que se bloquea
- Si el servidor está sobrecargado
- Si se produce una falla en la red

En estas condiciones, la conmutación por error es normalmente transparente para el usuario. Por lo tanto, la conmutación por error puede ocurrir en cualquier momento sin interrumpir los procesos que se están ejecutando en el cliente.

La conmutación por error requiere que el sistema de archivos sea montado como de sólo lectura. Los sistemas de archivos deben ser idénticos para que la conmutación por error se produzca correctamente. Consulte [“¿Qué es un sistema de archivos replicado?” en la página 197](#) para obtener una descripción de qué es lo que hace que un sistema de archivos sea idéntico. Un sistema de archivos estático o un sistema de archivos que no se cambia frecuentemente es el mejor candidato para la conmutación por error.

No puede utilizar CacheFS y conmutación por error por parte del cliente en el mismo montaje NFS. Se almacena información adicional para cada sistema de archivos CacheFS. Esta información no se puede actualizar durante la conmutación por error, por lo que sólo una de estas dos funciones se puede utilizar para montar un sistema de archivos.

El número de réplicas que es necesario establecer para cada sistema de archivos depende de muchos factores. En una situación ideal, debe tener un mínimo de dos servidores. Cada servidor debe admitir varias subredes. Esta configuración es mejor que tener un único servidor en cada subred. El proceso requiere que se compruebe cada servidor que figure. Por lo tanto, si figuran más de un servidor, cada montaje es más lento.

## Terminología de conmutación por error

Para comprender completamente el proceso, debe comprender dos términos.

- *Conmutación por error*: el proceso de seleccionar un servidor de una lista de servidores que admiten un sistema de archivos replicado. Normalmente, se utiliza el siguiente servidor de la lista ordenada, a menos que no responda.
- *Reasignar*: utilizar un servidor nuevo. Normalmente, los clientes almacenan el nombre de ruta de acceso de cada archivo activo en el sistema de archivos remoto. Durante la reasignación, estos nombres de ruta se evalúan para localizar los archivos en el nuevo servidor.

## ¿Qué es un sistema de archivos replicado?

Para la conmutación por error, un sistema de archivos puede llamarse *réplica* cuando cada archivo es del mismo tamaño y tiene el mismo tamaño de archivo o tipo de archivo que el sistema de archivos original. Los permisos, fechas de creación y otros atributos de los archivos no se toman en consideración. Si el tamaño de archivo o los tipos de archivo son diferentes, la reasignación falla y el proceso se bloquea hasta que el antiguo servidor esté disponible. En NFS versión 4, el comportamiento es diferente. Consulte [“Conmutación por error por parte del cliente en NFS versión 4” en la página 198](#).

Puede mantener un sistema de archivos replicado si utiliza `rdist`, `cpio` u otro mecanismo de transferencia de archivos. Como la actualización de los sistemas de archivos replicados causa incoherencia, para obtener mejores resultados tenga en cuenta estas precauciones:

- Cambie el nombre de la versión anterior del archivo antes de instalar una nueva versión del archivo.
- Ejecute las actualizaciones de noche, cuando el uso del cliente es bajo.
- Mantenga actualizaciones pequeñas.
- Minimice el número de copias.

## **Conmutación por error y bloqueo NFS**

Algunos paquetes de software requieren bloqueos de lectura en los archivos. Para evitar que estos productos se interrumpan, los bloqueos de lectura de los sistemas de archivos de sólo lectura se permiten, pero sólo son visibles para el lado del cliente. Los bloqueos persisten durante la reasignación, ya que el servidor no “conoce” los bloqueos. Como los archivos no deben cambiar, no necesita bloquear el archivo por parte del servidor.

## **Conmutación por error por parte del cliente en NFS versión 4**

En la versión 4 de NFS, si no se puede establecer una réplica porque los tamaños de archivo son diferentes o los tipos de archivo no son los mismos, ocurre lo siguiente.

- El archivo se marca como inoperativo.
- Se imprime una advertencia.
- La aplicación recibe un fallo en la llamada de sistema.

---

**Nota** – Si reinicia la aplicación y vuelve a intentar acceder al archivo, no debería tener problemas.

---

En la versión 4 de NFS, dejará de recibir errores de replicación para los directorios de diferentes tamaños. En versiones anteriores de NFS, esta condición se trataba como error e impedía el proceso de reasignación.

Además, en la versión 4 de NFS, si una operación de lectura no es correcta, la operación es realizada por el siguiente servidor en la lista. En versiones anteriores de NFS, las operaciones de lectura incorrectas hacían que la reasignación fallara y el proceso se bloqueara hasta que el servidor original estuviera disponible.

## Archivos de gran tamaño

El SO admite archivos de más de 2 Gbytes. De manera predeterminada, los sistemas de archivos UFS se montan con la opción `-largefiles` para admitir la nueva capacidad. Si es necesario, consulte [“Cómo deshabilitar archivos grandes en un servidor NFS” en la página 93](#) para obtener instrucciones.

Si el sistema de archivos del servidor se monta con la opción `-largefiles`, un cliente NFS de Solaris 2.6 puede acceder a archivos de gran tamaño sin necesidad de cambios. Sin embargo, no todos los comandos de Solaris 2.6 pueden manejar estos archivos grandes. Consulte [`largefile\(5\)`](#) para obtener una lista de los comandos que pueden manejar archivos grandes. Los clientes que no son compatibles con el protocolo NFS versión 3 con grandes extensiones de archivos no pueden acceder a ningún archivo grande. Si bien los clientes que ejecutan la versión Solaris 2.5 pueden utilizar el protocolo NFS versión 3, la compatibilidad con archivos grandes no estaba incluida en dicha versión.

## Cómo funciona el registro del servidor NFS

El registro del servidor NFS registra lecturas y escrituras de NFS, así como operaciones que modifican el sistema de archivos. Estos datos se pueden utilizar para realizar un seguimiento del acceso a la información. Además, los registros pueden proporcionar una forma cuantitativa de medir su interés por la información.

Cuando se accede a un sistema de archivos con registro habilitado, el núcleo escribe los datos sin formato en un archivo de memoria intermedia. Entre estos elementos, se incluyen:

- Una indicación de hora
- La dirección IP del cliente
- El UID del solicitante
- El identificador de archivo del archivo o el objeto de directorio al que se accede
- El tipo de operación que se ha producido

El daemon `nfslogd` convierte estos datos sin formato en registros ASCII que se almacenan en los archivos de registro. Durante la conversión, las direcciones IP se modifican por nombres de host y los UID se modifican por inicios de sesión si el servicio de nombres que está habilitado puede encontrar coincidencias. Los identificadores de archivos también se convierten en nombres de ruta. Para realizar la conversión, el daemon realiza un seguimiento de los identificadores de archivos y almacena información en una tabla independiente de identificador de archivo a ruta. De esa manera, la ruta no tiene que ser identificada de nuevo cada vez que se accede a un identificador de archivos. Como no se realizan cambios en las asignaciones en la tabla de identificador de archivo a rutas, si el comando `nfslogd` está desactivado, debe mantener el daemon en ejecución.

---

**Nota** – El registro del servidor no se admite en NFS versión 4.

---

## Cómo funciona el servicio WebNFS

El servicio WebNFS hace que los archivos de un directorio estén disponibles para los clientes mediante un identificador de archivos público. Un identificador de archivos es una dirección generada mediante el núcleo que identifica un archivo para los clientes NFS. El *identificador de archivos público* tiene un valor predefinido, por lo que no es necesario que el servidor genere un identificador de archivos para el cliente. La posibilidad de utilizar este identificador de archivos predefinido reduce el tráfico de red mediante la eliminación del protocolo MOUT. Esta capacidad debería acelerar los procesos para los clientes.

De manera predeterminada, el identificador de archivos público en un servidor NFS se establece en el sistema de archivos root. Este valor predeterminado proporciona acceso WebNFS a los clientes que ya tienen los privilegios de montaje en el servidor. Puede cambiar el identificador de archivos público para que señale a cualquier sistema de archivos mediante el comando `share`.

Cuando el cliente tiene el identificador de archivos para el sistema de archivos, se ejecuta un comando `LOOKUP` para determinar el identificador de archivos del archivo al que se va a acceder. El protocolo NFS permite la evaluación de sólo un componente de nombre de ruta a la vez. Cada nivel adicional de jerarquía de directorios requiere otro comando `LOOKUP`. Un servidor WebNFS puede evaluar todo un nombre de ruta con una sola transacción de consulta multicomponente cuando el comando `LOOKUP` es relativo al identificador de archivos público. La consulta multicomponente permite que el servidor WebNFS envíe el identificador de archivos al archivo deseado sin necesidad de intercambiar identificadores de archivos para cada nivel del directorio en el nombre de la ruta.

Además, un cliente NFS puede iniciar descargas simultáneas a través de una única conexión TCP. Esta conexión proporciona acceso rápido sin la carga adicional del servidor provocada por la configuración de múltiples conexiones. Aunque las aplicaciones de exploradores web admiten la descarga simultánea de varios archivos, cada archivo tiene su propia conexión. Mediante una conexión, el software WebNFS reduce la carga en el servidor.

Si el componente final en el nombre de ruta es un enlace simbólico a otro sistema de archivos, el cliente puede acceder al archivo si el cliente ya tiene acceso mediante actividades de NFS normales.

Normalmente, una URL de NFS se evalúa en relación con el identificador de archivos público. La evaluación se puede cambiar para que sea relativa al sistema de archivos root del servidor al



agregar una barra diagonal adicional al comienzo de la ruta de acceso. En este ejemplo, estas dos URL de NFS son equivalentes si el identificador de archivos público que se ha establecido en el sistema de archivos `/export/ftp`.

```
nfs://server/junk  
nfs://server//export/ftp/junk
```

---

**Nota** – El protocolo NFS versión 4 se prefiere frente al servicio WebNFS. La versión 4 de NFS integra completamente toda la negociación de seguridad agregada al protocolo MOUNT y al servicio WebNFS.

---

## Cómo funciona la negociación de seguridad WebNFS

El servicio NFS incluye un protocolo que permite que un cliente WebNFS negocie un mecanismo de seguridad seleccionado con un servidor WebNFS. El nuevo protocolo utiliza consulta multicomponente de negociación de seguridad, que es una extensión de la consulta multicomponente que se había utilizado en versiones anteriores del protocolo WebNFS.

El cliente WebNFS inicia el proceso al realizar una solicitud de consulta multicomponente regular mediante el identificador de archivos público. Como el cliente no tiene constancia de cómo el servidor protege la ruta, se utiliza el valor del mecanismo de seguridad predeterminado. Si el valor predeterminado del mecanismo de seguridad no es suficiente, el servidor responde con un error `AUTH_TOOWEAK`. Esta respuesta indica que el mecanismo predeterminado no es válido. El cliente debe utilizar un mecanismo predeterminado más fuerte.

Cuando el cliente recibe el error `AUTH_TOOWEAK`, el cliente envía una solicitud al servidor para determinar qué mecanismos de seguridad son necesarios. Si la solicitud se realiza correctamente, el servidor responde con una matriz de los mecanismos de seguridad que son necesarios para la ruta especificada. Según el tamaño de la matriz de los mecanismos de seguridad, es posible que el cliente tenga que realizar más solicitudes para obtener la matriz completa. Si el servidor no admite la negociación de seguridad WebNFS, la solicitud falla.

Después de una solicitud correcta, el cliente WebNFS selecciona el primer mecanismo de seguridad de la matriz que el cliente admite. A continuación, el cliente emite una solicitud de consulta multicomponente regular mediante el mecanismo de seguridad seleccionado para adquirir el identificador de archivos. Las siguientes peticiones NFS se realizan mediante el mecanismo de seguridad seleccionado y el identificador de archivos.

---

**Nota** – El protocolo NFS versión 4 se prefiere frente al servicio WebNFS. La versión 4 de NFS integra completamente toda la negociación de seguridad agregada al protocolo MOUNT y al servicio WebNFS.

---

## Limitaciones WebNFS con uso de explorador web

Muchas de las funciones que puede proporcionar un sitio web que utiliza HTTP no son compatibles con el software WebNFS. Estas diferencias provienen del hecho de que el servidor NFS sólo envía el archivo, por lo que cualquier procesamiento especial debe realizarse en el cliente. Si necesita tener un sitio web configurado para acceso WebNFS y HTTP, tenga en cuenta las siguientes cuestiones:

- La exploración NFS no ejecuta secuencias de comandos CGI. Por lo tanto, un sistema de archivos con un sitio web activo que utiliza muchas secuencias de comandos CGI podría no ser apropiado para la exploración NFS.
- El explorador podría iniciar diferentes visores para manejar archivos en formatos de archivo diferentes. El acceso a estos archivos a través de una URL de NFS inicia un visor externo si el tipo de archivo puede determinarse por medio del nombre del archivo. El explorador debe reconocer cualquier extensión de nombre de archivo para un tipo MIME estándar cuando se utiliza una URL de NFS. El software WebNFS no comprueba dentro del archivo para determinar el tipo de archivo. Por lo tanto, la única manera de determinar un tipo de archivo es la extensión del nombre del archivo.
- La exploración NFS no puede utilizar los mapas de imágenes por parte del servidor (imágenes interactivas). Sin embargo, la exploración NFS puede utilizar mapas de imágenes por parte del cliente (imágenes interactivas) porque las direcciones URL se definen con la ubicación. No se necesitan respuestas adicionales del servidor de documentos.

## Sistema NFS seguro

El entorno NFS es una forma poderosa y conveniente de compartir sistemas de archivos en una red de distintas arquitecturas de equipos y sistemas operativos. Sin embargo, las mismas funciones que hacen que el uso compartido de sistemas de archivos a través de la operación NFS sea cómodo, también plantean algunos problemas de seguridad. Históricamente, la mayoría de las implementaciones NFS han utilizado autenticación UNIX (o AUTH\_SYS) pero también ha habido métodos de autenticación más seguros, como AUTH\_DH, disponibles. Al utilizar autenticación UNIX, un servidor NFS autentica una solicitud de archivo al autenticar el equipo que formula la solicitud, pero no el usuario. Por lo tanto, un usuario cliente puede ejecutar su y suplantar al responsable de un archivo. Si se utiliza la autenticación DH, el servidor NFS autentica el usuario, lo cual hace que este tipo de suplantación sea mucho más difícil.

Con acceso root y conocimiento de programación de red, cualquier usuario puede introducir datos arbitrarios en la red y extraer cualquier dato de ella. Los ataques más peligrosos son los que implican la introducción de datos. Un ejemplo es la suplantación de un usuario mediante la generación de paquetes correctos o mediante la grabación de “conversaciones” y su posterior reproducción. Estos ataques afectan la integridad de los datos. Los ataques que implican

intrusiones pasivas, es decir, recibir el tráfico de la red sin suplantar a nadie, no son tan peligrosos, porque integridad de los datos no queda comprometida. Los usuarios pueden proteger la privacidad de la información confidencial mediante el cifrado de los datos que se envían a través de la red.

Un enfoque común para los problemas de seguridad de la red es dejar la solución a cada aplicación. Un mejor enfoque es implementar un sistema de autenticación estándar en un nivel que cubra todas las aplicaciones.

El sistema operativo Solaris incluye un sistema de autenticación en el nivel de llamada de procedimiento remoto (RPC), que es el mecanismo en el que se crea la operación NFS. Este sistema, conocido como RPC seguras, mejora mucho la seguridad de los entornos de red y proporciona seguridad adicional a los servicios como, por ejemplo, el sistema NFS. Cuando el sistema NFS utiliza las utilidades que se proporcionan con RPC seguras, esto se conoce como sistema NFS seguro.

## RPC segura

Las RPC seguras son fundamentales para un sistema NFS seguro. El objetivo de las RPC seguras es crear un sistema que sea tan seguro, como mínimo, como un sistema de tiempo compartido. En un sistema de tiempo compartido, todos los usuarios comparten un único equipo. Un sistema de tiempo compartido autentifica un usuario mediante una contraseña de conexión. Con la autenticación estándar de cifrado de datos (DES), se completa el mismo proceso de datos de autenticación. Los usuarios pueden iniciar sesión en cualquier equipo remoto al igual que los usuarios pueden iniciar sesión en una terminal local. Las contraseñas de inicio de sesión de los usuarios son sus garantías de seguridad de la red. En un entorno de tiempo compartido, el administrador del sistema tiene una obligación ética de no cambiar una contraseña para sustituir a alguien. En las RPC seguras, se confía que el administrador de la red no modificará entradas en una base de datos que almacena *las claves públicas*.

Debe conocer dos términos para entender un sistema de autenticación RPC: credenciales y verificadores. Con las insignias de ID como ejemplo, la credencial es lo que identifica una persona: un nombre, dirección y fecha de nacimiento. El verificador es la fotografía que se adjunta a la insignia. Puede tener la certeza de que la insignia no se ha robado al comprobar la fotografía que aparece en ella con la persona que la lleva. En RPC, el proceso del cliente envía una credencial y un verificador al servidor con cada solicitud de RPC. El servidor vuelve a enviar sólo un verificador porque el cliente ya “conoce” las credenciales del servidor.

La autenticación de RPC es abierta, lo que significa que es posible conectar una variedad de sistemas de autenticación, como UNIX, DH y KERB.

Cuando un servicio de red usa la autenticación UNIX, las credenciales contienen el nombre de host del cliente, UID, GID y la lista de acceso de grupos. Sin embargo, el verificador no contiene nada. Como no existe un verificador, un superusuario puede falsificar las credenciales

adecuadas mediante comandos como `su`. Otro problema con la autenticación UNIX es que asume que todos los equipos de una red son equipos UNIX. La autenticación UNIX se desglosa cuando se aplica a otros sistemas operativos en una red heterogénea.

Para superar los problemas de autenticación UNIX, las RPC seguras utilizan autenticación DH.

## Autenticación DH

La autenticación DH utiliza el estándar de cifrado de datos (DES) y criptografía por clave pública Diffie-Hellman para autenticar a los usuarios y los equipos en la red. DES es un mecanismo de cifrado estándar. La criptografía por clave pública Diffie-Hellman es un sistema de cifrado que involucra dos claves: una pública y una secreta. Las claves públicas y las claves secretas se almacenan en el espacio de nombres. NIS almacena las claves en el mapa de claves públicas. Estos mapas contienen la clave pública y la clave secreta de todos los usuarios potenciales. Consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)* para obtener más información sobre cómo configurar los mapas.

La seguridad de la autenticación DH se basa en la capacidad del remitente de cifrar la hora actual, que el receptor luego puede descifrar y verificar con su propio reloj. La indicación de hora se cifra con DES. Los requisitos para que este esquema funcione son los siguientes:

- Los dos agentes deben coincidir en el tiempo actual.
- El emisor y el receptor deben utilizar la misma clave de cifrado.

Si una red ejecuta un programa de sincronización de tiempo, el tiempo del cliente y el servidor se sincronizan automáticamente. Si un programa de sincronización de tiempo no está disponible, los indicadores de tiempo se pueden calcular utilizando el horario del servidor en lugar del de la red. El cliente solicita el tiempo al servidor antes de iniciar la sesión RPC y, a continuación, calcula la diferencia de tiempo entre su propio reloj y el del servidor. Esta diferencia se utiliza para compensar el reloj del cliente al calcular los indicadores de tiempo. Si los relojes del cliente y el servidor dejan de estar sincronizados, el servidor empieza a rechazar las solicitudes del cliente. El sistema de autenticación DH en el cliente se vuelve a sincronizar con el servidor.

El cliente y el servidor llegan a la misma clave de cifrado al generar una *clave de conversación* aleatoria, también conocida como *clave de sesión* y al usar criptografía por clave pública para deducir una *clave común*. La clave común es una clave que sólo el cliente y el servidor son capaces de deducir. La clave de conversación se utiliza para cifrar y descifrar la indicación de hora del cliente. La clave común se emplea para cifrar y descifrar la clave de conversación.

## Autenticación KERB

Kerberos es un sistema de autenticación desarrollado en el MIT. Kerberos ofrece una gran variedad de tipos de cifrado, incluidos DES. La compatibilidad con Kerberos ya no es proporcionada como parte de RPC seguras, pero se incluye una implementación por parte del

servidor y por parte del cliente en la versión. Consulte el [Capítulo 21, “Introducción al servicio Kerberos”](#) de *Guía de administración del sistema: servicios de seguridad* para obtener más información acerca de la implementación de la autenticación de Kerberos.

## Uso de RPC seguras con NFS

Tenga en cuenta los siguientes puntos si tiene planificado utilizar RPC seguras:

- Si un servidor se bloquea cuando no hay nadie cerca (después de un fallo de energía, por ejemplo), se eliminan todas las claves secretas almacenadas en el sistema. Entonces no hay ningún proceso que pueda acceder a los servicios de red seguros o montar un sistema de archivos NFS. Los procesos importantes durante un reinicio se ejecutan normalmente como root. Por lo tanto, estos procesos funcionarían si la clave secreta root se hubiera almacenado en otro lugar, pero nadie estaría disponible para escribir la contraseña que los descifra. `keylogin -r` permite que root almacene la clave secreta borrada en `/etc/.rootkey`, que `keyserv` lee.
- Algunos sistemas se inician en modo de usuario único, con un shell de inicio de sesión root en la consola y sin solicitud de contraseña. La seguridad física es imperativa en estos casos.
- El inicio de equipos sin disco no es totalmente seguro. Otra persona puede conectarse como el servidor de inicio e iniciar un núcleo ilícito que, por ejemplo, haga un registro de la clave secreta en un equipo remoto. El sistema NFS seguro proporciona protección sólo después de que el núcleo y el servidor de claves se ejecuten. De lo contrario, no hay forma de autenticar las respuestas que son dadas por el servidor de inicio. Esta limitación podría ser un problema grave, pero la limitación requiere un ataque sofisticado, utilizando código fuente del núcleo. Además, el delito dejaría evidencia. Si sondea la red para los servidores de inicio, detectaría la ubicación del servidor de inicio ilícito.
- La mayoría de los programas `setuid` son responsabilidad de root. Si la clave secreta de root se almacena en `/etc/.rootkey`, estos programas se comportan como siempre. Si un programa `setuid` es responsabilidad de un usuario, es posible que no siempre funcione el programa `setuid`. Por ejemplo, supongamos que un programa `setuid` es responsabilidad de `dave` y `dave` no ha iniciado sesión en el equipo desde que se inició. El programa no podría acceder a los servicios de red segura.
- Si inicia sesión en un equipo remoto (con `login`, `rlogin` o `telnet`) y usa `keylogin` para obtener acceso, otorga acceso a su cuenta. El motivo es que su clave secreta se transfiere al servidor de ese equipo, que luego almacena la clave secreta. Este proceso sólo es una preocupación si no confía en el equipo remoto. Si tiene dudas, sin embargo, no inicie sesión en un equipo remoto si éste requiere una contraseña. En su lugar, utilice el entorno NFS para montar los sistemas de archivos que compartirá el equipo remoto. Como alternativa, puede utilizar `keylogout` para suprimir la clave secreta del servidor de claves.
- Si un directorio principal se comparte con la opción `-o sec=dh`, los inicios de sesión remotos pueden ser un problema. Si los archivos `/etc/hosts.equiv` o `~/ .rhosts` no están configurados para solicitar una contraseña, el inicio de sesión se realiza correctamente. Sin

embargo, los usuarios no pueden acceder a sus directorios principales porque no se ha producido la autenticación localmente. Si se le pide una contraseña al usuario, el usuario tiene acceso a su directorio principal si la contraseña coincide con la contraseña de la red.

## Mapas autofs

Autofs utiliza tres tipos de mapas:

- Mapa maestro
- Mapas directos
- Mapas indirectos

### Mapa autofs maestro

El mapa `auto_master` asocia un directorio con un mapa. El mapa es una lista maestra que especifica todos los mapas que autofs debe comprobar. El siguiente ejemplo muestra lo que un archivo `auto_master` puede contener.

**EJEMPLO 6-3** Archivo de muestra `/etc/auto_master`

```
# Master map for automounter
#
+auto_master
/net          -hosts          -nosuid,nobrowse
/home        auto_home      -nobrowse
/-           auto_direct    -ro
```

Este ejemplo muestra el archivo genérico `auto_master` con una adición para el mapa `auto_direct`. Cada línea del mapa maestro `/etc/auto_master` tiene la siguiente sintaxis:

*punto\_montaje nombre\_mapa [ opciones\_montaje ]*

*punto\_montaje*      *punto\_montaje* es el nombre de ruta de un directorio (absoluto). Si el directorio no existe, autofs crea el directorio si es posible. Si el directorio existe y no está vacío, el montaje en el directorio oculta su contenido. En esta situación, autofs emitirá un aviso.

La notación `/ -` como punto de montaje indica que este mapa particular es un mapa directo. La notación también significa que ningún punto de montaje concreto está asociado con el mapa.

*nombre\_mapa*      *nombre\_mapa* es el mapa que autofs utiliza para buscar instrucciones de ubicaciones o información de montaje. Si el nombre está precedido por una barra diagonal (`/`), autofs interpreta el nombre como un archivo local. De lo contrario, autofs busca la información de montaje mediante

la búsqueda que se especifica en el archivo de configuración de cambios del servicio de nombres (`/etc/nsswitch.conf`). También se utilizan mapas especiales para `/net`. Consulte “[Punto de montaje /net](#)” en la página 207 para obtener más información.

*opciones\_montaje* *opciones\_montaje* es una lista opcional de opciones separadas por comas que se aplican al montaje de las entradas que se especifican en *nombre\_mapa*, a menos que las entradas de *nombre\_mapa* presenten otras opciones. Las opciones para cada tipo específico de sistema de archivos se muestran en la página del comando `man` de montaje para ese sistema de archivos. Por ejemplo, consulte la página del comando `man mount_nfs(1M)` para obtener opciones de montaje específicas de NFS. Las opciones `bg` (en segundo plano) y `fg` (en primer plano) no se aplican para los puntos de montaje específicos de NFS.

Una línea que comienza con `#` es un comentario. Todos los texto que siguen hasta el final de la línea se ignoran.

Para dividir las líneas y hacerlas más cortas, coloque una barra diagonal inversa (`\`) al final de la línea. El número máximo de caracteres de una entrada es 1024.

---

**Nota** – Si el mismo punto de montaje se utiliza en dos entradas, la primera entrada es utilizada por el comando `automount`. La segunda entrada se ignora.

---

## Punto de montaje /home

El punto de montaje `/home` es el directorio en el que se van a montar las entradas en `/etc/auto_home` (un mapa indirecto).

---

**Nota** – Autofs funciona en todos los equipos y admite de manera predeterminada `/net` y `/home` (directorios principales de montaje automático). Estos valores predeterminados se pueden sustituir mediante entradas en el mapa `NIS auto.master` o la tabla `NIS+ auto_master`, o por la modificación del archivo `/etc/auto_master`.

---

## Punto de montaje /net

Autofs monta en el directorio `/net` todas las entradas del mapa especial `-hosts`. El mapa es un mapa incorporado que utiliza sólo la base de datos de `hosts`. Por ejemplo, si el equipo `gumbo` está en la base de datos `hosts` y exporta cualquiera de sus sistemas de archivos. El siguiente comando cambia el directorio actual por el directorio `root` del equipo `gumbo`.

```
% cd /net/gumbo
```

Autofs puede montar sólo los sistemas de archivos *exportados* del host gumbo, es decir, los sistemas de archivos en un servidor que están disponibles para los usuarios de red en lugar de los sistemas de archivos en un disco local. Por lo tanto, no todos los archivos y directorios en gumbo podrían estar disponibles mediante `/net/gumbo`.

Con el método de acceso `/net`, el nombre de servidor está en la ruta de acceso y depende de la ubicación. Si desea mover un sistema de archivos exportado de un servidor a otro, es posible que la ruta ya no funcione. Debe configurar una entrada en un mapa específicamente para el sistema de archivos que desea en lugar de utilizar `/net`.

---

**Nota** – Autofs verifica la lista de exportaciones del servidor sólo en el momento de montaje. Después montar los sistemas de archivos de un servidor, autofs no vuelve a comprobar con el servidor hasta que los sistemas de archivos del servidor se desmontan automáticamente. Por lo tanto, los sistemas de archivos recién exportados no son “visibles” hasta que los sistemas de archivos en el cliente se desmontan y se vuelven a montar.

---

## Mapas autofs directos

Un mapa directo es un punto de montaje automático. Con un mapa directo, existe una asociación directa entre un punto de montaje en el cliente y un directorio en el servidor. Los mapas directos tienen un nombre de ruta completo e indican la relación explícitamente. El siguiente es un mapa `/etc/auto_direct` típico:

```
/usr/local      - ro \
  /bin           ivy:/export/local/sun4 \
  /share         ivy:/export/local/share \
  /src           ivy:/export/local/src
/usr/man        - ro oak:/usr/man \
                rose:/usr/man \
                willow:/usr/man
/usr/games      - ro peach:/usr/games
/usr/spool/news - ro pine:/usr/spool/news \
                willow:/var/spool/news
```

Las líneas de un mapa directo tienen la siguiente sintaxis:

*clave* [ *opciones\_montaje* ] *ubicación*

*clave*                      *clave* es el nombre de ruta del punto de montaje en un mapa directo.

*opciones\_montaje*        *opciones\_montaje* corresponde a las opciones que desea aplicar a este montaje en particular. Estas opciones son necesarias sólo si las opciones son distintas a las del mapa predeterminado. Las opciones para cada tipo específico de sistema de archivos se muestran en la página del comando



man de montaje para ese sistema de archivos. Por ejemplo, consulte la página del comando `man mount_nfs(1M)` para obtener opciones de montaje específicas de NFS.

*ubicación* *ubicación* es la ubicación del sistema de archivos. Uno o más sistemas de archivos se especifican como *servidor: nombre\_ruta* para sistemas de archivos NFS o *:nombre\_dispositivo* para sistemas de archivos High Sierra (HSFS).

---

**Nota** – El *nombre\_ruta* no debe incluir un punto de montaje de montaje automático. El *nombre\_ruta* debe ser la ruta real absoluta del sistema de archivos. Por ejemplo, la ubicación de un directorio principal debe aparecer como *servidor: /export/home/ nombre de usuario*, no como *servidor : /home/nombre\_usuario*.

---

Como en el mapa maestro, una línea que comienza con # es un comentario. Todos los texto que siguen hasta el final de la línea se ignoran. Coloque una barra diagonal inversa al final de la línea para dividir las líneas largas y hacerlas más cortas.

De todos los mapas, las entradas de un mapa directo se asemejan más a las entradas correspondientes en `/etc/vfstab`. Una entrada puede aparecer en `/etc/vfstab` de la siguiente manera:

```
dancer:/usr/local - /usr/local/tmp nfs - yes ro
```

La entrada equivalente aparece en un mapa directo de la siguiente manera:

```
/usr/local/tmp      -ro      dancer:/usr/local
```

---

**Nota** – No hay opciones de concatenación entre los mapas del montador automático. Cualquiera de las opciones que se agregan a un montador automático, sustituyen todas las opciones que aparecen en los mapas buscados anteriormente. Por ejemplo, las opciones que se incluyen en el mapa `auto_master` se sustituirían con las entradas correspondientes en cualquier otro mapa.

---

Consulte “[Cómo selecciona autof los archivos de sólo lectura más cercanos para los clientes \(ubicaciones múltiples\)](#)” en la [página 216](#) para conocer otras características importantes asociadas con este tipo de mapas.

### Punto de montaje /—

En el [Ejemplo 6–3](#), el punto de montaje /— indica a autof que no asocie las entradas en `auto_direct` con ningún punto de montaje específico. Los mapas indirectos utilizan los puntos

de montaje que se definen en el archivo `auto_master`. Los mapas directos utilizan puntos de montaje que se especifican en el mapa mencionado. Recuerde que, en un mapa directo, la clave, o punto de montaje, es un nombre de ruta completo.

Un archivo `auto_master` NIS o NIS+ sólo puede tener un mapa directo, ya que el punto de montaje debe ser un valor único en el espacio de nombre. Un archivo `auto_master` que sea un archivo local puede tener cualquier número de entradas de mapa directo si las entradas no se duplican.

## Mapas autofs indirectos

Un mapa indirecto usa un valor de sustitución de una clave para establecer la asociación entre un punto de montaje en el cliente y el directorio en el servidor. Los mapas indirectos son útiles para acceder a sistemas de archivos específicos, como directorios principales. El mapa `auto_home` es un ejemplo de un mapa indirecto.

Las líneas de los mapas indirectos tienen la siguiente sintaxis general:

*clave* [ *opciones\_montaje* ] *ubicación*

*clave* *clave* es un nombre sin barras diagonales en un mapa indirecto.

*opciones\_montaje* *opciones\_montaje* corresponde a las opciones que desea aplicar a este montaje en particular. Estas opciones son necesarias sólo si las opciones son distintas a las del mapa predeterminado. Las opciones para cada tipo específico de sistema de archivos se muestran en la página del comando `man` de montaje para ese sistema de archivos. Por ejemplo, consulte la página del comando `man mount_nfs(1M)` para obtener opciones de montaje específicas de NFS.

*ubicación* *ubicación* es la ubicación del sistema de archivos. Uno o más sistemas de archivos se especifican como *servidor: nombre\_ruta*.

---

**Nota** – El *nombre\_ruta* no debe incluir un punto de montaje de montaje automático. El *nombre\_ruta* debe ser la ruta real absoluta del sistema de archivos. Por ejemplo, la ubicación de un directorio debe aparecer en la lista como *servidor: /usr/local*, no como *servidor: /net/servidor/usr/local*.

---

Como en el mapa maestro, una línea que comienza con `#` es un comentario. Todos los texto que siguen hasta el final de la línea se ignoran. Coloque una barra diagonal inversa (`\`) al final de la línea para dividir las líneas largas y hacerlas más cortas. El [Ejemplo 6-3](#) muestra un mapa `auto_master` que contiene la siguiente entrada:

```
/home      auto_home      -nobrowse
```

auto\_home es el nombre del mapa indirecto que contiene las entradas que se montarán en /home. Un mapa típico auto\_home puede contener lo siguiente:

```
david      willow:/export/home/david
rob        cypress:/export/home/rob
gordon     poplar:/export/home/gordon
rajan      pine:/export/home/rajan
tammy      apple:/export/home/tammy
jim        ivy:/export/home/jim
linda      -rw,nosuid    peach:/export/home/linda
```

Por ejemplo, supongamos que el mapa anterior está en el host oak. Suponga que el usuario linda tiene una entrada en la base de datos de contraseñas que especifica su directorio principal como /home/linda. Siempre que linda se conecta al equipo oak, autofs monta el directorio /export/home/linda que reside en el equipo peach. Su directorio principal está montado como de lectura y escritura, nosuid.

Suponga que se producen las siguientes condiciones: el directorio principal del usuario linda aparece en la base de datos de contraseñas como /home/linda. Nadie, ni siquiera Linda, tiene acceso a esta ruta desde cualquier equipo que se haya configurado con el mapa maestro que haga referencia al mapa en el ejemplo anterior.

En estas condiciones, el usuario linda puede ejecutar login o rlogin en cualquiera de estos equipos y tener su directorio principal montado en el lugar para ella.

Además, ahora Linda también puede escribir el comando siguiente:

```
% cd ~david
```

autofs monta el directorio principal de David para ella (si lo autorizan todos los permisos).

---

**Nota** – No hay opciones de concatenación entre los mapas del montador automático. Cualquiera de las opciones que se agregan a un montador automático, sustituyen todas las opciones que aparecen en los mapas buscados anteriormente. Por ejemplo, las opciones que se incluyen en el mapa auto\_master se sustituirían con las entradas correspondientes en cualquier otro mapa.

---

En una red sin un servicio de nombre, debe cambiar todos los archivos relevantes (como /etc/passwd) en todos los sistemas de la red para permitir que Linda acceda a sus archivos. Con NIS, realice los cambios en el servidor NIS maestro y propague las bases de datos relevantes a los servidores esclavos. En una red ejecutando NIS+, la propagación de las bases de datos relevantes para los servidores esclavos se realiza automáticamente después de realizados los cambios.

# Cómo funciona autofs

Autofs es un servicio por parte del cliente que monta automáticamente el sistema de archivos adecuado. Los componentes que trabajan juntos para lograr el montaje automático son los siguientes:

- El comando automount
- El sistema de archivos autofs
- El daemon automountd

El servicio automount, `svc:/system/filesystem/autofs`, que se invoca en el momento de inicio del sistema, lee el archivo de mapa maestro `auto_master` para crear el conjunto inicial de montajes de autofs. Estos montajes de autofs no se montan automáticamente en momento de inicio. Estos montajes son puntos en los que los sistemas de archivos se montan en el futuro. Estos puntos también se conocen como nodos desencadenadores.

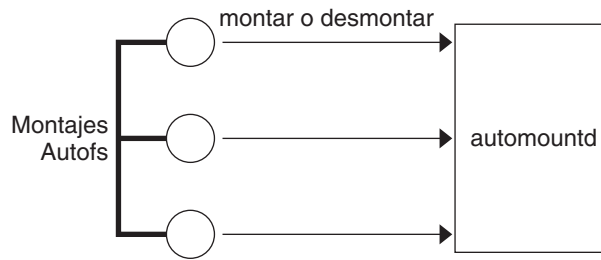
Después de que los montajes autofs están configurados, estos montajes puede desencadenar sistemas de archivos para que se monten en ellos. Por ejemplo, cuando autofs recibe una solicitud para acceder a un sistema de archivos que no está montado en la actualidad, autofs invoca el comando `automountd`, que monta el sistema de archivos solicitado.

Después del montaje inicial de autofs, se utiliza el comando `automount` para actualizar los montajes autofs según sea necesario. El comando compara la lista de los montajes en el mapa `auto_master` con la lista de sistemas de archivos montados en el archivo de tabla de montaje `/etc/mnttab` (anteriormente `/etc/mtab`). `automount` realiza los cambios adecuados. Este proceso les permite a los administradores del sistema cambiar la información de montaje dentro de `auto_master` y que los procesos autofs utilicen esos cambios sin detener y reiniciar el daemon autofs. Una vez que el sistema de archivos está montado, no es necesario que `automountd` realice ninguna acción hasta que el sistema de archivos se desmonte automáticamente.

A diferencia de `mount`, `automount` no lee el archivo `/etc/vfstab` (que es específico para cada equipo) para obtener una lista de sistemas de archivos para montar. El comando `automount` se controla dentro de un dominio y en los equipos a través de espacio de nombres o archivos locales.

A continuación se muestra una descripción general simplificada de cómo funciona autofs.

El daemon `automountd` se inicia en el momento del inicio mediante el servicio `svc:/system/filesystem/autofs`. Consulte la [Figura 6–3](#). Este servicio también ejecuta el comando `automount`, que lee el mapa maestro e instala los puntos de montaje de autofs. Consulte “[Cómo Autofs inicia el proceso de navegación \(mapa maestro\)](#)” en la [página 214](#) para obtener más información.

FIGURA 6-3 El servicio `svc:/system/filesystem/autofs` inicia `automount`

Autofs es un sistema de archivos de núcleos que admite montaje y desmontaje automático.

Cuando se realiza una solicitud para acceder a un sistema de archivos en un punto de montaje autofs, se produce lo siguiente:

1. Autofs intercepta la solicitud.
2. Autofs envía un mensaje al comando `automountd` para el sistema de archivos solicitado que se montará.
3. `automountd` localiza la información del sistema de archivos en un mapa, crea el nodo desencadenador y realiza el montaje.
4. Autofs permite que continúe la solicitud interceptada.
5. Autofs desmonta el sistema de archivos después de un período de inactividad.

---

**Nota** – Los montajes que se administran a través de los servicios autofs no deben montarse ni desmontarse manualmente. Aunque la operación se realizara correctamente, el servicio autofs no comprueba que el objeto se haya desmontado, lo que da como resultado posibles incoherencias. Si se reinicia, se eliminan todos los puntos de montaje de autofs.

---

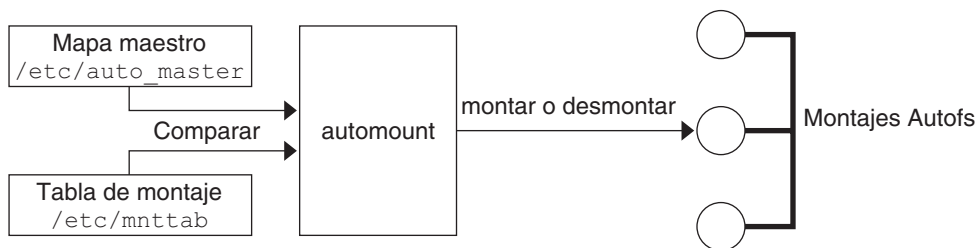
## Cómo navega autofs por la red (mapas)

Autofs busca una serie de mapas para navegar a través de la red. Los mapas son archivos que contienen información como las entradas de las contraseñas de todos los usuarios en una red o los nombres de todos los equipos de una red. De hecho, los mapas contienen equivalentes para toda la red de los archivos de administración de UNIX. Los mapas están disponibles localmente o a través de un servicio de nombres de red, como NIS o NIS+. Consulte [“Modificar cómo navega autofs por la red \(modificación de mapas\)”](#) en la página 222.

## Cómo Autofs inicia el proceso de navegación (mapa maestro)

El comando automount lee el mapa maestro en el inicio del sistema. Cada entrada del mapa maestro es un nombre de mapa directo o un nombre de mapa indirecto, su ruta de acceso y sus opciones de montaje, como se muestra en la [Figura 6-4](#). El orden específico de las entradas no es importante. automount compara las entradas del mapa maestro con las entradas en la tabla de montaje para generar una lista actual.

FIGURA 6-4 Navegación por el mapa maestro



## Proceso de montaje autofs

Lo que hace el servicio autofs cuando se desencadena una solicitud de montaje depende de cómo estén configurados los mapas del montador automático. El proceso de montaje normalmente es el mismo para todos los montajes. Sin embargo, el resultado final cambia según el punto de montaje que se especifica y la complejidad de los mapas. El proceso de montaje incluye la creación de nodos desencadenadores.

### Montaje autofs simple

Para ayudar a explicar el proceso de montaje autofs, supongamos que los siguientes archivos están instalados.

```

$ cat /etc/auto_master
# Master map for automounter
#
+auto_master
/net      -hosts      -nosuid,nobrowse
/home     auto_home   -nobrowse
/share    auto_share
$ cat /etc/auto_share
# share directory map for automounter
#
ws        gumbo:/export/share/ws
  
```

Cuando se accede al directorio `/share`, el servicio `autofs` crea un nodo desencadenador para `/share/ws`, que es una entrada de `/etc/mnttab` que se parece a la siguiente entrada:

```
-hosts /share/ws      autofs  nosuid,nobrowse,ignore,nest,dev=###
```

Cuando se accede al directorio `/share/ws`, el servicio `autofs` completa el proceso con estos pasos:

1. Comprueba la disponibilidad del servicio de montaje del servidor.
2. Monta el sistema de archivos solicitados en `/share`. Ahora el archivo `/etc/mnttab` contiene las siguientes entradas.

```
-hosts /share/ws      autofs  nosuid,nobrowse,ignore,nest,dev=###  
gumbo:/export/share/ws /share/ws  nfs    nosuid,dev=####  #####
```

## Montaje jerárquico

Cuando se definen varias capas en los archivos del montador automático, el proceso de montaje se hace más complejo. Por ejemplo, si amplía el archivo `/etc/auto_shared` del ejemplo anterior para incluir lo siguiente:

```
# share directory map for automounter  
#  
ws      /      gumbo:/export/share/ws  
        /usr   gumbo:/export/share/ws/usr
```

El proceso de montaje es básicamente igual que el ejemplo anterior en el que se accede al punto de montaje `/share/ws`. Además, se crea un nodo desencadenador hacia el siguiente nivel (`/usr`) en el sistema de archivos `/share/ws` de forma que el siguiente nivel se puede montar si es que se accede a él. En este ejemplo, `/export/share/ws/usr` debe existir en el servidor NFS para que se cree el nodo desencadenador.



---

**Precaución** – No utilice la opción `-soft` al especificar capas jerárquicas. Consulte [“Desmontaje de autofs” en la página 215](#) para obtener una explicación de esta limitación.

---

## Desmontaje de autofs

El desmontaje que se produce después de un cierto tiempo de inactividad es ascendente (orden inverso de montaje). Si uno de los directorios en un nivel superior en la jerarquía está ocupado, sólo los sistemas de archivos debajo de ese directorio se desmontan. Durante el proceso de desmontaje, se eliminan todos los nodos desencadenadores y se desmonta el sistema de archivos. Si el sistema de archivos está ocupado, el desmontaje falla y los nodos desencadenadores se vuelven a instalar.



**Precaución** – No utilice la opción `-soft` al especificar capas jerárquicas. Si se utiliza la opción `-soft`, las solicitudes para volver a instalar los nodos desencadenadores se ponen en tiempo de espera. Si no se vuelven a instalar los nodos desencadenadores, no se obtiene acceso al siguiente nivel de montajes. La única forma para eliminar este problema es que el montador automático desmonte todos los componentes de la jerarquía. El montador automático puede completar el desmontaje si espera que los sistemas de archivos se desmonten automáticamente o si reinicia el sistema.

## Cómo selecciona autofs los archivos de sólo lectura más cercanos para los clientes (ubicaciones múltiples)

El mapa directo de ejemplo contiene lo siguiente:

```
/usr/local      -ro \
  /bin          ivy:/export/local/sun4\
  /share        ivy:/export/local/share\
  /src          ivy:/export/local/src
/usr/man        -ro oak:/usr/man \
                rose:/usr/man \
                willow:/usr/man
/usr/games      -ro peach:/usr/games
/usr/spool/news -ro pine:/usr/spool/news \
                willow:/var/spool/news
```

Los puntos de montaje `/usr/man` y `/usr/spool/news` muestran más de una ubicación, tres ubicaciones para el primer punto de montaje y dos ubicaciones para el segundo punto de montaje. Cualquiera de las ubicaciones replicadas puede proporcionar el mismo servicio para cualquier usuario. Este procedimiento sólo es necesario cuando se monta un sistema de archivos de sólo lectura, ya que debe tener algún control sobre las ubicaciones de los archivos que escribe o modifica. Debe evitar modificar archivos en un servidor en un momento y, minutos más tarde, modificar el “mismo” archivo en otro servidor. El beneficio es que se utiliza automáticamente el mejor servidor disponible sin esfuerzo por parte del usuario.

Si los sistemas de archivos están configurados como réplicas (consulte “¿Qué es un sistema de archivos replicado?” en la página 197), los clientes tienen la ventaja de utilizar conmutación por error. No sólo se determina automáticamente el mejor servidor, sino que si el servidor deja de estar disponible, el cliente utiliza automáticamente el siguiente mejor servidor.

Un ejemplo de un buen sistema de archivos para configurar como una réplica son las páginas del comando `man`. En una red grande, más de un servidor puede exportar el conjunto actual de páginas del comando `man`. No importa desde qué servidor se montan las páginas del comando `man` si el servidor ejecuta y exporta sus sistemas de archivos. En el ejemplo anterior, se expresan varias ubicaciones de montaje como una lista de ubicaciones de montaje en la entrada de mapa.



```
/usr/man -ro oak:/usr/man rose:/usr/man willow:/usr/man
```

En este ejemplo, puede montar las páginas del comando man de los servidores oak, rose o willow. El mejor servidor depende de una serie de factores, incluidos los siguientes:

- El número de servidores que admiten un nivel de protocolo NFS particular
- La proximidad del servidor
- La ponderación

Durante el proceso de ordenación, se realiza un recuento del número de servidores que admiten cada versión del protocolo NFS. La versión del protocolo compatible con la mayoría de los servidores se convierte en el protocolo que se utiliza de manera predeterminada. Esta selección proporciona al cliente el número máximo de servidores de los que puede depender.

Una vez que se encuentra el mayor subconjunto de servidores con la misma versión del protocolo, esa lista de servidores se ordena por proximidad. Para determinar la proximidad, se inspeccionan las direcciones IPv4. Las direcciones IPv4 muestran qué servidores se incluyen en cada subred. Los servidores en una subred local obtienen preferencia sobre los servidores en una subred remota. La preferencia del servidor más cercano reduce la latencia y el tráfico en la red.

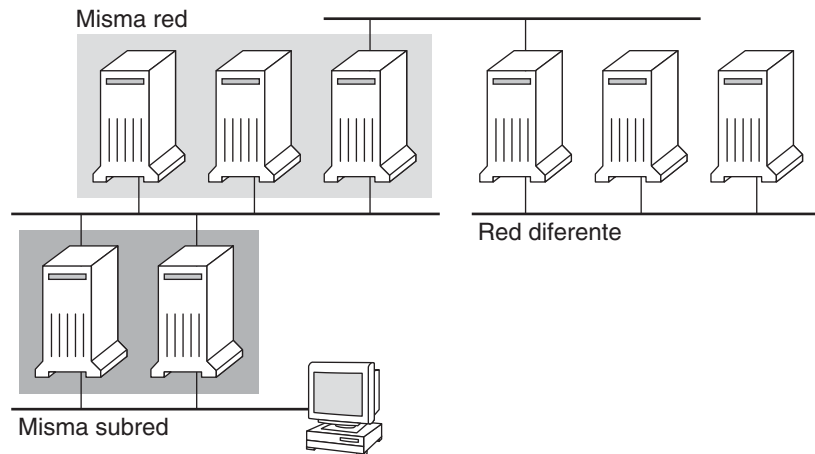
---

**Nota** – La proximidad no se puede determinar para réplicas que utilizan direcciones IPv6.

---

La [Figura 6–5](#) ilustra la proximidad de servidor.

**FIGURA 6–5** Proximidad de servidor



Si varios servidores que admiten el mismo protocolo se encuentran en la subred local, se determina el tiempo de conexión de cada servidor y se utiliza el servidor más rápido. El proceso de ordenación también puede estar influido por el uso de ponderación (consulte [“Autofs y ponderación” en la página 219](#)).

Por ejemplo, si hay más servidores versión 4, la versión 4 pasa a ser el protocolo que se utiliza de manera predeterminada. Sin embargo, ahora el proceso de ordenación es más complejo. A continuación se exponen algunos ejemplos de cómo la funciona el proceso de ordenación:

- Los servidores en una subred local obtienen preferencia sobre los servidores en una subred remota. Por lo tanto, si un servidor versión 3 está en la subred local y el servidor versión 4 más próximo se encuentra en una subred remota, el servidor versión 3 tiene preferencia. Del mismo modo, si la subred local tiene servidores versión 2, éstos tienen preferencia sobre las subredes remotas con servidores versión 3 y versión 4.
- Si la subred local tiene un número variado de servidores versión 2, versión 3 y versión 4, es necesario seguir realizando el proceso de ordenación. El montador automático prefiere la versión más alta de la subred local. En este ejemplo, la versión 4 es la versión más alta. Sin embargo, si la subred local tiene más servidores versión 3 o versión 2 que servidores versión 4, el montador automático “disminuye” de la versión más alta en la subred local de a una versión. Por ejemplo, si la subred local dispone de tres servidores con la versión 4, tres servidores con la versión 3 y diez servidores con la versión 2, se selecciona un servidor versión 3.
- De igual forma, si la subred local tiene un número variado de servidores versión 2 y versión 3, el montador automático primero busca qué versión representa la versión más alta de la subred local. A continuación, el montador automático recuenta el número de servidores que ejecuta cada versión. Si la versión más alta en la subred local también representa a la mayoría de los servidores, se selecciona la versión más alta. Si una versión más baja tiene más servidores, el montador automático disminuye de la versión más alta en la subred local de a una versión. Por ejemplo, si hay más servidores versión 2 en la subred local que servidores versión 3, se selecciona un servidor versión 2.

---

**Nota** – La ponderación también está influenciada por los valores de palabra clave en el archivo `/etc/default/nfs`. Específicamente, los valores de `NFS_SERVER_VERSMIN`, `NFS_CLIENT_VERSMIN`, `NFS_SERVER_VERSMAX` y `NFS_CLIENT_VERSMAX` pueden hacer que algunas versiones se excluyan del proceso de ordenación. Para obtener más información sobre estas palabras clave, consulte [“Palabras clave para el archivo `/etc/default/nfs`” en la página 142](#).

---

Con la conmutación por errores, la ordenación se comprueba en el momento del montaje cuando se selecciona un servidor. Es útil contar con varias ubicaciones en un entorno donde los servidores individuales no puedan exportar sus sistemas de archivos temporalmente.

La conmutación por errores es especialmente útil en una red grande con muchas subredes. Autofs elige el servidor adecuado y es capaz de confinar el tráfico de red NFS a un segmento de la red local. Si un servidor tiene varias interfaces de red, puede mostrar el nombre de host que está asociado con cada una de las interfaces de red si la interfaz fuera otro servidor. Autofs selecciona la interfaz más próxima al cliente.

**Nota** – No se realizan comprobaciones de ponderación ni de proximidad con los montajes manuales. El comando `mount` prioriza los servidores que se muestran de izquierda a derecha.

Para obtener más información, consulte la página del comando `man automount(1M)`.

## Autofs y ponderación

Puede influir en la selección de los servidores con el mismo nivel de proximidad si añade un valor de ponderación al mapa autofs. Por ejemplo:

```
/usr/man -ro oak,rose(1),willow(2):/usr/man
```

Los números entre paréntesis indican una ponderación. Los servidores sin una ponderación tienen un valor de cero y, por lo tanto, es más probable que se seleccionen. Cuanto mayor sea el valor de ponderación, menos probabilidades hay de que se seleccione ese servidor.

**Nota** – Todos los demás factores de selección de servidor son más importantes que la ponderación. La ponderación sólo se tiene en cuenta al seleccionar entre los servidores con la misma proximidad de red.

## Variables en una entrada de mapa

Puede crear una variable específica del cliente si agrega un signo de dólar (\$) a su nombre. La variable le ayuda a acomodar diferentes tipos de arquitecturas que están accediendo a la misma ubicación del sistema de archivos. También puede utilizar llaves para delimitar el nombre de la variable de las letras o dígitos agregados. La [Tabla 6–2](#) muestra las variables de mapa predefinidas.

**TABLA 6–2** Variables de mapa predefinidas

Variable	Significado	Deriva de	Ejemplo
ARCH	Tipo de arquitectura	uname -m	sun4

TABLA 6-2 Variables de mapa predefinidas (Continuación)

Variable	Significado	Deriva de	Ejemplo
CPU	Tipo de procesador	uname -p	sparc
HOST	Nombre de host	uname -n	dinky
OSNAME	Nombre del sistema operativo	uname -s	SunOS
OSREL	Versión del sistema operativo	uname -r	5.8
OSVERS	Versión del sistema operativo (versión de lanzamiento)	uname -v	GENERIC

Puede utilizar variables en cualquier parte de una línea de entrada excepto como clave. Por ejemplo, suponga que tiene un servidor de archivos que exporta binarios para SPARC y arquitecturas x86 de `/usr/local/bin/sparc` y `/usr/local/bin/x86` respectivamente. Los clientes pueden montarse mediante una entrada de mapa como la siguiente:

```
/usr/local/bin      -ro      server:/usr/local/bin/$CPU
```

La misma entrada para todos los clientes se aplica a todas las arquitecturas.

**Nota** – La mayoría de las aplicaciones escritas para cualquiera de las arquitecturas sun4 puede ejecutarse en todas las plataformas sun4. La variable `-ARCH` está codificada de forma rígida en sun4.

## Mapas que hacen referencia a otros mapas

Una entrada de mapa `+nombre_mapa` que se usa en un mapa de archivos hace que automount lea el mapa especificado como si estuviera incluido en el archivo actual. Si `nombre_mapa` no está precedido por una barra diagonal, autofs trata el nombre de mapa como una cadena de caracteres y utiliza la política de conmutación de nombre y servicio para buscar el nombre del mapa. Si el nombre de ruta es un nombre de ruta absoluto, automount comprueba un mapa local de dicho nombre. Si el nombre del mapa comienza con un guión (`-`), automount consulta el mapa integrado adecuado, como `hosts`.

Este archivo de conmutador de nombre y servicio contiene una entrada para autofs con la etiqueta `automount`, que contiene el orden en que los servicios de nombres se buscan. El siguiente archivo es un ejemplo de un archivo de conmutador de nombre y servicio.

```
#
# /etc/nsswitch.nis:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it uses NIS (YP) in conjunction with files.
#
```

```
# "hosts:" and "services:" in this file are used only if the /etc/netconfig
# file contains "switch.so" as a nametoaddr library for "inet" transports.
# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:      files nis
group:       files nis

# consult /etc "files" only if nis is down.
hosts:       nis [NOTFOUND=return] files
networks:    nis [NOTFOUND=return] files
protocols:   nis [NOTFOUND=return] files
rpc:         nis [NOTFOUND=return] files
ethers:      nis [NOTFOUND=return] files
netmasks:    nis [NOTFOUND=return] files
bootparams:  nis [NOTFOUND=return] files
publickey:   nis [NOTFOUND=return] files
netgroup:    nis
automount:   files nis
aliases:     files nis
# for efficient getservbyname() avoid nis
services:    files nis
```

En este ejemplo, los mapas locales se buscan antes que los mapas NIS. Por lo tanto, puede tener unas pocas entradas en su mapa /etc/auto\_home para los directorios principales a los que se accede con más frecuencia. A continuación, puede utilizar el conmutador a fin de volver al mapa NIS para las otras entradas.

```
bill          cs.csc.edu:/export/home/bill
bonny         cs.csc.edu:/export/home/bonny
```

Después de consultar el mapa incluido, si no se encuentra ninguna coincidencia, automount continúa la exploración del mapa actual. Por lo tanto, puede agregar más entradas después de una entrada +.

```
bill          cs.csc.edu:/export/home/bill
bonny         cs.csc.edu:/export/home/bonny
+auto_home
```

El mapa que se incluye puede ser un archivo local o un mapa integrado. Recuerde, sólo los archivos locales pueden contener entradas +.

```
+auto_home_finance    # NIS+ map
+auto_home_sales       # NIS+ map
+auto_home_engineering # NIS+ map
+/etc/auto_mystuff     # local map
+auto_home             # NIS+ map
+.-hosts               # built-in hosts map
```

---

**Nota** – No puede usar entradas + en los mapas NIS+ o NIS.

---

## Mapas autofs ejecutables

Puede crear un mapa autofs que ejecute algunos comandos para generar puntos de montaje autofs. Puede beneficiarse del uso de un mapa autofs ejecutable si necesita poder crear la estructura autofs desde una base de datos o un archivo plano. El inconveniente que presenta el uso de un mapa ejecutable es que el mapa debe instalarse en cada host. Un mapa ejecutable no puede incluirse en el servicio de nombres NIS o NIS+.

El mapa ejecutable debe contener una entrada en el archivo `auto_master`.

```
/execute    auto_execute
```

A continuación se muestra un ejemplo de mapa ejecutable:

```
#!/bin/ksh
#
# executable map for autofs
#

case $1 in
    src) echo '-nosuid,hard bee:/export1' ;;
esac
```

Para que este ejemplo funcione, el archivo debe ser instalado como `/etc/auto_execute` y debe disponer de un conjunto de bits ejecutable. Establezca los permisos en 744. En estas circunstancias, si ejecuta el siguiente comando, hace que se monte el sistema de archivos `/export1` de bee:

```
% ls /execute/src
```

## Modificar cómo navega autofs por la red (modificación de mapas)

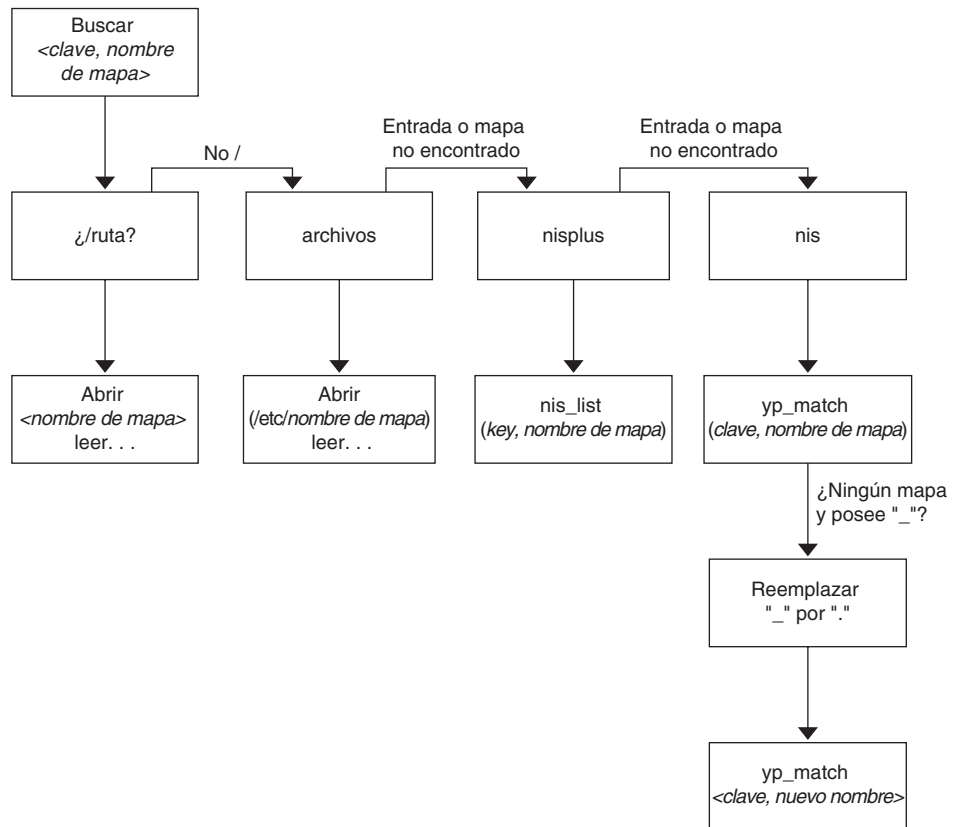
Puede modificar, suprimir o agregar entradas a mapas para satisfacer las necesidades de su entorno. Cuando las aplicaciones y otros sistemas de archivos que los usuarios necesitan cambian su ubicación, los mapas deben reflejar los cambios. Puede modificar los mapas autofs en cualquier momento. Que las modificaciones sean efectivas la próxima vez que automountd monte un sistema de archivos depende de qué mapa se modifique y de qué tipo de cambios realice.

## Comportamiento predeterminado de autofs con los servicios de nombres

En el momento del inicio, el servicio `svc:/system/filesystem/autofs` invoca a autofs, y autofs comprueba el mapa maestro `auto_master`. Autofs está sujeto a las reglas que se tratan más adelante.

Autofs utiliza el servicio de nombres que se especifica en la entrada automount del archivo `/etc/nsswitch.conf`. Si NIS+ se especifica, en contraposición con los archivos locales o NIS, todos los nombres de mapas se utilizan tal como están. Si se selecciona NIS y autofs no puede encontrar un mapa que autofs necesite, pero encuentra un nombre de mapa que contiene uno o más guiones bajos, los guiones bajos se cambian por puntos. Este cambio permite que los antiguos nombres NIS funcionen. A continuación, autofs vuelve a comprobar el mapa, como se muestra en la [Figura 6-6](#).

FIGURA 6-6 Cómo utiliza autofs el servicio de nombres



La actividad de la pantalla para esta sesión se asemeja al ejemplo siguiente.

```

$ grep /home /etc/auto_master
/home          auto_home

$ ypmatch brent auto_home
Can't match key brent in map auto_home. Reason: no such map in
server's domain.
  
```

```
$ ypmatch brent auto.home
diskus:/export/home/diskus1/&
```

Si selecciona “archivos” como servicio de nombres, se asume que todos los mapas serán archivos locales en el directorio /etc. Autofs interpreta un nombre de mapa que comienza con una barra diagonal (/) como local, independientemente de qué servicio de nombres utilice autofs.

# Referencia de autofs

Las secciones restantes de este capítulo describen características y temas más avanzados de autofs.

## Autofs y metacaracteres

Autofs reconoce que algunos caracteres tienen un significado especial. Algunos caracteres se utilizan para las sustituciones, y algunos caracteres se utilizan para proteger a los demás caracteres del analizador de mapa autofs.

### Y comercial (&)

Si tiene un mapa con muchos subdirectorios especificados, como el siguiente, tenga en cuenta utilizar sustituciones de cadenas.

john	willow:/home/john
mary	willow:/home/mary
joe	willow:/home/joe
able	pine:/export/able
baker	peach:/export/baker

Puede utilizar el carácter de Y comercial (&) para sustituir la clave siempre que la clave aparezca. Si se utiliza el símbolo &, el mapa anterior cambia por el siguiente:

john	willow:/home/&
mary	willow:/home/&
joe	willow:/home/&
able	pine:/export/&
baker	peach:/export/&

También puede utilizar sustituciones de claves en un mapa directo, en situaciones como la siguiente:

/usr/man	willow,cedar,poplar:/usr/man
----------	------------------------------

También puede simplificar más la entrada de la siguiente manera:

/usr/man	willow,cedar,poplar:&
----------	-----------------------



Tenga en cuenta que la sustitución de & utiliza toda la cadena de la clave. Por lo tanto, si la clave en un mapa directo se inicia con una / (como debería ser), la barra diagonal se incluye en la sustitución. Por lo tanto, por ejemplo, no puede hacer lo siguiente:

```
/progs          &1,&2,&3:/export/src/progs
```

El motivo es que autofs interpretaría el ejemplo, como lo siguiente:

```
/progs          /progs1,/progs2,/progs3:/export/src/progs
```

## Asterisco (\*)

Puede utilizar el carácter de sustitución universal, el asterisco (\*), para que coincida con cualquier clave. Puede montar el sistema de archivos /export desde todos los hosts a través de esta entrada de mapa.

```
*              &:/export
```

Cada & se sustituye por el valor de cualquier clave dada. Autofs interpreta el asterisco como un carácter de fin de archivo.

## Autofs y caracteres especiales

Si cuenta con una entrada de mapa que contiene caracteres especiales, es posible que deba montar directorios que tienen nombres que confunden al analizador de mapa autofs. El analizador autofs es sensible a los nombres que contienen dos puntos, comas y espacios, por ejemplo. Estos nombres deben estar entre comillas dobles, como en el caso siguiente:

```
/vms    -ro    vmsserver: - - - "rc0:dk1 - "  
/mac    -ro    gator:/ - "Mr Disk - "
```



## **P A R T E   I I I**

### **Temas sobre el SLP**

En esta sección, se proporciona información general e información de planificación, tareas y referencia para el servicio de protocolo de ubicación de servicios (SLP).



## SLP (descripción general)

---

El protocolo de ubicación de servicios (SLP) proporciona una estructura portátil independiente de plataforma para la detección y el aprovisionamiento de servicios de red habilitados para SLP. En este capítulo, se describen la arquitectura del SLP y la implementación de Solaris del SLP para intranets de IP.

- [“Arquitectura del SLP” en la página 229](#)
- [“Implementación del SLP” en la página 232](#)

### Arquitectura del SLP

En esta sección, se detalla el funcionamiento esencial del SLP y se describen los agentes y procesos que se utilizan en la administración del SLP.

SLP proporciona todos los siguientes servicios automáticamente, con poca o sin configuración.

- La aplicación cliente solicita información necesaria para acceder a un servicio.
- Anuncio de servicios en servidores de software o dispositivos de hardware de red; por ejemplo, impresoras, servidores de archivos, cámaras de vídeo y servidores HTTP.
- Recuperación gestionada tras fallos de servidores principales.

Además, puede hacer lo siguiente para administrar y ajustar el funcionamiento del SLP si es necesario.

- Organizar los servicios y usuarios en *ámbitos* que están compuestos por grupos lógicos o funcionales.
- Permitir el registro del SLP para supervisar y solucionar problemas del funcionamiento del SLP en la red.
- Ajustar los parámetros de sincronización del SLP para mejorar el rendimiento y la escalabilidad.

- Configurar el SLP para que no envíe ni procese mensajes de multidifusión cuando el SLP se implementa en redes que no admiten el enrutamiento de multidifusión.
- Implementar agentes de directorio del SLP para mejorar la escalabilidad y el rendimiento.

## Resumen del diseño del SLP

Las bibliotecas del SLP informan a los agentes para redes que anuncian servicios para que dichos servicios se detecten por medio de una red. Los agentes del SLP mantienen información actualizada sobre el tipo y la ubicación de servicios. Esos agentes también pueden utilizar registros de proxy para anunciar servicios que no están directamente habilitados para SLP. Para obtener más información, consulte el [Capítulo 10, “Incorporación de servicios antiguos”](#).

Las aplicaciones cliente dependen de bibliotecas del SLP que realizan solicitudes directamente a los agentes que anuncian servicios.

## Agentes y procesos del SLP

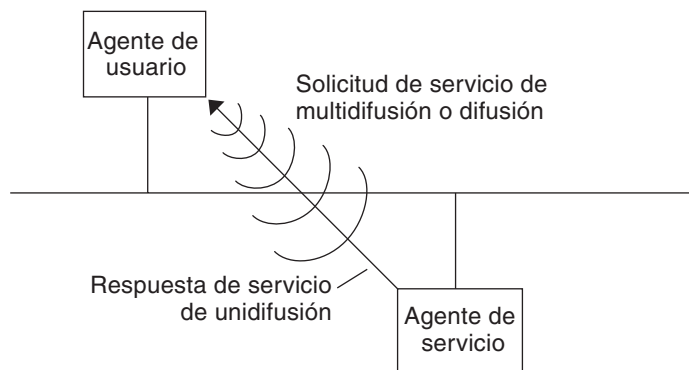
En la siguiente tabla, se describen los agentes del SLP. Para obtener definiciones ampliadas de estos términos y otros términos que se utilizan en este volumen, consulte el [Glosario](#).

TABLA 7-1 Agentes del SLP

Agente del SLP	Descripción
Agente de directorio (DA)	Proceso que almacena en la antememoria anuncios del SLP que son registrados por agentes de servicio (SA). El DA reenvía anuncios de servicios a agentes de usuario (UA) a petición.
Agente de servicio (SA)	Agente del SLP que actúa en nombre de un servicio para distribuir anuncios de servicios y registrar el servicio con agentes de directorio (DA).
Agente de usuario (UA)	Agente del SLP que actúa en nombre de un usuario o una aplicación para obtener información sobre anuncios de servicios.
ámbito	Una agrupación administrativa o lógica de servicios.

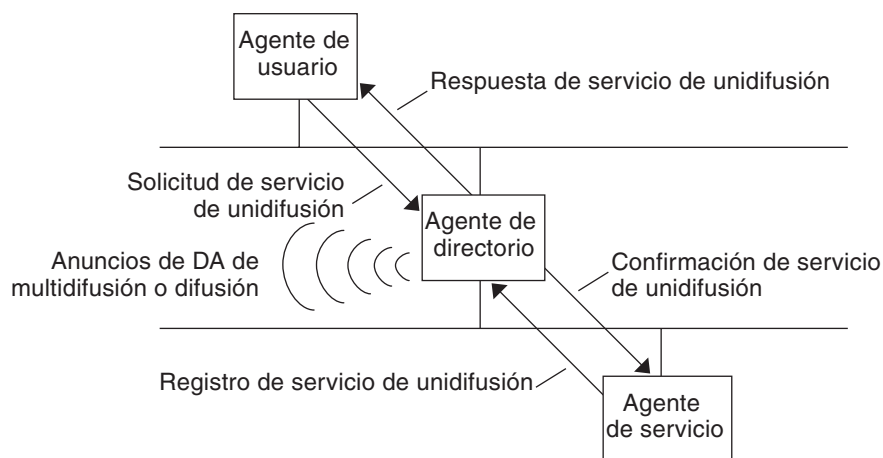
En la siguiente figura, se muestran los agentes y procesos básicos que implementan la arquitectura del SLP. La figura representa una implementación predeterminada del SLP. No se ha realizado ninguna configuración especial. Sólo dos agentes son necesarios: el UA y el SA. La estructura del SLP permite al UA enviar una multidifusión de solicitudes de servicios al SA. El SA envía una unidifusión de una respuesta al UA. Por ejemplo, cuando el UA envía un mensaje de solicitud de servicio, el SA responde con un mensaje de respuesta de servicio. La respuesta de servicio contiene la ubicación de los servicios que coinciden con los requisitos del cliente. Otras solicitudes y respuestas son posibles para atributos y tipos de servicio. Para obtener más información, consulte el [Capítulo 11, “SLP \(referencia\)”](#).

FIGURA 7-1 Agentes y procesos básicos del SLP



En la siguiente figura, se muestran los agentes y procesos básicos que implementan la arquitectura del SLP cuando un DA se implementa en la estructura.

FIGURA 7-2 Agentes y procesos arquitectónicos del SLP implementados con un DA



Al implementar DA, menos mensajes se envían en la red, y los UA pueden recuperar información mucho más rápido. Los DA son esenciales cuando el tamaño de una red aumenta o en situaciones en las que no se admite el enrutamiento de multidifusión. El DA sirve como una antememoria para anuncios de servicios registrados. Los SA envían mensajes de registro (SrvReg) que muestran todos los servicios que anuncian para los DA. Los SA, a continuación, reciben confirmaciones (SrvAck) en respuesta. Los anuncios de servicios se actualizan con el

DA o caducan según la duración que se establece para el anuncio. Después de que un UA detecta un DA, el UA envía una unidifusión de una solicitud al DA en lugar de enviar una multidifusión de solicitudes a los SA.

Para obtener más información sobre los mensajes del SLP de Solaris, consulte el [Capítulo 11, “SLP \(referencia\)”](#).

## Implementación del SLP

En la implementación del SLP de Solaris, los SA, los UA, los DA, los servidores de SA, los ámbitos y otros componentes arquitectónicos del SLP en la [Tabla 7–1](#) son parcialmente asignados en `slpd` y en procesos de aplicación. El daemon del SLP, `slpd`, organiza determinadas interacciones del SLP fuera del host para realizar lo siguiente:

- Emplear la detección pasiva y activa de agentes de directorio para detectar todos los DA en la red.
- Mantener una tabla actualizada de DA para utilizar los UA y SA en el host local.
- Actuar como un servidor de SA de proxy para anuncios de servicios antiguos (registro de proxy).

Además, puede establecer la propiedad `net.slpisDA` para configurar `slpd` para que actúe como un DA. Consulte el [Capítulo 9, “Administración del SLP \(tareas\)”](#).

Para obtener más información sobre el daemon del SLP, consulte [slpd\(1M\)](#).

Además de `slpd`, las bibliotecas de cliente de Java y C/C++ (`libslp.so` y `slp.jar`) permiten el acceso a la estructura del SLP para los clientes de UA y SA. Las bibliotecas de cliente proporcionan las siguientes funciones:

- Software que ofrece servicios de red que pueden registrar y anular registros de anuncios de servicios.
- Software cliente que puede solicitar servicios emitiendo consultas de anuncios de servicios.
- La lista de ámbitos del SLP disponibles para registro y solicitudes.

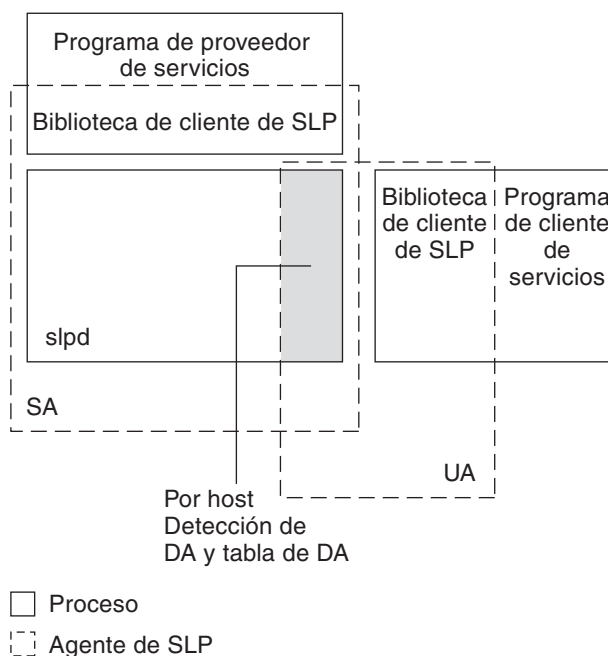
No se necesita ninguna configuración especial para habilitar la comunicación entre procesos entre `slpd` y las bibliotecas de cliente que proporcionan los servicios anteriores. Sin embargo, debe ejecutar el proceso `slpd` antes de cargar las bibliotecas de cliente para que las bibliotecas funcionen.

En la siguiente figura, la biblioteca de cliente del SLP en el programa de proveedor de servicios emplea la funcionalidad del SA. El programa de proveedor de servicios utiliza la biblioteca de cliente del SLP para registrar y anular registros de servicios con `slpd`. La biblioteca de cliente del SLP en el programa de cliente de servicios emplea la funcionalidad del UA. El programa de cliente de servicios utiliza la biblioteca de cliente del SLP para realizar solicitudes. La biblioteca



de cliente del SLP envía multidifusiones de solicitudes a los SA o envía unidifusiones de solicitudes a los DA. Esta comunicación es transparente para la aplicación, excepto que el método de unidifusión para emitir solicitudes es más rápido. El comportamiento de la biblioteca de cliente puede verse afectado al establecer distintas propiedades de configuración del SLP. Para obtener más información, consulte el [Capítulo 9, “Administración del SLP \(tarear\)”](#). El proceso `slpd` gestiona todas las funciones del SA, como la respuesta a solicitudes de multidifusión y el registro con DA.

FIGURA 7-3 Implementación del SLP



## Otras fuentes de información del SLP

Consulte los siguientes documentos para obtener más información sobre el SLP:

- Kempf, James y St. Pierre, Pete. *Service Location Protocol for Enterprise Networks (Protocolo de ubicación de servicios para redes empresariales)*. John Wiley & Sons, Inc. Número ISBN: 0-471-31587-7.
- *Authentication Management Infrastructure Administration Guide (Guía de administración de infraestructura de gestión de autenticación)*. Número de referencia: 805-1139-03.

- Guttman, Erik; Perkins, Charles; Veizades, John; y Day, Michael. *Service Location Protocol, Version 2, RFC 2608 (Protocolo de ubicación de servicios, versión 2, RFC 2608)* del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [<http://www.ietf.org/rfc/rfc2608.txt>]
- Kempf, James y Guttman, Erik. *An API for Service Location, RFC 2614 (Una API para ubicación de servicios, RFC 2614)* del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [<http://www.ietf.org/rfc/rfc2614.txt>]

## Planificación y habilitación del SLP (tareas)

---

En este capítulo, se proporciona información sobre la planificación y habilitación del SLP. En las siguientes secciones, se tratan la configuración del SLP y el proceso para habilitar el SLP.

- [“Consideraciones para la configuración del SLP” en la página 235](#)
- [“Uso de snoop para supervisar la actividad del SLP” en la página 236](#)

### Consideraciones para la configuración del SLP

El daemon del SLP está preconfigurado con propiedades predeterminadas. Si su empresa funciona bien con los valores predeterminados, la implementación del SLP prácticamente no exige ninguna administración.

En algunas situaciones, sin embargo, quizá desee modificar las propiedades del SLP para ajustar las operaciones de red o activar ciertas características. Con unos pocos cambios de configuración, por ejemplo, puede habilitar el registro del SLP. La información en un registro del SLP y en los rastreos de snoop puede ayudar a decidir si es necesario realizar una configuración adicional.

Las propiedades de configuración del SLP residen en el archivo `slp.conf`, que se encuentra en el directorio `/etc/inet`. Si decide cambiar los valores predeterminados de las propiedades, consulte el [Capítulo 9, “Administración del SLP \(tareas\)”](#) para obtener los procedimientos apropiados.

Antes de modificar los valores de configuración del SLP, tenga en cuenta las siguientes preguntas que están relacionadas con aspectos clave de la administración de redes:

- ¿Qué tecnologías de red funcionan en la empresa?
- ¿Cuánto tráfico de red pueden manejar las tecnologías sin inconvenientes?
- ¿Cuántos servicios hay disponibles en la red? ¿De qué tipo son?
- ¿Cuántos usuarios hay en la red? ¿Qué servicios necesitan? ¿Dónde se encuentran los usuarios en relación con los servicios a los que acceden con más frecuencia?

## Toma de decisiones con respecto a qué reconfigurar

Puede usar la utilidad snoop habilitada para SLP y las utilidades de registro del SLP para decidir si la reconfiguración es necesaria y qué propiedades necesita modificar. Por ejemplo, puede reconfigurar determinadas propiedades para realizar lo siguiente:

- Incluir una combinación de medios de red que tienen distintas latencias y características de ancho de banda.
- Recuperar la empresa de fallos de red o particiones no planificadas.
- Agregar DA para reducir la proliferación de multidifusiones del SLP.
- Implementar nuevos ámbitos para organizar usuarios con los servicios a los que acceden con más frecuencia.

## Uso de snoop para supervisar la actividad del SLP

La utilidad snoop es una herramienta administrativa pasiva que proporciona información sobre el tráfico de la red. La propia utilidad genera un tráfico mínimo y permite ver toda la actividad en su red a medida que se produce.

La utilidad snoop proporciona rastreos del tráfico de mensajes del SLP real. Por ejemplo, al ejecutar snoop con el argumento de línea de comandos `s lp`, la utilidad muestra rastreos con información sobre los registros y las anulaciones de registros del SLP. Puede utilizar la información para evaluar la carga de la red mediante la comprobación de los servicios que se registran y de cuánta actividad de reregistro se produce.

La utilidad snoop también es útil para observar el flujo del tráfico entre los hosts del SLP de la empresa. Al ejecutar snoop con el argumento de línea de comandos `s lp`, puede supervisar los siguientes tipos de actividad del SLP para determinar si es necesaria la reconfiguración de la red o el agente:

- El número de hosts que está utilizando un DA determinado. Utilice esta información para decidir si se deben implementar más DA para el equilibrio de carga.
- El número de hosts que está utilizando un DA determinado. Utilice esta información para determinar si se deben configurar ciertos hosts con ámbitos nuevos o diferentes.
- Si el UA solicita un tiempo de espera o la confirmación del DA es lenta. Puede determinar si un DA está sobrecargado mediante la supervisión de los tiempos de espera y las retransmisiones del UA. También puede comprobar si el DA requiere más de unos segundos para enviar confirmaciones de registro a un SA. Utilice esta información para volver a equilibrar la carga de la red en el DA, si es necesario, implementando más DA o cambiando las configuraciones del ámbito.

Mediante snoop con el argumento de línea de comandos `-v` (detallado), puede obtener duraciones de registro y el valor del indicador `fresh` en `SrvReg` para determinar si el número de reregistros debe reducirse.

También puede utilizar snoop para rastrear otros tipos de tráfico del SLP, como los siguientes:

- El tráfico entre clientes de UA y DA.
- El tráfico entre clientes de UA de multidifusión y SA de respuesta.

Para obtener más información sobre snoop, consulte [snoop\(1M\)](#).

---

**Consejo** – Utilice el comando `netstat` junto con snoop para ver estadísticas de congestión y tráfico. Para obtener más información sobre `netstat`, consulte [netstat\(1M\)](#).

---

## ▼ Cómo utilizar snoop para ejecutar rastreos del SLP

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Ejecute snoop con el argumento de línea de comandos `s lp`.

**Brief Mode:**  
`# snoop s lp`

Al ejecutar snoop en el modo *breve* predeterminado, una salida continua se entrega a la pantalla. Los mensajes del SLP se truncan para que entren en una línea por rastreo de SLP.

**Verbose Mode:**  
`# snoop -v s lp`

Al ejecutar snoop en modo *detallado*, snoop entrega una salida sin abreviar y continua a su pantalla, que proporciona la siguiente información:

- La dirección completa de la URL del servicio.
- Todos los atributos del servicio.
- La duración del registro.
- Todos los parámetros y los indicadores de seguridad, si hay alguno disponible.

---

**Nota** – Puede utilizar el argumento de línea de comandos `s lp` con otras opciones de snoop.

---

## Análisis de un rastreo de snoop `s lp`

En el siguiente ejemplo, `s lpd` se ejecuta en `slphost1` en el modo predeterminado como un servidor de SA. El daemon del SLP se inicializa y registra `slphost2` como un servidor de eco. A continuación, el proceso `snoop s lp` se invoca en `slphost1`.

---

**Nota** – Para simplificar la descripción de los resultados del rastreo, las líneas en la siguiente salida snoop se marcan con números de línea.

---

```
(1) slphost1 -> 239.255.255.253 SLP V@ SrvRqst [24487] service:directory-agent []
(2) slphost2 -> slphost1 SLP V2 DAAdvert [24487] service:directory-agent://129
(3) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(4) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(5) slphost1 -> slphost2 SLP V2 SrvReg [24488/tcp] service:echo.sun:tcp://slphost1:
(6) slphost2 -> slphost1 SLP V2 SrvAck [24488/tcp] ok
(7) slphost1 -> slphost2 SLP V2 SrvDereg [24489/tcp] service:echo.sun:tcp://slphost1:
(8) slphost2 -> slphost1 SLP V2 SrvAck [24489/tcp] ok
```

1. Muestra un *slpd* en *slphost1* que realiza una detección activa de agentes de directorio mediante el envío de una multidifusión a la dirección de grupo de multidifusión del SLP en búsqueda de agentes de directorio. El número de mensaje, 24487, para la detección activa se indica entre corchetes en la pantalla de rastreo.
2. Indica que la solicitud de detección activa 24487 del rastreo 1 es respondida por *slpd*, que se está ejecutando como un DA en el host *slphost2*. La URL del servicio de *slphost2* se ha truncado para que entre en una única línea. El DA ha enviado un anuncio de DA en respuesta al mensaje de detección de agentes de directorio de multidifusión, según lo indicado por los números de mensaje coincidentes en los rastreos 1 y 2.
3. Muestra multidifusiones de los UA en *slphost1* para DA adicionales. Debido a que *slphost2* ya ha respondido la solicitud, se abstiene de responder de nuevo, y ningún otro DA responde.
4. Repite la operación de multidifusión que se muestra en la línea anterior.
5. Muestra un *slpd* en *slphost1* que reenvía registros de clientes de SA al DA en *slphost2*. Un registro de servicio de unidifusión (SrvReg) para un servidor de eco es realizado por *slphost1* para el DA en *slphost2*.
6. Muestra un *slphost2* que responde a *slphost1* SrvReg con una confirmación de servicio (SrvAck) que indica que el registro se ha realizado correctamente.

El tráfico entre el servidor de eco que ejecuta el cliente del SA y el daemon del SLP en *slphost1* no aparece en el rastreo de snoop. Esta falta de información se debe a que la operación de snoop se realiza por medio de un bucle de retorno de red.

7. Muestra el servidor de eco en *slphost1* que anula el registro del anuncio del servicio de eco. El daemon del SLP en *slphost1* reenvía la anulación del registro al DA en *slphost2*.
8. Muestra un *slphost2* que responde a *slphost1* con una confirmación de servicio (SrvAck) que indica que la anulación del registro se ha realizado correctamente.

El parámetro /tcp que se agrega al número de mensaje en las líneas 5, 6, 7 y 8 indica que el intercambio de mensajes ocurrió por TCP.

## Dónde proseguir

Después de controlar el tráfico del SLP, puede utilizar la información que se recopiló de los rastreos de snoop para determinar si es necesario realizar la reconfiguración de los valores predeterminados del SLP. Utilice la información relacionada en el [Capítulo 9, “Administración del SLP \(tareas\)”](#) para configurar los valores de las propiedades del SLP. Para obtener más información sobre los registros de servicios y el envío de mensajes del SLP, consulte el [Capítulo 11, “SLP \(referencia\)”](#).





## Administración del SLP (tareas)

---

En las secciones siguientes, se proporcionan información y tareas para configurar agentes y procesos del SLP.

- “Configuración de propiedades del SLP” en la página 241
- “Modificación de frecuencia de detección y anuncios del DA” en la página 244
- “Adaptación de diferentes medios de red, topologías o configuraciones” en la página 249
- “Modificación de tiempos de espera en solicitudes de detección de SLP” en la página 254
- “Implementación de ámbitos” en la página 258
- “Implementación de DA” en la página 261
- “SLP y función de hosts múltiples” en la página 265

### Configuración de propiedades del SLP

Las propiedades de configuración del SLP controlan las interacciones de red, las características de agente del SLP, el estado y el registro. En la mayoría de las situaciones, la configuración predeterminada de estas propiedades no requiere ninguna modificación. Sin embargo, puede utilizar los procedimientos de este capítulo cuando el medio de red o la topología cambian, y para lograr los siguientes objetivos:

- Compensar las latencias de red
- Reducir la congestión de la red
- Agregar agentes o reasignar direcciones IP
- Activar el registro del SLP

Puede editar el archivo de configuración del SLP, `/etc/inet/slp.conf`, para realizar operaciones, como las que se muestran en la siguiente tabla.

TABLA 9-1 Operaciones de configuración del SLP

Operación	Descripción
Especifique si <code>slpd</code> debe actuar como servidor de DA. El servidor de SA es el valor predeterminado.	Establezca la propiedad <code>net.slp.isDA</code> en <code>True</code> .
Establezca el intervalo para mensajes de multidifusión de DA.	Establezca la propiedad <code>net.slp.DAHeartBeat</code> para controlar la frecuencia con la que un DA envía una multidifusión de un anuncio no solicitado del DA.
Habilite el registro de DA para supervisar el tráfico de la red.	Establezca la propiedad <code>net.slp.traceDATraffic</code> en <code>True</code> .

## Archivo de configuración del SLP: elementos básicos

El archivo `/etc/inet/slp.conf` define y activa toda la actividad del SLP cada vez que reinicia el daemon del SLP. El archivo de configuración consta de los siguientes elementos:

- Propiedades de configuración
- Líneas de comentario y notaciones

### Propiedades de configuración

Todas las propiedades básicas del SLP, como, por ejemplo, `net.slp.isDA` y `net.slp.DAHeartBeat`, se nombran en el siguiente formato.

`net.slp.<keyword>`

El comportamiento del SLP es definido por el valor de una propiedad o una combinación de propiedades en el archivo `slp.conf`. Las propiedades se estructuran como pares de clave y valor en el archivo de configuración del SLP. Como se muestra en el siguiente ejemplo, un par de clave y valor consta de un nombre de propiedad y un valor de configuración asociado.

`<property name>=<value>`

La clave para cada propiedad es el nombre de la propiedad. El valor establece los parámetros numéricos (distancia o tiempo), de estado `true/false` o de valor de cadena para la propiedad. Los valores de propiedades constan de uno de los siguientes tipos de datos:

- Configuración `True/False` (booleana)
- Números enteros
- Lista de números enteros
- Cadenas
- Lista de cadenas

Si el valor definido no está permitido, se utiliza el valor predeterminado para dicho nombre de propiedad. Además, se registra un mensaje de error mediante `syslog`.

## Líneas de comentario y notaciones

Puede agregar comentarios al archivo `slp.conf`, que describen la naturaleza y la función de la línea. Las líneas de comentario son opcionales en el archivo, pero pueden resultar útiles para la administración.

---

**Nota** – Los valores en el archivo de configuración no distinguen mayúsculas de minúsculas. Para obtener más información, consulte: Guttman, Erik; Kempf, James; y Perkins, Charles, “Service Templates and service: scheme” (Plantillas de servicio y servicio: esquema), RFC 2609 del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [<http://www.ietf.org/rfc/rfc2609.txt>]

---

## ▼ Cómo cambiar la configuración del SLP

Utilice este procedimiento para cambiar los valores de propiedades del archivo de configuración del SLP. El software de servicio o cliente habilitado para SLP también puede alterar la configuración del SLP mediante la API del SLP. Esta API está documentada en “An API for Service Location” (Una API para ubicación de servicios), RFC 2614 del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force). [<http://www.ietf.org/rfc/rfc2614.txt>]

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

### 4 Edite los valores de propiedades en el archivo `/etc/inet/slp.conf` según sea necesario.

Consulte “[Propiedades de configuración](#)” en la [página 242](#) para obtener información general sobre los valores de propiedades del SLP. Consulte las secciones que siguen este procedimiento para ver ejemplos de distintos escenarios en los que puede cambiar las propiedades de `slp.conf`. Consulte [slp.conf\(4\)](#).

### 5 Guarde los cambios y cierre el archivo.

### 6 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

**Nota** – El daemon del SLP obtiene información del archivo de configuración cuando se detiene o se inicia `slpd`.

**Ejemplo 9-1** Configuración de `slpd` para funcionar como servidor de DA

Puede cambiar el servidor de SA predeterminado para permitir que `slpd` funcione como un servidor de DA estableciendo la propiedad `net.slp.isDA` en `True`, en el archivo `slpd.conf`.

```
net.slp.isDA=True
```

En cada área, varias propiedades controlan diferentes aspectos de la configuración. En las secciones siguientes, se describen distintos escenarios en los que puede cambiar los valores de propiedades predeterminados que se utilizan en la configuración del SLP.

# Modificación de frecuencia de detección y anuncios del DA

En situaciones como las siguientes, puede modificar las propiedades que controlan el intervalo de anuncios y solicitudes de detección del DA.

- Cuando desee que el SA o UA obtengan información de la configuración del DA estáticamente de la propiedad `net.slp.DAAddresses` en el archivo `slp.conf`, puede deshabilitar la detección del DA.
- Cuando la red está sujeta a particiones recurrentes, puede cambiar la frecuencia de anuncios pasivos y detección activa.
- Si los clientes de UA y SA acceden a DA en el otro lado de una conexión de acceso telefónico, puede reducir la frecuencia de latidos del DA y el intervalo de detección activa para disminuir el número de veces que una línea de acceso telefónico se activa.
- Si la congestión de la red es alta, puede limitar la multidifusión.

Los procedimientos de esta sección explican cómo modificar las siguientes propiedades.

**TABLA 9-2** Propiedades de solicitud de detección e intervalo de anuncios del DA

Propiedad	Descripción
<code>net.slp.passiveDADetection</code>	Valor booleano que especifica si <code>slpd</code> escucha anuncios no solicitados del DA
<code>net.slp.DAActiveDiscoveryInterval</code>	Valor que especifica con qué frecuencia <code>slpd</code> realiza la detección activa del DA para un nuevo DA
<code>net.slp.DAHeartBeat</code>	Valor que especifica con qué frecuencia un DA envía una multidifusión de un anuncio no solicitado del DA

## Limitación de UA y SA a DA configurados estáticamente

Es posible que, a veces, necesite limitar los UA y SA para obtener direcciones de DA de la información de la configuración estática en el archivo `slp.conf`. En el siguiente procedimiento, puede modificar dos propiedades que hacen que `slpd` obtenga información del DA exclusivamente de la propiedad `net.slp.DAAddresses`.

### ▼ Cómo limitar UA y SA a DA configurados estáticamente

Utilice el siguiente procedimiento para cambiar las propiedades `net.slp.passiveDADetection` y `net.slp.DAActiveDiscoveryInterval`.

---

**Nota** – Utilice este procedimiento sólo en hosts que ejecutan UA y SA que están restringidos a configuraciones estáticas.

---

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

#### 3 Realice una copia de seguridad del archivo `etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

#### 4 Establezca la propiedad `net.slp.passiveDADetection` en `False`, en el archivo `slp.conf`, para deshabilitar la detección pasiva. Este valor hace que `slpd` ignore los anuncios no solicitados del DA.

```
net.slp.passiveDADetection=False
```

#### 5 Establezca `net.slp.DAActiveDiscoveryInterval` en `-1` para deshabilitar la detección activa inicial y periódica.

```
net.slp.DAActiveDiscoveryInterval=-1
```

#### 6 Guarde los cambios y cierre el archivo.

#### 7 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

## Configuración de detección de DA para redes de acceso telefónico

Si los UA o SA están separados del DA por una red de acceso telefónico, puede configurar la detección de DA para reducir o eliminar el número de solicitudes de detección y anuncios del DA. Las redes de acceso telefónico, normalmente, generan un costo cuando se activan. La minimización de llamadas externas puede reducir el costo de utilizar la red de acceso telefónico.

---

**Nota** – Puede deshabilitar la detección de DA completamente con el método que se describe en [“Limitación de UA y SA a DA configurados estáticamente” en la página 245.](#)

---

### ▼ Cómo configurar la detección de DA para redes de acceso telefónico

Puede utilizar el siguiente procedimiento para reducir los anuncios no solicitados del DA y la detección activa mediante el aumento del período de latidos del DA y el intervalo de detección activa.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**2 Detenga s<sub>l</sub>pd y toda la actividad del SLP en el host.**

```
# svcadm disable network/slp
```

**3 Realice una copia de seguridad del archivo /etc/inet/s<sub>l</sub>p.conf predeterminado antes de cambiar los valores de configuración.**

**4 Aumente la propiedad net.s<sub>l</sub>p.DAHeartbeat en el archivo s<sub>l</sub>pd.conf.**

```
net.slp.DAHeartbeat=value
```

*value* Un número entero de 32 bits que establece el número de segundos para el latido de anuncio de DA pasivo

Valor predeterminado= 10.800 s (3 h)

Rango de valores= de 2000 s a 259.200.000 s

Por ejemplo, puede establecer el latido del DA en 18 h aproximadamente en un host que está ejecutando un DA:

```
net.slp.DAHeartbeat=65535
```

**5 Aumente la propiedad `net.slp.DAActiveDiscoveryInterval` en el archivo `slpd.conf`:**

```
net.slp.DAActiveDiscoveryInterval value
```

*value* Un número entero de 32 bits que establece el número de segundos para consultas de detección activa del DA

Valor predeterminado= 900 s (15 min)

Rango de valores= de 300 s a 10.800 s

Por ejemplo, puede establecer el intervalo de detección activa del DA en 18 h en un host que está ejecutando un UA y un SA:

```
net.slp.DAActiveDiscoveryInterval=65535
```

**6 Guarde los cambios y cierre el archivo.****7 Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

## Configuración del latido del DA para particiones frecuentes

Los SA son necesarios para registrarse con todos los DA que admiten sus ámbitos. Un DA puede aparecer después de que `slpd` ha realizado la detección activa. Si el DA admite ámbitos `slpd`, el daemon del SLP registra todos los anuncios en su host con el DA.

Una manera en la que `slpd` detecta DA es por el anuncio no solicitado inicial que un DA envía cuando se inicia. El daemon del SLP utiliza el anuncio no solicitado periódico (el latido) para determinar si un DA aún está activo. Si el latido no aparece, el daemon elimina los DA que el daemon utiliza y los DA que el daemon ofrece a los UA.

Por último, cuando un DA sufre un cierre controlado, transmite un anuncio de DA especial que informa a los servicios de SA de escucha que estará fuera de servicio. El daemon del SLP también utiliza este anuncio para eliminar DA inactivos de la antememoria.

Si la red está sujeta a particiones frecuentes y los SA son de larga duración, `slpd` puede eliminar DA de la antememoria durante la partición si no se reciben anuncios de latidos. Al disminuir el tiempo de latidos, puede reducir el retraso antes de que un DA desactivado se restaure en la antememoria después de que la partición se ha reparado.

## ▼ Cómo configurar latidos del DA para particiones frecuentes

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.DAHeartBeat` con el fin de reducir el período de latidos del DA.

---

**Nota** – Si la detección de DA está completamente deshabilitada, la propiedad `net.slp.DAAddresses` se debe establecer en `slp.conf` en los hosts que ejecutan UA y SA para que accedan al DA correcto.

---

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Detenga `slpd` y toda la actividad del SLP en el host.**

```
# svcadm disable network/slp
```

**3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

**4 Reduzca el valor `net.slp.DAHeartBeat` a 1 h (3600 s). De manera predeterminada, el período de latidos del DA se establece en 3 h (10.800 s).**

```
net.slp.DAHeartBeat=3600
```

**5 Guarde los cambios y cierre el archivo.**

**6 Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

## Liberación de la congestión de la red

Si la congestión de la red es alta, puede limitar la cantidad de actividad de multidifusión. Si los DA aún no han sido implementados en la red, su implementación puede reducir drásticamente la cantidad de multidifusión relacionada con el SLP.

Sin embargo, incluso después de implementar los DA, la multidifusión es necesaria para la detección de DA. Puede reducir la cantidad de multidifusión necesaria para la detección de DA con el método que se describe en [“Cómo configurar la detección de DA para redes de acceso](#)



telefónico” en la página 246. Puede eliminar totalmente la multidifusión para la detección de DA con el método que se describe en “Limitación de UA y SA a DA configurados estáticamente” en la página 245.

## Adaptación de diferentes medios de red, topologías o configuraciones

En esta sección, se describen escenarios posibles en los que puede cambiar las siguientes propiedades para ajustar el rendimiento del SLP.

TABLA 9-3 Propiedades de rendimiento del SLP

Propiedad	Descripción
<code>net.slp.DAAttributes</code>	El intervalo de actualización mínimo que un DA acepta para los anuncios.
<code>net.slp.multicastTTL</code>	El valor <i>time-to-live</i> especificado para los paquetes de multidifusión.
<code>net.slp.MTU</code>	El tamaño en bytes establecido para los paquetes de red. El tamaño incluye encabezados IP y TCP o UDP.
<code>net.slp.isBroadcastOnly</code>	El valor booleano que se establece para indicar si la difusión se debe utilizar para la detección de servicios basada en DA y no basada en DA.

## Reducción de reregistros de SA

Los SA necesitan actualizar periódicamente los anuncios de servicios antes de caducar. Si un DA maneja una carga extremadamente pesada de muchos UA y SA, las actualizaciones frecuentes pueden provocar que el DA se sobrecargue. Si el DA se sobrecarga, las solicitudes del UA comienzan a agotar el tiempo de espera y, luego, se eliminan. Hay muchas causas posibles por las que las solicitudes de UA pueden agotar su tiempo de espera. Antes de asumir que la sobrecarga del DA es el problema, utilice un rastreo de snoop para comprobar la duración de los anuncios de servicios que se han registrado con un registro de servicio. Si las duraciones son cortas y los reregistros se producen con frecuencia, los tiempos de espera agotados, probablemente, sean el resultado de reregistros frecuentes.

**Nota** – Un registro de servicio es un *reregistro* si el indicador FRESH no está definido. Consulte el [Capítulo 11, “SLP \(referencia\)”](#) para obtener más información sobre los mensajes de registro de servicios.

## ▼ Cómo reducir reregistros de SA

Utilice el siguiente procedimiento para aumentar el intervalo de actualización mínimo de los SA y reducir los reregistros.

**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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Detenga `slpd` y toda la actividad del SLP en el host.**

```
# svcadm disable network/slp
```

**3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

**4 Aumente el valor del atributo `min-refresh-interval` de la propiedad `net.slp.DAAAttributes`.**

El período de reregistro mínimo predeterminado es cero. El valor predeterminado de cero permite que los SA se vuelvan a registrar en cualquier punto. En el siguiente ejemplo, el intervalo se aumenta a 3600 s (1 h).

```
net.slp.DAAAttributes(min-refresh-interval=3600)
```

**5 Guarde los cambios y cierre el archivo.**

**6 Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

## Configuración de la propiedad Time-to-Live de multidifusión

La propiedad `time-to-live` de multidifusión (`net.slp.multicastTTL`) determina el rango en el que un paquete de multidifusión se propaga en la intranet. La propiedad TTL de multidifusión se configura estableciendo la propiedad `net.slp.multicastTTL` en un número entero entre 1 y 255. El valor predeterminado de la propiedad TTL de multidifusión es de 255, lo que significa que, en teoría, el enrutamiento de paquetes no está restringido. Sin embargo, una TTL de 255 hace que un paquete de multidifusión penetre la intranet hasta los enrutadores de límite en el borde del dominio administrativo. Se necesita una configuración correcta de multidifusión en los enrutadores de límite para evitar que los paquetes de multidifusión se filtren en la red principal de multidifusión de Internet o en su ISP.

El ámbito de la TTL de multidifusión es similar a la TTL de IP estándar, con la excepción de que se realiza una comparación de TTL. A cada interfaz en un enrutador habilitado para multidifusión se le asigna un valor TTL. Cuando llega un paquete de multidifusión, el enrutador

compara la TTL del paquete con la TTL de la interfaz. Si la TTL del paquete es mayor o igual que la TTL de la interfaz, la TTL del paquete se reduce en uno, al igual que con la TTL de IP estándar. Si la TTL pasa a cero, el paquete se descarta. Al utilizar el ámbito TTL para la multidifusión del SLP, los enrutadores deben estar correctamente configurados para limitar los paquetes a una determinada subsección de la intranet.

## ▼ Cómo configurar la propiedad Time-to-Live de multidifusión

Utilice el siguiente procedimiento para restablecer la propiedad `net.slp.multicastTTL`.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

### 4 Cambie la propiedad `net.slp.multicastTTL` en el archivo `slpd.conf`:

```
net.slp.multicastTTL=value
```

*value* Un número entero positivo menor o igual que 255 que define la TTL de multidifusión

---

**Nota** – Puede reducir el rango de propagación de multidifusión reduciendo el valor TTL. Si el valor TTL es 1, el paquete está restringido a la subred. Si el valor es 32, el paquete está restringido al sitio. Lamentablemente, el término *sitio* no es definido por la RFC 1075, donde se tratan las TTL de multidifusión. Los valores superiores a 32 hacen referencia al enrutamiento teórico en Internet y no deben utilizarse. Los valores inferiores a 32 se pueden utilizar para restringir la multidifusión a un conjunto de subredes accesibles si los enrutadores están correctamente configurados con TTL.

---

### 5 Guarde los cambios y cierre el archivo.

### 6 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

## Configuración del tamaño de paquete

El tamaño de paquete predeterminado para SLP es 1400 bytes. El tamaño debe ser suficiente para la mayoría de las redes de área local. Para redes inalámbricas o redes de área extensa, puede reducir el tamaño de paquete para evitar la fragmentación de mensajes y disminuir el tráfico en la red. Para redes de área local que tienen paquetes más grandes, el aumento del tamaño de paquete puede mejorar el rendimiento. Puede determinar si el tamaño de paquete se tiene que reducir al comprobar el tamaño de paquete mínimo para su red. Si el medio de red tiene un tamaño de paquete más pequeño, puede reducir el valor `net.slp.MTU` en consecuencia.

Puede aumentar el tamaño de paquete si el medio de red tiene paquetes más grandes. Sin embargo, a menos que los anuncios de servicios de SA o las consultas de UA desborden con frecuencia el tamaño de paquete predeterminado, no debe tener que cambiar el valor `net.slp.MTU`. Puede utilizar `snoop` para determinar si las solicitudes de UA desbordan con frecuencia el tamaño de paquete predeterminado y se vuelven a implementar para utilizar TCP en lugar de UDP.

La propiedad `net.slp.MTU` mide el tamaño de paquete de IP completo, incluidos el encabezado de capa de enlace, el encabezado IP, el encabezado UDP o TCP, y el mensaje SLP.

### ▼ Cómo configurar el tamaño de paquete

Utilice el siguiente procedimiento para cambiar el tamaño de paquete predeterminado ajustando la propiedad `net.slp.MTU`.

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

#### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

#### 4 Cambie la propiedad `net.slp.MTU` en el archivo `slpd.conf`:

```
net.slp.MTU=value
```

*value* Un número entero de 16 bits que especifica en bytes el tamaño de paquete de red

Valor predeterminado= 1400

Rango de valores= de 128 a 8192

- 5 **Guarde los cambios y cierre el archivo.**
- 6 **Reinicie `slpd` para activar los cambios.**  
`# svcadm enable network/slp`

## Configuración de enrutamiento de sólo difusión

SLP está diseñado para utilizar la multidifusión para la detección de servicios en la ausencia de DA y para la detección de DA. Si la red no implementa el enrutamiento de multidifusión, puede configurar el SLP para utilizar la difusión estableciendo la propiedad `net.slp.isBroadcastOnly` en `True`.

A diferencia de la multidifusión, los paquetes de difusión no se propagan por subredes de manera predeterminada. Por este motivo, la detección de servicios sin DA en una red que no es de multidifusión funciona sólo en una única subred. Además, se deben tener en cuenta consideraciones especiales al implementar DA y ámbitos en las redes en las que se utiliza la difusión. Un DA en un host múltiple puede unir la detección de servicios entre varias subredes con la multidifusión deshabilitada. Consulte [“Asignación de nombre de ámbito y colocación de DA” en la página 269](#) para obtener más información sobre cómo implementar DA en hosts múltiples.

### ▼ Cómo configurar el enrutamiento de sólo difusión

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.isBroadcastOnly` a `True`.

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Detenga `slpd` y toda la actividad del SLP en el host.**  
`# svcadm disable network/slp`
- 3 **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**
- 4 **Cambie la propiedad `net.slp.isBroadcastOnly` en el archivo `slpd.conf` a `True`:**  
`net.slp.isBroadcastOnly=True`
- 5 **Guarde los cambios y cierre el archivo.**

6 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

# Modificación de tiempos de espera en solicitudes de detección de SLP

Es posible que dos situaciones requieran la modificación de los tiempos de espera para solicitudes de detección de SLP:

- Si los agentes del SLP están separados por varias subredes, líneas de acceso telefónico u otras WAN, la latencia de red puede ser lo suficientemente alta como para que los tiempos de espera predeterminados sean insuficientes para que una solicitud o un registro se completen. Por el contrario, si la red tiene una latencia baja, puede mejorar el rendimiento disminuyendo los tiempos de espera.
- Si la red está sujeta a un gran volumen de tráfico o a tasas altas de colisión, el período máximo que los SA y UA tienen que esperar antes de enviar un mensaje podría ser insuficiente para garantizar transacciones sin colisión.

## Cambio de tiempos de espera predeterminados

La latencia alta de red puede provocar que los UA y SA agoten el tiempo de espera antes de que se devuelva una respuesta para solicitudes y registros. La latencia puede ser un problema si un UA está separado de un SA o si ambos, un UA y un SA, están separados de un DA por varias subredes, una línea de acceso telefónico o una WAN. Puede determinar si la latencia es un problema al comprobar si las solicitudes del SLP fallan debido a tiempos de espera en solicitudes y registros de UA y SA. También puede utilizar el comando `ping` para medir la latencia real.

En la siguiente tabla, se muestran las propiedades de configuración que controlan los tiempos de espera. Puede utilizar los procedimientos de esta sección para modificar estas propiedades.

TABLA 9-4 Propiedades de tiempo de espera

Propiedad	Descripción
<code>net.slp.multicastTimeouts</code>	Las propiedades que controlan los tiempos de espera para transmisiones de mensajes UDP de unidifusión y multidifusión antes de que la transmisión se abandone.
<code>net.slp.DADiscoveryTimeouts</code>	
<code>net.slp.datagramTimeouts</code>	

TABLA 9-4 Propiedades de tiempo de espera (Continuación)

Propiedad	Descripción
<code>net.slp.multicastMaximumWait</code>	La propiedad que controla la cantidad máxima de tiempo que un mensaje de multidifusión se transmite antes de ser abandonado.
<code>net.slp.datagramTimeouts</code>	El límite superior de un tiempo de espera de DA que está especificado por la suma de los valores que se muestran para esta propiedad. Un datagrama UDP se envía repetidamente a un DA hasta que se recibe una respuesta o hasta que se alcanza el límite de tiempo de espera.

Si los tiempos de espera se agotan con frecuencia durante la detección de servicios de multidifusión o la detección de DA, aumente la propiedad `net.slp.multicastMaximumWait` del valor predeterminado de 15.000 ms (15 s). Al aumentar el período máximo de espera se genera más tiempo para que las solicitudes en redes de latencia alta se completen. Después de cambiar `net.slp.multicastMaximumWait`, también debe modificar `net.slp.multicastTimeouts` y `net.slp.datagramTimeouts`. La suma de los valores de tiempo de espera para estas propiedades es igual al valor `net.slp.multicastMaximumWait`.

## ▼ Cómo cambiar tiempos de espera predeterminados

Utilice el siguiente procedimiento para cambiar las propiedades del SLP que controlan los tiempos de espera.

- 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.
- 2 Detenga `slpd` y toda la actividad del SLP en el host.**  
`# svcadm disable network/slp`
- 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**
- 4 Cambie la propiedad `net.slp.multicastMaximumWait` en el archivo `slpd.conf`:**  
`net.slp.multicastMaximumWait=value`  
*valor*      Un número entero de 32 bits que muestra la suma de los valores que se establecen para `net.slp.multicastTimeouts` y `net.slp.DADiscoveryTimeouts`  
  
Valor predeterminado= 15.000 ms (15 s)

Rango de valores= de 1000 ms a 60.000 ms

Por ejemplo, si determina que las solicitudes de multidifusión requieren 20 s (20.000 ms), debe ajustar a 20.000 ms los valores enumerados para las propiedades `net.slp.multicastTimeouts` y `net.slp.DADiscoveryTimeouts`.

```
net.slp.multicastMaximumWait=20000
net.slp.multicastTimeouts=2000,5000,6000,7000
net.slp.DADiscoveryTimeouts=3000,3000,6000,8000
```

## 5 Si es necesario, cambie la propiedad `net.slp.datagramTimeouts` en el archivo `slpd.conf`:

```
net.slp.datagramTimeouts=value
```

*valor* Una lista de números enteros de 32 bits que especifican tiempos de espera, en milisegundos, para implementar la transmisión de datagramas de unidifusión en DA

Valor predeterminado= 3000, 3000, 3000

Por ejemplo, puede aumentar el tiempo de espera de datagramas a 20.000 ms para evitar que los tiempos de espera se agoten con frecuencia.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

En redes de alto rendimiento, puede reducir el límite de tiempo de espera para la transmisión de datagramas UDP de unidifusión y multidifusión. Al reducir el límite de tiempo de espera, disminuye la latencia que es necesaria para cumplir las solicitudes del SLP.

## 6 Guarde los cambios y cierre el archivo.

## 7 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

# Configuración del límite de espera aleatoria

En redes con un gran volumen de tráfico o una tasa alta de colisión, la comunicación con un DA puede resultar afectada. Cuando las tasas de colisión son altas, el agente de envío debe retransmitir el datagrama UDP. Puede determinar si la retransmisión se está produciendo mediante snoop para supervisar el tráfico de una red de hosts que están ejecutando `slpd` como un servidor de SA y un host que está ejecutando `slpd` como un DA. Si varios mensajes de registro de servicios para el mismo servicio aparecen en el rastreo de snoop del host que está ejecutando `slpd` como servidor de SA, es posible que haya notado colisiones.

Las colisiones pueden ser especialmente preocupantes en el momento del inicio. Cuando un DA se inicia por primera vez, envía anuncios no solicitados, y los SA responden con registros. El SLP requiere que los SA esperen durante una cantidad de tiempo aleatoria tras recibir un anuncio del DA antes de responder. El límite de espera aleatoria se distribuye de manera



uniforme con un valor máximo que está controlado por `net.slp.randomWaitBound`. El límite de espera aleatoria predeterminado es 1000 ms (1 s).

## ▼ Cómo configurar el límite de espera aleatoria

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.RandomWaitBound` en el archivo `slp.conf`.

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

### 4 Cambie la propiedad `net.slp.RandomWaitBound` en el archivo `slpd.conf`:

```
net.slp.RandomWaitBound=value
```

*valor* El límite superior para calcular el tiempo de espera aleatoria antes de intentar ponerse en contacto con un DA

Valor predeterminado= 1000 ms (1 s)

Rango de valores= de 1000 ms a 3000 ms

Por ejemplo, puede alargar el tiempo máximo de espera a 2000 ms (2 s).

```
net.slp.randomWaitBound=2000
```

Cuando alarga el límite de espera aleatoria, ocurre un retraso más prolongado en el registro. Los SA pueden completar los registros con DA recién detectados más lentamente para evitar colisiones y tiempos de espera agotados.

### 5 Si es necesario, cambie la propiedad `net.slp.datagramTimeouts` en el archivo `slpd.conf`:

```
net.slp.datagramTimeouts=value
```

*valor* Una lista de números enteros de 32 bits que especifican tiempos de espera, en milisegundos, para implementar la transmisión de datagramas de unidifusión en DA

Valor predeterminado= 3000, 3000, 3000

Por ejemplo, puede aumentar el tiempo de espera de datagramas a 20.000 ms para evitar que los tiempos de espera se agoten con frecuencia.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

En redes de alto rendimiento, puede reducir el límite de tiempo de espera para la transmisión de datagramas UDP de unidifusión y multidifusión. Este valor reduce la cantidad de latencia al cumplir solicitudes SLP.

**6 Guarde los cambios y cierre el archivo.**

**7 Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

## Implementación de ámbitos

Con ámbitos, puede proporcionar servicios que dependen de agrupaciones lógicas, físicas y administrativas de usuarios. Puede utilizar ámbitos para administrar el acceso a anuncios de servicios.

Utilice la propiedad `net.slp.useScopes` para crear ámbitos. Por ejemplo, en el archivo `/etc/inet/slp.conf` en un host, agregue un nuevo ámbito, denominado `newscope`, tal como se muestra:

```
net.slp.useScopes=newscope
```

Es posible que su organización, por ejemplo, tenga un sector de dispositivos conectados en red, como impresoras y faxes, al final de la sala sur, en el segundo piso del edificio 6. Esos dispositivos podrían ser utilizados por todas las personas del segundo piso, o usted podría restringir el uso para los miembros de un departamento determinado. Los ámbitos ofrecen una manera de otorgar acceso a los anuncios de servicios de esos equipos.

Si los dispositivos están dedicados a un solo departamento, puede crear un ámbito con el nombre del departamento, por ejemplo, `mktg`. Los dispositivos que pertenecen a otros departamentos se pueden configurar con nombres de ámbitos diferentes.

En otra situación, los departamentos podrían estar separados. Por ejemplo, los departamentos de ingeniería mecánica y CAD/CAM podrían estar divididos entre los pisos 1 y 2. Sin embargo, puede proporcionar los equipos del piso 2 para los hosts en ambos pisos asignándolos al mismo ámbito. Puede implementar los ámbitos de cualquier manera que funcione bien con su red y sus usuarios.

---

**Nota** – Los UA que tienen un ámbito particular no tienen prohibido utilizar los servicios que están anunciados en otros ámbitos. La configuración de ámbitos controla sólo qué anuncios de servicios detecta un UA. El servicio es responsable de aplicar cualquier restricción de control de acceso.

---

## Cuándo configurar ámbitos

El SLP puede funcionar adecuadamente sin la configuración de ningún ámbito. En el entorno operativo de Solaris, el ámbito predeterminado para SLP es `default`. Si no se configuran ámbitos, `default` es el ámbito de todos los mensajes SLP.

Puede configurar ámbitos en cualquiera de las siguientes circunstancias.

- Las organizaciones que respalda desean restringir el acceso a los anuncios de servicios para sus propios miembros.
- La distribución física de la organización sugiere que los servicios en una determinada área pueden ser utilizados por usuarios concretos.
- Los anuncios de servicios que son adecuados para usuarios específicos deben ser particionados.

Un ejemplo de la primera circunstancia fue citado en “[Configuración de detección de DA para redes de acceso telefónico](#)” en la [página 246](#). Un ejemplo de la segunda circunstancia es una situación en la que una organización está dividida entre dos edificios, y usted desea que los usuarios de un edificio accedan a los servicios locales de dicho edificio. Puede configurar a los usuarios en el edificio 1 con el ámbito B1 y configurar a los usuarios en el edificio 2 con el ámbito B2.

## Consideraciones al configurar ámbitos

Cuando modifica la propiedad `net.slp.useScopes` en el archivo `slpd.conf`, configura ámbitos para todos los agentes en el host. Si el host está ejecutando algún SA o está actuando como un DA, debe configurar esta propiedad si desea configurar el SA o DA en ámbitos que no sean `default`. Si sólo UA se están ejecutando en el equipo, y los UA deben detectar SA y DA que admiten ámbitos que no sean `default`, no es necesario configurar la propiedad, a menos que desee restringir los ámbitos que los UA utilizan. Si la propiedad no está configurada, los UA pueden detectar automáticamente DA y ámbitos disponibles mediante `slpd`. El daemon del SLP utiliza la detección activa y pasiva de DA para encontrar DA, o utiliza la detección de SA si no hay DA en ejecución. Como alternativa, si la propiedad está configurada, los UA usan sólo los ámbitos configurados y no los descartan.

Si decide configurar ámbitos, debe considerar mantener el ámbito `default` en la lista de ámbitos configurados, a menos que esté seguro de que todos los SA de la red tienen ámbitos configurados. Si algunos SA se dejan sin configurar, los UA con ámbitos configurados no los pueden encontrar. Esta situación se produce porque los SA no configurados tienen automáticamente el ámbito `default`, pero los UA tienen los ámbitos configurados.

Si también decide configurar DA estableciendo la propiedad `net.slp.DAAddresses`, asegúrese de que los ámbitos admitidos por los DA configurados sean los mismos que los ámbitos que ha configurado con la propiedad `net.slp.useScopes`. Si los ámbitos son diferentes, `slpd` imprime un mensaje de error cuando se reinicia.

## ▼ Cómo configurar ámbitos

Utilice el siguiente procedimiento para agregar nombres de ámbitos a la propiedad `net.slp.useScopes` en el archivo `slp.conf`.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

### 4 Cambie la propiedad `net.slp.useScopes` en el archivo `slpd.conf`:

```
net.slp.useScopes=<scope names>
```

*scope names*      Una lista de cadenas que indican qué ámbitos un DA o SA está autorizado a utilizar al realizar solicitudes o qué ámbitos un DA debe admitir

Valor predeterminado= valor predeterminado para SA y DA/sin asignar para UA

---

#### Nota –

Utilice lo siguiente para construir nombres de ámbitos:

- Cualquier carácter alfanumérico, mayúscula o minúscula
- Cualquier carácter de puntuación (excepto: `"`, `\`, `!`, `<`, `=`, `>` y `~`)
- Espacios que se consideran parte del nombre

- Caracteres que no son ASCII

Utilice una barra diagonal inversa para caracteres de escape que no son ASCII. Por ejemplo, la codificación UTF-8 utiliza el código hexadecimal `0xc3a9` para representar la letra *e* con el acento *agudo* francés. Si la plataforma no admite UTF-8, utilice el código hexadecimal UTF-8 como la secuencia de escape `\c3\a9`.

Por ejemplo, para especificar ámbitos para grupos `eng` y `mktg` en `bldg6`, cambie la línea `net.slp.useScopes` a lo siguiente.

```
net.slp.useScopes=eng,mktg,bldg6
```

**5 Guarde los cambios y cierre el archivo.**

**6 Reinicie `slpd` para activar los cambios.**

```
# svcadm enable network/slp
```

## Implementación de DA

En esta sección, se describe la implementación estratégica de DA en una red que está ejecutando el SLP.

El SLP funciona adecuadamente sólo con los agentes base (UA y SA) y sin DA implementados ni ámbitos configurados. Todos los agentes que carecen de configuraciones específicas utilizan el ámbito `default`. Los DA funcionan como antememorias para los anuncios de servicios. La implementación de DA reduce el número de mensajes que se envían en la red y reduce el tiempo que es necesario para recibir respuestas a mensajes. Esta capacidad permite al SLP alojar redes de mayor tamaño.

### ¿Por qué implementar un DA de SLP?

El motivo principal para implementar DA es reducir la cantidad de tráfico de multidifusión y los retrasos que están asociados con la recopilación de respuestas de unidifusión. En una red grande con muchos UA y SA, la cantidad de tráfico de multidifusión que participa en la detección de servicios puede volverse tan grande que el rendimiento de la red disminuye. Mediante la implementación de uno o más DA, los UA deben enviar una unidifusión a los DA para servicios, y los SA deben registrarse con los DA mediante la unidifusión. La única multidifusión registrada con SLP en una red con DA es para la detección activa y pasiva de DA.

Los SA se registran automáticamente con cualquier DA que detectan dentro de un conjunto de ámbitos comunes, en lugar de aceptar solicitudes de servicio de multidifusión. No obstante, el SA aún responde directamente solicitudes de multidifusión en ámbitos que no son admitidos por el DA.

Las solicitudes de servicio de UA se envían por unidifusión a los DA en lugar de enviarse por multidifusión en la red cuando un DA se implementa dentro de los ámbitos del UA. Por lo tanto, los DA dentro de los ámbitos del UA reducen la multidifusión. Al eliminar la multidifusión para solicitudes de UA comunes, el tiempo que se necesita para obtener respuestas a las preguntas se reduce en gran medida (de segundos a milisegundos).

Los DA actúan como un punto focal para la actividad de SA y UA. La implementación de uno o varios DA para una colección de ámbitos proporciona un punto centralizado para supervisar la actividad del SLP. Es más sencillo supervisar los registros y las solicitudes activando el registro de DA que comprobando los registros de varios SA que están distribuidos por toda la red. Puede implementar cualquier número de DA para un determinado ámbito o para varios ámbitos, según la necesidad de equilibrar la carga.

En redes que no tienen el enrutamiento de multidifusión habilitado, puede configurar el SLP para utilizar la difusión. Sin embargo, la difusión es muy ineficaz, porque necesita que cada host procese el mensaje. Además, la difusión, por lo general, no se propaga entre enrutadores. Como resultado, en una red sin enrutamiento de multidifusión, los servicios se pueden detectar sólo en la misma subred. Si el enrutamiento de multidifusión se admite parcialmente, se genera una capacidad inconsistente para detectar servicios en una red. Los mensajes de multidifusión se utilizan para detectar DA. La compatibilidad parcial con el enrutamiento de multidifusión, por lo tanto, implica que los UA y SA registran servicios con todos los DA conocidos en el ámbito del SA. Por ejemplo, si un UA consulta a un DA denominado DA1, y el SA ha registrado servicios con DA2, el UA no podrá detectar un servicio. Consulte [“Configuración de enrutamiento de sólo difusión” en la página 253](#) para obtener más información sobre cómo implementar el SLP en redes que no tienen la multidifusión habilitada.

En una red con compatibilidad inconsistente de todo el sitio para el enrutamiento de multidifusión, debe configurar los UA y SA del SLP con una lista consistente de ubicaciones de DA mediante la propiedad `net.slp.DAAddresses`.

Por último, el DA de SLPv2 admite la interoperabilidad con SLPv1. La interoperabilidad con SLPv1 está habilitada de manera predeterminada en el DA de Si la red contiene dispositivos SLPv1, como las impresoras, o si es necesario interoperar con Novell Netware 5, que utiliza SLPv1 para la detección de servicios, debe implementar un DA. Sin un DA, los UA del SLP de Solaris no pueden encontrar servicios anunciados de SLPv1.

## Cuándo implementar DA

Implemente DA en su empresa si se cumple alguna de las siguientes condiciones:

- El tráfico SLP de multidifusión se excede en un 1 % del ancho de banda de la red, medido por snoop.
- Los clientes de UA experimentan retrasos o tiempos de espera largos durante las solicitudes de servicio de multidifusión.
- Desea centralizar la supervisión de anuncios de servicios de SLP para ámbitos particulares en uno o varios hosts.
- La red no tiene la multidifusión habilitada y se compone de varias subredes que deben compartir servicios.
- La red emplea dispositivos que admiten las versiones anteriores de SLP (SLPv1), o usted desea que la detección de servicios del SLP interopere con Novell Netware 5.

## ▼ Cómo implementar DA

Utilice el siguiente procedimiento para establecer la propiedad `net.slp.isDA` en `True`, en el archivo `slp.conf`.

---

**Nota** – Sólo puede asignar un DA por host.

---

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Detenga `slpd` y toda la actividad del SLP en el host.

```
# svcadm disable network/slp
```

### 3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.

### 4 Establezca la propiedad `net.slp.isDA` del archivo `slpd.conf` en `True`:

```
net.slp.isDA=True
```

### 5 Guarde los cambios y cierre el archivo.

### 6 Reinicie `slpd` para activar los cambios.

```
# svcadm enable network/slp
```

## Dónde colocar DA

En esta sección, se proporcionan sugerencias acerca de dónde colocar DA en diferentes situaciones.

- Cuando el enrutamiento de multidifusión no está habilitado y los DA son necesarios para unir la detección de servicios entre subredes

En esta situación, un DA debe colocarse en un host con interfaces y todas las subredes que comparten servicios. La propiedad de configuración `net.slp.interfaces` *no* se debe establecer, a menos que los paquetes IP no se enruten entre las interfaces. Consulte [“Configuración de la función de hosts múltiples para SLP” en la página 265](#) para obtener más información sobre cómo configurar la propiedad `net.slp.interfaces`.

- Cuando se implementan DA para escalabilidad y la consideración principal es la optimización del acceso de agentes

Los UA, normalmente, realizan muchas solicitudes de servicios a los DA. Un SA se registra con el DA una vez y puede actualizar el anuncio en intervalos periódicos, pero con poca frecuencia. Como resultado, el acceso de UA a DA es mucho más frecuente que el acceso de SA. El número de anuncios de servicios también suele ser menor que el número de solicitudes. Por lo tanto, la mayoría de las implementaciones de DA son más eficaces si la implementación se optimiza para el acceso de UA.

- Colocación de los DA de manera que estén topológicamente cerca de los UA en la red para optimizar el acceso de los UA

Naturalmente, debe configurar el DA con un ámbito que sea compartido por los clientes de UA y SA.

## Colocación de varios DA para el equilibrio de carga

Puede implementar varios DA para el mismo conjunto de ámbitos como una manera de equilibrio de carga. Implemente los DA en cualquiera de las siguientes circunstancias:

- Las solicitudes de UA a un DA están agotando el tiempo de espera o se están devolviendo con el error `DA_BUSY_NOW`.
- El registro de DA muestra que muchas solicitudes del SLP se están perdiendo.
- La red de los usuarios que comparten servicios en los ámbitos abarca un número de edificios o sitios físicos.

Puede ejecutar un rastreo de snoop de tráfico de SLP para determinar cuántas solicitudes de UA regresan con el error `DA_BUSY_NOW`. Si el número de solicitudes de UA devuelto es alto, los UA en los edificios que se encuentran física y topológicamente alejados del DA pueden presentar respuestas lentas o tiempos de espera excesivos. En este escenario, se puede implementar un DA en cada edificio para mejorar la respuesta para los clientes de UA dentro del edificio.



Los enlaces que conectan edificios son, por lo general, más lentos que las redes de área local dentro de los edificios. Si la red abarca varios edificios o sitios físicos, establezca la propiedad `net.slp.DAAddresses` en el archivo `/etc/inet/slp.conf` para una lista de direcciones o nombres de host específicos para que los UA sólo accedan a los DA que especifique.

Si un DA determinado está utilizando grandes cantidades de memoria de host para los registros de servicios, reduzca el número de registros de SA disminuyendo el número de ámbitos que el DA admite. Puede dividir en dos un ámbito que tiene muchos registros. Puede admitir uno de los nuevos ámbitos mediante la implementación de otro DA en otro host.

## SLP y función de hosts múltiples

Un servidor de hosts múltiples actúa como un host en varias subredes IP. El servidor puede, a veces, tener más de una tarjeta de interfaz de red y puede actuar como enrutador. Los paquetes IP, incluidos los paquetes de multidifusión, se enrutan entre las interfaces. En algunas situaciones, el enrutamiento entre interfaces está deshabilitado. En las secciones siguientes, se describe cómo configurar el SLP para esas situaciones.

### Configuración de la función de hosts múltiples para SLP

Sin configuración, el `slpd` escucha la multidifusión y la unidifusión UDP/TCP en la interfaz de red predeterminada. Si el enrutamiento de unidifusión y multidifusión está habilitado entre las interfaces de un equipo de hosts múltiples, no se necesita ninguna configuración adicional. Esto se debe a que los paquetes de multidifusión que llegan a otra interfaz se enrutan correctamente a la interfaz predeterminada. Como resultado, las solicitudes de multidifusión para DA u otros anuncios de servicios llegan a `slpd`. Si el enrutamiento no está activado por algún motivo, es necesario realizar la configuración.

### Cuándo realizar la configuración para múltiples interfaces de red no enrutadas

Si existe una de las condiciones siguientes, quizá deba configurar equipos de hosts múltiples.

- El enrutamiento de unidifusión está habilitado entre las interfaces y el enrutamiento de multidifusión está deshabilitado.
- El enrutamiento de unidifusión y el enrutamiento de multidifusión están deshabilitados entre las interfaces.

Cuando el enrutamiento de multidifusión está deshabilitado entre interfaces, normalmente, se debe a que la multidifusión no ha sido implementada en la red. En tal situación, la difusión se usa, por lo general, para la detección de servicios que no se basa en DA y para la detección de DA en las subredes individuales. La difusión se configura estableciendo la propiedad `net.slp.isBroadcastOnly` en `True`.

## Configuración de múltiples interfaces de red no enrutadas (mapa de tareas)

TABLA 9-5 Configuración de múltiples interfaces de red no enrutadas

Tarea	Descripción	Para obtener instrucciones
Configurar la propiedad <code>net.slp.interfaces</code>	Establezca esta propiedad para que <code>slpd</code> escuche solicitudes del SLP de unidifusión y multidifusión/difusión en las interfaces especificadas.	<a href="#">“Configuración de la propiedad <code>net.slp.interfaces</code>” en la página 266</a>
Organizar anuncios de servicios de proxy de modo que los UA en subredes obtengan direcciones URL de servicio con direcciones accesibles	Restrinja anuncios de proxy a un equipo que está ejecutando <code>slpd</code> conectado a una única subred en lugar de un host múltiple.	<a href="#">“Anuncios de proxy y hosts múltiples” en la página 268</a>
Colocar DA y configurar ámbitos para garantizar la accesibilidad entre UA y SA	Configure la propiedad <code>net.slp.interfaces</code> en hosts múltiples con una dirección o un nombre de host de interfaz único.  Ejecute un DA en un host múltiple, pero configure ámbitos para que los SA y UA de cada subred utilicen hosts diferentes.	<a href="#">“Asignación de nombre de ámbito y colocación de DA” en la página 269</a>

## Configuración de la propiedad `net.slp.interfaces`

Si la propiedad `net.slp.interfaces` está establecida, `slpd` escucha solicitudes del SLP de unidifusión y multidifusión/difusión en las interfaces que aparecen en la propiedad, en lugar de la interfaz predeterminada.

Por lo general, establece la propiedad `net.slp.interfaces` junto con la habilitación de la difusión estableciendo la propiedad `net.slp.isBroadcastOnly`, porque la multidifusión no se ha implementado en la red. Sin embargo, si la multidifusión se ha implementado, pero no se enruta en este host múltiple particular, una solicitud de multidifusión puede llegar a `slpd` de más de una interfaz. Esta situación se puede producir cuando el enrutamiento de paquetes es manejado por otro host múltiple o enrutador que conecta las subredes que son servidas por las interfaces.

Cuando tal situación se produce, el servidor de SA o el UA que envía la solicitud recibe dos respuestas de `sldap` en el host múltiple. Las respuestas se filtran por las bibliotecas del cliente, y el cliente no las ve. Sin embargo, las respuestas están visibles en el rastreo de snoop.

---

**Nota –**

Si el enrutamiento de unidifusión está desactivado, es posible que no se pueda acceder a los servicios anunciados por clientes de SA en hosts múltiples desde todas las subredes. Si no se puede acceder a los servicios, los clientes de SA pueden realizar lo siguiente:

- Anunciar una URL de servicio para cada subred.
  - Garantizar que las solicitudes de una subred particular se respondan con una URL accesible.
- 

La biblioteca del cliente de SA no hace nada para garantizar que las direcciones URL accesibles se anuncien. El programa de servicio, que puede o no manejar un host múltiple sin ningún enrutamiento, es responsable de asegurar que las direcciones URL accesibles sean anunciadas.

Antes de desplegar un servicio en un host múltiple con enrutamiento de unidifusión deshabilitado, use snoop para determinar si el servicio maneja las solicitudes de varias subredes correctamente. Además, si tiene previsto implementar un DA en el host múltiple, consulte [“Asignación de nombre de ámbito y colocación de DA” en la página 269](#).

## ▼ **Cómo configurar la propiedad `net.slp.interfaces`**

Utilice el siguiente procedimiento para cambiar la propiedad `net.slp.interfaces` en el archivo `slp.conf`.

### **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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### **2 Detenga `sldap` y toda la actividad del SLP en el host.**

```
# svcadm disable network/slp
```

### **3 Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**

### **4 Cambie la propiedad `net.slp.interfaces` en el archivo `sldap.conf`:**

```
net.slp.interfaces=value
```

*valor*      Lista de direcciones IPv4 o nombres de host de las tarjetas de interfaz de red en las que el DA o SA deben escuchar mensajes TCP, UDP de unidifusión y multidifusión en el puerto 427

Por ejemplo, un servidor con tres tarjetas de red y enrutamiento de multidifusión desactivado está conectado a tres subredes. Las direcciones IP de las tres interfaces de red son 192.147.142.42, 192.147.143.42 y 192.147.144.42. La máscara de subred es 255.255.255.0. El siguiente valor de propiedad hace que `sldap` escuche en las tres interfaces mensajes de unidifusión y multidifusión/difusión:

```
net.slp.interfaces=192.147.142.42,192.147.143.42,192.147.144.42
```

---

**Nota** – Puede especificar direcciones IP o nombres de host que se pueden resolver para la propiedad `net.slp.interfaces`.

---

**5 Guarde los cambios y cierre el archivo.**

**6 Reinicie `sldap` para activar los cambios.**

```
# svcadm enable network/slp
```

## Anuncios de proxy y hosts múltiples

Si un host con varias interfaces anuncia servicios mediante `sldap` y registro de proxy, las direcciones URL de servicio anunciadas por `sldap` deben contener direcciones o nombres de host accesibles. Si el enrutamiento de unidifusión está habilitado entre las interfaces, los hosts en todas las subredes pueden acceder a los hosts de otras subredes. Los registros de proxy también se pueden realizar para un servicio en cualquier subred. Sin embargo, si el enrutamiento de unidifusión está deshabilitado, los clientes de servicio en una subred no pueden acceder a servicios en otra subred por medio del host múltiple. Es posible, no obstante, que dichos clientes puedan acceder a los servicios mediante otro enrutador.

Por ejemplo, suponga que el host con el nombre de host predeterminado `bigguy` tiene tres tarjetas de interfaz en tres subredes enrutadas diferentes. Los nombres de host en estas subredes son `bigguy`, con dirección IP 192.147.142.42, `bigguy1`, con dirección IP 192.147.143.42 y `bigguy2`, con dirección IP 192.147.144.42. Ahora, suponga que una impresora antigua, `oldprinter`, está conectada a la subred 143 y que la dirección URL `service:printing:lpr://oldprinter/queue1` está configurada con `net.slp.interfaces` para escuchar en todas las interfaces. La URL `oldprinter` tiene anuncios de proxy en todas las interfaces. Los equipos de las subredes 142 y 144 reciben la dirección URL en respuesta a solicitudes de servicio, pero no pueden acceder al servicio `oldprinter`.

La solución a este problema es realizar los anuncios de proxy con `sldap` ejecutándose en un equipo que está conectado sólo a la subred 143, en lugar de en el host múltiple. Sólo los hosts de la subred 143 pueden obtener el anuncio en respuesta a una solicitud de servicio.

## Asignación de nombre de ámbito y colocación de DA

La colocación de DA y la asignación de nombres de ámbito en una red con un host múltiple se deben realizar cuidadosamente para garantizar que los clientes obtengan servicios accesibles. Sea especialmente cauteloso cuando el enrutamiento esté deshabilitado y la propiedad `net.slp.interfaces` esté configurada. De nuevo, si el enrutamiento de unidifusión está habilitado entre las interfaces en un equipo de hosts múltiples, no es necesaria ninguna configuración especial de DA ni ámbito. Los anuncios se almacenan en la antememoria con los servicios de identificación de DA a los que se puede acceder desde cualquiera de las subredes. Sin embargo, si el enrutamiento de unidifusión está deshabilitado, la colocación incorrecta de DA puede generar problemas.

Para ver los problemas que pueden ocurrir en el ejemplo anterior, considere qué sucedería si `bigguy` ejecuta un DA y los clientes en todas las subredes tienen los mismos ámbitos. Los SA en la subred 143 registran sus anuncios de servicios con el DA. Los UA en la subred 144 pueden obtener esos anuncios de servicios, aunque no se pueda acceder a los hosts de la subred 143.

Una solución a este problema es ejecutar un DA en cada subred y no en el host múltiple. En esta situación, la propiedad `net.slp.interfaces` en los hosts múltiples debe configurarse con una dirección o un nombre de host de interfaz único, o debe dejarse sin configurar, con lo que se fuerza el uso de la interfaz predeterminada. La desventaja de esta solución es que los hosts múltiples son, a menudo, grandes equipos que podrían manejar mejor la carga computacional de un DA.

Otra solución es ejecutar un DA en el host múltiple, pero configurar ámbitos para que los SA y UA en cada subred tengan un ámbito diferente. Por ejemplo, en la situación anterior, los UA y SA en la subred 142 pueden tener un ámbito que se denomina `scope142`. Los UA y SA en la subred 143 pueden tener otro ámbito que se denomina `scope143`, y los UA y SA en la subred 144 pueden tener un tercer ámbito que se denomina `scope144`. Puede configurar la propiedad `net.slp.interfaces` en `bigguy` con las tres interfaces, de modo que el DA atienda tres ámbitos en las tres subredes.

## Consideraciones al configurar múltiples interfaces de red no enrutadas

La configuración de la propiedad `net.slp.interfaces` permite que un DA en el host múltiple anuncie servicios entre las subredes. Dicha configuración es útil si el enrutamiento de multidifusión está desactivado en la red, pero el enrutamiento de unidifusión entre interfaces en un host múltiple está habilitado. Debido a que la unidifusión se enruta entre las interfaces, los hosts en una subred diferente de la subred en la que el servicio se encuentra pueden ponerse en contacto con el servicio cuando reciben la URL del servicio. Sin el DA, los servidores de SA

en una subred en particular reciben sólo difusiones que se realizaron en la misma subred, por lo que no pueden buscar servicios fuera de su subred.

La situación más común que requiere la configuración de la propiedad `net.slp.interfaces` se produce cuando la multidifusión no está implementada en la red y la difusión se utiliza en su lugar. Otras situaciones exigen una cuidadosa consideración y planificación para evitar respuestas duplicadas innecesarias o servicios inaccesibles.

## Incorporación de servicios antiguos

---

Los servicios antiguos son servicios de red que anteceden el desarrollo y la implementación del SLP. Los servicios como el Line Printer Daemon (`lpd`), el servicio de archivos NFS y el servicio de nombres NIS/NIS+, por ejemplo, no contienen SA internos para el SLP. En este capítulo, se describen cuándo y cómo anunciar servicios antiguos.

- “Cuándo anunciar servicios antiguos” en la página 271
- “Anuncio de servicios antiguos” en la página 271
- “Consideraciones al anunciar servicios antiguos” en la página 275

### Cuándo anunciar servicios antiguos

Con el anuncio de servicios antiguos, puede habilitar los UA del SLP para buscar dispositivos y servicios, como los que se detallan a continuación, en las redes. Puede buscar dispositivos de hardware y servicios de software que no contienen SA del SLP. Cuando las aplicaciones con UA del SLP necesitan encontrar impresoras o bases de datos que no contienen SA del SLP, por ejemplo, los anuncios antiguos podrían ser necesarios.

### Anuncio de servicios antiguos

Utilice cualquiera de los siguientes métodos para anunciar servicios antiguos.

- Modificar el servicio para incorporar un SA del SLP.
- Escribir un programa pequeño que anuncie en nombre de un servicio que no esté habilitado para SLP.
- Utilizar los anuncios de proxy para que `slpd` anuncie el servicio.

## Modificación del servicio

Si el código de origen del servidor de software está disponible, se puede incorporar un SA del SLP. Las API de Java y C para SLP son relativamente sencillas de utilizar. Consulte las páginas del comando `man` para obtener información sobre la API C y documentación sobre la API de Java. Si el servicio es un dispositivo de hardware, el fabricante puede tener una PROM actualizada que incorpora SLP. Póngase en contacto con el fabricante del dispositivo para obtener más información.

## Anuncio de un servicio que no está habilitado para SLP

Si el código de origen o una PROM actualizada que contienen el SLP no están disponibles, puede escribir una aplicación pequeña que utiliza la biblioteca de cliente del SLP para anunciar el servicio. Esta aplicación puede funcionar como un daemon pequeño que se inicia o se detiene desde la misma secuencia de comandos del shell que se utiliza para iniciar y detener el servicio.

## Registro del proxy de SLP

Solaris `slpd` admite anuncios de servicios antiguos con un archivo de registro de proxy. El archivo de registro de proxy es una lista de anuncios de servicios en un formato portátil.

### ▼ Cómo habilitar el registro del proxy de SLP

- 1 Cree un archivo de registro de proxy en el sistema de archivos de host o en cualquier directorio de red al que HTTP puede acceder.

- 2 Determine si hay una plantilla de tipo de servicio para el servicio.

La plantilla es una descripción de la URL del servicio y los atributos de un tipo de servicio. Una plantilla se usa para definir los componentes de un anuncio para un tipo de servicio determinado:

- Si existe una plantilla de tipo de servicio, utilice la plantilla para construir el registro del proxy. Consulte la RFC 2609 para obtener más información sobre las plantillas de tipo de servicio.
- Si una plantilla de tipo de servicio no está disponible para el servicio, seleccione una colección de atributos que describen precisamente el servicio. Utilice una autoridad de asignación de nombres diferente del valor predeterminado para el anuncio. La autoridad de asignación de nombres predeterminada sólo se permite para tipos de servicio que se han estandarizado. Consulte la RFC 2609 para obtener más información sobre las autoridades de asignación de nombres.



Por ejemplo, suponga que una compañía que se denomina *BizApp* tiene una base de datos local que se utiliza para realizar un seguimiento de defectos de software. Para anunciar la base de datos, la compañía puede utilizar una dirección URL con el tipo de servicio `service:bugdb.bizapp`. La autoridad de asignación de nombres sería `bizapp`.

- 3 **Siga los siguientes pasos para configurar la propiedad `net.slp.serializedRegURL` en el archivo `/etc/inet/slp.conf` con la ubicación del archivo de registro que se creó en los pasos anteriores.**
- 4 **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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 5 **Detenga `slpd` y toda la actividad de SLP en el host.**  

```
# svcadm disable network/slp
```
- 6 **Realice una copia de seguridad del archivo `/etc/inet/slp.conf` predeterminado antes de cambiar los valores de configuración.**
- 7 **Especifique la ubicación del archivo de registro de proxy en la propiedad `net.slp.serializedRegURL` del archivo `/etc/inet/slp.conf`.**  

```
net.slp.net.slp.serializedRegURL=proxy registration file URL
```

Por ejemplo, si el archivo de registro en serie es `/net/inet/slp.reg`, configure la propiedad como se muestra en el siguiente ejemplo:

```
net.slp.serializedRegURL=file:/etc/inet/slp.reg
```
- 8 **Guarde los cambios y cierre el archivo.**
- 9 **Reinicie `slpd` para activar los cambios.**  

```
# svcadm enable network/slp
```

## Uso del registro del proxy de SLP para anunciar

Un anuncio de servicio consta de líneas que identifican la URL del servicio, un ámbito optativo y una serie de definiciones de atributos. El daemon del SLP lee, registra y mantiene anuncios de proxy exactamente como un cliente de SA lo haría. A continuación se muestra un ejemplo de un anuncio de un archivo de registro de proxy.

En el ejemplo, se anuncian una impresora antigua que admite el protocolo LPR y un servidor FTP. Números de línea se han agregado para fines descriptivos y no forman parte del archivo.

```
(1)#Advertise legacy printer.  
(2)  
(3)service:lpr://bizserver/mainspool,en,65535  
(4)scope=eng,corp  
(5)make-model=Laserwriter II  
(6)location-description=B16-2345  
(7)color-supported=monochromatic  
(8)fonts-supported=Courier,Times,Helvetica 9 10  
(9)  
(10)#Advertise FTP server  
(11)  
(12)ftp://archive/usr/src/public,en,65535,src-server  
(13)content=Source code for projects  
(14)
```

**Nota** – El archivo de registro de proxy admite la misma convención para caracteres que no son ASCII de escape que el archivo de configuración. Para obtener más información sobre el formato del archivo de registro de proxy, consulte la RFC 2614.

**TABLA 10-1** Descripción del archivo de registro de proxy de SLP

Números de línea	Descripción
1 y 10	Las líneas de comentario comienzan con un símbolo de número (#) y no afectan la operación del archivo. Todos los caracteres hasta el final de una línea de comentario se ignoran.
2, 9 y 14	Líneas en blanco que delimitan los anuncios.
3, 12	Direcciones URL del servicio que cuentan con tres campos necesarios y un campo opcional que están separados por comas: <ul style="list-style-type: none"><li>■ Genérica o service: URL anunciada. Consulte la RFC 2609 para obtener la especificación de cómo formar una service: URL.</li><li>■ Idioma del anuncio. En el ejemplo anterior, el campo se ha establecido en inglés, <i>en</i>. El idioma es una etiqueta de idioma de RFC 1766.</li><li>■ Duración del registro, medida en segundos. La duración se limita a un número entero no firmado de 16 bits. Si la duración es menor que el máximo, 65535, <i>slpd</i> agota el tiempo de espera del anuncio. Si la duración es 65535, <i>slpd</i> actualiza el anuncio periódicamente, y la duración se considera permanente, hasta que <i>slpd</i> se cierra.</li><li>■ (Opcional) Campo de tipo de servicio: si se usa, este campo define el tipo de servicio. Si la URL del servicio se define, puede cambiar el tipo de servicio bajo el cual se anuncia la dirección URL. En el ejemplo anterior de un archivo de registro de proxy, la línea 12 contiene una URL de FTP genérica. El campo de tipo opcional hace que la dirección URL se anuncie bajo el nombre de tipo de servicio <i>src-server</i>. El prefijo <i>service</i> no se ha agregado de manera predeterminada en el nombre del tipo.</li></ul>

TABLA 10-1 Descripción del archivo de registro de proxy de SLP (Continuación)

Números de línea	Descripción
4	Designación de ámbito.  La línea opcional consta del token <code>scope</code> , seguido de un signo igual y una lista separada por comas de nombres de ámbitos. Los nombres de ámbitos están definidos por la propiedad de configuración <code>net.slp.useScopes</code> . Sólo ámbitos que se han configurado para el host se deben incluir en la lista. Cuando una línea de ámbito no se ha agregado, el registro se realiza en todos los ámbitos donde <code>slpd</code> está configurado. La línea de ámbito debe figurar inmediatamente después de la línea de la dirección URL. De lo contrario, los nombres de ámbitos se reconocen como atributos.
De 5 a 8	Definiciones de atributos.  Después de la línea de ámbito opcional, la mayor parte del anuncio del servicio contiene líneas de pares de listas de valores o atributos. Cada par consta de la etiqueta de atributo, seguida de un signo igual y un valor de atributo o una lista separada por comas de valores. En el ejemplo anterior de un archivo de registro de proxy, la línea 8 ilustra una lista de atributos con varios valores. Todas las otras listas tienen valores únicos. El formato de los valores y los nombres de atributos es el mismo que el de los mensajes de SLP en el cable.

## Consideraciones al anunciar servicios antiguos

Por lo general, se prefiere la modificación del código de origen para agregar un SLP antes que la escritura de un servicio habilitado para SLP que utiliza la API de SLP para anunciar en nombre de otros servicios. También se prefiere la modificación del código de origen antes que el registro del proxy. Al modificar el código de origen, puede agregar funciones específicas del servicio y realizar detenidamente un seguimiento de la disponibilidad del servicio. Si el código de origen no está disponible, la escritura de un servicio auxiliar habilitado para SLP que anuncia en nombre de otros servicios se prefiere antes que el registro del proxy. Idealmente, este servicio auxiliar está integrado en el procedimiento de inicio o detención del servicio que se utiliza para controlar la activación y la desactivación. El anuncio del proxy es, normalmente, la tercera opción, cuando no hay ningún código de origen disponible y la escritura de un SA independiente es poco práctica.

Los anuncios de proxy sólo se mantienen si `slpd` se ejecuta para leer el archivo de registro de proxy. No existe ninguna conexión directa entre el anuncio del proxy y el servicio. Si un anuncio agota el tiempo de espera o `slpd` se detiene, el anuncio del proxy ya no está disponible.

Si el servicio se cierra, `slpd` se debe detener. El archivo de registro en serie se edita para comentar o eliminar el anuncio del proxy, y `slpd` se reinicia. Debe seguir el mismo procedimiento cuando el servicio se reinicia o se vuelve a instalar. La falta de conexión entre el anuncio del proxy y el servicio es una desventaja importante de los anuncios de proxy.



## SLP (referencia)

---

En este capítulo, se describen los códigos de estado y los tipos de mensaje del SLP. Los tipos de mensaje del SLP se muestran con las abreviaturas y los códigos de función. Los códigos de estado del SLP se muestran con descripciones y códigos de función que se utilizan para indicar que se recibe una solicitud (código 0) o que el receptor está ocupado.

---

**Nota** – El daemon del SLP (`slpd`) devuelve códigos de estado para mensajes de unidifusión solamente.

---

## Códigos de estado del SLP

TABLA 11-1 Códigos de estado del SLP

Tipo de estado	Código de estado	Descripción
Ningún error	0	La solicitud se procesó sin errores.
LANGUAGE_NOT_SUPPORTED	1	Para un mensaje AttrRqst o SrvRqst, hay datos para el tipo de servicio en el ámbito, pero no en el idioma que se indica.
PARSE_ERROR	2	El mensaje no puede seguir la sintaxis del SLP.
INVALID_REGISTRATION	3	El mensaje SrvReg tiene problemas. Por ejemplo, una duración igual a cero o una etiqueta de idioma omitida.
SCOPE_NOT_SUPPORTED	4	El mensaje del SLP no incluía un ámbito en su lista de ámbitos admitida por el SA o el DA que respondieron la solicitud.
AUTHENTICATION_UNKNOWN	5	El DA o SA recibieron una solicitud para una SPI del SLP no admitida.

TABLA 11-1 Códigos de estado del SLP (Continuación)

Tipo de estado	Código de estado	Descripción
AUTHENTICATION_ABSENT	6	El UA o DA esperaban una autenticación de URL y atributo en el mensaje SrvReg, pero no la recibieron.
AUTHENTICATION_FAILED	7	El UA o DA detectaron un error de autenticación en un bloque de autenticación.
VER_NOT_SUPPORTED	9	Número de versión no admitido en el mensaje.
INTERNAL_ERROR	10	Se produjo un error desconocido en el DA o SA. Por ejemplo, el sistema operativo no tenía espacio de archivo restante.
DA_BUSY_NOW	11	El UA o SA deben reintentar mediante la interrupción exponencial. El DA está ocupado con el procesamiento de otros mensajes.
OPTION_NOT_UNDERSTOOD	12	El DA o SA recibieron una opción desconocida del rango obligatorio.
INVALID_UPDATE	13	El DA recibió un mensaje SrvReg sin FRESH establecido para un servicio no registrado o con tipos de servicio inconsistentes.
MSG_NOT_SUPPORTED	14	El SA recibió un mensaje AttrRqst o SrvTypeRqst, pero no lo admite.
REFRESH_REJECTED	15	El SA envió un mensaje SrvReg o SrvDereg parcial a un DA con más frecuencia que el intervalo de actualización mínimo del DA.

## Tipos de mensaje del SLP

TABLA 11-2 Tipos de mensaje del SLP

Tipo de mensaje	Abreviatura	Código de función	Descripción
Solicitud de servicio	SrvRqst	1	Emitido por un UA para buscar servicios o por un servidor de UA o SA durante la detección activa de DA.
Respuesta de servicio	SrvRply	2	La respuesta del DA o SA a una solicitud de servicio.
Registro de servicio	SrvReg	3	Permite que los SA registren nuevos anuncios para actualizar los anuncios existentes con atributos nuevos y modificados, y para actualizar las duraciones de las direcciones URL.

TABLA 11-2 Tipos de mensaje del SLP (Continuación)

Tipo de mensaje	Abreviatura	Código de función	Descripción
Anulación de registro de servicio	SrvDereg	4	Utilizado por el SA para anular el registro de sus anuncios cuando el servicio que representan ya no está disponible.
Confirmación	SrvAck	5	La respuesta del DA a una solicitud de servicio o un mensaje de anulación de registro de servicio del SA.
Solicitud de atributo	AttrRqst	6	Realizado por la dirección URL o por el tipo de servicio para solicitar una lista de atributos.
Respuesta de atributo	AttrRply	7	Utilizado para devolver la lista de atributos.
Anuncio de DA	DAAdvert	8	La respuesta del DA para realizar la multidifusión de solicitudes de servicio.
Solicitud de tipo de servicio	SrvTypeRqst	9	Utilizado para consultar sobre tipos de servicio registrados que tienen una autoridad de asignación de nombres particular y se encuentran en un conjunto determinado de ámbitos.
Respuesta de tipo de servicio	SrvTypeRply	10	El mensaje que se devuelve en respuesta a la solicitud de tipo de servicio.
Anuncio de SA	SAAadvert	11	Los UA utilizan el mensaje SAAadvert para detectar SA y sus ámbitos en las redes en las que no hay DA implementados.





## **P A R T E I V**

### **Servicios de correo (temas)**

Esta sección proporciona información sobre la descripción general, las tareas y la referencia del servicio de correo.



## Servicios de correo (descripción general)

---

La configuración y el mantenimiento de un servicio de correo electrónico implican tareas complejas que son críticas para el funcionamiento diario de la red. Como administrador de la red, es posible que deba ampliar un servicio de correo existente. Asimismo, es posible que deba configurar un servicio de correo en una red nueva o en una subred. Los capítulos sobre servicios de correo pueden ayudar a planificar y configurar un servicio de correo para la red. Este capítulo proporciona enlaces a descripciones de las nuevas funciones de `sendmail`, además de una lista de otras fuentes de información. El capítulo también proporciona una descripción general de los componentes de software y hardware que son necesarios para establecer un servicio de correo.

- [“Novedades de los servicios de correo” en la página 283](#)
- [“Otras fuentes de información de `sendmail`” en la página 285](#)
- [“Introducción a los componentes de los servicios de correo” en la página 285](#)

Consulte el [Capítulo 13, “Servicios de correo \(tareas\)”](#) para obtener información sobre los procedimientos para configurar y administrar servicios de correo. Para obtener detalles, consulte [“Mapa de tareas para servicios de correo” en la página 289](#).

Consulte el [Capítulo 14, “Servicios de correo \(referencia\)”](#) para obtener una descripción más detallada de los componentes de los servicios de correo. En este capítulo, también se describen los programas y archivos del servicio de correo, el proceso de enrutamiento del correo, las interacciones de `sendmail` con los servicios de nombres y las funciones de la versión 8.13 de `sendmail`. Consulte [“Cambios en la versión 8.13 de `sendmail`” en la página 379](#).

## Novedades de los servicios de correo

Esta sección brinda información sobre las nuevas funciones en diferentes versiones de Solaris.

## Cambios en esta versión

Se realizaron los siguientes cambios en la Versión de actualización 10 de Oracle Solaris 10

- La versión predeterminada de sendmail se actualizó a 8.14.
- La instancia de sendmail se dividió en dos instancias para proporcionar una mejor gestión del daemon tradicional (`svc:/network/smtp:sendmail`) y el ejecutor de colas de cliente (`svc:/network/smtp:sendmail-client`).
- El sistema se puede configurar para que vuelva a generar automáticamente los archivos de configuración `sendmail.cf` y `submit.mc`. Los pasos necesarios se documentan en [“Cómo volver a generar automáticamente un archivo de configuración” en la página 305](#).
- De manera predeterminada, el daemon de sendmail se ejecuta en el nuevo modo de daemon local. El modo sólo local acepta únicamente correo entrante del host local o conexiones SMTP de bucle de retorno. Por ejemplo, se acepta correo de un trabajo cron o entre usuarios locales. El correo saliente se enruta del modo esperado; sólo se modifica el correo entrante. La opción `-bl` se usa para seleccionar el modo sólo local, también conocido como modo Become Local. Para obtener más información sobre este modo, consulte la página del comando `man sendmail(1M)`. Para obtener instrucciones acerca de cómo regresar al modo `-bd` o Become Daemon, consulte [“Cómo usar sendmail en el modo abierto” en la página 306](#).

## Cambios en la versión Solaris 10 1/06

A partir de Solaris 10 1/06, sendmail admite SMTP mediante Seguridad de la capa de transporte (TLS). Para obtener más información, consulte lo siguiente:

- [“Compatibilidad para ejecutar SMTP con TLS en la versión 8.13 de sendmail” en la página 380](#)
- [“Cómo configurar SMTP para que utilice TLS” en la página 307](#)

Para obtener una lista completa de las funciones de Solaris 10 1/06, consulte [Novedades de Oracle Solaris 10 8/11](#).

## Cambios en la versión Solaris 10

De manera predeterminada, se usa la versión 8.13 de sendmail. Para obtener información acerca de la versión 8.13 y otros cambios, consulte las siguientes secciones:

- [“Indicadores utilizados y no utilizados para compilar sendmail” en la página 340](#)
- [“MILTER, API de filtro de correo para sendmail” en la página 341](#)
- [“Versiones del archivo de configuración” en la página 342](#)
- [“Mejoras en la utilidad `vacation`” en la página 355](#)
- [“Contenido del directorio `/etc/mail/cf`” en la página 357](#)

- “Cambios en la versión 8.13 de sendmail” en la página 379
- “Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail” en la página 388

Además, el servicio de correo es gestionado por la utilidad de gestión de servicios. Las acciones administrativas de este servicio, como la activación, la desactivación o el reinicio, pueden realizarse con el comando `svcadm`. Utilice el comando `svcs` para consultar el estado del servicio. Para obtener más información sobre la utilidad de gestión de servicios, consulte la página del comando `man smf(5)` y el Capítulo 18, “Gestión de servicios (descripción general)” de *Guía de administración del sistema: administración básica*.

## Otras fuentes de información de sendmail

A continuación, se muestra una lista de las fuentes de información adicionales sobre sendmail.

- Costales, Bryan. *sendmail, Third Edition* (sendmail, tercera edición). O'Reilly & Associates, Inc., 2002.
- Página principal de sendmail. <http://www.sendmail.org>.
- Preguntas frecuentes de sendmail. <http://www.sendmail.org/faq>.
- LÉAME de los nuevos archivos de configuración de sendmail. <http://www.sendmail.org/m4/readme.html>.
- Guía para los problemas relacionados con la migración a versiones más recientes de sendmail. <http://www.sendmail.org/vendor/sun/>.

## Introducción a los componentes de los servicios de correo

Se necesitan varios componentes de software y hardware para establecer un servicio de correo. Las siguientes secciones proporcionan una introducción rápida a estos componentes. Estas secciones también proporcionan algunos de los términos que se utilizan para describir los componentes.

La primera sección, “Descripción general de los componentes de software” en la página 285, define los términos que se utilizan al analizar los componentes de software del sistema de entrega de correo. La siguiente sección, “Descripción general de los componentes de hardware” en la página 286, se centra en las funciones de los sistemas de hardware en una configuración de correo.

## Descripción general de los componentes de software

La siguiente tabla presenta algunos de los componentes de software de un sistema de correo. Consulte “Componentes de software” en la página 343 para obtener una descripción completa de todos los componentes de software.

Componente	Descripción
archivos . forward	Archivos que es posible configurar en el directorio principal de un usuario para redireccionar correo o para enviar correo a un programa automáticamente.
buzón	Archivo en un servidor de correo que constituye el destino final de los mensajes de correo electrónico.
direcciones de correo	Dirección que contiene el nombre del destinatario y el sistema al que se envía un mensaje de correo.
alias de correo	Nombre alternativo que se utiliza en una dirección de correo.
cola de correo	Recopilación de mensajes de correo que el servidor de correo debe procesar.
postmaster	Alias de correo especial que se utiliza para informar problemas y formular preguntas sobre el servicio de correo.
archivo de configuración de sendmail	Archivo que contiene toda la información necesaria para el enrutamiento del correo.

## Descripción general de los componentes de hardware

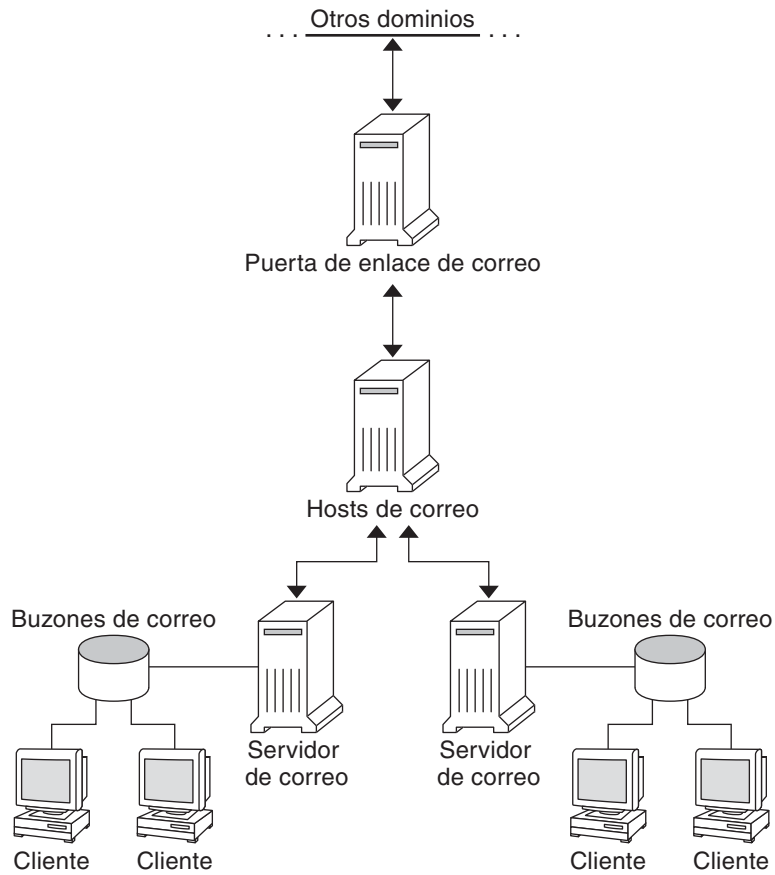
Una configuración de correo requiere tres elementos, que se pueden combinar en el mismo sistema o se pueden proporcionar en sistemas independientes.

- Un host de correo: un sistema configurado para manejar las direcciones de correo electrónico que son difíciles de resolver.
- Un servidor de correo como mínimo: un sistema configurado para alojar uno o varios buzones.
- Clientes de correo: sistemas que acceden al correo desde un servidor de correo.

Si los usuarios deben comunicarse con redes fuera del dominio, también se debe agregar un cuarto elemento, es decir, una puerta de enlace de correo.

La [Figura 12–1](#) muestra una configuración típica de correo electrónico, con los tres elementos de correo básicos más una puerta de enlace de correo.

FIGURA 12-1 Configuración típica de correo electrónico



Cada elemento se describe de forma detallada en [“Componentes de hardware” en la página 351](#).





## Servicios de correo (tareas)

---

En este capítulo, se describe cómo configurar y administrar los servicios de correo. Si no está familiarizado con la administración de servicios de correo, lea el [Capítulo 12, “Servicios de correo \(descripción general\)”](#) para obtener una introducción de los componentes de servicios de correo. En este capítulo, también se proporciona una descripción de la configuración típica de un servicio de correo, como se muestra en la [Figura 12–1](#). La siguiente lista ayuda a buscar grupos de procedimientos relacionados que están comprendidos en este capítulo.

- “Mapa de tareas para servicios de correo” en la página 289
- “Configuración de los servicios de correo (mapa de tareas)” en la página 294
- “Modificación de la configuración de sendmail (mapa de tareas)” en la página 303
- “Administración de los archivos de alias de correo (mapa de tareas)” en la página 313
- “Administración de los directorios de la cola (mapa de tareas)” en la página 324
- “Administración de los archivos . forward (mapa de tareas)” en la página 328
- “Procedimientos y consejos para la resolución de problemas en servicios de correo (mapa de tareas)” en la página 331

Consulte el [Capítulo 14, “Servicios de correo \(referencia\)”](#) para obtener una descripción más detallada de los componentes de servicios de correo. En este capítulo, también se describen los programas y archivos del servicio de correo, el proceso de enrutamiento del correo, las interacciones de sendmail con los servicios de nombres y las funciones de la versión 8.13 de sendmail que no se describen en su totalidad en la página del comando `man sendmail(1M)`.

## Mapa de tareas para servicios de correo

La siguiente tabla hace referencia a otros mapas de tareas que se centran en un grupo específico de procedimientos.

Tarea	Descripción	Para obtener instrucciones
Configurar los servicios de correo	Utilice estos procedimientos para configurar cada componente del servicio de correo. Aprenda a configurar un servidor de correo, un cliente de correo, un host de correo y una puerta de enlace de correo. Aprenda a utilizar DNS con sendmail.	<a href="#">“Configuración de los servicios de correo (mapa de tareas)” en la página 294</a>
Modificar la configuración de sendmail	Utilice estos procedimientos para modificar los archivos de configuración o las propiedades del servicio.	<a href="#">“Modificación de la configuración de sendmail (mapa de tareas)” en la página 303</a>
Administrar los archivos de alias de correo	Utilice estos procedimientos para crear alias en la red. Aprenda a gestionar entradas en las tablas NIS+. Además, descubra cómo configurar un mapa NIS, un alias de correo local, un archivo de mapa con clave y un alias postmaster.	<a href="#">“Administración de los archivos de alias de correo (mapa de tareas)” en la página 313</a>
Administrar la cola de correo	Utilice estos procedimientos para ofrecer un procesamiento de cola sin complicaciones. Aprenda a mostrar y mover la cola de correo, forzar el procesamiento de la cola de correo y ejecutar un subconjunto de la cola de correo. Además, aprenda a ejecutar la cola de correo antigua.	<a href="#">“Administración de los directorios de la cola (mapa de tareas)” en la página 324</a>
Administrar los archivos .forward	Utilice estos procedimientos para deshabilitar los archivos .forward o para cambiar la ruta de búsqueda del archivo .forward. Además, aprenda a crear y rellenar /etc/shells para permitir que los usuarios utilicen el archivo .forward.	<a href="#">“Administración de los archivos .forward (mapa de tareas)” en la página 328</a>
Procedimientos y consejos para la resolución de problemas en servicios de correo	Utilice estos procedimientos y consejos para resolver problemas con el servicio de correo. Conozca cómo probar la configuración de correo, comprobar los alias de correo, probar los conjuntos de reglas de sendmail, verificar las conexiones con otros sistemas y registrar mensajes. Además, descubra dónde buscar otro tipo de información de diagnóstico de correo.	<a href="#">“Procedimientos y consejos para la resolución de problemas en servicios de correo (mapa de tareas)” en la página 331</a>
Resolver los mensajes de error	Utilice la información de esta sección para resolver algunos mensajes de error relacionados con el correo.	<a href="#">“Resolución de los mensajes de error” en la página 336</a>

# Planificación del sistema de correo

La siguiente lista describe algunas de las inquietudes que deben formar parte del proceso de planificación.

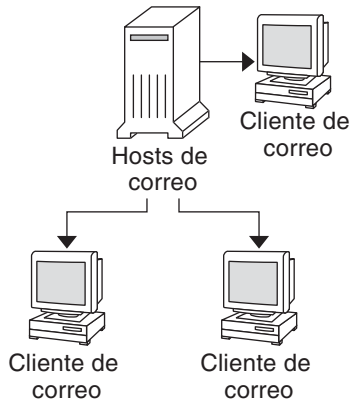
- Determine el tipo de configuración de correo que cumple sus requisitos. En esta sección, se describen dos tipos básicos de configuración de correo y se muestra brevemente lo que necesita para definir cada configuración. Si necesita configurar un nuevo sistema de correo o si desea ampliar uno existente, esta sección le resultará útil. [“Sólo correo local” en la página 291](#) describe el primer tipo de configuración y [“Correo local y una conexión remota” en la página 292](#) describe el segundo tipo.
- Según sea necesario, seleccione los sistemas que se utilizarán como servidores de correo, hosts de correo y puertas de enlace de correo.
- Realice una lista de todos los clientes de correo para los que prestará el servicio e incluya la ubicación de los buzones. Esta lista puede resultarle útil cuando esté listo para crear alias de correo para los usuarios.
- Decida cómo actualizar los alias y reenviar los mensajes de correo. Puede configurar un buzón de alias como un lugar para que los usuarios envíen solicitudes para el reenvío de correo. Los usuarios también pueden utilizar este buzón para enviar solicitudes para cambiar sus alias de correo predeterminados. Si el sistema utiliza NIS o NIS+, es posible administrar el reenvío de correo, en lugar de solicitar a los usuarios que gestionen el reenvío. [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313](#) proporciona una lista de las tareas relacionadas con la creación de alias. [“Administración de los archivos . forward \(mapa de tareas\)” en la página 328](#) proporciona una lista de las tareas relacionadas con la gestión de archivos . forward.

Una vez completado el proceso de planificación, configure los sistemas de su sitio para que realicen las funciones que se describen en [“Configuración de los servicios de correo \(mapa de tareas\)” en la página 294](#). Para obtener información sobre otras tareas, consulte [“Mapa de tareas para servicios de correo” en la página 289](#).

## Sólo correo local

La configuración de correo más sencilla, como se muestra en la [Figura 13–1](#), consta de dos o más estaciones de trabajo conectadas a un host de correo. El correo es completamente local. Todos los clientes almacenan el correo en sus discos locales. Los clientes actúan como servidores de correo. Las direcciones de correo se analizan mediante los archivos `/etc/mail/aliases`.

FIGURA 13-1 Configuración de correo local



Para configurar este tipo de configuración de correo, necesita lo siguiente:

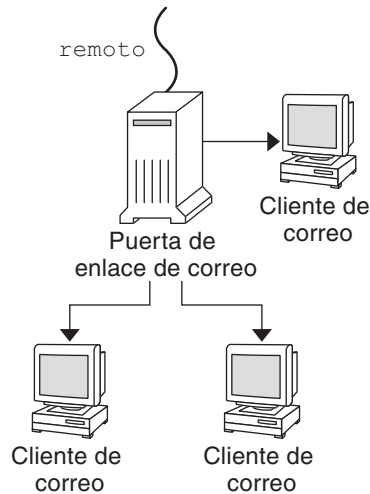
- El archivo `/etc/mail/sendmail.cf` predeterminado, que no necesita ninguna edición, en cada sistema del cliente de correo.
- Un servidor designado como host de correo. Si utiliza NIS o NIS+, puede agregar `mailhost.domain-name` al archivo `/etc/hosts` del host de correo para realizar esta designación. Si utiliza otro servicio de nombres, por ejemplo, DNS o LDAP, debe proporcionar información adicional en el archivo `/etc/hosts`. Consulte [“Cómo configurar un host de correo” en la página 298](#).
- Si utiliza un servicio de nombres diferente de NIS o NIS+, necesita archivos `/etc/mail/aliases` idénticos en todos los sistemas que tengan un buzón local.
- Espacio suficiente en `/var/mail`, en cada sistema del cliente de correo, para alojar los buzones.

Para obtener información sobre cómo configurar el servicio de correo, consulte [“Configuración de los servicios de correo” en la página 294](#). Si desea buscar un procedimiento específico relacionado con la configuración del servicio de correo, consulte [“Configuración de los servicios de correo \(mapa de tareas\)” en la página 294](#).

## Correo local y una conexión remota

La configuración de correo más común en una red pequeña se muestra en la [Figura 13-2](#). Un sistema incluye el servidor de correo, el host de correo y la puerta de enlace de correo que proporciona la conexión remota. El correo se distribuye mediante los archivos `/etc/mail/aliases` en la puerta de enlace de correo. No se necesita ningún nombre de servicios.

FIGURA 13-2 Configuración de correo local con una conexión UUCP



En esta configuración, puede asumir que los clientes de correo montan sus archivos de correo desde `/var/mail` en el host de correo. Para configurar este tipo de configuración de correo, necesita lo siguiente:

- El archivo `/etc/mail/sendmail.cf` predeterminado en cada sistema del cliente de correo. Este archivo no necesita ninguna edición.
- Un servidor designado como host de correo. Si utiliza NIS o NIS+, puede agregar `mailhost.domain-name` al archivo `/etc/hosts` del host de correo para realizar esta designación. Si utiliza otro servicio de nombres, por ejemplo, DNS o LDAP, debe proporcionar información adicional en el archivo `/etc/hosts`. Consulte [“Cómo configurar un host de correo” en la página 298](#).
- Si utiliza un servicio de nombres diferente de NIS o NIS+, necesita archivos `/etc/mail/aliases` idénticos en todos los sistemas que tengan un buzón local.
- Espacio suficiente en `/var/mail`, en el servidor de correo, para alojar los buzones del cliente.

Para obtener información sobre cómo configurar el servicio de correo, consulte [“Configuración de los servicios de correo” en la página 294](#). Si desea buscar un procedimiento específico relacionado con la configuración del servicio de correo, consulte [“Configuración de los servicios de correo \(mapa de tareas\)” en la página 294](#).

# Configuración de los servicios de correo (mapa de tareas)

La siguiente tabla describe los procedimientos para configurar servicios de correo.

Tarea	Descripción	Para obtener instrucciones
Configurar un servidor de correo	Pasos para permitir a un servidor enrutar correo.	<a href="#">“Cómo configurar un servidor de correo” en la página 295</a>
Configurar un cliente de correo	Pasos para permitir a un usuario recibir correo.	<a href="#">“Cómo configurar un cliente de correo” en la página 297</a>
Configurar un host de correo	Pasos para establecer un host de correo que pueda resolver direcciones de correo electrónico.	<a href="#">“Cómo configurar un host de correo” en la página 298</a>
Configurar una puerta de enlace de correo	Pasos para gestionar la comunicación con redes fuera del dominio.	<a href="#">“Cómo configurar una puerta de enlace de correo” en la página 300</a>
Usar DNS con sendmail	Pasos para habilitar las búsquedas de host DNS.	<a href="#">“Cómo usar DNS con sendmail” en la página 302</a>

## Configuración de los servicios de correo

Puede configurar fácilmente un servicio de correo si su sitio no proporciona conexiones con servicios de correo electrónico fuera de la compañía o si su compañía se encuentra en un único dominio.

El correo necesita dos tipos de configuraciones para el correo local. Consulte la [Figura 13–1 en “Sólo correo local” en la página 291](#) para ver una representación de estas configuraciones. El correo necesita dos configuraciones más para la comunicación con redes fuera del dominio. Consulte la [Figura 12–1 en “Descripción general de los componentes de hardware” en la página 286](#) o la [Figura 13–2 en “Correo local y una conexión remota” en la página 292](#) para ver una representación de estas configuraciones. Puede combinar estas configuraciones en el mismo sistema o proporcionar estas configuraciones en sistemas independientes. Por ejemplo, si las funciones de host de correo y servidor de correo se encuentran en el mismo sistema, siga las instrucciones de esta sección para configurar ese sistema como un host de correo. A continuación, siga las instrucciones de esta sección para configurar el mismo sistema como un servidor de correo.

**Nota** – Los siguientes procedimientos para configurar un servidor de correo y un cliente de correo se aplican cuando los buzones están montados en NFS. Sin embargo, los buzones normalmente se mantienen en directorios `/var/mail` montados de manera local, lo que elimina la necesidad de realizar los siguientes procedimientos.

## ▼ Cómo configurar un servidor de correo

No se necesitan pasos especiales para configurar un servidor de correo que sólo presta servicios de correo para los usuarios locales. El usuario debe tener una entrada en el archivo de contraseñas o en el espacio de nombres. Asimismo, para que se entregue el correo, el usuario debe tener un directorio principal local para comprobar el archivo `~/ .forward`. Por este motivo, los servidores del directorio principal a menudo se configuran como el servidor de correo. “[Componentes de hardware](#)” en la página 351 en el [Capítulo 14](#), “[Servicios de correo \(referencia\)](#)” proporciona más información acerca del servidor de correo.

El servidor de correo puede enrutar correo para muchos clientes de correo. Este tipo de servidor de correo debe tener un espacio adecuado para trabajos en cola para los buzones del cliente.

---

**Nota** – El programa `mail.local` crea automáticamente buzones en el directorio `/var/mail` la primera vez que se entrega un mensaje. No es necesario crear buzones individuales para los clientes de correo.

Para que los clientes accedan a sus buzones, el directorio `/var/mail` debe estar disponible para el montaje remoto. Asimismo, los servicios como Protocolo de oficina de correos (POP) o Protocolo de acceso a mensajes de Internet (IMAP) deben estar disponible en el servidor. La siguiente tarea muestra cómo configurar un servidor de correo mediante el directorio `/var/mail`. Proporcionar instrucciones de configuración para POP o IMAP está fuera del alcance de este documento.

---

Para la siguiente tarea, asegúrese de que el archivo `/etc/dfs/dfstab` muestre que el directorio `/var/mail` se exportó.

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Detenga `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

### 3 Compruebe si el directorio `/var/mail` está disponible para el acceso remoto.

```
# share
```

Si se muestra el directorio `/var/mail`, continúe con el paso 5.

Si no se muestra el directorio `/var/mail` o si no aparece ninguna lista, continúe con el paso secundario adecuado.

**a. (Opcional) Si no hay ninguna lista, inicie los servicios NFS.**

Siga el procedimiento “[Cómo configurar el uso compartido de sistema de archivos automático](#)” en la [página 87](#) para utilizar el directorio `/var/mail` para iniciar los servicios NFS.

**b. (Opcional) Si el directorio `/var/mail` no está incluido en la lista, agregue el directorio a `/etc/dfs/dfstab`.**

Agregue la siguiente línea de comandos al archivo `/etc/dfs/dfstab`.

```
share -F nfs -o rw /var/mail
```

**4 Permita que el sistema de archivos esté disponible para el montaje.**

```
# shareall
```

**5 Asegúrese de que se ha iniciado el servicio de nombres.**

**a. (Opcional) Si ejecuta NIS, utilice este comando.**

```
# ypwhich
```

Para obtener más información, consulte la página del comando `man ypwhich(1)`.

**b. (Opcional) Si ejecuta NIS+, utilice este comando.**

```
# nisl
```

Para obtener más información, consulte la página del comando `man nisl(1)`.

**c. (Opcional) Si ejecuta DNS, utilice este comando.**

```
# nslookup hostname
```

`nombre_host` Utilice el nombre del host.

Para obtener más información, consulte la página del comando `man nslookup(1M)`.

**d. (Opcional) Si ejecuta LDAP, utilice este comando.**

```
# ldaplist
```

Para obtener más información, consulte la página del comando `man ldaplist(1)`.

**6 Reinicie sendmail.**

```
# svcadm enable network/smtp:sendmail
```



## ▼ Cómo configurar un cliente de correo

Un cliente de correo es un usuario de servicios de correo con un buzón en un servidor de correo. Además, el cliente de correo tiene un alias de correo en el archivo `/etc/mail/aliases` que señala la ubicación del buzón.

---

**Nota** – También es posible realizar configurar un cliente de correo mediante un servicio como Protocolo de oficina de correos (POP) o Protocolo de acceso a mensajes de Internet (IMAP). Sin embargo, proporcionar instrucciones de configuración para POP o IMAP está fuera del alcance de este documento.

---

### 1 Debe convertirse en superusuario en el sistema del cliente de correo o asumir un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Detenga sendmail.

```
# svcadm disable -t network/smtp:sendmail
```

### 3 Asegúrese de que exista un punto de montaje `/var/mail` en el sistema del cliente de correo.

El punto de montaje se debe haber creado durante el proceso de instalación. Puede utilizar `ls` para asegurarse de que el sistema de archivos existe. El siguiente ejemplo muestra la respuesta que se recibe si el sistema de archivos no se ha creado.

```
# ls -l /var/mail
/var/mail not found
```

### 4 Asegúrese de que no haya ningún archivo en el directorio `/var/mail`.

Si existen archivos de correo en este directorio, debe moverlos para que no queden cubiertos cuando se monte el directorio `/var/mail` desde el servidor.

### 5 Monte el directorio `/var/mail` desde el servidor de correo.

Puede montar el directorio de correo automáticamente o en el inicio.

#### a. (Opcional) Monte `/var/mail` automáticamente.

Agregue una entrada como la siguiente en el archivo `/etc/auto_direct`.

```
/var/mail -rw,hard,actimeo=0 server:/var/mail
```

*servidor*      Utilice el nombre del servidor asignado.

**b. (Opcional) Monte /var/mail en el inicio.**

Agregue la siguiente entrada en el archivo `/etc/vfstab`. Esta entrada permite el directorio `/var/mail` en el servidor de correo especificado para montar el directorio `/var/mail` local.

```
server:/var/mail - /var/mail nfs - no rw,hard,actimeo=0
```

El buzón del cliente se monta automáticamente cada vez que se reinicia el sistema. Si no desea reiniciar el sistema, escriba el siguiente comando para montar el buzón del cliente.

```
# mountall
```



---

**Precaución** – Para que el acceso y el bloqueo del buzón funcionen correctamente, debe incluir la opción `actimeo=0` al montar correo desde un servidor NFS.

---

**6 Actualice /etc/hosts.**

Edite el archivo `/etc/hosts` y agregue una entrada para el servidor de correo. Este paso no es necesario si utiliza un servicio de nombres.

```
# cat /etc/hosts
#
# Internet host table
#
..
IP-address      mailhost mailhost mailhost.example.com
dirección_IP    Utilice las direcciones IP asignadas.
ejemplo.com     Utilice el dominio asignado.
host_correo     Utilice el host de correo asignado.
```

Para obtener más información, consulte la página del comando `man hosts(4)`.

**7 Agregue una entrada para el cliente en uno de los archivos de alias.**

Consulte “[Administración de los archivos de alias de correo \(mapa de tareas\)](#)” en la página 313 para ver un mapa de tareas acerca de la administración de archivos de alias de correo. Tenga en cuenta que el programa `mail.local` crea automáticamente buzones en el directorio `/var/mail` la primera vez se entrega un mensaje. No es necesario crear buzones individuales para los clientes de correo.

**8 Reinicie sendmail.**

```
# svcadm enable network/smtp:sendmail
```

## ▼ Cómo configurar un host de correo

Un host de correo resuelve las direcciones de correo electrónico y vuelve a enrutar el correo dentro del dominio. Un buen candidato para designar como host de correo es un sistema que

proporcione una conexión remota para la red o que conecte la red con un dominio principal. El siguiente procedimiento muestra cómo configurar un host de correo.

**1 Debe convertirse en superusuario en el sistema del host de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Detenga sendmail.**

```
# svcadm disable -t network/smtp:sendmail
```

**3 Verifique la configuración del nombre de host.**

Ejecute la secuencia de comandos `check-hostname` para verificar que `sendmail` pueda identificar el nombre de host completo para este servidor.

```
% /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

Si esta secuencia de comandos no puede identificar el nombre de host completo, debe agregar el nombre de host completo como el primer alias del host en `/etc/hosts`.

**4 Actualice el archivo `/etc/hosts`.**

Elija el paso adecuado para su caso.

**a. (Opcional) Si utiliza NIS o NIS+, edite el archivo `/etc/hosts` en el sistema que será el nuevo host de correo.**

Agregue la palabra `mailhost` y `mailhost.domain` después de la dirección IP y el nombre del sistema del host de correo.

```
IP-address mailhost mailhost mailhost.domain loghost
```

*dirección\_IP*      Utilice la dirección IP asignada.

*host\_correo*      Utilice el nombre del sistema del host de correo.

*dominio*          Utilice el nombre de dominio ampliado.

El sistema está designado ahora como host de correo. El valor de *dominio* debe ser idéntico a la cadena que se proporciona como nombre del subdominio en la salida del siguiente comando.

```
% /usr/lib/sendmail -bt -d0 </dev/null
Version 8.13.1+Sun
Compiled with: LDAPMAP MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7
               NAMED_BIND NDBM NETINET NETINET6 NETUNIX NEWDB NIS
               NISPLUS QUEUE SCANF SMTP USERDB XDEBUG
```

```
===== SYSTEM IDENTITY (after readcf) =====
(short domain name) $w = phoenix
```

```
(canonical domain name) $j = phoenix.example.com
(subdomain name) $m = example.com
(node name) $k = phoenix
```

=====

Observe el siguiente ejemplo de cómo se debería ver el archivo `hosts` después estos cambios.

```
# cat /etc/hosts
#
# Internet host table
#
172.31.255.255    localhost
192.168.255.255  phoenix mailhost mailhost.example.com loghost
```

**b. (Opcional) Si no utiliza NIS o NIS+, edite el archivo `/etc/hosts` en cada sistema de la red.**

Cree la siguiente entrada.

```
IP-address mailhost mailhost mailhost.domain loghost
```

**5 Reinicie sendmail.**

```
# svcadm enable network/smtp:sendmail
```

**6 Pruebe la configuración del correo.**

Consulte [“Cómo probar la configuración de correo” en la página 332](#) para obtener instrucciones.

---

**Nota** – Para obtener más información sobre los hosts de correo, consulte [“Componentes de hardware” en la página 351](#) en el [Capítulo 14, “Servicios de correo \(referencia\)”](#).

---

## ▼ **Cómo configurar una puerta de enlace de correo**

Una puerta de enlace de correo gestiona la comunicación con las redes fuera del dominio. La aplicación de correo de la puerta de enlace de envío puede coincidir con la aplicación de correo del sistema de recepción.

Un buen candidato para designar como una puerta de enlace de correo es un sistema que esté conectado con Ethernet y líneas telefónicas. Otro buen candidato sería un sistema que esté configurado como enrutador para Internet. Puede configurar el host de correo u otro sistema como puerta de enlace de correo. Puede elegir si desea configurar más de una puerta de enlace de correo para el dominio. Si tiene conexiones de programa de copia de UNIX a UNIX (UUCP), debe configurar el sistema (o los sistemas) con conexiones UUCP como puerta de enlace de correo.

**1 Debe convertirse en superusuario en la puerta de enlace de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Detenga sendmail.**

```
# svcadm disable -t network/smtp:sendmail
```

**3 Verifique la configuración del nombre de host.**

Ejecute la secuencia de comandos `check-hostname` para verificar que `sendmail` pueda identificar el nombre de host completo para este servidor.

```
# /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

Si esta secuencia de comandos no puede identificar el nombre de host completo, debe agregar el nombre de host completo como el primer alias del host en `/etc/hosts`. Si necesita ayuda con este paso, consulte el [Paso 4](#) de “[Cómo configurar un host de correo](#)” en la [página 298](#).

**4 Asegúrese de que se ha iniciado el servicio de nombres.****a. (Opcional) Si ejecuta NIS, utilice este comando.**

```
# ypwhich
```

Para obtener más información, consulte la página del comando `man ypwhich(1)`.

**b. (Opcional) Si ejecuta NIS+, utilice este comando.**

```
# nisl
```

Para obtener más información, consulte la página del comando `man nisl(1)`.

**c. (Opcional) Si ejecuta DNS, utilice este comando.**

```
# nslookup hostname
```

`nombre_host` Utilice el nombre del host.

Para obtener más información, consulte la página del comando `man nslookup(1M)`.

**d. (Opcional) Si ejecuta LDAP, utilice este comando.**

```
# ldaplist
```

Para obtener más información, consulte la página del comando `man ldaplist(1)`.

**5 Reinicie sendmail.**

```
# svcadm enable network/smtp:sendmail
```

## 6 Pruebe la configuración del correo.

Consulte [“Cómo probar la configuración de correo” en la página 332](#) para obtener instrucciones.

---

**Nota** – Para obtener más información sobre la puerta de enlace de correo, consulte [“Componentes de hardware” en la página 351](#) en el [Capítulo 14, “Servicios de correo \(referencia\)”](#).

---

## ▼ Cómo usar DNS con sendmail

El servicio de nombres DNS no admite alias para personas. Este servicio de nombres no admite alias para hosts o dominios que utilizan registros del agente de intercambio de correo (MX) y registros CNAME. Puede especificar nombres de host, nombres de dominio o ambos nombres en la base de datos DNS. Para obtener más información sobre sendmail y DNS, consulte [“Interacciones de sendmail con servicios de nombres” en la página 374](#) en el [Capítulo 14, “Servicios de correo \(referencia\)”](#) o consulte la *Guía de administración del sistema: Servicios de nombres y directorios (DNS, NIS y LDAP)*.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Habilite las búsquedas de host DNS (NIS+ solamente).

Edite el archivo `/etc/nsswitch.conf` y elimine `#` de la definición de `hosts` que incluye el indicador `dns`. La entrada de `host` debe incluir el indicador `dns`, como se muestra en el siguiente ejemplo, para que se utilicen los alias del host DNS.

```
# grep hosts /etc/nsswitch.conf
#hosts:      nisplus [NOTFOUND=return] files
hosts:      dns nisplus [NOTFOUND=return] files
```

### 3 Compruebe si existe una entrada para `mailhost` y `mailhost.domain`.

Utilice `nslookup` para asegurarse de que existe una entrada para `mailhost` y `mailhost.domain` en la base de datos DNS. Para obtener más información, consulte la página del comando `man nslookup(1M)`.

## Modificación de la configuración de sendmail (mapa de tareas)

Tarea	Descripción	Para obtener instrucciones
Generar un archivo de configuración de sendmail	Utilice este procedimiento para modificar el archivo <code>sendmail.cf</code> . Se incluye un ejemplo de cómo habilitar el enmascaramiento de dominios.	<a href="#">“Cómo generar un nuevo archivo <code>sendmail.cf</code>” en la página 304</a>
Configurar un host virtual	Pasos para configurar sendmail para aceptar correo de más de un dominio.	<a href="#">“Configuración de un host virtual” en la página 305</a>
Configurar la nueva generación automática del archivo de configuración de sendmail	Utilice este procedimiento para modificar el servicio sendmail de modo que los archivos de configuración <code>sendmail.cf</code> y <code>submit.mc</code> se vuelvan a generar de forma automática después de una actualización.	<a href="#">“Cómo volver a generar automáticamente un archivo de configuración” en la página 305</a>
Ejecutar sendmail en el modo abierto	Utilice este procedimiento para modificar las propiedades del servicio sendmail a fin de habilitar el modo abierto.	<a href="#">“Cómo usar sendmail en el modo abierto” en la página 306</a>
Configurar SMTP para que utilice Seguridad de la capa de transporte (TLS)	Utilice este procedimiento para permitir que SMTP tenga conexiones seguras con TLS.	<a href="#">“Cómo configurar SMTP para que utilice TLS” en la página 307</a>
Gestionar la entrega de correo con una configuración alternativa	Utilice este procedimiento para evitar los problemas en la entrega de correo que se pueden producir si el daemon maestro está deshabilitado.	<a href="#">“Cómo gestionar la entrega de correo mediante una configuración alternativa de <code>sendmail.cf</code>” en la página 312</a>

## Modificación de la configuración de sendmail

“[Cómo generar un nuevo archivo `sendmail.cf`” en la página 304](#) muestra cómo generar el archivo de configuración. Si bien aún puede utilizar las versiones anteriores de los archivos `sendmail.cf`, la práctica recomendada es utilizar el nuevo formato.

Para obtener más detalles, consulte el siguiente material:

- `/etc/mail/cf/README` proporciona una descripción completa del proceso de configuración.
- <http://www.sendmail.org> proporciona información en línea sobre la configuración de sendmail.

- “Versiones del archivo de configuración” en la página 342 y “Archivo de configuración de sendmail” en la página 365, en el Capítulo 14, “Servicios de correo (referencia)”, proporcionan instrucciones.
- “Macros de configuración m4 revisadas y adicionales de la versión 8.12 de sendmail” en la página 395 también es útil.

## ▼ Cómo generar un nuevo archivo `sendmail.cf`

El siguiente procedimiento muestra cómo generar un nuevo archivo de configuración.

---

**Nota** – `/usr/lib/mail/cf/main-v7sun.mc` ahora es `/etc/mail/cf/cf/sendmail.mc`.

---

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Detenga sendmail.

```
# svcadm disable -t network/smtp:sendmail
```

### 3 Realice una copia de los archivos de configuración que desea cambiar.

```
# cd /etc/mail/cf/cf
# cp sendmail.mc myhost.mc
```

`mi_host`      Seleccione un nuevo nombre para el archivo `.mc`.

### 4 Edite los nuevos archivos de configuración (por ejemplo, `myhost.mc`), según sea necesario.

Por ejemplo, agregue la siguiente línea de comandos para habilitar el enmascaramiento de dominios.

```
# cat myhost.mc
```

```
...
MASQUERADE_AS('host.domain')
```

`host.domain`      Utilice el nombre de host y el nombre de dominio deseados.

En este ejemplo, `MASQUERADE_AS` provoca que el correo enviado se etiquete como procedente de `host.domain`, en lugar de `$j`.

### 5 Genere el archivo de configuración con m4.

```
# /usr/ccs/bin/make myhost.cf
```

### 6 Pruebe el nuevo archivo de configuración y utilice la opción `-C` para especificar el nuevo archivo.

```
# /usr/lib/sendmail -C myhost.cf -v testaddr </dev/null
```



Cuando este comando muestra mensajes, envía un mensaje a `testaddr`. Sólo el correo saliente se puede probar sin reiniciar el servicio `sendmail` en el sistema. Para los sistemas que aún no gestionan correo, utilice el procedimiento de prueba completo detallado en “[Cómo probar la configuración de correo](#)” en la página 332.

## 7 Instale el nuevo archivo de configuración después de realizar una copia del original.

```
# cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.save
# cp myhost.cf /etc/mail/sendmail.cf
```

## 8 Reinicie el servicio `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

# Configuración de un host virtual

Si necesita asignar más de una dirección IP a un host, consulte el siguiente sitio web: <http://www.sendmail.org/tips/virtualHosting>. Este sitio brinda instrucciones completas acerca de cómo usar `sendmail` para configurar un host virtual. Sin embargo, en la sección “Configuración de `sendmail`”, no realice el paso 3b, como se muestra a continuación.

```
# cd sendmail-VERSION/cf/cf
# ./Build mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

En su lugar, para el sistema operativo Solaris, lleve a cabo los siguientes pasos.

```
# cd /etc/mail/cf/cf
# /usr/ccs/bin/make mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

`servidor_correo` Utilice el nombre del archivo `.cf`.

“[Modificación de la configuración de `sendmail`](#)” en la página 303 describe los mismos tres pasos como parte del proceso de generación.

Después de generar el archivo `/etc/mail/sendmail.cf`, puede continuar con los siguientes pasos para crear una tabla de usuario virtual.

## ▼ Cómo volver a generar automáticamente un archivo de configuración

Si generó su propia copia de `sendmail.cf` o `submit.cf`, el archivo de configuración no se reemplaza durante el proceso de actualización. El siguiente procedimiento muestra cómo configurar las propiedades del servicio `sendmail` para que el archivo `sendmail.cf` se vuelva a generar automáticamente. Para obtener instrucciones sobre cómo generar automáticamente el

archivo de configuración `submit.cf`, consulte el [Ejemplo 13–1](#). Puede combinar estos procedimientos si necesita generar ambos archivos.

**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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Configure las propiedades de sendmail.**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/path_to_sendmail_mc=/etc/mail/cf/cf/myhost.mc
svc:/network/smtp:sendmail> quit
```

**3 Actualice y reinicie el servicio sendmail.**

El primer comando inserta los cambios en la instantánea en ejecución. El segundo comando reinicia el servicio sendmail con las nuevas opciones.

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

### **Ejemplo 13–1** Cómo establecer la nueva generación automática de `submit.cf`

Este procedimiento configura el servicio sendmail de manera que el archivo de configuración `submit.mc` se vuelva a generar automáticamente.

```
# svccfg -s sendmail-client:default
svc:/network/smtp:sendmail> setprop config/path_to_submit_mc=/etc/mail/cf/cf/submit-myhost.mc
svc:/network/smtp:sendmail> exit
# svcadm refresh svc:/network/sendmail-client
# svcadm restart svc:/network/sendmail-client
```

## **▼ Cómo usar sendmail en el modo abierto**

En Solaris 10, el servicio sendmail se modificó para que se ejecute en modo sólo local de manera predeterminada. El modo sólo local significa que se acepta únicamente correo del host local. Se rechazan los mensajes de cualquier otro sistema. Las versiones anteriores estaban configuradas para aceptar correo entrante de todos los sistemas remotos, lo que se conoce como modo abierto. Para usar el modo abierto, utilice el siguiente procedimiento.



**Precaución** – La ejecución de sendmail en el modo sólo local es mucho más segura que la ejecución en el modo abierto. Asegúrese de que conoce los posibles riesgos de seguridad si sigue este procedimiento.

---

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Configure las propiedades de sendmail.**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/local_only = false
svc:/network/smtp:sendmail> quit
```

**3 Actualice y reinicie el servicio sendmail.**

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

**▼ Cómo configurar SMTP para que utilice TLS**

A partir de Solaris 10 1/06, SMTP puede utilizar Seguridad de la capa de transporte (TLS) en la versión 8.13 de sendmail. Este servicio ofrece a los servidores y clientes SMTP comunicaciones autenticadas y privadas a través de Internet, además de protección frente a ataques o escuchas no deseadas. Tenga en cuenta que este servicio no está habilitado de manera predeterminada.

El siguiente procedimiento utiliza datos de ejemplo para mostrar cómo configurar los certificados que permiten que sendmail utilice TLS. Para obtener más información, consulte [“Compatibilidad para ejecutar SMTP con TLS en la versión 8.13 de sendmail” en la página 380](#).

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Detenga sendmail.**

```
# svcadm disable -t network/smtp:sendmail
```

**3 Configure los certificados que permiten que sendmail utilice TLS.****a. Complete los siguientes pasos:**

```
# cd /etc/mail
# mkdir -p certs/CA
# cd certs/CA
# mkdir certs crt newcerts private
# echo "01" > serial
# cp /dev/null index.txt
# cp /etc/sfw/openssl/openssl.cnf .
```

b. Utilice el editor de texto que desee para cambiar el valor de `dir` en el archivo `openssl.cnf` de `/etc/sfw/openssl` a `/etc/mail/certs/CA`.

c. Utilice la herramienta de línea de comandos `openssl` para implementar TLS.

Tenga en cuenta que la siguiente línea de comandos genera texto interactivo.

```
# openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

<code>req</code>	Este comando crea y procesa solicitudes de certificado.
<code>-new</code>	Esta opción <code>req</code> genera una nueva solicitud de certificado.
<code>-x509</code>	Esta opción <code>req</code> crea un certificado autofirmado.
<code>-keyout private/cakey.pem</code>	Esta opción <code>req</code> permite asignar <code>private/cakey.pem</code> como nombre de archivo para la clave privada recién creada.
<code>-out cacert.pem</code>	Esta opción <code>req</code> permite asignar <code>cacert.pem</code> como archivo de salida.
<code>-days 365</code>	Esta opción <code>req</code> permite realizar un certificado por 365 días. El valor predeterminado es 30.
<code>-config openssl.cnf</code>	Esta opción <code>req</code> permite especificar <code>openssl.cnf</code> como archivo de configuración.

Tenga en cuenta que este comando requiere que proporcione lo siguiente:

- Country Name, como US.
- State or Province Name, como California.

- Locality Name, como Menlo Park.
- Organization Name, como Sun Microsystems.
- Organizational Unit Name, como Solaris.
- Common Name, que representa el nombre de host completo del equipo. Para obtener más información, consulte la página del comando `man check-hostname(1M)`.
- Email Address, como `someuser@example.com`.

**4 (Opcional) Si necesita una nueva conexión segura, realice un nuevo certificado y fírmelo con la autoridad de certificación.**

**a. Realice un nuevo certificado.**

```
# cd /etc/mail/certs/CA
# openssl req -nodes -new -x509 -keyout newreq.pem -out newreq.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

Este comando requiere que proporcione la misma información que indicó en el paso 3c.

Tenga en cuenta que, en este ejemplo, el certificado y la clave privada están en el archivo `newreq.pem`.

**b. Firme el nuevo certificado con la autoridad de certificación.**

```
# cd /etc/mail/certs/CA
# openssl x509 -x509toreq -in newreq.pem -signkey newreq.pem -out tmp.pem
Getting request Private Key
Generating certificate request
# openssl ca -config openssl.cnf -policy policy_anything -out newcert.pem -infiles tmp.pem
Using configuration from openssl.cnf
Enter pass phrase for /etc/mail/certs/CA/private/akey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
    Serial Number: 1 (0x1)
```

```
Validity
  Not Before: Jun 23 18:44:38 2005 GMT
  Not After : Jun 23 18:44:38 2006 GMT
Subject:
  countryName           = US
  stateOrProvinceName   = California
  localityName          = Menlo Park
  organizationName       = Sun Microsystems
  organizationalUnitName = Solaris
  commonName            = somehost.somedomain.example.com
  emailAddress           = someuser@example.com
X509v3 extensions:
  X509v3 Basic Constraints:
    CA:FALSE
  Netscape Comment:
    OpenSSL Generated Certificate
X509v3 Subject Key Identifier:
  93:D4:1F:C3:36:50:C5:97:D7:5E:01:E4:E3:4B:5D:0B:1F:96:9C:E2
X509v3 Authority Key Identifier:
  keyid:99:47:F7:17:CF:52:2A:74:A2:C0:13:38:20:6B:F1:B3:89:84:CC:68
  DirName:/C=US/ST=California/L=Menlo Park/O=Sun Microsystems/OU=Solaris/\
  CN=someuser@example.com/emailAddress=someuser@example.com
  serial:00
```

Certificate is to be certified until Jun 23 18:44:38 2006 GMT (365 days)

Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y

Write out database with 1 new entries

Data Base Updated

```
# rm -f tmp.pem
```

En este ejemplo, el archivo `newreq.pem` contiene la clave privada y el certificado sin firmar. El archivo `newcert.pem` contiene el certificado firmado.

utilidad `x509`      Muestra información de certificados, convierte certificados a diversos formatos y firma solicitudes de certificado.

aplicación `ca`      Se utiliza para firmar solicitudes de certificado en una variedad de formatos y para generar CRL (listas de revocación de certificados).

## 5 Agregue las siguientes líneas al archivo `.mc` para permitir que `sendmail` utilice los certificados.

```
define('confCACERT_PATH', '/etc/mail/certs')dnl
define('confCACERT', '/etc/mail/certs/CAcert.pem')dnl
define('confSERVER_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confSERVER_KEY', '/etc/mail/certs/MYkey.pem')dnl
define('confCLIENT_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confCLIENT_KEY', '/etc/mail/certs/MYkey.pem')dnl
```

Para obtener más información, consulte [“Opciones de archivo de configuración para ejecutar SMTP con TLS” en la página 381](#).

**6 Vuelva a generar e instale el archivo `sendmail.cf` en el directorio `/etc/mail`.**

Para obtener instrucciones detalladas, consulte “[Modificación de la configuración de sendmail](#)” en la [página 303](#).

**7 Cree enlaces simbólicos de los archivos que creó con `openssl` a los archivos que definió en el archivo `.mc`.**

```
# cd /etc/mail/certs
# ln -s CA/cacert.pem CAcert.pem
# ln -s CA/newcert.pem MYcert.pem
# ln -s CA/newreq.pem MYkey.pem
```

**8 Para mayor seguridad, debe denegar el permiso de lectura en el grupo y otros para `MYkey.pem`.**

```
# chmod go-r MYkey.pem
```

**9 Utilice un enlace simbólico para instalar los certificados de la autoridad de certificación en el directorio asignado a `confCACERT_PATH`.**

```
# C=CAcert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

**10 Para el correo seguro con otros hosts, instale sus certificados de host.****a. Copie el archivo definido por la opción `confCACERT` del otro host en `/etc/mail/certs/host.domain.cert.pem`.**

Reemplace *host.domain* con el nombre completo del otro host.

**b. Utilice un enlace simbólico para instalar los certificados de la autoridad de certificación en el directorio asignado a `confCACERT_PATH`.**

```
# C=host.domain.cert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

Reemplace *host.domain* con el nombre completo del otro host.

**11 Reinicie `sendmail`.**

```
# svcadm enable network/smtp:sendmail
```

**Ejemplo 13-2 Encabezado de correo Received :**

El siguiente es un ejemplo de un encabezado Received : para correo seguro con TLS.

```
Received: from his.example.com ([IPv6:2001:db8:3c4d:15::1a2f:1a2b])
    by her.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNUB8i242496
    (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
    for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:11 -0800 (PST)
Received: from her.example.com (her.city.example.com [192.168.0.0])
    by his.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNU7cl571102
    version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
```

```
for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:07 -0800 (PST)
```

Tenga en cuenta que el valor de `verify` es OK, lo que significa que la autenticación se realizó correctamente. Para obtener más información, consulte [“Macros para ejecutar SMTP con TLS” en la página 383](#).

**Véase también** Las siguientes páginas del comando `man` de OpenSSL:

- `openssl(1)` (<http://www.openssl.org/docs/apps/openssl.html>).
- `req(1)` (<http://www.openssl.org/docs/apps/req.html>).
- `x509(1)` (<http://www.openssl.org/docs/apps/x509.html>).
- `ca(1)` (<http://www.openssl.org/docs/apps/ca.html>).

## ▼ Cómo gestionar la entrega de correo mediante una configuración alternativa de `sendmail.cf`

Para facilitar el transporte del correo entrante y el correo saliente, la nueva configuración predeterminada de `sendmail` utiliza un daemon y un ejecutor de colas de cliente. El ejecutor de colas de cliente debe poder enviar correo al daemon en el puerto SMTP local. Si el daemon no recibe conexiones en el puerto SMTP, el correo permanece en la cola. Para evitar este problema, realice la siguiente tarea. Para obtener más información sobre el daemon y el ejecutor de colas de cliente, y para comprender por qué es posible que deba utilizar esta configuración alternativa, consulte [“Archivo de configuración `submit.cf` de la versión 8.12 de `sendmail`” en la página 389](#).

Este procedimiento garantiza que el daemon sólo se ejecute para aceptar conexiones del host local.

### 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 \(mapa de tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#).

### 2 Detenga el servicio cliente `sendmail`.

```
# svcadm disable -t sendmail-client
```

### 3 Realice una copia del archivo de configuración que desea cambiar.

```
# cd /etc/mail/cf/cf
# cp submit.mc submit-myhost.mc
```

*myhost*      Seleccione un nuevo nombre para el archivo `.mc`.



**4 Edite el nuevo archivo de configuración (por ejemplo, `submit-myhost.mc`).**

Cambie la dirección IP del host de recepción a la definición msp.

```
# grep msp submit-myhost.mc
FEATURE('msp', '[#.#.#]')dnl
```

**5 Genere el archivo de configuración con m4.**

```
# /usr/ccs/bin/make submit-myhost.cf
```

**6 Instale el nuevo archivo de configuración después de realizar una copia del original.**

```
# cp /etc/mail/submit.cf /etc/mail/submit.cf.save
# cp submit-myhost.cf /etc/mail/submit.cf
```

**7 Reinicie el servicio cliente sendmail.**

```
# svcadm enable sendmail-client
```

## Administración de los archivos de alias de correo (mapa de tareas)

La siguiente tabla describe los procedimientos para administrar archivos de alias de correo. Para obtener más información sobre este tema, consulte [“Archivos de alias de correo” en la página 367](#) en el [Capítulo 14, “Servicios de correo \(referencia\)”](#).

Tarea	Descripción	Para obtener instrucciones
Gestionar entradas de alias en una tabla NIS+ mail_aliases	Si el servicio de nombres es NIS+, utilice estos procedimientos para gestionar el contenido de la tabla mail_aliases.  Inicie una tabla NIS+ mail_aliases.	<a href="#">“Cómo iniciar una tabla NIS+ mail_aliases” en la página 315</a>
	Muestre el contenido de la tabla NIS+ mail_aliases.  Este procedimiento incluye ejemplos de cómo mostrar entradas individuales y cómo mostrar coincidencias parciales.	<a href="#">“Cómo mostrar el contenido de la tabla NIS+ mail_aliases” en la página 315</a>
	Agregue alias en la tabla NIS+ mail_aliases desde la línea de comandos.	<a href="#">“Cómo agregar alias en la tabla NIS+ mail_aliases desde la línea de comandos” en la página 316</a>
	Agregue entradas mediante la edición de una tabla NIS+ mail_aliases.	<a href="#">“Cómo agregar entradas mediante la edición de una tabla NIS+ mail_aliases” en la página 317</a>

Tarea	Descripción	Para obtener instrucciones
	Edite las entradas en una tabla NIS+ mail_aliases.  Este procedimiento incluye un ejemplo de cómo eliminar una entrada.	<a href="#">“Cómo editar entradas en una tabla NIS+ mail_aliases” en la página 318</a>
Configurar un mapa NIS mail_aliases	Si el servicio de nombres es NIS, siga estas instrucciones para crear alias con un mapa mail_aliases.	<a href="#">“Cómo configurar un mapa NIS mail_aliases” en la página 319</a>
Configurar un archivo de alias de correo local	Si no utiliza un servicio de nombres (como NIS o NIS+), siga estas instrucciones para crear alias con el archivo /etc/mail/aliases.	<a href="#">“Cómo configurar un archivo de alias correo local” en la página 320</a>
Crear un archivo de mapa con clave	Utilice estos pasos para crear alias con un archivo de mapa con clave.	<a href="#">“Cómo crear un archivo de mapa con clave” en la página 321</a>
Configurar el alias postmaster	Utilice los procedimientos de esta sección para gestionar el alias postmaster. Debe tener este alias.	<a href="#">“Gestión del alias postmaster” en la página 322</a>

## Administración de los archivos de alias de correo

Los alias de correo deben ser únicos dentro del dominio. En esta sección, se proporcionan los procedimientos para administrar archivos de alias de correo. Asimismo, puede utilizar la función de lista de correo de Solaris Management Console para realizar estas tareas en la base de datos de alias.

Además, puede crear archivos de base de datos para el host de correo local mediante makemap. Consulte la página del comando `man makemap(1M)`. El uso de estos archivos de base de datos no ofrece todas las ventajas que implica utilizar un servicio de nombres, como NIS o NIS+. Sin embargo, debería recuperar los datos de estos archivos de base de datos locales con mayor rapidez, ya que no hay búsquedas de red involucradas. Para obtener más información, consulte [“Interacciones de sendmail con servicios de nombres” en la página 374](#) y [“Archivos de alias de correo” en la página 367](#) en el Capítulo 14, “Servicios de correo (referencia)”.

Elija entre los siguientes procedimientos:

- [“Cómo iniciar una tabla NIS+ mail\\_aliases” en la página 315](#)
- [“Cómo mostrar el contenido de la tabla NIS+ mail\\_aliases” en la página 315](#)
- [“Cómo agregar alias en la tabla NIS+ mail\\_aliases desde la línea de comandos” en la página 316](#)
- [“Cómo agregar entradas mediante la edición de una tabla NIS+ mail\\_aliases” en la página 317](#)
- [“Cómo editar entradas en una tabla NIS+ mail\\_aliases” en la página 318](#)

- “Cómo configurar un mapa NIS `mail.aliases`” en la página 319
- “Cómo configurar un archivo de alias correo local” en la página 320
- “Cómo crear un archivo de mapa con clave” en la página 321

## ▼ Cómo iniciar una tabla NIS+ `mail_aliases`

Puede utilizar el comando `aliasadm` para gestionar entradas en una tabla NIS+. Para crear una tabla, siga estas instrucciones. Para obtener más información, consulte la página del comando `man aliasadm(1M)`.

- 1 **Debe ser miembro del grupo NIS+ que es propietario de la tabla, o bien convertirse en root en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Inicie una tabla NIS+.**

```
# aliasadm -I
```

- 3 **Agregue entradas en la tabla.**

- Para agregar dos o tres alias, consulte “[Cómo agregar alias en la tabla NIS+ `mail\_aliases` desde la línea de comandos](#)” en la página 316.
- Para agregar más de dos o tres alias, consulte “[Cómo agregar entradas mediante la edición de una tabla NIS+ `mail\_aliases`](#)” en la página 317.

## ▼ Cómo mostrar el contenido de la tabla NIS+ `mail_aliases`

Para ver una lista completa del contenido de la tabla, siga estas instrucciones.

- 1 **Debe ser miembro del grupo NIS+ que es propietario de la tabla, o bien convertirse en root en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 **Muestre todas las entradas en orden alfabético por alias.**

```
# aliasadm -l
```

Para obtener más información, consulte la página del comando `man aliasadm(1M)`.

**Ejemplo 13-3** Cómo mostrar una entrada individual en la tabla NIS+ mail\_aliases

Asimismo, puede utilizar el comando `aliasadm` para mostrar entradas individuales. Después de completar el primer paso de este procedimiento, escriba lo siguiente:

```
# aliasadm -m ignatz
ignatz: ignatz@saturn # Alias for Iggy Ignatz
```

El comando sólo busca coincidencias con el nombre de alias completo, no con cadenas parciales. No puede utilizar metacaracteres, como `*` y `?`, con `aliasadm -m`.

**Ejemplo 13-4** Cómo mostrar coincidencias parciales en la tabla NIS+ mail\_aliases

Además, puede utilizar el comando `aliasadm` para mostrar coincidencias parciales. Después de completar el primer paso de este procedimiento, escriba lo siguiente:

```
# aliasadm -l | grep partial-string
```

Reemplace *partial-string* por la cadena deseada para la búsqueda.

## ▼ Cómo agregar alias en la tabla NIS+ mail\_aliases desde la línea de comandos

Para agregar dos o tres alias en la tabla, siga las instrucciones indicadas a continuación. Si desea agregar más de dos o tres alias, consulte [“Cómo agregar entradas mediante la edición de una tabla NIS+ mail\\_aliases” en la página 317](#).

- 1 **Compile una lista de cada uno de los clientes de correo, las ubicaciones de los buzones y los nombres de los sistemas de servidores de correo.**
- 2 **Debe ser miembro del grupo NIS+ que es propietario de la tabla, o bien convertirse en root en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 3 **(Opcional) Si es necesario, inicie una tabla NIS+.**

Si desea crear una tabla NIS+ mail\_aliases completamente nueva, primero debe iniciar la tabla. Para completar esta tarea, consulte [“Cómo iniciar una tabla NIS+ mail\\_aliases” en la página 315](#).

- 4 **Agregue alias en la tabla.**

Observe este ejemplo de una entrada típica.

```
# aliasadm -a iggy iggy.ignatz@saturn "Iggy Ignatz"
```

La siguiente lista describe la entrada del ejemplo anterior.

-a	Opción para agregar un alias.
iggy	Forma abreviada del nombre de alias.
iggy.ignatz@saturn	Nombre de alias ampliado.
"Iggy Ignatz"	Nombre del alias entre comillas.

**5 Muestre la entrada que creó y asegúrese de que la entrada sea correcta.**

```
# aliasadm -m alias
```

*alias*      Entrada creada.

Para obtener más información, consulte la página del comando `man aliasadm(1M)`.

## ▼ Cómo agregar entradas mediante la edición de una tabla NIS+ `mail_aliases`

Puede utilizar el comando `aliasadm` para gestionar entradas en una tabla NIS+. Para agregar más de dos o tres alias en la tabla, siga estas instrucciones.

- 1 Compile una lista de cada uno de los clientes de correo, las ubicaciones de los buzones y los nombres de los sistemas de servidores de correo.**
- 2 Debe ser miembro del grupo NIS+ que es propietario de la tabla, o bien convertirse en root en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**3 Muestre y edite la tabla de alias.**

```
# aliasadm -e
```

Este comando muestra la tabla y permite editarla. El editor utilizado se estableció con la variable de entorno `$EDITOR`. Si no se estableció esta variable, `vi` es el editor predeterminado.

**4 Utilice el siguiente formato para escribir cada alias en una línea separada.**

```
alias: expanded-alias # ["option" # "comments"]
```

*alias*                      Esta columna es para la forma abreviada del nombre de alias.

*alias\_ampliado*          Esta columna es para el nombre de alias ampliado.

*opción*                    Esta columna está reservada para uso futuro.

*comentarios* Esta columna se utiliza para comentarios sobre el alias individual, como un nombre para el alias.

Si deja la columna de opción en blanco, escriba comillas vacías ("" ) y agregue los comentarios.

El orden de las entradas no es importante para la tabla NIS+ `mail_aliases`. El comando `aliasadm -l` clasifica la lista y muestra las entradas en orden alfabético.

Para obtener más información, consulte “Archivos de alias de correo” en la página 367 y la página del comando man `aliasadm(1M)`.

## ▼ **Cómo editar entradas en una tabla NIS+ `mail_aliases`**

Para editar entradas en la tabla, siga estas instrucciones.

- 1 Debe ser miembro del grupo NIS+ que es propietario de la tabla, o bien convertirse en root en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “Configuración de RBAC (mapa de tareas)” de *Guía de administración del sistema: servicios de seguridad*.

- 2 Muestre la entrada de alias.**

```
# aliasadm -m alias
```

Reemplace *alias* por el nombre de alias asignado.

- 3 Edite la entrada de alias, según sea necesario.**

```
# aliasadm -c alias expanded-alias [options comments]
```

*alias* Si es necesario, edite el nombre de alias.

*alias\_ampliado* Si es necesario, edite el nombre de alias ampliado.

*opciones* Si es necesario, edite la opción.

*comentarios* Si es necesario, edite el comentario para esta entrada.

Para obtener más información, consulte la página del comando man `aliasadm(1M)` y “Archivos de alias de correo” en la página 367.

- 4 Muestre la entrada que editó y asegúrese de que la entrada sea correcta.**

```
# aliasadm -m alias
```

Para obtener más información, consulte la página del comando man `aliasadm(1M)`.

**Ejemplo 13-5** Eliminación de entradas de una tabla NIS+ mail\_aliases

Para eliminar entradas de la tabla, utilice la siguiente sintaxis después de completar el primer paso de este procedimiento:

```
# aliasadm -d alias
```

Reemplace *alias* por el nombre de alias para la entrada que desea eliminar.

## ▼ Cómo configurar un mapa NIS mail\_aliases

Utilice el siguiente procedimiento para crear alias con un mapa NIS mail\_aliases.

- 1 **Compile una lista de cada uno de los clientes de correo, las ubicaciones de los buzones y los nombres de los sistemas de servidores de correo.**
- 2 **Debe convertirse en root en el servidor maestro NIS o asumir un rol equivalente.**  
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)
- 3 **Edita el archivo /etc/mail/aliases y realice las siguientes entradas.**

**a. Agregue una entrada para cada cliente de correo.**

```
# cat /etc/mail/aliases
```

```
..
alias: expanded-alias
```

*alias* Utilice el nombre de alias abreviado.

*alias\_ampliado* Utilice el nombre de alias ampliado (user@host.domain.com).

**b. Asegúrese de que tiene una entrada Postmaster: root.**

```
# cat /etc/mail/aliases
```

```
..
Postmaster: root
```

**c. Agregue un alias para root. Utilice la dirección de correo de la persona designada como postmaster.**

```
# cat /etc/mail/aliases
```

```
..
root: user@host.domain.com
```

*user@host.domain.com* Utilice la dirección asignada del postmaster designado.

- 4 **Asegúrese de que el servidor maestro NIS ejecute un servicio de nombres para resolver los nombres de host en cada servidor de correo.**

- 5 **Cambie al directorio `/var/yp`.**

```
# cd /var/yp
```

- 6 **Aplique el comando `make`.**

```
# make
```

Los cambios en los archivos `/etc/hosts` y `/etc/mail/aliases` se propagan a los sistemas esclavos NIS. Los cambios estarán activos en unos minutos, como máximo.

## ▼ **Cómo configurar un archivo de alias correo local**

Utilice el siguiente procedimiento para resolver alias con un archivo de alias de correo local.

- 1 **Compile una lista de cada uno de los usuarios y las ubicaciones de los buzones.**

- 2 **Debe convertirse en `root` en el servidor de correo o asumir un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

- 3 **Edite el archivo `/etc/mail/aliases` y realice las siguientes entradas.**

- a. **Agregue una entrada para cada usuario.**

```
user1: user2@host.domain
```

```
usuario 1
```

Utilice el nombre del nuevo alias.

```
usuario2@host.dominio
```

Utilice la dirección real del nuevo alias.

- b. **Asegúrese de que tiene una entrada `Postmaster: root`.**

```
# cat /etc/mail/aliases
```

```
..
```

```
Postmaster: root
```

- c. **Agregue un alias para `root`. Utilice la dirección de correo de la persona designada como `postmaster`.**

```
# cat /etc/mail/aliases
```

```
..
```

```
root: user@host.domain.com
```

```
usuario@host.dominio.com
```

Utilice la dirección asignada del postmaster designado.



#### 4 Vuelva a generar la base de datos de alias.

```
# newaliases
```

La configuración de la opción `AliasFile` en `/etc/mail/sendmail.cf` determina si este comando genera en formato binario el archivo individual, `/etc/mail/aliases.db`, o el par de archivos, `/etc/mail/aliases.dir` y `/etc/mail/aliases.pag`.

#### 5 Realice uno de los siguientes pasos para copiar los archivos generados.

##### a. (Opcional) Copie los archivos `/etc/mail/aliases`, `/etc/mail/aliases.dir` y `/etc/mail/aliases.pag` en cada uno de los otros sistemas.

Puede copiar los tres archivos mediante los comandos `rcp` o `rdist`. Consulte la página del comando `man rcp(1)` o la página del comando `man rdist(1)` para obtener más información. También puede crear una secuencia de comandos para realizar esta tarea.

Al copiar estos archivos, no será necesario ejecutar el comando `newaliases` en cada de los otros sistemas. Sin embargo, recuerde que debe actualizar todos los archivos `/etc/mail/aliases` cada vez que agregue o elimine un cliente de correo.

##### b. (Opcional) Copie los archivos `/etc/mail/aliases` y `/etc/mail/aliases.db` en cada uno de los otros sistemas.

Puede copiar estos archivos mediante los comandos `rcp` o `rdist`. Consulte la página del comando `man rcp(1)` o la página del comando `man rdist(1)` para obtener más información. También puede crear una secuencia de comandos para realizar esta tarea.

Al copiar estos archivos, no será necesario ejecutar el comando `newaliases` en cada de los otros sistemas. Sin embargo, recuerde que debe actualizar todos los archivos `/etc/mail/aliases` cada vez que agregue o elimine un cliente de correo.

## ▼ Cómo crear un archivo de mapa con clave

Para crear un archivo de mapa con clave, siga estas instrucciones.

#### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

#### 2 Cree un archivo de entrada.

Las entradas pueden tener la siguiente sintaxis.

```
old-name@newdomain.com    new-name@newdomain.com
old-name@olddomain.com    error:nouser No such user here
@olddomain.com            %1@newdomain.com
```

<i>nombre_anterior@dominionnuevo.com</i>	Utilice el nombre de usuario que se asignó anteriormente con el dominio que recién se asignó.
<i>nombre_nuevo@dominionnuevo.com</i>	Utilice la dirección que recién se asignó.
<i>nombre_anterior@dominioanterior.com</i>	Utilice el nombre de usuario que se asignó anteriormente con el dominio que se asignó anteriormente.
<i>dominioanterior.com</i>	Utilice el dominio que se asignó anteriormente.
<i>dominionnuevo.com</i>	Utilice el dominio que recién se asignó.

La primera entrada redirige el correo a un nuevo alias. La siguiente entrada crea un mensaje cuando se utiliza un alias incorrecto. La última entrada redirige todo el correo entrante de `olddomain` a `newdomain`.

### 3 Cree el archivo de base de datos.

```
# /usr/sbin/makemap maptype newmap < newmap
```

*tipo\_mapa*      Seleccione un tipo de base de datos, como `dbm`, `bt ree` o `hash`.

*mapa\_nuevo*      Utilice el nombre del archivo de entrada y la primera parte del nombre del archivo de base de datos. Si se selecciona el tipo de base de datos `dbm`, los archivos de base de datos se crean con un sufijo `.pag` y `.dir`. Para los otros dos tipos de base de datos, el nombre de archivo está seguido por `.db`.

## Gestión del alias postmaster

Todos los sistemas deben poder enviar correo al buzón de un postmaster. Puede crear un alias NIS o NIS+ para postmaster, o puede crear el alias en cada archivo `/etc/mail/aliases` local. Consulte estos procedimientos.

- “Cómo crear un alias postmaster en cada archivo `/etc/mail/aliases` local” en la página 322
- “Cómo crear un buzón independiente para postmaster” en la página 323
- “Cómo agregar el buzón del postmaster a los alias en el archivo `/etc/mail/aliases`” en la página 324

### ▼ Cómo crear un alias postmaster en cada archivo `/etc/mail/aliases` local

Si desea crear el alias postmaster en cada archivo `/etc/mail/aliases` local, siga estas instrucciones.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Vea la entrada `/etc/mail/aliases`.**

```
# cat /etc/mail/aliases
# Following alias is required by the mail protocol, RFC 2821
# Set it to the address of a HUMAN who deals with this system's
# mail problems.
Postmaster: root
```

**3 Edite el archivo `/etc/mail/aliases` de cada sistema.**

Cambie `root` a la dirección de correo de la persona designada como `postmaster`.

```
Postmaster: mail-address
```

`dirección_correo` Utilice la dirección asignada de la persona designada como `postmaster`.

**4 (Opcional) Cree un buzón independiente para el `postmaster`.**

La creación de un buzón independiente para el `postmaster` permite mantener el correo del `postmaster` separado del correo personal. Si crea un buzón independiente, utilice la dirección del buzón en lugar de la dirección de correo personal del `postmaster` al editar los archivos `/etc/mail/aliases`. Para obtener detalles, consulte [“Cómo crear un buzón independiente para `postmaster`” en la página 323](#).

**▼ Cómo crear un buzón independiente para `postmaster`**

Si desea crear un buzón independiente para `postmaster`, siga estas instrucciones.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Cree una cuenta de usuario para la persona designada como `postmaster`. Coloque un asterisco (\*) en el campo de contraseña.**

Para obtener detalles sobre cómo agregar una cuenta de usuario, consulte [“Configuración de cuentas de usuario \(mapa de tareas\)” de Guía de administración del sistema: administración básica](#).

**3 Una vez entregado el correo, habilite el programa `mail` para que pueda leer y escribir en el nombre del buzón.**

```
# mail -f postmaster
```

*postmaster*      Utilice la dirección asignada.

▼ **Cómo agregar el buzón del postmaster a los alias en el archivo /etc/mail/aliases**

Si desea agregar el buzón de un postmaster a los alias en el archivo /etc/mail/aliases, siga estas instrucciones.

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)
- 2

**Agregue un alias para root. Utilice la dirección de correo de la persona designada como postmaster.**

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

*usuario@host.dominio.com*      Utilice la dirección asignada de la persona designada como postmaster.
- 3

**En el sistema local del postmaster, cree una entrada en el archivo /etc/mail/aliases que define el nombre del alias. sysadmin es un ejemplo. Además, incluya la ruta del buzón local.**

```
# cat /etc/mail/aliases
..
sysadmin: /usr/somewhere/somefile
```

*sysadmin*      Cree un nombre para un nuevo alias.

*/usr/somewhere/somefile*      Utilice la ruta del buzón local.
- 4

**Vuelva a generar la base de datos de alias.**

```
# newaliases
```

# Administración de los directorios de la cola (mapa de tareas)

En la siguiente tabla, se describen los procedimientos para administrar la cola de correo.

Tarea	Descripción	Para obtener instrucciones
Mostrar el contenido de la cola de correo, /var/spool/mqueue	Utilice este procedimiento para ver cuántos mensajes hay en la cola y con qué rapidez los mensajes se borran de la cola.	<a href="#">“Cómo mostrar el contenido de la cola de correo, /var/spool/mqueue” en la página 325</a>

Tarea	Descripción	Para obtener instrucciones
Forzar el procesamiento de la cola de correo, <code>/var/spool/mqueue</code>	Utilice este procedimiento para procesar los mensajes en un sistema que anteriormente no podía recibir mensajes.	<a href="#">“Cómo forzar el procesamiento de la cola de correo, <code>/var/spool/mqueue</code>” en la página 326</a>
Ejecutar un subconjunto de la cola de correo, <code>/var/spool/mqueue</code>	Utilice este procedimiento para forzar el procesamiento de una subcadena de una dirección, como un nombre de host. Además, utilice este procedimiento para forzar la salida de un mensaje específico de la cola.	<a href="#">“Cómo ejecutar un subconjunto de la cola de correo, <code>/var/spool/mqueue</code>” en la página 326</a>
Mover la cola de correo, <code>/var/spool/mqueue</code>	Utilice este procedimiento para mover la cola de correo.	<a href="#">“Cómo mover la cola de correo, <code>/var/spool/mqueue</code>” en la página 327</a>
Ejecutar la cola de correo antigua, <code>/var/spool/omqueue</code>	Utilice este procedimiento para ejecutar una cola de correo antigua.	<a href="#">“Cómo ejecutar la cola de correo antigua, <code>/var/spool/omqueue</code>” en la página 328</a>

## Administración de los directorios de la cola

En esta sección, se describen algunas tareas útiles para la administración de la cola. Para obtener información sobre la cola de clientes únicamente, consulte [“Archivo de configuración `submit.cf` de la versión 8.12 de `sendmail`” en la página 389](#). Para obtener información relacionada adicional, puede consultar [“Funciones de cola adicionales de la versión 8.12 de `sendmail`” en la página 401](#).

Consulte lo siguiente:

- [“Cómo mostrar el contenido de la cola de correo, `/var/spool/mqueue`” en la página 325](#)
- [“Cómo forzar el procesamiento de la cola de correo, `/var/spool/mqueue`” en la página 326](#)
- [“Cómo ejecutar un subconjunto de la cola de correo, `/var/spool/mqueue`” en la página 326](#)
- [“Cómo mover la cola de correo, `/var/spool/mqueue`” en la página 327](#)
- [“Cómo ejecutar la cola de correo antigua, `/var/spool/omqueue`” en la página 328](#)

### ▼ Cómo mostrar el contenido de la cola de correo, `/var/spool/mqueue`

- Conozca cuántos mensajes hay en la cola y con qué rapidez se borran de la cola.

Escriba lo siguiente:

```
# /usr/bin/mailq | more
```

Este comando proporciona la siguiente información.

- Los ID de la cola.

- El tamaño del mensaje.
- La fecha en la que el mensaje ingresó en la cola.
- El estado del mensaje.
- El remitente y los destinatarios.

Además, este comando ahora comprueba la existencia del atributo de autorización, `solaris.admin.mail.mailq`. Si la comprobación es correcta, se ejecuta el equivalente de especificar el indicador `-bp` con `sendmail`. Si falla la comprobación, se imprime un mensaje de error. De manera predeterminada, este atributo de autorización está habilitado para todos los usuarios. El atributo de autorización se puede deshabilitar modificando la entrada de usuario en `prof_attr`. Para obtener más información, consulte las páginas del comando `man` de `prof_attr(4)` y `mailq(1)`.

## ▼ **Cómo forzar el procesamiento de la cola de correo, `/var/spool/mqueue`**

Utilice este procedimiento, por ejemplo, para procesar los mensajes en un sistema que anteriormente no podía recibir mensajes.

### **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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### **2 Force el procesamiento de la cola y muestre el progreso de los trabajos a medida que se borra la cola.**

```
# /usr/lib/sendmail -q -v
```

## ▼ **Cómo ejecutar un subconjunto de la cola de correo, `/var/spool/mqueue`**

Utilice este procedimiento, por ejemplo, para forzar el procesamiento de una subcadena de una dirección, como un nombre de host. Además, utilice este procedimiento para forzar la salida de un mensaje específico de la cola.

### **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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### **2 Ejecute un subconjunto de la cola de correo en cualquier momento con `-qRcadena`.**

```
# /usr/lib/sendmail -qRstring
```

*cadena* Utilice el alias de un destinatario o una subcadena de *user@host.domain*, como un nombre de host.

Asimismo, puede ejecutar un subconjunto de la cola de correo con `-qInnnnn`.

```
# /usr/lib/sendmail -qInnnnn
```

*nnnnn* Utilice un ID de cola.

## ▼ Cómo mover la cola de correo, `/var/spool/mqueue`

Si desea mover la cola de correo, siga estas instrucciones.

### 1 Debe convertirse en root en el host de correo o asumir un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Finalice el daemon de sendmail.

```
# svcadm disable network/smtp:sendmail
```

Ahora sendmail ya no procesa el directorio de la cola.

### 3 Cambie al directorio `/var/spool`.

```
# cd /var/spool
```

### 4 Mueva el directorio `mqueue`, y todo su contenido al directorio `omqueue`. A continuación, cree un nuevo directorio vacío con el nombre `mqueue`.

```
# mv mqueue omqueue; mkdir mqueue
```

### 5 Defina los permisos del directorio en lectura/escritura/ejecución por propietario y lectura/ejecución por grupo. Además, establezca el propietario y el grupo en `daemon`.

```
# chmod 750 mqueue; chown root:bin mqueue
```

### 6 Inicie sendmail.

```
# svcadm enable network/smtp:sendmail
```

## ▼ Cómo ejecutar la cola de correo antigua, /var/spool/omqueue

Para ejecutar una cola de correo antigua, siga estas instrucciones.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**2 Ejecute la cola de correo antigua.**

```
# /usr/lib/sendmail -oQ/var/spool/omqueue -q
```

El indicador -oQ especifica un directorio de cola alternativo. El indicador -q indica la ejecución de todos los trabajos en la cola. Utilice el indicador -v si se muestra la salida detallada en la pantalla.

**3 Elimine el directorio vacío.**

```
# rmdir /var/spool/omqueue
```

## Administración de los archivos . forward (mapa de tareas)

En la siguiente tabla, se describen los procedimientos para administrar archivos . forward. Para obtener más información, consulte [“Archivos . forward” en la página 370 en el Capítulo 14, “Servicios de correo \(referencia\)”](#).

Tarea	Descripción	Para obtener instrucciones
Deshabilitación de los archivos . forward	Utilice este procedimiento si, por ejemplo, desea evitar el reenvío automatizado.	<a href="#">“Cómo deshabilitar los archivos . forward” en la página 329</a>
Cambio de la ruta de búsqueda de los archivos . forward	Utilice este procedimiento si, por ejemplo, desea mover todos los archivos . forward a un directorio común.	<a href="#">“Cómo cambiar la ruta de búsqueda de los archivos . forward” en la página 330</a>
Creación y relleno de /etc/shells	Utilice este procedimiento para permitir que los usuarios utilicen el archivo . forward para reenviar correo a un programa o a un archivo.	<a href="#">“Cómo crear y rellenar /etc/shells” en la página 330</a>



# Administración de los archivos . forward

Esta sección contiene varios procedimientos que están relacionadas con la administración de archivos . forward. Dado que los usuarios pueden editar estos archivos, los archivos pueden causar problemas. Para obtener más información, consulte [“Archivos . forward” en la página 370](#) en el [Capítulo 14, “Servicios de correo \(referencia\)”](#).

Consulte lo siguiente:

- [“Cómo deshabilitar los archivos . forward” en la página 329](#)
- [“Cómo cambiar la ruta de búsqueda de los archivos . forward” en la página 330](#)
- [“Cómo crear y rellenar /etc/shells” en la página 330](#)

## ▼ Cómo deshabilitar los archivos . forward

Este procedimiento, que impide el reenvío automatizado, deshabilita los archivos . forward de un host específico.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Realice una copia de /etc/mail/cf/domain/solaris-generic.m4 o del archivo m4 del dominio específico del sitio.

```
# cd /etc/mail/cf/domain
# cp solaris-generic.m4 mydomain.m4
```

*mydomain* Utilice el nombre de archivo que desee.

### 3 Agregue la siguiente línea al archivo que acaba de crear.

```
define('confFORWARD_PATH', '')dnl
```

Si ya existe un valor para confFORWARD\_PATH en el archivo m4, reemplace el valor por este valor nulo.

### 4 Genere e instale un nuevo archivo de configuración.

Si necesita ayuda con este paso, consulte [“Cómo generar un nuevo archivo sendmail.cf” en la página 304](#).

---

**Nota** – Al editar el archivo .mc, recuerde cambiar DOMAIN('solaris-generic') por DOMAIN('mydomain').

---

## ▼ Cómo cambiar la ruta de búsqueda de los archivos . forward

Si, por ejemplo, desea colocar todos los archivos . forward en un directorio común, siga estas instrucciones.

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Realice una copia de /etc/mail/cf/domain/solaris-generic.m4 o del archivo m4 del dominio específico del sitio.

```
# cd /etc/mail/cf/domain
# cp solaris-generic.m4 mydomain.m4
```

*mydomain*      Utilice el nombre de archivo que desee.

### 3 Agregue la siguiente línea al archivo que acaba de crear.

```
define('confFORWARD_PATH', '$/.forward:/var/forward/$u')dnl
```

Si ya existe un valor para confFORWARD\_PATH en el archivo m4, reemplace el valor por este nuevo valor.

### 4 Genere e instale un nuevo archivo de configuración.

Si necesita ayuda con este paso, consulte “[Cómo generar un nuevo archivo sendmail.cf](#)” en la [página 304](#).

---

**Nota** – Al editar el archivo .mc, recuerde cambiar DOMAIN('solaris-generic') por DOMAIN('mydomain').

---

## ▼ Cómo crear y rellenar /etc/shells

Este archivo no se incluye en la versión estándar. Debe agregar el archivo si desea permitir que los usuarios utilicen archivos . forward para reenviar correo a un programa o a un archivo. Puede crear el archivo manualmente mediante grep para identificar todos los shells incluidos en el archivo de contraseñas. A continuación, puede escribir los shells en el archivo. Sin embargo, el siguiente procedimiento, que emplea una secuencia de comandos que se puede descargar, resulta más fácil de utilizar.

### 1 Descargue la secuencia de comandos.

<http://www.sendmail.org/vendor/sun/gen-etc-shells.html>

**2 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**3 Para generar una lista de shells, ejecute la secuencia de comandos gen-etc-shells.**

```
# ./gen-etc-shells.sh > /tmp/shells
```

Esta secuencia de comandos utiliza el comando `getent` para recopilar los nombres de los shells que se incluyen en los orígenes de archivo de contraseñas enumerados en `/etc/nsswitch.conf`.

**4 Inspeccione y edite la lista de shells en /tmp/shells.**

Con el editor que desee, elimine los shells que no incluirá.

**5 Mueva el archivo a /etc/shells.**

```
# mv /tmp/shells /etc/shells
```

## Procedimientos y consejos para la resolución de problemas en servicios de correo (mapa de tareas)

En la siguiente tabla, se describen los procedimientos y consejos para la resolución de problemas en servicios de correo.

Tarea	Descripción	Para obtener instrucciones
Probar la configuración de correo	Pasos para probar los cambios en el archivo de configuración de <code>sendmail</code> .	<a href="#">“Cómo probar la configuración de correo” en la página 332</a>
Comprobar los alias de correo	Paso para confirmar que se puede o no se puede entregar correo a un destinatario específico.	<a href="#">“Cómo comprobar los alias de correo” en la página 333</a>
Probar los conjuntos de reglas	Pasos para comprobar la entrada y las devoluciones de los conjuntos de reglas de <code>sendmail</code> .	<a href="#">“Cómo probar los conjuntos de reglas de <code>sendmail</code>” en la página 333</a>
Verificar las conexiones con otros sistemas	Consejos para verificar las conexiones con otros sistemas.	<a href="#">“Cómo verificar las conexiones con otros sistemas” en la página 334</a>
Registrar mensajes con el programa <code>syslogd</code>	Consejos para recopilar información sobre mensajes de error.	<a href="#">“Registro de los mensajes de error” en la página 335</a>

Tarea	Descripción	Para obtener instrucciones
Comprobar otras fuentes de información de diagnóstico	Consejos para obtener información de diagnóstico de otras fuentes.	<a href="#">“Otras fuentes de información de diagnóstico de correo” en la página 336</a>

# Procedimientos y consejos para la resolución de problemas en servicios de correo

Esta sección proporciona algunos procedimientos y consejos que puede utilizar para resolver problemas con los servicios de correo.

## ▼ Cómo probar la configuración de correo

Para probar los cambios realizados en el archivo de configuración, siga estas instrucciones.

- 1 Reinicie sendmail en cualquier sistema que tenga un archivo de configuración revisado.**  
`# svcadm refresh network/smtp:sendmail`
- 2 Envíe mensajes de prueba desde cada sistema.**  
`# /usr/lib/sendmail -v names </dev/null`  
*nombres*      Especifique la dirección de correo electrónico de un destinatario.  
  
Este comando envía un mensaje nulo al destinatario especificado y muestra la actividad de mensajes en el monitor.
- 3 Envíese un correo a usted mismo o a otras personas en el sistema local. Para ello, escriba en el mensaje la dirección de un nombre de usuario común.**
- 4 (Opcional) Si está conectado a una red, envíe correo en tres direcciones a una persona de otro sistema.**
  - Del sistema principal a un sistema cliente
  - De un sistema cliente al sistema principal
  - De un sistema cliente a otro sistema cliente
- 5 (Opcional) Si tiene una puerta de enlace de correo, envíe correo del host de correo a otro dominio para garantizar que la aplicación de correo y el host de retransmisión estén configurados correctamente.**
- 6 (Opcional) Si configuró una conexión UUCP en la línea telefónica con otro host, envíe un correo a una persona de ese host. Pídale a esa persona que le envíe otro correo o que lo llame cuando reciba el mensaje.**

**7 Solicite a alguien que le envíe un correo a través de la conexión UUCP.**

El programa `sendmail` no puede detectar si se envía el mensaje porque transfiere el mensaje a UUCP para su entrega.

**8 Desde diferentes sistemas, envíe un mensaje a `postmaster` y asegúrese de que el mensaje se entregue al buzón del `postmaster`.**

## Cómo comprobar los alias de correo

El siguiente ejemplo muestra cómo verificar un alias.

```
% mconnect
connecting to host localhost (127.0.0.1), port 25
connection open
220 your.domain.com ESMTP Sendmail 8.13.6+Sun/8.13.6; Tue, 12 Sep 2004 13:34:13 -0800 (PST)
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
221 2.0.0 your.domain.com closing connection
%
```

En este ejemplo, el programa `mconnect` abrió una conexión con un servidor de correo en un host local y le permitió probar esa conexión. El programa se ejecuta de manera interactiva, para que pueda emitir varios comandos de diagnóstico. Para obtener una descripción completa, consulte la página del comando `man mconnect(1)`. La entrada, `expn sandy`, proporcionó la dirección ampliada, `sandy@phoenix.example.com`. Por lo tanto, ha verificado que es posible entregar correo cuando se usa el alias `sandy`.

Recuerde evitar bucles y bases de datos inconsistentes cuando se utilicen alias locales y de todo el dominio. Sea especialmente cuidadoso para evitar la creación de bucles de alias cuando mueva un usuario de un sistema a otro.

## ▼ Cómo probar los conjuntos de reglas de `sendmail`

Para comprobar la entrada y las devoluciones de los conjuntos de reglas de `sendmail`, siga estas instrucciones.

**1 Cambie al modo de prueba de direcciones.**

```
# /usr/lib/sendmail -bt
```

**2 Pruebe una dirección de correo.**

Proporcione los siguientes números y la siguiente dirección en el último indicador (`>`).

```
> 3,0 mail-sraddress
```

*dirección\_mail* Utilice la dirección de correo que desea probar.

### 3 Finalice la sesión.

Presione Control + D.

## Ejemplo 13–6 Salida del modo de prueba de direcciones

A continuación, se muestra un ejemplo de la salida del modo de prueba de direcciones.

```
% /usr/lib/sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 sandy@phoenix
canonify          input: sandy @ phoenix
Canonify2         input: sandy < @ phoenix >
Canonify2         returns: sandy < @ phoenix . example . com . >
canonify          returns: sandy < @ phoenix . example . com . >
parse            input: sandy < @ phoenix . example . com . >
Parse0           input: sandy < @ phoenix . example . com . >
Parse0           returns: sandy < @ phoenix . example . com . >
ParseLocal       input: sandy < @ phoenix . example . com . >
ParseLocal       returns: sandy < @ phoenix . example . com . >
Parse1           input: sandy < @ phoenix . example . com . >
MailerToTriple   input: < mailhost . phoenix . example . com >
                 sandy < @ phoenix . example . com . >
MailerToTriple   returns: $# relay @$ mailhost . phoenix . example . com
                 $: sandy < @ phoenix . example . com . >
Parse1           returns: $# relay @$ mailhost . phoenix . example . com
                 $: sandy < @ phoenix . example . com . >
parse            returns: $# relay @$ mailhost . phoenix . example . com
                 $: sandy < @ phoenix . example . com . >
```

## Cómo verificar las conexiones con otros sistemas

El programa `mconnect` abre una conexión con un servidor de correo en un host especificado y le permite probar esa conexión. El programa se ejecuta de manera interactiva, para que pueda emitir varios comandos de diagnóstico. Consulte la página del comando `man mconnect(1)` para obtener una descripción completa. El siguiente ejemplo verifica que se pueda entregar correo al nombre de usuario `sandy`.

```
% mconnect phoenix

connecting to host phoenix (172.31.255.255), port 25
connection open
220 phoenix.example.com ESMTP Sendmail 8.13.1+Sun/8.13.1; Sat, 4 Sep 2004 3:52:56 -0700
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
```

Si no puede utilizar `mconnect` para conectarse con un puerto SMTP, compruebe estas condiciones.

- ¿La carga del sistema es demasiado elevada?
- ¿El daemon de `sendmail` está en ejecución?
- ¿El sistema tiene el archivo `/etc/mail/sendmail.cf` adecuado?
- ¿Está activo el puerto 25, es decir, el puerto que utiliza `sendmail`?

## Registro de los mensajes de error

El servicio de correo registra la mayoría de los mensajes de error mediante el programa `syslogd`. De manera predeterminada, el programa `syslogd` envía estos mensajes a un sistema denominado `loghost`, que se especifica en el archivo `/etc/hosts`. Puede definir `loghost` para que almacene todos los registros de un dominio NIS completo. Si no se especifica ningún `loghost`, no se informan los mensajes de error de `syslogd`.

El archivo `/etc/syslog.conf` controla dónde reenvía los mensajes el programa `syslogd`. Puede cambiar la configuración predeterminada mediante la edición del archivo `/etc/syslog.conf`. Debe reiniciar el daemon `syslog` para que los cambios se vuelvan activos. Para recopilar información sobre el correo, puede agregar las siguientes selecciones en el archivo.

- `mail.alert`: mensajes acerca de las condiciones que deben solucionarse ahora.
- `mail.crit`: mensajes críticos.
- `mail.warning`: mensajes de advertencia.
- `mail.notice`: mensajes que no son errores, pero es posible que necesiten atención.
- `mail.info`: mensajes informativos.
- `mail.debug`: mensajes de depuración.

La siguiente entrada del archivo `/etc/syslog.conf` envía una copia de todos los mensajes críticos, informativos y de depuración a `/var/log/syslog`.

```
mail.crit;mail.info;mail.debug                /var/log/syslog
```

Cada línea del registro del sistema contiene una indicación de hora, el nombre del sistema que generó la línea y un mensaje. El archivo `syslog` puede registrar una gran cantidad de información.

El registro se organiza en una serie de niveles. En el nivel más bajo, sólo se registran las instancias poco usuales. En el nivel más alto, se registran incluso los eventos más triviales y de menor interés. Por convención, los niveles de registro por debajo de 10 se consideran "útiles". Los niveles de registro superiores a 10 se utilizan normalmente para la depuración. Consulte

“Personalización del registro de mensajes del sistema” de *Guía de administración del sistema: Administración avanzada* para obtener información sobre loghost y el programa syslogd.

## Otras fuentes de información de diagnóstico de correo

Para obtener otro tipo de información de diagnóstico, consulte las siguientes fuentes.

- Observe las líneas `Received` en el encabezado del mensaje. Estas líneas rastrean la ruta que usó el mensaje durante la retransmisión. Recuerde que debe tener en cuenta las diferencias de zona horaria.
- Observe los mensajes de MAILER-DAEMON. Estos mensajes normalmente informan problemas de entrega.
- Consulte el registro del sistema que muestra los problemas de entrega para su grupo de sistemas. El programa `sendmail` siempre guarda sus actividades en el registro del sistema. Es posible modificar el archivo `crontab` para que ejecute una secuencia de comandos de shell todas las noches. La secuencia de comandos busca mensajes `SYSERR` en el registro y envía por correo cualquier mensaje que encuentra al postmaster.
- Utilice el programa `mailstats` para probar los tipos de correo y determine la cantidad de mensajes entrantes y mensajes salientes.

## Resolución de los mensajes de error

En esta sección, se describe cómo puede resolver algunos mensajes de error relacionados con `sendmail`. También puede consultar <http://www.sendmail.org/faq>.

Los siguientes mensajes de error contienen dos o más de los siguientes tipos de información.

- **Causa:** lo que puede haber sucedido para provocar el mensaje.
- **Descripción:** lo que el usuario estaba haciendo cuando se produjo el mensaje de error.
- **Solución:** lo que puede hacer para corregir el problema o para continuar con su trabajo.

451 timeout waiting for input during *source*

**Causa:** Cuando `sendmail` realiza lecturas desde cualquier origen cuyo tiempo de espera puede agotarse, como una conexión SMTP, el programa define un temporizador en el valor de diferentes opciones `Timeout` antes de que comience la lectura. Si la lectura no se completa antes de que se agote el temporizador, aparece este mensaje y se detiene la lectura. Normalmente, esta situación se produce durante RCPT. El mensaje de correo se pone luego en la cola para su posterior entrega.



**Solución:** Si este mensaje aparece con frecuencia, aumente el valor de diferentes opciones Timeout en el archivo `/etc/mail/sendmail.cf`. Si el temporizador ya se definió en un número alto, busque problemas de hardware, por ejemplo, conexiones o cables de red deficientes.

#### 550 *nombre\_host*... Host unknown

**Causa:** Este mensaje de sendmail indica que el equipo host de destino, especificado por la parte de la dirección después del símbolo arroba (@), no se encontró durante la consulta del sistema de nombres de dominio (DNS).

**Solución:** Utilice el comando `nslookup` para verificar que el host de destino exista en ese dominio o en otros dominios, quizá con una ortografía ligeramente diferente. En caso contrario, póngase en contacto con el destinatario deseado y solicite una dirección adecuada.

#### 550 *nombre\_usuario*... User unknown

**Causa:** Este mensaje de sendmail indica que el destinatario deseado, especificado por la parte de la dirección antes del símbolo arroba (@), no se pudo encontrar en el equipo host de destino.

**Solución:** Compruebe la dirección de correo electrónico e inténtelo de nuevo, quizá con una ortografía ligeramente diferente. Si esta solución no funciona, póngase en contacto con el destinatario deseado y solicite una dirección adecuada.

#### 554 *nombre\_host*... Local configuration error

**Causa:** Este mensaje de sendmail normalmente indica que el host local está intentando enviar un correo a sí mismo.

**Solución:** Compruebe el valor de la macro `$j` en el archivo `/etc/mail/sendmail.cf` para asegurarse de que este valor sea un nombre de dominio completo.

**Descripción:** Cuando el sistema de envío proporciona su nombre de host al sistema de recepción en el comando SMTP HELO, el sistema de recepción compara su nombre con el nombre del remitente. Si estos nombres son idénticos, el sistema de recepción emite este mensaje de error y cierra la conexión. El nombre que se proporciona en el comando HELO representa el valor de la macro `$j`.

Para obtener información adicional, consulte <http://www.sendmail.org/faq/section4#4.5>.

#### config error: mail loops back to myself.

**Causa:** Este mensaje de error se produce si configura un registro MX y convierte al host *bar* en el agente de intercambio de correo del dominio *foo*. Sin embargo, no configura el host *bar* para que identifique que es el agente de intercambio de correo del dominio *foo*.

Además, otra posibilidad es que el sistema de envío y el sistema de recepción se identifiquen como el mismo dominio.

**Solución:** Para obtener instrucciones, consulte <http://www.sendmail.org/faq/section4#4.5>.

#### host name configuration error

**Descripción:** Éste es un mensaje antiguo de sendmail, que reemplazó a `refuse to talk to myself` y fue sustituido por el mensaje `Local configuration error`.

**Solución:** Siga las instrucciones que se proporcionaron para resolver este mensaje de error, `554 nombre_host... Local configuration error`.

#### user unknown

**Causa:** Cuando intenta enviar correo a un usuario, se muestra el error `Username... user unknown`. El usuario está en el mismo sistema.

**Solución:** Buque si hay un error tipográfico en la dirección de correo electrónico indicada. De lo contrario, es posible que el usuario tenga un alias para una dirección de correo electrónico inexistente en `/etc/mail/aliases` o en el archivo `.mailrc` del usuario. Compruebe también si hay caracteres en mayúscula en el nombre de usuario. Preferiblemente, las direcciones de correo electrónico no deben distinguir mayúsculas de minúsculas.

Para obtener información adicional, consulte <http://www.sendmail.org/faq/section4#4.17>.

## Servicios de correo (referencia)

---

El programa `sendmail` es un agente de transporte de correo. El programa utiliza un archivo de configuración para proporcionar alias y reenvío, enrutamiento automático a puertas de enlace de red y configuración flexible. El sistema operativo Solaris ofrece archivos de configuración estándar que la mayoría de los sitios pueden utilizar. El [Capítulo 12, “Servicios de correo \(descripción general\)”](#) proporciona una introducción a los componentes de servicios de correo y una descripción de una configuración típica de un servicio de correo. El [Capítulo 13, “Servicios de correo \(tareas\)”](#) explica cómo configurar y administrar un sistema de correo electrónico. En este capítulo, se ofrece información acerca de los siguientes temas.

- “La versión de Solaris de `sendmail`” en la página 340
- “Componentes de software y hardware de servicios de correo” en la página 343
- “Archivos y programas de servicio de correo” en la página 354
- “Direcciones de correo y enrutamiento de correo” en la página 373
- “Interacciones de `sendmail` con servicios de nombres” en la página 374
- “Cambios en la versión 8.13 de `sendmail`” en la página 379
- “Cambios de la versión 8.12 de `sendmail`” en la página 388

Para obtener información que no esté incluida en estos capítulos, consulte las siguientes páginas del comando `man`:

- `sendmail(1M)`
- `mail.local(1M)`
- `mailstats(1)`
- `makemap(1M)`
- `editmap(1M)`

# La versión de Solaris de sendmail

En esta sección, que incluye los siguientes temas, se describen algunas de las diferencias en la versión de Solaris de sendmail en comparación con la versión genérica de Berkeley.

- “Indicadores utilizados y no utilizados para compilar sendmail” en la página 340
- “MILTER, API de filtro de correo para sendmail” en la página 341
- “Comandos sendmail alternativos” en la página 342
- “Versiones del archivo de configuración” en la página 342

## Indicadores utilizados y no utilizados para compilar sendmail

A partir de la versión Solaris 10, los siguientes indicadores se utilizan para compilar sendmail. Si la configuración requiere otros indicadores, debe descargar el origen y volver a compilar el binario. Puede encontrar información sobre este proceso en <http://www.sendmail.org>.

TABLA 14-1 Indicadores generales de sendmail

Indicador	Descripción
SOLARIS=21000	Compatibilidad con la versión Solaris 10.
MILTER	Compatibilidad con la API de filtro de correo. En la versión 8.13 de sendmail, este indicador está habilitado de manera predeterminada. Consulte “MILTER, API de filtro de correo para sendmail” en la página 341.
NETINET6	Compatibilidad con IPv6. Este indicador se ha transferido de conf.h a Makefile.

TABLA 14-2 Mapas y tipos de base de datos

Indicador	Descripción
NDBM	Compatibilidad con bases de datos ndbm.
NEWDB	Compatibilidad con bases de datos Berkeley DB.
USERDB	Compatibilidad con la base de datos del usuario.
NIS	Compatibilidad con bases de datos nis.
NISPLUS	Compatibilidad con bases de datos nisplus.
LDAPMAP	Compatibilidad con mapas LDAP.
MAP_REGEX	Compatibilidad con mapas de expresiones regulares.

**TABLA 14-3** Indicadores del sistema operativo

Indicador	Descripción
SUN_EXTENSIONS	Compatibilidad con extensiones de que se incluyen en sun_compat.o.
SUN_INIT_DOMAIN	Para la compatibilidad de retroceso, se admite el uso de nombres de dominio NIS para completar el nombre de host local. Para obtener más información, busque información específica del proveedor en <a href="http://www.sendmail.org">http://www.sendmail.org</a> .
SUN_SIMPLIFIED_LDAP	Compatibilidad con la API de LDAP simplificada, que es específica para Sun. Para obtener más información, busque información específica del proveedor en <a href="http://www.sendmail.org">http://www.sendmail.org</a> .
VENDOR_DEFAULT=VENDOR_SUN	Selecciona a Sun como el proveedor predeterminado.

En la siguiente tabla, se muestran los indicadores genéricos que no se usan para compilar la versión de sendmail que se entrega con la versión Solaris 10.

**TABLA 14-4** Indicadores genéricos que no se utilizan en esta versión de sendmail

Indicador	Descripción
SASL	Autenticación sencilla y capa de seguridad (RFC 2554)
STARTTLS	Seguridad de nivel de transacción (RFC 2487)

Para ver una lista de los indicadores que se utilizan para compilar sendmail, utilice el siguiente comando.

```
% /usr/lib/sendmail -bt -d0.10 < /dev/null
```

**Nota** – El comando anterior no enumera los indicadores que son específicos para Sun.

## MILTER, API de filtro de correo para sendmail

MILTER, la API de filtro de correo de sendmail, permite que los programas de terceros accedan a los mensajes de correo a medida que se van procesando para filtrar la metainformación y el contenido. No tiene que crear el filtro ni configurar sendmail para utilizarla. Esta API está habilitada de manera predeterminada en la versión 8.13 de sendmail.

Para más información, consulte los siguientes sitios:

- <http://www.sendmail.org>
- <https://www.milter.org/>

## Comandos sendmail alternativos

La versión de Solaris no incluye todos los sinónimos de comandos que se proporcionan en la versión genérica de sendmail.org. Esta tabla incluye una lista completa de alias de comandos. La tabla también muestra si los comandos están incluidos en la versión de Solaris y cómo generar el mismo comportamiento mediante sendmail.

TABLA 14-5 Comandos sendmail alternativos

Nombre alternativo	En esta versión	Opciones con sendmail
hoststat	No	sendmail -bh
mailq	Sí	sendmail -bp
newaliases	Sí	sendmail -bi
purgestat	No	sendmail -bH
smtpd	No	sendmail -bd

## Versiones del archivo de configuración

A partir de la versión Solaris 10, sendmail incluye una opción de configuración que permite definir la versión del archivo sendmail.cf. Esta opción permite que los archivos de configuración más antiguos se utilicen con la versión actual de sendmail. Puede establecer el nivel de versión entre los valores 0 y 10. También puede definir el proveedor. Tanto Berkeley como Sun son una opción de proveedor válida. Si el nivel de versión está especificado, pero no hay ningún proveedor definido, Sun se utiliza como el valor predeterminado de proveedor. La siguiente tabla muestra algunas de las opciones válidas.

TABLA 14-6 Valores de versión para el archivo de configuración

Campo	Descripción
V7/Sun	Configuración que se utilizó para la versión 8.8 de sendmail.
V8/Sun	Configuración que se utilizó para la versión 8.9 de sendmail. Este valor fue incluido en la versión Solaris 8.
V9/Sun	Configuración que se utilizó para las versiones 8.10 y 8.11 de sendmail.

TABLA 14–6 Valores de versión para el archivo de configuración (Continuación)

Campo	Descripción
V10/Sun	Configuración que se utiliza para las versiones 8.12 y 8.13 de sendmail. La versión 8.12 es el valor predeterminado para la versión Solaris 9. A partir de la versión Solaris 10, la versión 8.13 se usa de forma predeterminada.

**Nota** – Se le pide que no utilice V1/Sun. Para obtener más información, consulte <http://www.sendmail.org/vendor/sun/differences.html#4>.

Para obtener información sobre las tareas, consulte “Modificación de la configuración de sendmail” en la página 303 en el Capítulo 13, “Servicios de correo (tareas)”.

## Componentes de software y hardware de servicios de correo

En esta sección, se describen los componentes de software y hardware de un sistema de correo.

- “Componentes de software” en la página 343
- “Componentes de hardware” en la página 351

### Componentes de software

Cada servicio de correo incluye, al menos, uno de los siguientes componentes de software.

- “Agente de usuario de correo” en la página 343
- “Agente de transferencia de correo” en la página 344
- “Agente de entrega local” en la página 344

En esta sección, también se describen estos componentes de software.

- “Servicios de envío de correo y sendmail” en la página 344
- “Direcciones de correo” en la página 346
- “Archivos de buzón” en la página 348
- “Alias de correo” en la página 350

### Agente de usuario de correo

El *agente de usuario de correo* es el programa que actúa como la interfaz entre el usuario y el agente de transferencia de correo. El programa sendmail es un agente de transferencia de correo. El sistema operativo Solaris proporciona los siguientes agentes de usuario de correo.

- /usr/bin/mail
- /usr/bin/mailx

- `/usr/dt/bin/dtmail`

## Agente de transferencia de correo

El *agente de transferencia de correo* es responsable del enrutamiento de mensajes de correo y de la resolución de direcciones de correo. Este agente también se conoce como agente de *transporte* de correo. El agente de transferencia para el sistema operativo Solaris es `sendmail`. El agente de transferencia realiza estas funciones.

- Acepta mensajes del agente de usuario de correo.
- Resuelve direcciones de destino.
- Selecciona un agente de entrega adecuado para entregar el correo.
- Recibe correo entrante de otros agentes de transferencia de correo.

## Agente de entrega local

Un *agente de entrega local* es un programa que implementa un protocolo de entrega de correo. Los siguientes agentes de entrega local se proporcionan con el sistema operativo Solaris.

- El agente de entrega local del UUCP, que utiliza `uux` para entregar el correo.
- El agente de entrega local, que es `mail.local` en la versión estándar de Solaris.

En la sección “Cambios de la versión 8.12 de `sendmail`” en la página 388, se proporciona información sobre estos temas relacionados.

- “Indicadores de agente de entrega adicionales de la versión 8.12 de `sendmail`” en la página 399
- “Ecuaciones adicionales para agentes de entrega de la versión 8.12 de `sendmail`” en la página 400

## Servicios de envío de correo y `sendmail`

*Aplicación de correo* es un término específico de `sendmail`. Una *aplicación de correo* es utilizada por `sendmail` para identificar una instancia específica de un agente de entrega local personalizado o de un agente de transferencia de correo personalizado. Debe especificar, al menos, una aplicación de correo en el archivo `sendmail.cf`. Para obtener información sobre las tareas, consulte “Modificación de la configuración de `sendmail`” en la página 303 en el Capítulo 13, “Servicios de correo (tareas)”. En esta sección, se proporciona una breve descripción de los dos tipos de servicios de envío de correo.

- “Servicios de envío de correo del protocolo simple de transferencia de correo (SMTP)” en la página 345
- “Servicios de envío de correo del programa de copia de UNIX a UNIX (UUCP)” en la página 345

Para obtener más información sobre los servicios de envío de correo, consulte <http://www.sendmail.org/m4/readme.html> o `/etc/mail/cf/README`.



## Servicios de envío de correo del protocolo simple de transferencia de correo (SMTP)

El SMTP es el protocolo de correo estándar que se utiliza en Internet. Este protocolo define estos servicios de envío de correo.

- smtp proporciona transferencias SMTP regulares a otros servidores.
- esmtp proporciona transferencias SMTP extendidas a otros servidores.
- smtp8 proporciona transferencias SMTP a otros servidores sin convertir datos de 8 bits a MIME.
- dsmtpp proporciona entrega a petición utilizando el indicador de aplicación de correo F=%. Consulte “Cambios en la declaración MAILER() de la versión 8.12 de sendmail” en la página 398 y “Indicadores de agente de entrega adicionales de la versión 8.12 de sendmail” en la página 399.

## Servicios de envío de correo del programa de copia de UNIX a UNIX (UUCP)

Si es posible, evite el uso del UUCP. Para obtener una explicación, consulte [http://www.sendmail.org/m4/uucp\\_mailers.html](http://www.sendmail.org/m4/uucp_mailers.html) o realice una búsqueda en /etc/mail/cf/README en esta cadena: USING UUCP MAILERS.

El UUCP define estos servicios de envío de correo.

- |          |   |
|----------|---|
| uucp-old | Los nombres en la clase \$=U se envían a uucp-old. uucp es el nombre obsoleto para esta aplicación de correo. La aplicación de correo uucp-old utiliza una dirección con signo de exclamación en los encabezados.   |
| uucp-new | Los nombres en la clase \$=Y se envían a uucp-new. Utilice esta aplicación de correo cuando sepa que la aplicación de correo del UUCP receptor puede administrar varios destinatarios en una transferencia. suucp es el nombre obsoleto para esta aplicación de correo. La aplicación de correo uucp-new también utiliza una dirección con signo de exclamación en los encabezados. |

Si MAILER(smtp) también se especifica en la configuración, se definen dos servicios de envío de correo más.

- |            |  |
|------------|--|
| uucp-dom   | Esta aplicación de correo utiliza direcciones de estilo de dominio y, básicamente, aplica las reglas de reescritura del SMTP.  |
| uucp-uudom | Los nombres en la clase \$=Z se envían a uucp-uudom. uucp-uudom y uucp-dom utilizan el mismo formato de dirección de encabezado, es decir, direcciones de estilo de dominio. |

**Nota** – Debido a que la aplicación de correo smtp modifica la aplicación de correo del UUCP, coloque siempre MAILER(smtp) antes de MAILER(uucp) en el archivo .mc.

## Direcciones de correo

La *dirección de correo* contiene el nombre del destinatario y el sistema al cual se entrega el mensaje de correo. Cuando administra un sistema de correo pequeño que no utiliza un servicio de nombres, el direccionamiento de correo es sencillo. Los nombres de inicio de sesión identifican de forma exclusiva a los usuarios. Sin embargo, si administra un sistema de correo que tiene más de un sistema con buzones o que tiene uno o más dominios, el direccionamiento resulta complejo. Puede resultar incluso más complejo si tiene una conexión de correo (u otro tipo) del UUCP a servidores que se encuentran fuera de la red. La información de las secciones siguientes puede ayudar a comprender las partes y complejidades de una dirección de correo.

- “Dominios y subdominios” en la página 346
- “Nombre de dominio de servicio de nombres y nombre de dominio de correo” en la página 347
- “Formato típico para direcciones de correo” en la página 347
- “Direcciones de correo independientes de ruta” en la página 348

## Dominios y subdominios

El direccionamiento de correo electrónico utiliza dominios. Un *dominio* es una estructura de directorios de nombres de direcciones de red. Un dominio puede tener uno o más *subdominios*. El dominio y los subdominios de una dirección se pueden comparar con la jerarquía de un sistema de archivos. Así como se considera que un subdirectorio está dentro del directorio que se encuentra sobre él, se considera que cada subdominio en una dirección de correo está dentro de la ubicación que se encuentra a su derecha.

En la siguiente tabla, se muestran algunos dominios de nivel superior.

TABLA 14-7 Dominios de nivel superior

Dominio	Descripción
com	Sitios comerciales
edu	Sitios educativos
gov	Instalaciones gubernamentales de los Estados Unidos
mil	Instalaciones militares de los Estados Unidos
net	Organizaciones de redes
org	Otras organizaciones sin fines de lucro

Los dominios no distinguen mayúsculas de minúsculas. Puede usar mayúsculas, minúsculas o ambos tipos en la parte del dominio de una dirección sin cometer ningún error.

## Nombre de dominio de servicio de nombres y nombre de dominio de correo

Cuando trabaja con nombres de dominio de servicio de nombres y nombres de dominio de correo, recuerde lo que se detalla a continuación.

- De manera predeterminada, el programa `sendmail` filtra el primer componente del nombre de dominio NIS o NIS+ para formar el nombre de dominio de correo. Por ejemplo, si un nombre de dominio NIS+ fuera `bldg5.example.com`, el nombre de dominio de correo sería `example.com`.
- Aunque las direcciones de dominio de correo no distinguen mayúsculas de minúsculas, el nombre de dominio NIS o NIS+ sí lo hace. Para obtener los mejores resultados, utilice caracteres en minúscula al configurar los nombres de dominio NIS o NIS+, y de correo.
- El nombre de dominio DNS y el nombre de dominio de correo deben ser idénticos.

Para obtener más información, consulte [“Interacciones de `sendmail` con servicios de nombres” en la página 374](#).

## Formato típico para direcciones de correo

Normalmente, una dirección de correo tiene el siguiente formato. Para obtener más información, consulte [“Direcciones de correo independientes de ruta” en la página 348](#).

*user@subdomain. ... .subdomain2.subdomain1.top-level-domain*

La parte de la dirección a la izquierda del signo @ es la dirección local. La dirección local puede contener lo siguiente.

- Información sobre el enrutamiento con otro transporte de correo (por ejemplo, `bob::vmsvax@gateway` o `smallberries%mill.uucp@gateway`)
- Un alias (por ejemplo, `iggy.ignatz`)

---

**Nota** – La aplicación de correo receptora es responsable de determinar qué significa la parte local de la dirección. Para obtener información sobre los servicios de envío de correo, consulte [“Servicios de envío de correo y `sendmail`” en la página 344](#).

---

La parte de la dirección a la derecha del signo @ muestra los niveles de dominios, que es donde la dirección local reside. Un punto separa cada subdominio. La parte del dominio de la dirección puede ser una organización, un área física o una región geográfica. Además, el orden de la información del dominio es jerárquica, de manera que cuanto más local sea el subdominio, más cerca estará el subdominio del signo @.

## Direcciones de correo independientes de ruta

Las direcciones de correo pueden ser independientes de ruta. El direccionamiento independiente de ruta requiere que el remitente de un mensaje de correo electrónico especifique el nombre del destinatario y el destino final. Una red de alta velocidad, como Internet, utiliza direcciones independientes de ruta. Las direcciones independientes de ruta pueden tener este formato.

*user@host.domain*

Las direcciones independientes de ruta para las conexiones del UUCP pueden tener este formato de dirección.

*host.domain!user*

La creciente popularidad del esquema de nomenclatura por jerarquía en dominio para los equipos está haciendo que las direcciones independientes de ruta sean más comunes. En realidad, la dirección independiente de ruta más común omite el nombre de host y se basa en el servicio de nombres del dominio para identificar correctamente el destino final del mensaje de correo electrónico.

*user@domain*

Las direcciones independientes de ruta se leen primero buscando el signo @. Luego, la jerarquía del dominio se lee de la derecha (el nivel superior) a la izquierda (la parte más específica de la dirección a la derecha del signo @).

## Archivos de buzón

Un *buzón* es un archivo que es el destino final para los mensajes de correo electrónico. El nombre del buzón puede ser el nombre de usuario o la identidad de una función específica, como el administrador de correo. Los buzones se encuentran en el archivo */var/mail/username*, que puede existir en el sistema local del usuario o en un servidor de correo remoto. En cualquier caso, el buzón está en el sistema al cual se envía el correo.

El correo siempre se debe entregar a un sistema de archivos local, de manera que el agente de usuario pueda extraer el correo de la cola de impresión de correo y almacenarlo en el buzón local. No utilice sistemas de archivos montados en NFS como destino para el buzón de un usuario. En concreto, no dirija el correo a un cliente de correo que está montando el sistema de archivos */var/mail* desde un servidor remoto. El correo para el usuario, en esta instancia, debe dirigirse al servidor de correo y no al nombre de host del cliente. Los sistemas de archivos montados en NFS pueden causar problemas con la entrega y la administración del correo.

El archivo */etc/mail/aliases* y los servicios de nombres, como NIS o NIS+, ofrecen mecanismos de creación de alias para direcciones de correo electrónico. Por lo tanto, los usuarios no necesitan saber el nombre local exacto del buzón de un usuario.

En la siguiente tabla, se muestran algunas convenciones comunes de nomenclatura para buzones con fines especiales.

**TABLA 14-8** Convenciones para el formato de nombres de buzón

Formato	Descripción
<i>username</i>	Los nombres de usuario son, con frecuencia, los mismos que los nombres de buzón.
<i>nombre.apellido</i> <i>nombre_apellido</i> <i>inicial_nombre.apellido</i> <i>inicial_nombre_apellido</i>	Los nombres de usuario pueden identificarse como nombres completos con un punto (o un subrayado) que separa el primer nombre y el apellido. Asimismo, los nombres de usuario pueden identificarse por una primera inicial con un punto (o un subrayado) que separa la inicial y el apellido.
<i>postmaster</i>	Los usuarios pueden dirigir preguntas e informar problemas con el sistema de correo al buzón <i>postmaster</i> . Cada sitio y dominio deben tener un buzón <i>postmaster</i> .
MAILER-DAEMON	<code>sendmail</code> enruta automáticamente cualquier correo que se dirige a MAILER-DAEMON para el administrador de correo.
<i>nombre_alias-request</i>	Los nombres que terminan en <i>-request</i> son direcciones administrativas para las listas de distribución. Esta dirección debe redirigir el correo a la persona que mantiene la lista de distribución.
<i>owner-nombre_alias</i>	Los nombres que comienzan con <i>owner-</i> son direcciones administrativas para las listas de distribución. Esta dirección debe redirigir el correo a la persona que maneja los errores de correos.
<i>owner-owner</i>	Este alias se utiliza cuando no hay ningún alias <i>owner-aliasname</i> para los errores que se van a devolver. Esta dirección debe redirigir el correo a la persona que maneja los errores de correos. Esta dirección también debe definirse en cualquier sistema que contiene un gran número de alias.
<i>local%dominio</i>	El signo de porcentaje (%) marca una dirección local que se expande cuando el mensaje llega al destino. La mayoría de los sistemas de correo interpretan los nombres de buzón con caracteres % como direcciones de correo completas. El % se sustituye por una @, y el correo se redirige en consecuencia. Aunque muchas personas utilizan la convención %, esta convención no es un estándar formal. Esta convención se conoce como “percent hack”. Esta función se suele utilizar para depurar problemas con el correo.

A partir de la versión 8 de `sendmail`, el remitente del sobre del correo que se envía a un alias de grupo se ha cambiado a la dirección que se expande desde el alias del propietario si existe un alias de propietario. Este cambio permite que los errores de correos se envíen al alias del propietario, en lugar de ser devueltos al remitente. Con este cambio, los usuarios notan que el correo que se envió a un alias parece como si el correo hubiera provenido del alias del propietario, cuando se entrega. El siguiente formato de alias ayuda con algunos de los problemas que están asociados con este cambio.

```
mygroup: :include:/pathname/mygroup.list
owner-mygroup: mygroup-request
mygroup-request: sandys, ignatz
```

En este ejemplo, el alias `mygroup` es el alias real del correo para el grupo. El alias `owner-mygroup` recibe mensajes de error. El alias `mygroup-request` se debe utilizar para las solicitudes administrativas. Esta estructura significa que, en el correo enviado al alias `mygroup`, el remitente del sobre cambia a `mygroup-request`.

## Alias de correo

Un *alias* es un nombre alternativo. Para el correo electrónico, puede utilizar alias para asignar la ubicación de un buzón o para definir listas de correo. Para obtener un mapa de tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313](#) en el [Capítulo 13, “Servicios de correo \(tareas\)”](#). También puede consultar [“Archivos de alias de correo” en la página 367](#) en este capítulo.

Para grandes sitios, el alias de correo define, normalmente, la ubicación de un buzón. Proporcionar un alias de correo es como proporcionar un número de habitación como parte de la dirección de un individuo en una corporación grande que ocupa varias habitaciones. Si no proporciona el número de habitación, el correo se entrega a una dirección central. Sin un número de habitación, se necesita un esfuerzo adicional para determinar a dónde, dentro del edificio, se va a entregar el correo. Por lo tanto, la posibilidad de errores aumenta. Por ejemplo, si dos personas que tienen el nombre Kevin Smith están en el mismo edificio, sólo una de ellas podría recibir el correo. Para corregir el problema, cada Kevin Smith debe tener un número de habitación agregado a su dirección.

Use dominios y direcciones independientes de ubicación lo más posible al crear listas de correo. Para mejorar la portabilidad y flexibilidad de los archivos de alias, haga las entradas de alias en las listas de correo lo más genéricas e independientes del sistema que sea posible. Por ejemplo, si tiene un usuario denominado `ignatz` en el sistema `mars`, en el dominio `example.com`, cree el alias `ignatz@example` en lugar de `ignatz@mars`. Si el usuario `ignatz` cambia el nombre de su sistema, pero permanece en el dominio `example`, no es necesario actualizar los archivos de alias para reflejar el cambio en el nombre del sistema.

Al crear entradas de alias, escriba un alias por línea. Sólo debe tener una entrada que contiene el nombre del sistema del usuario. Por ejemplo, puede crear las siguientes entradas para el usuario `ignatz`.

```
ignatz: iggy.ignatz
iggyi: iggy.ignatz
iggy.ignatz: ignatz@mars
```

Puede crear un alias para los dominios o nombres locales. Por ejemplo, una entrada de alias para el usuario `fred`, que tiene un buzón en el sistema `mars` y está en el dominio `planets`, puede tener esta entrada en la tabla de alias `NIS+`.

```
fred: fred@planets
```

Al crear las listas de correo que incluyen usuarios fuera de su dominio, cree el alias con el nombre de usuario y el nombre de dominio. Por ejemplo, si tiene un usuario denominado

smallberries en el sistema `privet`, en el dominio `example.com`, cree el alias como `smallberries@example.com`. La dirección de correo electrónico del remitente se traduce automáticamente a un nombre de dominio completo cuando el correo sale del dominio del usuario.

En la siguiente lista, se describen los métodos para crear y administrar archivos de alias de correo.

- Puede crear alias de correo para uso global en la tabla `mail_aliases` NIS+, el mapa `aliases` NIS o los archivos `/etc/mail/aliases` locales. También puede crear y administrar listas de correo que utilizan los mismos archivos de alias.
- En función de la configuración de los servicios de correo, puede administrar alias mediante el servicio de nombres NIS o NIS+ para mantener una base de datos `aliases` global. De lo contrario, puede actualizar todos los archivos `/etc/mail/aliases` locales para mantener los alias sincronizados.
- Los usuarios también pueden crear y utilizar alias. Los usuarios pueden crear alias en el archivo `~/mailrc` local, que sólo el usuario puede utilizar, o en el archivo `/etc/mail/aliases` local, que cualquier usuario puede utilizar. Por lo general, los usuarios no pueden crear ni administrar archivos de alias NIS ni NIS+.

## Componentes de hardware

Puede proporcionar los tres elementos necesarios de configuración de correo en el mismo sistema o hacer que sistemas independientes proporcionen estos elementos.

- “Host de correo” en la página 351
- “Servidor de correo” en la página 352
- “Cliente de correo” en la página 353

Cuando los usuarios se van a comunicar con redes que se encuentran fuera de su dominio, también debe agregar un cuarto elemento: una puerta de enlace del correo. Para obtener más información, consulte “Puerta de enlace del correo” en la página 353. En las siguientes secciones, se describe cada componente de hardware.

### Host de correo

Un *host de correo* es el equipo que designa como el equipo de correo principal en la red. Un host de correo es el equipo al cual otros sistemas en el sitio reenvían el correo que no se puede entregar. Designe un sistema como host de correo en la base de datos `hosts` agregando la palabra `mailhost` a la derecha de la dirección IP en el archivo `/etc/hosts` local. También puede agregar la palabra `mailhost` de forma similar al archivo de `hosts` en el servicio de nombres. Para obtener información detallada sobre las tareas, consulte “Cómo configurar un host de correo” en la página 298 en el Capítulo 13, “Servicios de correo (tareas)”.

Un buen candidato para un host de correo es un sistema que está configurado como enrutador desde su red hasta la red global de Internet. Para obtener más información, consulte el [Capítulo 15, “Solaris PPP 4.0 \(descripción general\)”](#), el [Capítulo 24, “UUCP \(descripción general\)”](#) y la sección [“Configuración de un enrutador IPv4” de Guía de administración del sistema: servicios IP](#). Si ningún sistema de la red local tiene un módem, designe un sistema como el host de correo.

Algunos sitios utilizan equipos independientes que no están en red en una configuración de tiempo compartido. En concreto, el equipo independiente atiende a los terminales, que están adjuntos a sus puertos de serie. Puede configurar el correo electrónico para esta configuración designando el sistema autónomo como el host de correo de una red de único sistema. En la sección [“Descripción general de los componentes de hardware” en la página 286 del Capítulo 12, “Servicios de correo \(descripción general\)”](#), se incluye una figura que muestra una configuración típica de correo electrónico.

## Servidor de correo

Un *buzón* es un único archivo que contiene el correo electrónico de un usuario concreto. El correo se entrega al sistema donde reside el buzón del usuario, que puede estar en un equipo local o un servidor remoto. Un *servidor de correo* es cualquier sistema que contiene buzones de usuarios en el directorio `/var/mail`. Para obtener información sobre las tareas, consulte [“Cómo configurar un servidor de correo” en la página 295 en el Capítulo 13, “Servicios de correo \(tareas\)”](#).

El servidor de correo enruta todo el correo de un cliente. Cuando un cliente envía correo, el servidor de correo coloca el correo en una cola para la entrega. Una vez que el correo se encuentra en la cola, un usuario puede reiniciar o desactivar el cliente sin perder esos mensajes de correo. Cuando el destinatario recibe correo desde un cliente, la ruta en la línea `From` del mensaje contiene el nombre del servidor de correo. Si el destinatario responde, la respuesta va al buzón del usuario. Buenos candidatos para servidores de correo son los sistemas que proporcionan un directorio principal para los usuarios o sistemas a los que se les realiza copia de seguridad con regularidad.

Si el servidor de correo no es el sistema local del usuario, los usuarios que cuentan con configuraciones que utilizan el software NFS pueden montar el directorio `/var/mail` utilizando el archivo `/etc/vfstab` si tienen acceso a `root`. De lo contrario, los usuarios pueden utilizar el montador automático. Si la compatibilidad con NFS no está disponible, los usuarios pueden iniciar sesión en el servidor para leer el correo.

Si los usuarios de la red envían otros tipos de correo, como archivos de audio o archivos de sistemas de creación de publicaciones, necesita asignar más espacio en el servidor de correo para los buzones.

Al establecer un servidor de correo para todos los buzones, puede simplificar el proceso de copias de seguridad. Las copias de seguridad pueden resultar difíciles cuando el correo se distribuye en varios sistemas. La desventaja de almacenar muchos buzones en un servidor es



que el servidor puede ser un único punto de fallo para muchos usuarios. Sin embargo, las ventajas de proporcionar buenas copias de seguridad, por lo general, hacen que el riesgo valga la pena.

## Cliente de correo

Un cliente de correo es un usuario de servicios de correo con un buzón en un servidor de correo. Además, el cliente de correo tiene un alias de correo en el archivo `/etc/mail/aliases` que indica la ubicación del buzón. Para obtener información sobre las tareas, consulte [“Cómo configurar un cliente de correo” en la página 297 en el Capítulo 13, “Servicios de correo \(tareas\)”](#).

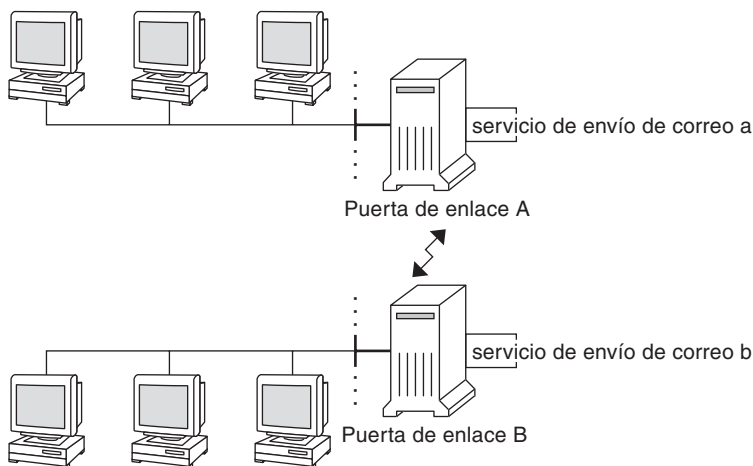
## Puerta de enlace del correo

La *puerta de enlace del correo* es un equipo que maneja conexiones entre redes que ejecutan distintos protocolos de comunicaciones o comunicaciones entre distintas redes que utilizan el mismo protocolo. Por ejemplo, una puerta de enlace de correo puede conectar una red TCP/IP a una red que ejecuta el conjunto de protocolos de la arquitectura de redes de sistemas (SCN).

La puerta de enlace del correo más sencilla para configurar es la puerta de enlace del correo que conecta dos redes que utilizan el mismo protocolo o aplicación de correo. Este sistema maneja el correo con una dirección para la que `sendmail` no puede encontrar un destinatario en el dominio. Si una puerta de enlace de correo existe, `sendmail` utiliza la puerta de enlace para enviar y recibir correo fuera del dominio.

Puede configurar una puerta de enlace de correo entre dos redes que utilizan servicios de envío de correo no coincidentes, como se muestra en la siguiente figura. Para admitir esta configuración, debe personalizar el archivo `sendmail.cf` en el sistema de la puerta de enlace del correo, lo que puede resultar un proceso difícil y que requiere mucho tiempo.

FIGURA 14-1 Puerta de enlace entre diferentes protocolos de comunicaciones



Si dispone de un equipo que proporciona conexiones a Internet, puede configurar ese equipo como la puerta de enlace del correo. Considere cuidadosamente las necesidades de seguridad del sitio antes de configurar una puerta de enlace de correo. Puede que necesite crear una puerta de enlace del cortafuegos entre la red corporativa y otras redes, y configurar esa puerta de enlace como la puerta de enlace del correo. Para obtener información sobre las tareas, consulte [“Cómo configurar una puerta de enlace de correo” en la página 300 en el Capítulo 13, “Servicios de correo \(tareas\)”](#).

## Archivos y programas de servicio de correo

Los servicios de correo incluyen muchos programas y daemons que interaccionan entre ellos. En esta sección, se presentan los archivos, los programas, las condiciones y los conceptos que se relacionan con la administración del correo electrónico.

- “Mejoras en la utilidad `vacation`” en la página 355
- “Contenido del directorio `/usr/bin`” en la página 355
- “Contenido del directorio `/etc/mail`” en la página 356
- “Contenido del directorio `/usr/lib`” en la página 360
- “Otros archivos utilizados para servicios de correo” en la página 360
- “Interacciones de programas de correo” en la página 361
- “Programa `sendmail`” en la página 362
- “Archivos de alias de correo” en la página 367
- “Archivos `.forward`” en la página 370
- “Archivo `/etc/default/sendmail`” en la página 372

## Mejoras en la utilidad `vacation`

A partir de la versión Solaris 10, la utilidad `vacation` ha sido mejorada con el objeto de que los usuarios puedan especificar qué mensajes entrantes reciben respuestas generadas automáticamente. Con esta mejora, el usuario puede evitar compartir información confidencial o de contacto con personas desconocidas. Los mensajes de personas desconocidas o que envían correo no deseado no reciben ninguna respuesta.

Esta mejora funciona mediante la comparación de la dirección de correo electrónico del remitente con una lista de dominios o direcciones de correo electrónico que figuran en el archivo `.vacation.filter`. Este archivo es creado por el usuario y se encuentra en el directorio principal de dicho usuario. Si se encuentra una coincidencia con un dominio o una dirección de correo electrónico, se envía una respuesta. En caso contrario, no se envía nada.

El archivo `.vacation.filter` puede contener entradas, como las siguientes:

```
company.com
mydomain.com
onefriend@hisisp.com
anotherfriend@herisp.com
```

Tenga en cuenta que cada línea contiene un dominio o una dirección de correo electrónico. Cada entrada debe estar en una línea separada. Para que la dirección de correo electrónico de un remitente coincida con una entrada de dirección de correo electrónico, la coincidencia debe ser exacta, excepto las mayúsculas y minúsculas. Si las letras en la dirección del remitente se escriben en minúsculas o en mayúsculas es indistinto. Para que la dirección de correo electrónico de un remitente coincida con una entrada del dominio, la dirección del remitente debe contener el dominio enumerado. Por ejemplo, tanto `somebody@dept.company.com` como `someone@company.com` serían una coincidencia de una entrada del dominio de `company.com`.

Para obtener más información, consulte la página del comando `man vacation(1)`.

## Contenido del directorio `/usr/bin`

En la siguiente tabla, se muestra el contenido del directorio `/usr/bin`, que se utiliza para los servicios de correo.

Nombre	Tipo	Descripción
<code>aliasadm</code>	Archivo	Un programa para manipular el mapa de alias NIS+.
<code>mail</code>	Archivo	Un agente de usuario.
<code>mailcompat</code>	Archivo	Un filtro para almacenar correo en el formato de buzón de SunOS 4.1.
<code>mailq</code>	Archivo	Un programa que muestra el contenido de la cola de correo.

Nombre	Tipo	Descripción
mailstats	Archivo	Un programa que se utiliza para leer estadísticas de correo que se almacenan en el archivo <code>/etc/mail/statistics</code> (si existe).
mailx	Archivo	Un agente de usuario.
mconnect	Archivo	Un programa que se conecta a la aplicación de correo para la verificación de dirección y la depuración.
praliases	Archivo	Un comando para descompilar la base de datos de alias. Consulte la información sobre descompilación que se proporciona en la página del comando <code>man</code> para <a href="#">praliases(1)</a> .
rmail	Enlace simbólico	Un enlace simbólico a <code>/usr/bin/mail</code> . Comando que se utiliza, a menudo, para permitir sólo el envío de correo.
vacation	Archivo	Un comando para configurar una respuesta automática al correo.

## Contenido del directorio `/etc/mail`

En la siguiente tabla, se muestra el contenido del directorio `/etc/mail`.

Nombre	Tipo	Descripción
Mail.rc	Archivo	Valores predeterminados para el agente de usuario de <code>mailx</code> .
aliases	Archivo	Información de reenvío de correo.
aliases.db	Archivo	Formato binario predeterminado de información de reenvío de correo que se crea mediante la ejecución de <code>newaliases</code> .
aliases.dir	Archivo	Formato binario de información de reenvío de correo que se crea mediante la ejecución de <code>newaliases</code> . Aún se puede utilizar, pero ya no se utiliza de manera predeterminada a partir de la versión Solaris 9.
aliases.pag	Archivo	Formato binario de información de reenvío de correo que se crea mediante la ejecución de <code>newaliases</code> . Aún se puede utilizar, pero ya no se utiliza de manera predeterminada a partir de la versión Solaris 9.
mailx.rc	Archivo	Valores predeterminados para el agente de usuario de <code>mailx</code> .
main.cf	Enlace simbólico	Para la compatibilidad de retroceso, se proporciona un enlace simbólico de este archivo de configuración de ejemplo para sistemas principales a <code>sendmail.cf</code> . Este archivo no es necesario en la versión 8.13 de <code>sendmail</code> .

Nombre	Tipo	Descripción
relay-domains	Archivo	Lista de todos los dominios para los que se permite la retransmisión. De manera predeterminada, sólo se permite el dominio local.
sendmail.cf	Archivo	Archivo de configuración para enrutamiento de correo.
submit.cf	Archivo	Nuevo archivo de configuración para el programa de envío de correo (MSP). Para obtener más información, consulte <a href="#">“Archivo de configuración submit.cf de la versión 8.12 de sendmail” en la página 389</a> .
local-host-names	Archivo	Archivo opcional que puede crear si el número de alias para el host de correo es demasiado grande.
helpfile	Archivo	Archivo de ayuda que es utilizado por el comando HELP del SMTP.
sendmail.pid	Archivo	Archivo que muestra el PID del daemon de escucha y ahora está en /var/run.
statistics	Archivo	Archivo de estadísticas de sendmail. Si este archivo está presente, sendmail registra la cantidad de tráfico por medio de cada aplicación de correo. Anteriormente, este archivo se denominaba sendmail.st.
subsidiary.cf	Enlace simbólico	Para la compatibilidad de retroceso, se proporciona un enlace simbólico de este archivo de configuración de ejemplo para sistemas secundarios a sendmail.cf. Este archivo no es necesario en la versión 8.13 de sendmail.
trusted-users	Archivo	Archivo que muestra a los usuarios (un usuario por línea) que son de confianza para realizar determinadas operaciones de correo. De manera predeterminada, sólo root está en este archivo. Algunas operaciones de correo, cuando son realizadas por usuarios que no son de confianza, resultan en la siguiente advertencia: X-Authentication-Warning: header being added to a message.

## Contenido del directorio /etc/mail/cf

En el directorio /etc/mail, hay un subdirectorio, cf, que contiene todos los archivos necesarios para crear un archivo sendmail.cf. El contenido de cf se muestra en la [Tabla 14–9](#).

A partir de la versión Solaris 10, para admitir un sistema de archivos /usr de sólo lectura, el contenido del directorio /usr/lib/mail se ha trasladado al directorio /etc/mail/cf. Tenga en cuenta, sin embargo, las siguientes excepciones. Las secuencias de comandos de shell /usr/lib/mail/sh/check-hostname y /usr/lib/mail/sh/check-permissions ahora se encuentran en el directorio /usr/sbin. Consulte [“Otros archivos utilizados para servicios de](#)

correo” en la página 360. Por razones de compatibilidad de retroceso, los enlaces simbólicos hacen referencia a las nuevas ubicaciones de los archivos.

**TABLA 14–9** Contenido del directorio `/etc/mail/cf` utilizado para servicios de correo

Nombre	Tipo	Descripción
README	Archivo	Describe los archivos de configuración.
<code>cf/main.cf</code>	Enlace simbólico	A partir de la versión Solaris 10, este nombre de archivo está enlazado a <code>cf/sendmail.cf</code> . Este archivo solía ser el archivo de configuración principal.
<code>cf/main.mc</code>	Enlace simbólico	A partir de la versión Solaris 10, este nombre de archivo está enlazado a <code>cf/sendmail.mc</code> . Este archivo era el archivo utilizado para crear el archivo de configuración principal.
<code>cf/Makefile</code>	Archivo	Proporciona reglas para crear archivos de configuración nuevos.
<code>cf/submit.cf</code>	Archivo	Archivo de configuración para el programa de envío de correo (MSP), que se utiliza para enviar mensajes.
<code>cf/submit.mc</code>	Archivo	Archivo utilizado para crear el archivo <code>submit.cf</code> . El archivo define macros <code>m4</code> para el programa de envío de correo (MSP).
<code>cf/sendmail.cf</code>	Archivo	Archivo de configuración principal para <code>sendmail</code> .
<code>cf/sendmail.mc</code>	Archivo	Contiene las macros <code>m4</code> que se utilizan para generar el archivo <code>sendmail.cf</code> .
<code>cf/subsidiary.cf</code>	Enlace simbólico	A partir de la versión Solaris 10, este nombre de archivo está enlazado a <code>cf/sendmail.cf</code> . Este archivo solía ser el archivo de configuración para los hosts que reciben <code>/var/mail</code> montado en NFS desde otro host.
<code>cf/subsidiary.mc</code>	Enlace simbólico	A partir de la versión Solaris 10, este nombre de archivo está enlazado a <code>cf/sendmail.mc</code> . Este archivo solía contener las macros <code>m4</code> que se utilizaban para generar el archivo <code>subsidiary.cf</code> .
<code>domain</code>	Directorio	Proporciona descripciones de subdominios dependientes de sitio.

TABLA 14-9 Contenido del directorio /etc/mail/cf utilizado para servicios de correo (Continuación)

Nombre	Tipo	Descripción
domain/generic.m4	Archivo	Archivo de dominio genérico de Berkeley Software Distribution.
domain/solaris-antispam.m4	Archivo	Archivo de dominio con cambios que hacen que sendmail funcione igual que las versiones anteriores de sendmail. Sin embargo, la retransmisión está completamente deshabilitada, las direcciones de remitentes sin nombre de host se rechazan y los dominios que no se pueden resolver se rechazan.
domain/solaris-generic.m4	Archivo	Archivo de dominio predeterminado con cambios que hacen que sendmail funcione igual que las versiones anteriores de sendmail.
feature	Directorio	Contiene definiciones de funciones específicas para hosts determinados. Consulte README para obtener una descripción completa de las funciones.
m4	Directorio	Contiene archivos de inclusión independientes de sitio.
mailer	Directorio	Contiene definiciones de servicios de envío de correo, que incluyen local, smtp y uucp.
main-v7sun.mc	Archivo	Obsoleto: a partir de la versión Solaris 10, este nombre de archivo cambia a cf/sendmail.mc.
ostype	Directorio	Describe varios entornos de sistemas operativos.
ostype/solaris2.m4	Archivo	Define la aplicación de correo local predeterminada como mail.local.
ostype/solaris2.ml.m4	Archivo	Define la aplicación de correo local predeterminada como mail.local.
ostype/solaris2.pre5.m4	Archivo	Define la aplicación de correo local como mail.
ostype/solaris8.m4	Archivo	Define la aplicación de correo local como mail.local (en modo LMTP), habilita IPv6, especifica /var/run como el directorio del archivo sendmail.pid.
subsidiary-v7sun.mc	Archivo	Obsoleto: a partir de la versión Solaris 10, este nombre de archivo cambia a cf/sendmail.mc.

## Contenido del directorio `/usr/lib`

En la siguiente tabla, se muestra el contenido del directorio `/usr/lib`, que se utiliza para los servicios de correo.

TABLA 14–10 Contenido del directorio `/usr/lib`

Nombre	Tipo	Descripción
<code>mail.local</code>	Archivo	Aplicación de correo que entrega correo a los buzones.
<code>sendmail</code>	Archivo	Programa de enrutamiento, también conocido como agente de transferencia de correo.
<code>smrsh</code>	Archivo	Programa de shell (shell restringido de sendmail) que usa la sintaxis “ program” de sendmail para restringir los programas que sendmail puede ejecutar a aquellos programas enumerados en el directorio <code>/var/adm/sm.bin</code> . Consulte la página del comando <code>man smrsh(1M)</code> para obtener recomendaciones sobre qué incluir en <code>/var/adm/sm.bin</code> . Para habilitarlo, incluya este comando <code>m4, FEATURE('smrsh')</code> , en el archivo <code>mc</code> .
<code>mail</code>	enlace simbólico	Un enlace simbólico hace referencia al directorio <code>/etc/mail/cf</code> . Para obtener más información, consulte “ <a href="#">Contenido del directorio /etc/mail/cf</a> ” en la <a href="#">página 357</a> .

## Otros archivos utilizados para servicios de correo

Se utilizan otros archivos y directorios para los servicios de correo, como se muestra en la [Tabla 14–11](#).

TABLA 14–11 Otros archivos utilizados para servicios de correo

Nombre	Tipo	Descripción
<code>/etc/default/sendmail</code>	Archivo	Muestra las variables de entorno para la secuencia de comandos de inicio de sendmail.
<code>/etc/shells</code>	Archivo	Muestra los shells de inicio de sesión válidos.
<code>/etc/mail/cf/sh</code>	Directorio	Contiene las secuencias de comandos de shell utilizadas por la ayuda de la migración y el proceso de compilación de <code>m4</code> .
<code>/usr/sbin/check-permissions</code>	Archivo	Comprueba los permisos de los alias <code>:include:</code> y de los archivos <code>.forward</code> y su ruta de directorio principal para determinar que sean correctos.

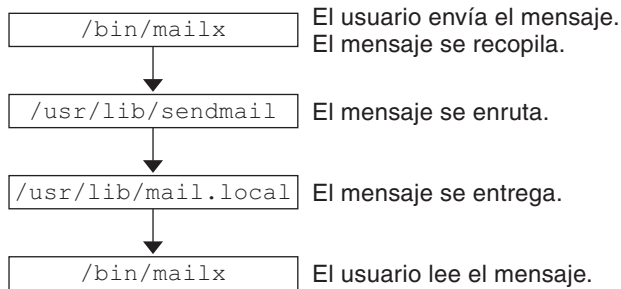


TABLA 14-11 Otros archivos utilizados para servicios de correo (Continuación)

Nombre	Tipo	Descripción
/usr/sbin/check-hostname	Archivo	Verifica que sendmail pueda determinar el nombre de host completo.
/usr/sbin/editmap	Archivo	Consulta y edita registros individuales en mapas de bases de datos para sendmail.
/usr/sbin/in.comsat	Archivo	Daemon de notificación de correo.
/usr/sbin/makemap	Archivo	Crea formatos binarios de mapas con clave.
/usr/sbin/newaliases	Enlace simbólico	Un enlace simbólico a /usr/lib/sendmail. Se utiliza para crear el formato binario de la base de datos de alias. Anteriormente en /usr/bin.
/usr/sbin/syslogd	Archivo	Registrador de mensajes de error, utilizado por sendmail.
/usr/sbin/etrn	Archivo	Secuencia de comandos Perl para iniciar la cola de correo remota en el cliente.
/usr/dt/bin/dtmail	Archivo	Agente de usuario de correo CDE.
/var/mail/mailbox1, /var/mail/mailbox2	Archivo	Buzones para correo entregado.
/var/spool/clientmqueue	Directorio	Almacenamiento para correo entregado por el daemon del cliente.
/var/spool/mqueue	Directorio	Almacenamiento para correo entregado por el daemon principal.
/var/run/sendmail.pid	Archivo	Archivo que muestra el PID del daemon de escucha.

## Interacciones de programas de correo

Los servicios de correo son proporcionados por una combinación de los siguientes programas, que interaccionan como se muestra en la ilustración simplificada de la [Figura 14-2](#).

**FIGURA 14-2** Interacciones de programas de correo

A continuación, se muestra una descripción de las interacciones de programas de correo.

1. Los usuarios envían mensajes mediante programas, como `mailx`. Consulte la página del comando `man mailx(1)` para obtener más información.
2. El mensaje es recopilado por el programa que ha generado el mensaje, y el mensaje es transferido al daemon `sendmail`.
3. El daemon `sendmail` *analiza* las direcciones (las divide en segmentos identificables) en el mensaje. El daemon utiliza la información del archivo de configuración, `/etc/mail/sendmail.cf`, para determinar la sintaxis del nombre de red, los alias, la información de reenvío y la topología de red. Mediante esta información, `sendmail` determina qué ruta debe seguir un mensaje para llegar a un destinatario.
4. El daemon `sendmail` pasa el mensaje al sistema apropiado.
5. El programa `/usr/lib/mail.local` en el sistema local entrega el correo al buzón en el directorio `/var/mail/username` del destinatario del mensaje.
6. El destinatario recibe un mensaje en el que se le notifica que el correo ha llegado y recupera el correo mediante `mail`, `mailx` o un programa similar.

## Programa sendmail

En la siguiente lista, se describen algunas de las capacidades del programa `sendmail`.

- `sendmail` puede usar diferentes tipos de protocolos de comunicaciones, como TCP/IP y UUCP.
- `sendmail` implementa un servidor SMTP, la cola de mensajes y las listas de correo.
- `sendmail` controla la interpretación de nombres mediante un sistema de coincidencia de patrón que puede funcionar con las siguientes convenciones de nomenclatura.
  - Convención de denominación basada en dominio. La técnica del dominio separa la emisión de nombres físicos de la emisión de nombres lógicos. Para obtener más información sobre los dominios, consulte [“Direcciones de correo” en la página 346](#).

- Técnicas improvisadas, como proporcionar nombres de red que aparecen como locales para hosts en otras redes.
- Sintaxis de nomenclatura (más antigua) arbitraria.
- Esquemas de nomenclatura distintos.

El sistema operativo Solaris utiliza el programa `sendmail` como enrutador de correo. En la siguiente lista, se describen algunas de sus funciones.

- `sendmail` es responsable de la recepción y entrega de mensajes de correo electrónico a un agente de entrega local, como `mail.local` o `procmail`.
- `sendmail` es un agente de transferencia de correo que acepta mensajes de agentes de usuario, como `mailx` y Mozilla Mail, y enruta los mensajes por medio de Internet a su destino.
- `sendmail` controla los mensajes de correo electrónico que los usuarios envían de la siguiente manera:
  - Evalúa las direcciones de los destinatarios.
  - Selecciona un programa de entrega adecuado.
  - Reescribe las direcciones en un formato que el agente de entrega puede manejar.
  - Reformatea los encabezados de correo según sea necesario.
  - Transfiere, finalmente, el mensaje transformado al programa de correo para la entrega.

Para obtener más información sobre el programa `sendmail`, consulte los siguientes temas.

- [“`sendmail` y sus mecanismos de reenrutamiento” en la página 363](#)
- [“Funciones de `sendmail`” en la página 365](#)
- [“Archivo de configuración de `sendmail`” en la página 365](#)

## **`sendmail` y sus mecanismos de reenrutamiento**

El programa `sendmail` admite tres mecanismos para reenrutamiento de correo. El mecanismo que elija dependerá del tipo de cambio que se trate.

- Un cambio de servidor
- Un cambio de todo el dominio
- Un cambio para un usuario

Además, el mecanismo de reenrutamiento que seleccione podrá afectar el nivel de administración que sea necesario. Considere las siguientes opciones.

1. Un mecanismo de reenrutamiento es la *creación de alias*.

La creación de alias puede asignar nombres a las direcciones en todo un servidor o en todo un servicio de nombres, según el tipo de archivo que utiliza.

Tenga en cuenta las siguientes ventajas y desventajas de la creación de alias del servicio de nombres.

- El uso de un archivo de alias de servicio de nombres permite que los cambios de reenrutamiento de correo sean administrados desde un único origen. Sin embargo, la creación de alias de servicio de nombres puede generar un desfase cuando se propaga el cambio de reenrutamiento.
- La administración del servicio de nombres, normalmente, está limitada a un grupo exclusivo de administradores de sistemas. Un usuario normal no administraría este archivo.

Tenga en cuenta las siguientes ventajas y desventajas de utilizar un archivo de alias de servidor.

- Al utilizar un archivo de alias de servidor, el reenrutamiento puede ser administrado por cualquier persona que pueda convertirse en root en el servidor designado.
- La creación de alias de servidor debe generar un pequeño desfase o ningún desfase cuando se propaga el cambio de reenrutamiento.
- El cambio sólo afecta el servidor local, que puede ser aceptable si la mayoría de los correos se envían a un servidor. Sin embargo, si necesita propagar este cambio a muchos servidores de correo, utilice un servicio de nombres.
- Un usuario normal no administraría este cambio.

Para obtener más información, consulte [“Archivos de alias de correo” en la página 367](#) en este capítulo. Para obtener un mapa de tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313](#) en el Capítulo 13, “Servicios de correo (tareas)”.

## 2. El siguiente mecanismo es el *reenvío*.

Este mecanismo permite a los usuarios administrar el reenrutamiento de correo. Los usuarios locales pueden reenrutar el correo entrante hacia lo siguiente.

- Otro buzón
- Una aplicación de correo diferente
- Otro host de correo

Este mecanismo es admitido mediante el uso de archivos `.forward`. Para obtener más información sobre estos archivos, consulte [“Archivos `.forward`” en la página 370](#) en este capítulo. Para obtener un mapa de tareas, consulte [“Administración de los archivos `.forward` \(mapa de tareas\)” en la página 328](#) en el Capítulo 13, “Servicios de correo (tareas)”.

## 3. El último mecanismo de reenrutamiento es la *inclusión*.

Este mecanismo permite a los usuarios mantener listas de alias en lugar de requerir el acceso a root. Para ofrecer esta función, el usuario root debe crear una entrada correspondiente en el archivo de alias en el servidor. Después de que esta entrada se crea, el usuario puede reenrutar el correo según sea necesario. Para obtener más información sobre la inclusión, consulte [“Archivo `/etc/mail/aliases`” en la página 367](#) en este capítulo. Para obtener un

mapa de tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)”](#) en la página 313 en el Capítulo 13, “Servicios de correo (tareas)”.

---

**Nota** – Los programas que leen correo, como `/usr/bin/mailx`, pueden tener alias propios, que se expanden antes de que el mensaje llega a `sendmail`. Los alias para `sendmail` pueden provenir de varios orígenes de servicios de nombres, como archivos locales, NIS o NIS+. El orden de la consulta está determinado por el archivo `nsswitch.conf`. Consulte la página del comando `man nsswitch.conf(4)`.

---

## Funciones de sendmail

El programa `sendmail` proporciona las siguientes funciones.

- `sendmail` es fiable. El programa está diseñado para entregar correctamente cada mensaje. Ningún mensaje se debe perder por completo.
- `sendmail` utiliza software existente para la entrega siempre que sea posible. Por ejemplo, el usuario interacciona con un programa de generación de correo y de envío de correo. Cuando se envía correo, el programa de generación de correo llama a `sendmail`, que enruta el mensaje a los servicios de envío de correo correctos. Debido a que algunos de los remitentes pueden ser servidores de red y algunos de los servicios de envío de correo pueden ser clientes de red, `sendmail` se puede utilizar como una puerta de enlace del correo de Internet. Consulte [“Interacciones de programas de correo”](#) en la página 361 para obtener una descripción más detallada del proceso.
- `sendmail` se puede configurar para administrar entornos complejos, incluidas varias redes. `sendmail` comprueba el contenido de una dirección, así como su sintaxis, para determinar qué aplicación de correo utilizar.
- `sendmail` utiliza los archivos de configuración para controlar la configuración del correo, en lugar de exigir que la información de la configuración se compile en el código.
- Los usuarios pueden mantener sus propias listas de correo. Además, los usuarios pueden especificar su propio mecanismo de reenvío sin modificar el archivo de alias de todo el dominio, normalmente, ubicado en los alias de todo el dominio que son mantenidos por NIS o NIS+.
- Cada usuario puede especificar una aplicación de correo personalizada para procesar el correo entrante. La aplicación de correo personalizada puede proporcionar funciones, como devolver un mensaje que lee: “De vacaciones”. Consulte la página del comando `man vacation(1)` para obtener más información.
- `sendmail` lotea direcciones en un solo host para reducir el tráfico en la red.

## Archivo de configuración de sendmail

Un *archivo de configuración* controla la forma en que `sendmail` realiza sus funciones. El archivo de configuración determina la elección de agentes de entrega, las reglas de reescritura de

dirección y el formato del encabezado del correo. El programa `sendmail` utiliza la información del archivo `/etc/mail/sendmail.cf` para realizar sus funciones.

El sistema operativo Solaris proporciona dos archivos de configuración predeterminados en el directorio `/etc/mail`.

1. `sendmail.cf`, un archivo de configuración utilizado para ejecutar `sendmail` en modo de daemon.
2. `submit.cf`, un archivo de configuración utilizado para ejecutar `sendmail` en modo de programa de envío de correo, en lugar de ejecutarlo en modo de daemon. Para obtener más información, consulte [“Archivo de configuración `submit.cf` de la versión 8.12 de `sendmail`” en la página 389](#).

Al configurar clientes de correo, servidores de correo, hosts de correo o puertas de enlace de correo, tenga en cuenta lo siguiente:

- Para los clientes de correo o servidores de correo, no es necesario que haga nada para configurar o editar el archivo de configuración predeterminado.
- Para configurar un host de correo o una puerta de enlace de correo, necesita establecer los parámetros de la aplicación de correo de retransmisión y del host de retransmisión que son necesarios para la configuración del correo. Para obtener información sobre las tareas, consulte [“Configuración de los servicios de correo \(mapa de tareas\)” en la página 294](#) o [“Modificación de la configuración de `sendmail`” en la página 303](#) en el [Capítulo 13](#), [“Servicios de correo \(tareas\)”](#). Tenga en cuenta que con la versión 8.13 de `sendmail`, ya no necesita el archivo `main.cf`.

En la siguiente lista, se describen algunos parámetros de configuración que puede cambiar en función de los requisitos de su sitio.

- Valores de tiempo, que especifican la siguiente información.
  - Tiempos de espera de lectura.
  - Longitud de tiempo que un mensaje permanece en la cola sin ser entregado antes de que el mensaje se devuelva al remitente. Consulte [“Funciones de cola adicionales de la versión 8.12 de `sendmail`” en la página 401](#). Para obtener un mapa de tareas, consulte [“Administración de los directorios de la cola \(mapa de tareas\)” en la página 324](#).
- Modos de entrega, que especifican la rapidez con la que el correo se entrega.
- Límites de carga, que aumentan la eficacia durante períodos ocupados. Estos parámetros evitan que `sendmail` intente entregar mensajes de gran tamaño, mensajes a varios destinatarios y mensajes a sitios que han estado cerrados por un tiempo.
- Nivel de registro, que especifica los tipos de problemas que se registran.

## Archivos de alias de correo

Puede utilizar cualquiera de los siguientes archivos, mapas o tablas para mantener alias.

- “Alias `.mailrc`” en la página 367
- “Archivo `/etc/mail/aliases`” en la página 367
- “Mapa `aliases NIS`” en la página 369
- “Tabla `mail_aliases NIS+`” en la página 369

El método de mantenimiento de alias depende de quién utiliza el alias y quién necesita poder cambiar el alias. Cada tipo de alias tiene requisitos de formato únicos.

Si busca información sobre las tareas, consulte “[Administración de los archivos de alias de correo \(mapa de tareas\)](#)” en la página 313 en el [Capítulo 13](#), “[Servicios de correo \(tareas\)](#)”.

### Alias `.mailrc`

Los alias que están enumerados en un archivo `.mailrc` están disponibles solamente para el usuario que es propietario del archivo. Esta restricción permite a los usuarios establecer un archivo de alias que controlan y que sólo el propietario puede utilizar. Los alias en un archivo `.mailrc` tienen el siguiente formato.

```
alias aliasname value value value ...
```

*nombres\_alias* es el nombre que el usuario utiliza al enviar correo, y *valor* es una dirección de correo electrónico válida.

Si un usuario establece un alias personal para `scott` que no coincide con la dirección de correo electrónico para `scott` en el servicio de nombres, se produce un error. El correo se enruta a la persona equivocada cuando las personas intentan responder el correo generado por este usuario. La única solución es utilizar cualquiera de los demás mecanismos de alias.

### Archivo `/etc/mail/aliases`

Cualquier alias que se establece en el archivo `/etc/mail/aliases` puede ser utilizado por cualquier usuario que conoce el nombre del alias y el nombre de host del sistema que contiene el archivo. Los formatos de una lista de distribución en un archivo `/etc/mail/aliases local` tienen el siguiente formato.

```
aliasname: value,value,value ...
```

*nombre\_alias* es el nombre que el usuario utiliza al enviar correo a este alias, y *valor* es una dirección de correo electrónico válida.

Si la red no está ejecutando un servicio de nombres, el archivo `/etc/mail/aliases` de cada sistema debe contener entradas para todos los clientes de correo. Puede editar el archivo en cada sistema o editar el archivo en un sistema y copiar el archivo en cada uno de los otros sistemas.

Los alias en el archivo `/etc/mail/aliases` se almacenan en formato de texto. Al editar el archivo `/etc/mail/aliases`, necesita ejecutar el programa `newaliases`. Este programa recompila la base de datos y hace que los alias estén disponibles en formato binario para el programa `sendmail`. Para obtener información sobre las tareas, consulte [“Cómo configurar un archivo de alias correo local” en la página 320 en el Capítulo 13, “Servicios de correo \(tareas\)”](#). De lo contrario, puede utilizar la función de lista de correo en Solaris Management Console para administrar los alias de correo que se almacenan en los archivos `/etc` locales.

Puede crear alias sólo para los nombres locales, como un nombre de host actual o ningún nombre de host. Por ejemplo, una entrada de alias para el usuario `ignatz` que tiene un buzón en el sistema `saturn` tendría la siguiente entrada en el archivo `/etc/mail/aliases`.

```
ignatz: ignatz@saturn
```

Debe crear una cuenta administrativa para cada servidor de correo. Cree una cuenta de este tipo asignando un buzón en el servidor de correo a `root` y agregando una entrada para `root` al archivo `/etc/mail/aliases`. Por ejemplo, si el sistema `saturn` es un servidor de buzones, agregue la entrada `root: sysadmin@saturn` al archivo `/etc/mail/aliases`.

Normalmente, sólo el usuario `root` puede editar este archivo. Sin embargo, cuando se utiliza Solaris Management Console, todos los usuarios del grupo 14, que es el grupo `sysadmin`, pueden cambiar el archivo local. Otra opción es crear la siguiente entrada.

```
aliasname: :include:/path/aliasfile
```

*nombre\_alias* es el nombre que el usuario utiliza al enviar correo, y */path/aliasfile* es la ruta completa al archivo que contiene la lista de alias. El archivo de alias debe incluir entradas de correo electrónico, una entrada en cada línea, y ninguna otra notación.

```
user1@host1  
user2@host2
```

Puede definir archivos de correo adicionales en `/etc/mail/aliases` para mantener un registro o una copia de seguridad. La siguiente entrada almacena todo el correo que se envía a *nombre\_alias* en *nombre\_archivo*.

```
aliasname: /home/backup/filename
```

También puede enrutar el correo a otro proceso. El ejemplo siguiente almacena una copia del mensaje de correo en *nombre\_archivo* e imprime una copia.

```
aliasname: "|tee -a /home/backup/filename |lp"
```

Para obtener un mapa de tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313 en el Capítulo 13, “Servicios de correo \(tareas\)”](#).



## Mapa `aliases` NIS

Todos los usuarios en un dominio local pueden utilizar las entradas que se encuentran en el mapa `aliases` NIS. El motivo es que el programa `sendmail` puede utilizar el mapa `aliases` NIS en lugar de los archivos `/etc/mail/aliases` locales para determinar las direcciones de correo. Para obtener más información, consulte la página del comando `man nsswitch.conf(4)`.

Los alias en el mapa `aliases` NIS tienen el siguiente formato.

*aliasname: value,value,value ...*

*nombre\_alias* es el nombre que el usuario utiliza al enviar correo, y *valor* es una dirección de correo electrónico válida.

El mapa `aliases` NIS debe contener entradas para todos los clientes de correo. En general, sólo el usuario `root` en el maestro NIS puede cambiar estas entradas. Es posible que este tipo de alias no sea una buena elección para los alias que cambian constantemente. Sin embargo, dichos alias pueden ser útiles si los alias hacen referencia a otro archivo de alias, como en el siguiente ejemplo de sintaxis.

*aliasname: aliasname@host*

*nombre\_alias* es el nombre que los usuarios utilizan al enviar correo, y *host* es el nombre de host para el servidor que contiene el archivo `/etc/mail/alias`.

Para obtener información sobre las tareas, consulte “[Cómo configurar un mapa NIS `mail.aliases`](#)” en la página 319 en el [Capítulo 13](#), “[Servicios de correo \(tareas\)](#)”.

## Tabla `mail_aliases` NIS+

La tabla `mail_aliases` NIS+ contiene los nombres por los que un sistema o una persona se conocen en el dominio local. El programa `sendmail` puede utilizar la tabla `mail_aliases` NIS+, en lugar de los archivos `/etc/mail/aliases` locales, para determinar las direcciones de correo. Para obtener más información, consulte las páginas del comando `man aliasadm(1M)` y `nsswitch.conf(4)`.

Los alias en la tabla `mail_aliases` NIS+ tienen el siguiente formato:

*alias: expansion # ["options" # "comments"]*

En la [Tabla 14–12](#), se describen las cuatro columnas que se encuentran en la tabla `mail_aliases` NIS+.

**TABLA 14–12** Columnas en la tabla `mail_aliases` NIS+

Columna	Descripción
<code>alias</code>	El nombre del alias

TABLA 14-12 Columnas en la tabla mail\_aliases NIS+ (Continuación)

Columna	Descripción
expansion	El valor del alias o una lista de alias como aparecería en un archivo /etc/mail/aliases de sendmail
options	La columna que está reservada para uso futuro
comments	La columna para comentarios sobre un alias individual

La tabla mail\_aliases NIS+ debe contener entradas para todos los clientes de correo. Puede enumerar, crear, modificar y eliminar entradas de la tabla aliases NIS+ con el comando aliasadm. Para utilizar el comando aliasadm, debe ser miembro del grupo NIS+ que posee la tabla aliases. Para obtener información sobre las tareas, consulte “Administración de los archivos de alias de correo (mapa de tareas)” en la página 313 en el Capítulo 13, “Servicios de correo (tareas)”. También puede utilizar Solaris Management Console para administrar los alias de correo NIS+.

**Nota** – Si va a crear una nueva tabla aliases NIS+, debe inicializarla antes de crear las entradas. Si la tabla existe, no es necesaria la inicialización.

## Archivos . forward

Los usuarios pueden crear un archivo . forward en sus directorios principales que sendmail, junto con otros programas, pueden utilizar para redireccionar o enviar correo. Consulte los siguientes temas.

- “Situaciones que se deben evitar” en la página 370
- “Controles para archivos . forward” en la página 371
- “Archivo . forward.hostname” en la página 371
- “Archivo . forward+detail” en la página 371

Para obtener un mapa de tareas, consulte “Administración de los archivos . forward (mapa de tareas)” en la página 328 en el Capítulo 13, “Servicios de correo (tareas)”.

## Situaciones que se deben evitar

En la siguiente lista, se describen algunas situaciones que puede evitar o corregir fácilmente.

- Si el correo no se entrega a la dirección esperada, compruebe el archivo . forward del usuario. Es posible que el usuario haya puesto el archivo . forward en el directorio principal de host1, que reenvía el correo a user@host2. Cuando el correo llega a host2, sendmail comprueba si existe user en los alias NIS o NIS+, y envía el mensaje de vuelta a user@host1. Este enrutamiento resulta en un bucle y más correo rechazado.
- Para evitar problemas de seguridad, nunca coloque archivos . forward en root ni cuentas bin. Si es necesario, reenvíe el correo mediante el archivo aliases, en su lugar.

## Controles para archivos `.forward`

Para que los archivos `.forward` sean una parte efectiva de la entrega de correo, asegúrese de que los siguientes controles (principalmente, la configuración de permisos) se apliquen correctamente.

- Solamente el propietario del archivo `.forward` puede escribirlo. Esta restricción evita que otros usuarios infrinjan la seguridad.
- Solamente `root` debe ser el propietario de las rutas que conducen al directorio principal y debe poder escribirlas. Por ejemplo, si un archivo `.forward` está en `/export/home/terry`, `/export` y `/export/home` sólo deben pertenecer a `root` y sólo deben poder ser escritos por él.
- Solamente el usuario debe poder escribir en el directorio principal real.
- El archivo `.forward` no puede ser un enlace simbólico, y este archivo no puede tener más de un enlace físico.

## Archivo `.forward.hostname`

Puede crear un archivo `.forward.hostname` para redirigir el correo que se envía a un host específico. Por ejemplo, si el alias de un usuario ha cambiado de `sandy@phoenix.example.com` a `sandy@example.com`, coloque un archivo `.forward.phoenix` en el directorio principal para `sandy`.

```
% cat .forward.phoenix
sandy@example.com
"/usr/bin/vacation sandy"
% cat .vacation.msg
From: sandy@example.com (via the vacation program)
Subject: my alias has changed
```

```
My alias has changed to sandy@example.com.
Please use this alias in the future.
The mail that I just received from you
has been forwarded to my new address.
```

Sandy

En este ejemplo, el correo se puede reenviar al lugar correcto, mientras que el remitente recibe una notificación del cambio de alias. Debido a que el programa `vacation` permite un solo archivo de mensaje, sólo puede reenviar un mensaje por vez. Sin embargo, si el mensaje no es específico de host, un archivo de mensaje de vacaciones puede ser utilizado por archivos `.forward` para muchos hosts.

## Archivo `.forward+detail`

Otra extensión del mecanismo de reenvío es el archivo `.forward+detalle`. La cadena *detalle* puede ser cualquier secuencia de caracteres, excepto caracteres de operador. Los caracteres de operador son `.:%&!^[ ]+`. Mediante este tipo de archivo, puede determinar si alguien está utilizando su dirección de correo electrónico sin que usted lo sepa. Por ejemplo, si un usuario le

indica a alguien que utilice la dirección de correo electrónico `sandy+test1@example.com`, el usuario podría identificar cualquier correo que se envíe a este alias. De manera predeterminada, cualquier correo que se envía al alias `sandy+test1@example.com` se comprueba con el alias y los archivos `.forward+detalle`. Si no hay ninguna coincidencia, el correo vuelve a `sandy@example.com`, pero el usuario puede ver un cambio en el encabezado del correo `To:`.

## Archivo `/etc/default/sendmail`

Este archivo se utiliza para almacenar las opciones de inicio de `sendmail`, de manera que las opciones no sean eliminadas cuando un host se actualiza. Las siguientes variables se pueden utilizar.

**CLIENTOPTIONS**=*“string”*

Selecciona opciones adicionales que se utilizarán con el daemon del cliente, que busca en la cola exclusiva del cliente (`/var/spool/clientmqueue`) y actúa como un ejecutor de colas de clientes. No se realiza la comprobación de la sintaxis, por lo que debe tener cuidado al realizar cambios en esta variable.

**CLIENTQUEUEINTERVAL**=#

Similar a la opción `QUEUEINTERVAL`, `CLIENTQUEUEINTERVAL` establece el intervalo de tiempo para las ejecuciones de la cola de correo. Sin embargo, la opción `CLIENTQUEUEINTERVAL` controla las funciones del daemon del cliente, en lugar de las funciones del daemon maestro. Normalmente, el daemon maestro puede entregar todos los mensajes al puerto SMTP. Sin embargo, si la carga de mensajes es demasiado alta o si el daemon maestro no se está ejecutando, los mensajes van a la cola exclusiva del cliente, `/var/spool/clientmqueue`. El daemon del cliente, que comprueba en la cola exclusiva del cliente, actúa como procesador de colas de clientes.

**ETRN\_HOSTS**=*“string”*

Permite que un servidor y cliente SMTP interaccionen inmediatamente sin esperar los intervalos de ejecución de colas, que son periódicos. El servidor puede entregar de inmediato la parte de su cola que va a los hosts especificados. Para más información, consulte la página del comando `man etrn(1M)`.

**MODE**=-bd

Selecciona el modo con el cual iniciar `sendmail`. Utilice la opción `-bd` o déjela sin definir.

**OPTIONS**=*string*

Selecciona opciones adicionales que se utilizarán con el daemon maestro. No se realiza la comprobación de la sintaxis, por lo que debe tener cuidado al realizar cambios en esta variable.

**QUEUEINTERVAL**=#

Establece el intervalo para las ejecuciones de colas de correo en el daemon maestro. # puede ser un número entero positivo seguido de `s` para segundos, `m` para minutos, `h` para horas, `d` para días o `w` para semanas. La sintaxis se comprueba antes de que `sendmail` se inicie. Si el

intervalo es negativo o si la entrada no termina con una letra adecuada, el intervalo se ignora y `sendmail` empieza por un intervalo de colas de 15 min.

#### `QUEUEOPTIONS=p`

Habilita un ejecutor de colas persistente que permanece inactivo entre los intervalos de ejecución de colas, en lugar de un nuevo ejecutor de colas para cada intervalo de ejecución de colas. Puede definir esta opción en `p`, que es la única configuración disponible. De lo contrario, esta opción no está definida.

## Direcciones de correo y enrutamiento de correo

La ruta que un mensaje de correo sigue durante la entrega depende de la configuración del sistema cliente y de la topología del dominio de correo. Cada nivel adicional de hosts de correo o dominios de correo puede agregar otra resolución de alias, pero el proceso de enrutamiento es básicamente el mismo en la mayoría de los hosts.

Puede configurar un sistema cliente para recibir correo localmente. La recepción de correo localmente se conoce como ejecución de `sendmail` en modo local. El modo local es el valor predeterminado para todos los servidores de correo y algunos clientes. En un servidor de correo o un cliente de correo en modo local, un mensaje de correo se enruta de la siguiente manera.

---

**Nota** – El ejemplo siguiente supone que se utiliza el conjunto de reglas predeterminado en el archivo `sendmail.cf`.

---

1. Expanda el alias de correo, si es posible, y reinicie el proceso de enrutamiento local.  
La dirección de correo se expande mediante la comprobación del alias de correo en el servicio de nombres y mediante la sustitución del nuevo valor, si se encuentra un nuevo valor. Este nuevo alias se comprueba nuevamente.
2. Si el correo es local, entregue el correo a `/usr/lib/mail.local`.  
El correo se entrega a un buzón local.
3. Si la dirección de correo incluye un host en este dominio de correo, entregue el correo a ese host.
4. Si la dirección no incluye un host en este dominio, reenvíe el correo al host de correo.  
El host de correo utiliza el mismo proceso de enrutamiento que el servidor de correo. Sin embargo, el host de correo puede recibir correo dirigido al nombre de dominio, así como al nombre de host.

## Interacciones de sendmail con servicios de nombres

En esta sección, se describen nombres de dominio que se aplican a sendmail y servicios de nombres. Además, en esta sección, se describen las reglas para el uso eficaz de los servicios de nombres y las interacciones específicas de sendmail con servicios de nombres. Para obtener detalles, consulte los siguientes temas.

- [“sendmail.cf y dominios de correo” en la página 374](#)
- [“sendmail y servicios de nombres” en la página 374](#)
- [“Interacciones de NIS y sendmail” en la página 376](#)
- [“Interacciones de sendmail con NIS y DNS” en la página 377](#)
- [“Interacciones de NIS+ y sendmail” en la página 377](#)
- [“Interacciones de sendmail con NIS+ y DNS” en la página 378](#)

Si busca información sobre tareas relacionadas, consulte [“Cómo usar DNS con sendmail” en la página 302](#) o [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313](#) en el Capítulo 13, “Servicios de correo (tareas)”.

### sendmail.cf y dominios de correo

El archivo sendmail.cf estándar utiliza dominios de correo para determinar si el correo se entrega directamente o mediante un host de correo. El correo intradominio se entrega mediante una conexión SMTP directa, mientras que el correo entredominio se reenvía a un host de correo.

En una red segura, sólo unos pocos hosts seleccionados están autorizados a generar paquetes que están dirigidos a destinos externos. Incluso si un host tiene la dirección IP del host remoto que es externo al dominio de correo, no se garantiza el establecimiento de una conexión SMTP. El sendmail.cf estándar asume lo siguiente.

- El host actual no está autorizado a enviar paquetes directamente a un host fuera del dominio de correo.
- El host de correo puede reenviar el correo a un host autorizado que puede transmitir paquetes directamente a un host externo. En realidad, el host de correo puede ser un host autorizado.

Con estos supuestos, el host de correo es responsable de entregar o reenviar correo interdominio.

### sendmail y servicios de nombres

sendmail impone diversos requisitos en los servicios de nombres. Para comprender mejor estos requisitos, en esta sección, primero, se describe la relación de dominios de correo con dominios de servicio de nombres. Luego, se describen los diversos requisitos. Consulte lo siguiente.

- “Dominios de correo y dominios de servicio de nombres” en la página 375
- “Requisitos para servicios de nombres” en la página 375
- Páginas del comando `man` para `NIS+(1)`, `nisaddent(1M)` y `nsswitch.conf(4)`

## Dominios de correo y dominios de servicio de nombres

El nombre de dominio de correo debe ser un sufijo del dominio de servicio de nombres. Por ejemplo, si el nombre de dominio del servicio de nombres es `A.B.C.D`, el nombre de dominio de correo puede ser uno de los siguientes.

- `A.B.C.D`
- `B.C.D`
- `C.D`
- `D`

Quando se establece por primera vez, el nombre de dominio de correo suele ser idéntico al dominio de servicio de nombres. A medida que la red crece, el dominio de servicio de nombres se puede dividir en fragmentos más pequeños para que el servicio de nombres sea más manejable. Sin embargo, el dominio de correo suele permanecer sin dividirse para proporcionar una creación de alias coherente.

## Requisitos para servicios de nombres

En esta sección, se describen los requisitos que sendmail impone sobre los servicios de nombres.

Se debe configurar un mapa o una tabla de host en un servicio de nombres para admitir tres tipos de consultas `gethostbyname()`.

- `mailhost`: algunas configuraciones de servicio de nombres cumplen este requisito automáticamente.
- Nombre de host completo (por ejemplo, `smith.admin.acme.com`): muchas configuraciones de servicio de nombres cumplen este requisito.
- Nombre de host corto (por ejemplo, `smith`): sendmail debe conectarse al host de correo para reenviar correo externo. Para determinar si una dirección de correo se encuentra dentro del dominio de correo actual, `gethostbyname()` se invoca con el nombre de host completo. Si la entrada se encuentra, la dirección se considera interna.  
  
NIS, NIS+ y DNS admiten `gethostbyname()` con un nombre de host corto como argumento, por lo que este requisito se cumple automáticamente.

Se deben seguir dos reglas adicionales sobre el servicio de nombres de host para establecer servicios sendmail efectivos dentro de un servicio de nombres.

- `gethostbyname()` con argumento de nombre de host completo y argumento de nombre de host corto debe generar resultados coherentes. Por ejemplo, `gethostbyname(smith.admin.acme.com)` debe devolver el mismo resultado que `gethostbyname(smith)` si ambas funciones son llamadas desde el dominio principal `admin.acme.com`.
- Para todos los dominios de servicio de nombres bajo un dominio de correo común, `gethostbyname()` con un nombre de host corto debe generar el mismo resultado. Por ejemplo, si se proporciona el dominio de correo `smith.admin.acme.com`, `gethostbyname(smith)` debe devolver el mismo resultado cuando la llamada se origina desde el dominio `ebb.admin.acme.com` o desde el dominio `esg.admin.acme.com`. El nombre de dominio de correo suele ser más corto que el dominio de servicio de nombres, lo cual da a este requisito implicaciones especiales para varios servicios de nombres.

Para obtener más información sobre la función `gethostbyname()`, consulte la página del comando `man gethostbyname(3NSL)`.

## Interacciones de NIS y sendmail

En la siguiente lista, se describen las interacciones de sendmail y NIS, y se proporciona cierta orientación.

- **Nombre de dominio de correo:** si está configurando NIS como el servicio de nombres principal, sendmail filtra automáticamente el primer componente del nombre de dominio NIS y utiliza el resultado como el nombre de dominio de correo. Por ejemplo, `ebs.admin.acme.com` se convierte en `admin.acme.com`.
- **Nombre de host de correo:** debe tener una entrada `mailhost` en el mapa de hosts NIS.
- **Nombres de host completos:** la configuración común de NIS no “comprende” el nombre de host completo. En lugar de intentar que NIS comprenda el nombre de host completo, desactive este requisito desde sendmail editando el archivo `sendmail.cf` y reemplazando todos los casos de `%l` con `%y`. Este cambio desactiva la detección de correo interdominio de sendmail. Si el host de destino puede resolverse en una dirección IP, se intenta una entrega SMTP directa. Asegúrese de que el mapa de hosts NIS no contenga ninguna entrada de host que sea externa al dominio de correo actual. De lo contrario, deberá personalizar aún más el archivo `sendmail.cf`.
- **Coincidencia de nombres de host completos y nombres de host cortos:** siga las instrucciones anteriores sobre cómo desactivar `gethostbyname()` para un nombre de host completo.
- **Varios dominios NIS en un dominio de correo:** todos los mapas de hosts NIS en un dominio de correo común deben tener el mismo conjunto de entradas de host. Por ejemplo, el mapa de hosts en el dominio `ebs.admin.acme.com` debe ser el mismo que el mapa de hosts en el dominio `esg.admin.acme.com`. De lo contrario, una dirección podría funcionar en un dominio NIS, pero no en el otro dominio NIS.



Para obtener información sobre las tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)”](#) en la página 313 en el Capítulo 13, “Servicios de correo (tareas)”.

## Interacciones de sendmail con NIS y DNS

En la siguiente lista, se describen las interacciones de sendmail con NIS y DNS, y se proporciona cierta orientación.

- **Nombre de dominio de correo:** si está configurando NIS como el servicio de nombres principal, sendmail filtra automáticamente el primer componente del nombre de dominio NIS y utiliza el resultado como el nombre de dominio de correo. Por ejemplo, `ebs.admin.acme.com` se convierte en `admin.acme.com`.
- **Nombre de host de correo:** cuando la función de reenvío de DNS está activada, las consultas que NIS no puede resolver se reenvían al DNS, así que no es necesario una entrada `mailhost` en el mapa de hosts NIS.
- **Nombres de host completos:** aunque NIS no “comprenda” nombres de host completos, el DNS los comprende. Este requisito se cumple cuando se sigue el procedimiento regular para configurar NIS y DNS.
- **Coincidencia de nombres de host completos y nombres de host cortos:** para cada entrada de host en la tabla de hosts NIS, debe tener una entrada de host correspondiente en DNS.
- **Varios dominios NIS en un dominio de correo:** todos los mapas de hosts NIS en un dominio de correo común deben tener el mismo conjunto de entradas de host. Por ejemplo, el mapa de hosts en el dominio `ebs.admin.acme.com` debe ser el mismo que el mapa de hosts en el dominio `esg.admin.acme.com`. De lo contrario, una dirección podría funcionar en un dominio NIS, pero no en el otro dominio NIS.

Para obtener información sobre las tareas, consulte [“Cómo usar DNS con sendmail”](#) en la página 302 y [“Administración de los archivos de alias de correo \(mapa de tareas\)”](#) en la página 313 en el Capítulo 13, “Servicios de correo (tareas)”.

## Interacciones de NIS+ y sendmail

En la siguiente lista, se describen las interacciones de sendmail con NIS+, y se proporciona cierta orientación.

- **Nombre de dominio de correo:** si está configurando NIS+ como el servicio de nombres principal, sendmail puede comprobar el dominio de correo de la tabla `sendmailvars` NIS+. Esta tabla NIS+ tiene una columna de claves y una columna de valores. Para configurar el dominio de correo, debe agregar una entrada a esta tabla. Esta entrada debe tener la columna de claves establecida como la cadena literal `maildomain` y la columna de valores establecida como el nombre de dominio de correo. Un ejemplo es `admin.acme.com`. Aunque NIS+ permita cualquier cadena en la tabla `sendmailvars`, la regla de sufijo todavía se aplica

para que el sistema de correo funcione correctamente. Puede utilizar `nistbladm` para agregar la entrada `maildomain` a la tabla `sendmailvars`. En el siguiente ejemplo, observe que el dominio de correo es un sufijo del dominio NIS+.

```
nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
```

- **Nombre de host Mailhost:** debe tener una entrada `mailhost` en la tabla de hosts NIS+.
- **Nombres de host completos:** NIS+ “comprende” el nombre de host completo. Si se sigue el procedimiento de configuración regular de NIS+, se cumple este requisito.
- **Coincidencia de nombres de host completos y nombres de host cortos:** para cumplir este requisito, puede duplicar las entradas de la tabla de hosts. De lo contrario, puede introducir todas las entradas de host de los dominios de servicio de nombres en una tabla de hosts principal del dominio de correo.
- **Varios dominios NIS en un dominio de correo:** para cumplir este requisito, puede duplicar las entradas de todas las tablas de hosts. De lo contrario, puede introducir todas las entradas de host de los dominios de servicio de nombres en una tabla de hosts principal del dominio de correo. Eficazmente, está fusionando varias tablas de hosts que son lógicas o físicas en una tabla de hosts. Por lo tanto, el mismo nombre de host no se puede volver a utilizar en el dominio de servicio de nombres múltiple que comparte un dominio de correo común.

Para obtener información sobre las tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313 en el Capítulo 13, “Servicios de correo \(tareas\)”](#).

## Interacciones de sendmail con NIS+ y DNS

En la siguiente lista, se describen las interacciones de sendmail con NIS+ y DNS, y se proporciona cierta orientación.

- **Nombre de dominio de correo:** si está configurando NIS+ como el servicio de nombres principal, sendmail puede comprobar el dominio de correo de la tabla `sendmailvars` NIS+. Esta tabla NIS+ tiene una columna de claves y una columna de valores. Para configurar el dominio de correo, debe agregar una entrada a esta tabla. Esta entrada debe tener la columna de claves establecida como la cadena literal `maildomain` y la columna de valores establecida como el nombre de dominio de correo. Un ejemplo es `admin.acme.com`. Aunque NIS+ permita cualquier cadena en la tabla `sendmailvars`, la regla de sufijo todavía se aplica para que el sistema de correo funcione correctamente. Puede utilizar `nistbladm` para agregar la entrada `maildomain` a la tabla `sendmailvars`. En el siguiente ejemplo, observe que el dominio de correo es un sufijo del dominio NIS+.

```
nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
```

- **Nombre de host Mailhost:** si la red utiliza NIS+ y DNS como el origen de la base de datos de hosts, puede incluir la entrada `mailhost` en la tabla de hosts NIS+ o DNS. Asegúrese de que los usuarios incluyan tanto a NIS+ como a DNS como el origen de la base de datos de hosts en el archivo `/etc/nsswitch.conf`.

- **Nombres de host completos:** tanto NIS+ como DNS “comprenden” nombres de host completos. Si se siguen los procedimientos de configuración regulares de NIS+ y DNS, se cumple este requisito.
- **Coincidencia de nombres de host completos y nombres de host cortos:** para cada entrada de host en la tabla de hosts NIS+, debe tener una entrada de host correspondiente en DNS.
- **Varios dominios NIS en un dominio de correo:** para cumplir este requisito, puede duplicar las entradas de todas las tablas de hosts. También puede introducir todas las entradas de host de los dominios de servicio de nombres en una tabla de hosts principal del dominio de correo.

Para obtener información sobre las tareas, consulte [“Administración de los archivos de alias de correo \(mapa de tareas\)” en la página 313](#) y [“Cómo usar DNS con sendmail” en la página 302](#) en el Capítulo 13, “Servicios de correo (tareas)”.

## Cambios en la versión 8.13 de sendmail

Aunque esta nueva versión de sendmail proporciona muchas funciones nuevas, la opción `FallBackSmartHost` es la más significativa. Gracias a esta opción, ya no es necesario utilizar `main.cf` ni `subsidiary.cf`. El archivo `main.cf` se usaba en entornos que admitían registros MX. El archivo `subsidiary.cf` se usaba en entornos que no contaban con un DNS totalmente operativo. En este tipo de entornos, se usaba un host inteligente en lugar de registros MX. La opción `FallBackSmartHost` proporciona una configuración unificada. Esta opción funciona como un registro MX que se usa como la última referencia posible para todos los entornos. Para garantizar la entrega de correo a los clientes, esta opción, cuando está habilitada, proporciona un host conectado (o inteligente) que sirve como copia de seguridad (o sistema de conmutación por error) para los registros MX que fallan.

Para obtener más información sobre la versión 8.13, consulte las secciones siguientes:

- [“Opciones de línea de comandos adicionales en la versión 8.13 de sendmail” en la página 385](#)
- [“Opciones de archivo de configuración revisadas y adicionales en la versión 8.13 de sendmail” en la página 385](#)
- [“Declaraciones FEATURE\(\) revisadas y adicionales en la versión 8.13 de sendmail” en la página 387](#)

Además, a partir de la versión Solaris 10 1/06, SMTP puede funcionar con la seguridad de la capa de transporte (TLS). Consulte la siguiente descripción.

## Compatibilidad para ejecutar SMTP con TLS en la versión 8.13 de sendmail

Las comunicaciones entre servidores y clientes SMTP, normalmente, no se controlan ni se consideran de confianza en cada extremo. Esta falta de seguridad puede permitir que un tercero supervise e incluso altere una comunicación entre un servidor y un cliente. A partir de la versión Solaris 10 1/06, SMTP puede utilizar la seguridad de capa de transporte (TLS) en la versión 8.13 de sendmail para resolver este problema. Este servicio ampliado para servidores y clientes SMTP proporciona lo siguiente:

- Comunicaciones autenticadas y privadas por medio de Internet
- Protección contra intrusos y atacantes

---

**Nota** – La implementación de TLS se basa en el protocolo de capa de sockets seguros (SSL).

---

STARTTLS es la palabra clave de SMTP que inicia una conexión SMTP segura mediante TLS. Esta conexión segura puede ocurrir entre dos servidores o entre un servidor y un cliente. Una conexión segura se define de la siguiente manera:

- La dirección de correo electrónico de origen y la dirección de destino están cifradas.
- El contenido del mensaje de correo electrónico está cifrado.

Cuando el cliente emite el comando STARTTLS, el servidor responde con una de las siguientes acciones:

- 220 Ready to start TLS
- 501 Syntax error (no parameters allowed)
- 454 TLS not available due to temporary reason

La respuesta 220 requiere que el cliente inicie la negociación TLS. La respuesta 501 nota que el cliente emitió incorrectamente el comando STARTTLS. STARTTLS se emite sin parámetros. La respuesta 454 exige que el cliente aplique valores de conjunto de reglas para determinar si va a aceptar o mantener la conexión.

Tenga en cuenta que para mantener la infraestructura SMTP de Internet, los servidores de uso público no deben requerir una negociación TLS. Sin embargo, un servidor que se utiliza de manera privada puede requerir que el cliente efectúe una negociación TLS. En esos casos, el servidor devuelve esta respuesta:

530 Must issue a STARTTLS command first

La respuesta 530 indica al cliente que emita el comando STARTTLS para establecer una conexión.

El servidor o el cliente puede rechazar una conexión si el nivel de autenticación y privacidad no es adecuado. Asimismo, dado que la mayoría de las conexiones SMTP no son seguras, el

servidor y el cliente pueden mantener una conexión no segura. La configuración del servidor y el cliente determina si se debe mantener o rechazar una conexión.

La compatibilidad para ejecutar SMTP con TLS no se encuentra habilitada de manera predeterminada. La TLS se habilita cuando el cliente SMTP emite el comando STARTTLS. Antes de que el cliente SMTP pueda emitir este comando, debe configurar los certificados que permiten que sendmail utilice TLS. Consulte [“Cómo configurar SMTP para que utilice TLS” en la página 307](#). Tenga en cuenta que este procedimiento incluye la definición de nuevas opciones de archivo de configuración y la reconstrucción del archivo `sendmail.cf`.

### Opciones de archivo de configuración para ejecutar SMTP con TLS

En la siguiente tabla, se describen las opciones de archivo de configuración que se utilizan para ejecutar SMTP con TLS. Si declara cualquiera de estas opciones, use una de las siguientes sintaxis:

- `0 OptionName=argument #` for the configuration file
- `-0 OptionName=argument #` for the command line
- `define('m4Name',argument) #` for m4 configuration

TABLA 14–13 Opciones de archivo de configuración para ejecutar SMTP con TLS

Opción	Descripción
CACertFile	<p>Nombre de m4: <code>confCACERT</code></p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene un certificado de autoridad de certificación.</p>
CACertPath	<p>Nombre de m4: <code>confCACERT_PATH</code></p> <p>Argumento: <i>ruta</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica la ruta al directorio que contiene certificados de autoridades de certificación.</p>
ClientCertFile	<p>Nombre de m4: <code>confCLIENT_CERT</code></p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene el certificado del cliente. Tenga en cuenta que este certificado se utiliza cuando sendmail actúa como cliente.</p>

TABLA 14-13 Opciones de archivo de configuración para ejecutar SMTP con TLS (Continuación)

Opción	Descripción
ClientKeyFile	<p>Nombre de m4: confCLIENT_KEY</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene la clave privada que pertenece al certificado del cliente.</p>
CRLFile	<p>Nombre de m4: confCRL</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene el estado de revocación del certificado, que se utiliza para la autenticación X.509v3.</p>
DHParameters	<p>Nombre de m4: confDH_PARAMETERS</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene los parámetros Diffie-Hellman (DH).</p>
RandFile	<p>Nombre de m4: confRAND_FILE</p> <p>Argumento: <i>file:nombre_archivo</i> o <i>egd:socket UNIX</i></p> <p>Valor predeterminado: sin definir</p> <p>Utiliza el prefijo <i>file:</i> para identificar el archivo que contiene datos aleatorios o utiliza el prefijo <i>egd:</i> para identificar el socket de UNIX. Tenga en cuenta que, debido a que el SO Solaris admite el dispositivo generador de números random, no es necesario especificar esta opción. Consulte la página del comando <code>man random(7D)</code>.</p>
ServerCertFile	<p>Nombre de m4: confSERVER_CERT</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: sin definir</p> <p>Identifica el archivo que contiene el certificado del servidor. Este certificado se utiliza cuando sendmail actúa como servidor.</p>
Timeout.starttls	<p>Nombre de m4: confTO_STARTTLS</p> <p>Argumento: <i>cantidad de tiempo</i></p> <p>Valor predeterminado: 1h</p> <p>Establece la cantidad de tiempo que el cliente SMTP espera una respuesta para el comando STARTTLS.</p>

TABLA 14-13 Opciones de archivo de configuración para ejecutar SMTP con TLS (Continuación)

Opción	Descripción
TLSSrvOptions	<p>Nombre de m4: confTLS_SRV_OPTIONS</p> <p>Argumento: V</p> <p>Valor predeterminado: sin definir</p> <p>Determina si el servidor solicita un certificado al cliente. Si esta opción está establecida en V, no se realiza la verificación del cliente.</p>

Para que sendmail admita el uso de TLS del SMTP, las siguientes opciones se deben definir:

- CACertPath
- CACertFile
- ServerCertFile
- ClientKeyFile

Otras opciones no son necesarias.

## Macros para ejecutar SMTP con TLS

En la tabla siguiente, se describen las macros utilizadas por el comando STARTTLS.

TABLA 14-14 Macros para ejecutar SMTP con TLS

Macro	Descripción
\${cert_issuer}	Contiene el nombre distinguido (DN) de la autoridad de certificación (CA), que es la emisora del certificado.
\${cert_subject}	Contiene el DN del certificado que se denomina <b>asunto de certificado</b> .
\${cn_issuer}	Contiene el nombre común (CN) de la autoridad de certificación (CA), que es la <b>emisora del certificado</b> .
\${cn_subject}	Contiene el CN del certificado que se denomina <b>asunto de certificado</b> .
\${tls_version}	Contiene la versión de TLS que se utiliza para la conexión.
\${cipher}	Contiene un conjunto de algoritmos criptográficos (conocido como <b>conjunto de cifrado</b> ) que se utiliza para la conexión.
\${cipher_bits}	Contiene en bits la longitud de clave del algoritmo de cifrado simétrico que se utiliza para la conexión.

TABLA 14-14    Macros para ejecutar SMTP con TLS    (Continuación)

Macro	Descripción
<code>\${verify}</code>	Contiene el resultado de la verificación del certificado que se ha presentado. Los valores posibles son los siguientes: <ul style="list-style-type: none"><li>■ OK: la verificación se completó con éxito.</li><li>■ NO: no se presentó ningún certificado.</li><li>■ NOT: no se solicitó ningún certificado.</li><li>■ FAIL: el certificado que se presentó no se pudo verificar.</li><li>■ NONE: STARTTLS no se ha realizado.</li><li>■ TEMP: se produjo un error temporal.</li><li>■ PROTOCOL: se produjo un error de SMTP.</li><li>■ SOFTWARE: el protocolo de enlace de STARTTLS falló.</li></ul>
<code>\${server_name}</code>	Contiene el nombre del servidor con la conexión SMTP saliente actual.
<code>\${server_addr}</code>	Contiene la dirección del servidor con la conexión SMTP saliente actual.

## Conjuntos de reglas para ejecutar SMTP con TLS

En la siguiente tabla, se describen los conjuntos de reglas que determinan si una conexión SMTP que utiliza TLS se debe aceptar, debe continuar o se debe rechazar.

TABLA 14-15    Conjuntos de reglas para ejecutar SMTP con TLS

Conjunto de reglas	Descripción
<code>tls_server</code>	Al actuar como un cliente, sendmail utiliza este conjunto de reglas para determinar si el servidor es actualmente admitido por TLS.
<code>tls_client</code>	Al actuar como un servidor, sendmail utiliza este conjunto de reglas para determinar si el cliente es actualmente admitido por TLS.
<code>tls_rcpt</code>	Este conjunto de reglas requiere la verificación del MTA del destinatario. Esta restricción del destinatario hace que los ataques, como la falsificación del DNS, sean imposibles.
<code>TLS_connection</code>	Este conjunto de reglas comprueba el requisito especificado por el RHS del mapa de acceso con los parámetros reales de la conexión TLS actual.
<code>try_tls</code>	sendmail utiliza este conjunto de reglas para determinar la viabilidad de utilizar STARTTLS al conectarse a otro MTA. Si el MTA no puede implementar correctamente STARTTLS, STARTTLS no se utiliza.

Para obtener más información, consulte <http://www.sendmail.org/m4/starttls.html>.



## Consideraciones de seguridad relacionadas con la ejecución de SMTP con TLS

Como un protocolo de correo estándar que define servicios de envío de correo que se ejecutan por medio de Internet, SMTP no es un mecanismo de extremo a extremo. Debido a la limitación de este protocolo, la seguridad TLS mediante SMTP no incluye agentes de usuario de correo. Los agentes de usuario de correo actúan como una interfaz entre los usuarios y un agente de transferencia de correo, como sendmail.

Además, el correo podría ser enrutado mediante varios servidores. Para obtener una seguridad SMTP completa, toda la cadena de conexiones SMTP debe admitir TLS.

Por último, se debe tener en cuenta el nivel de autenticación y privacidad negociadas entre cada par de servidores o un par de cliente y servidor. Para obtener más información, consulte “Servicios de autenticación” de *Guía de administración del sistema: servicios de seguridad*.

## Opciones de línea de comandos adicionales en la versión 8.13 de sendmail

En la siguiente tabla, se describen opciones de línea de comandos adicionales que están disponibles en la versión 8.13 de sendmail. Otras opciones de línea de comandos se describen en la página del comando `man sendmail(1M)`.

TABLA 14–16 Opciones de línea de comandos disponibles en la versión 8.13 de sendmail

Opción	Descripción
-D logfile	Envía la salida de depuración al archivo de registro (logfile) indicado, en lugar de incluir esta información con la salida estándar.
-q[!]Qsubstr	Especifica el procesamiento de trabajos en cuarentena que tienen esta subcadena (substr), que es una subcadena del motivo (reason) en cuarentena. Consulte la descripción de la opción -Qreason. Si ! se agrega, esta opción procesa los trabajos en cuarentena que no tienen esta subcadena (substr).
-Qreason	Pone en cuarentena un elemento de cola normal con este motivo (reason). Si no se especifica ningún motivo (reason), el elemento de la cola en cuarentena se quita de la cuarentena. Esta opción funciona con la opción -q[!]Qsubstr. substr es una parte (o subcadena) de reason.

## Opciones de archivo de configuración revisadas y adicionales en la versión 8.13 de sendmail

En la siguiente tabla, se describen las opciones de archivo de configuración revisadas y agregadas. Si declara cualquiera de estas opciones, use una de las siguientes sintaxis.

```
0 OptionName=argument      # for the configuration file
-0 OptionName=argument      # for the command line
define('m4Name',argument)  # for m4 configuration
```

TABLA 14-17 Opciones de archivo de configuración disponibles en la versión 8.13 de sendmail

Opción	Descripción
ConnectionRateWindowSize	<p>Nombre de m4: confCONNECTION_RATE_WINDOW_SIZE</p> <p>Argumento: <i>número</i></p> <p>Valor predeterminado: 60</p> <p>Define el número de segundos para las conexiones entrantes que se deben mantener.</p>
FallBackSmarthost	<p>Nombre de m4: confFALLBACK_SMARTHOST</p> <p>Argumento: <i>nombre_host</i></p> <p>Para garantizar la entrega de correo a los clientes, esta opción proporciona un host conectado que sirve como copia de seguridad (o sistema de conmutación por error) para los registros MX que fallan.</p>
InputMailFilters	<p>Nombre de m4: confINPUT_MAIL_FILTERS</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Muestra los filtros de correo de entrada para el daemon sendmail.</p>
PidFile	<p>Nombre de m4: confPID_FILE</p> <p>Argumento: <i>nombre_archivo</i></p> <p>Valor predeterminado: /var/run/sendmail.pid</p> <p>Como en las versiones anteriores, el nombre del archivo es expandido de macro antes de abrirse. Además, en la versión 8.13, el archivo se desvincula cuando sendmail se cierra.</p>
QueueSortOrder	<p>Nombre de m4: confQUEUE_SORT_ORDER</p> <p>Argumento agregado: none</p> <p>En la versión 8.13, none se utiliza para especificar que no hay ningún orden de clasificación.</p>
RejectLogInterval	<p>Nombre de m4: confREJECT_LOG_INTERVAL</p> <p>Argumento: <i>período de tiempo</i></p> <p>Valor predeterminado: 3h, que representa tres horas.</p> <p>Cuando una conexión de daemon se rechaza para el período (<i>period-of-time</i>) especificado, la información se registra.</p>

TABLA 14-17 Opciones de archivo de configuración disponibles en la versión 8.13 de sendmail (Continuación)

Opción	Descripción
SuperSafe	Nombre de m4: confSAFE_QUEUE  Nombre corto: s  Argumento agregado: postmilter  Valor predeterminado: true  Si postmilter está configurado, sendmail aplaza la sincronización del archivo de cola hasta que todas las milters hayan indicado la aceptación del mensaje. Para que este argumento sea útil, sendmail debe ejecutarse como un servidor SMTP. De lo contrario, postmilter funcionaría como si se estuviera utilizando el argumento true.

## Declaraciones FEATURE ( ) revisadas y adicionales en la versión 8.13 de sendmail

En la siguiente tabla, se describen las declaraciones FEATURE ( ) revisadas y agregadas. Esta macro m4 utiliza la siguiente sintaxis.

FEATURE('name', 'argument')

TABLA 14-18 Declaraciones FEATURE ( ) disponibles en la versión 8.13 de sendmail

Nombre de FEATURE ( )	Descripción
conncontrol	Funciona con el conjunto de reglas access_db para comprobar el número de conexiones SMTP entrantes. Para obtener detalles, consulte /etc/mail/cf/README.
greet_pause	Agrega el conjunto de reglas greet_pause, que habilita la protección contra el proxy abierto y el slamming de SMTP. Para obtener detalles, consulte /etc/mail/cf/README.
local_lmtp	El argumento predeterminado sigue siendo mail.local, que es la aplicación de correo compatible con LMTP en esta versión de Solaris. Sin embargo, en la versión 8.13, si se utiliza una aplicación de correo compatible con LMTP diferente, el nombre de la ruta se puede especificar como un segundo parámetro, y los argumentos que se transfieren al segundo parámetro se pueden especificar en el tercer parámetro. Por ejemplo:  FEATURE('local_lmtp', '/usr/local/bin/lmtp', 'lmtp')
mtamark	Proporciona compatibilidad experimental para la marcación de agentes de transferencia de correo en DNS invertido con registros de recursos TXT (MTAMark). Para obtener detalles, consulte /etc/mail/cf/README.
ratecontrol	Funciona con el conjunto de reglas access_db para controlar tasas de conexión para hosts. Para obtener detalles, consulte /etc/mail/cf/README.
use_client_ptr	Si esta FEATURE ( ) está habilitada, el conjunto de reglas check_relay sustituye su primer argumento con este argumento, \${client_ptr}.

## Cambios de la versión 8.12 de sendmail

Esta sección contiene información sobre los siguientes temas.

- “Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail” en la página 388
- “Archivo de configuración `submit.cf` de la versión 8.12 de sendmail” en la página 389
- “Opciones de línea de comandos descartadas o adicionales de la versión 8.12 de sendmail” en la página 391
- “Argumentos adicionales para las opciones `PidFile` y `ProcessTitlePrefix` de la versión 8.12 de sendmail” en la página 392
- “Macros definidas adicionales de la versión 8.12 de sendmail” en la página 392
- “Macros adicionales de la versión 8.12 de sendmail” en la página 393
- “Macros `MAX` adicionales de la versión 8.12 de sendmail” en la página 394
- “Macros de configuración `m4` revisadas y adicionales de la versión 8.12 de sendmail” en la página 395
- “Cambios en la declaración `FEATURE()` de la versión 8.12 de sendmail” en la página 395
- “Cambios en la declaración `MAILER()` de la versión 8.12 de sendmail” en la página 398
- “Indicadores de agente de entrega adicionales de la versión 8.12 de sendmail” en la página 399
- “Ecuaciones adicionales para agentes de entrega de la versión 8.12 de sendmail” en la página 400
- “Funciones de cola adicionales de la versión 8.12 de sendmail” en la página 401
- “Cambios en `LDAP` de la versión 8.12 de sendmail” en la página 401
- “Cambio en la aplicación de correo integrada de la versión 8.12 de sendmail” en la página 403
- “Conjuntos de reglas adicionales de la versión 8.12 de sendmail” en la página 403
- “Cambios en los archivos de la versión 8.12 de sendmail” en la página 404
- “Versión 8.12 de sendmail y direcciones IPv6 en configuración” en la página 405

## Compatibilidad con envoltorios TCP de la versión 8.12 de sendmail

Los envoltorios TCP proporcionan una forma de implementar controles de acceso comprobando que la dirección del host que solicita un servicio de red concreto aparece en una lista de control de acceso (ACL). Las solicitudes se conceden o se deniegan en función de ello. Además de proporcionar este mecanismo de control de acceso, los envoltorios TCP también registran solicitudes de los hosts para servicios de red, lo que constituye una función de supervisión muy útil. Entre los ejemplos de los servicios de red que se pueden someter al control de acceso, se incluyen `rlogind`, `telnetd` y `ftpd`.

A partir de la versión 8.12, `sendmail` permite el uso de envoltorios TCP. Esta comprobación no supone la omisión de otras medidas de seguridad. Al habilitar los envoltorios TCP en `sendmail`, se ha agregado una comprobación para validar el origen de una solicitud de red antes de que se acceda a dicha solicitud. Consulte la página del comando `man hosts_access(4)`.

---

**Nota** – La compatibilidad con envoltorios TCP en `inetd(1M)` y `sshd(1M)` comenzó con la versión Solaris 9.

---

Para obtener información sobre las ACL, consulte [“Uso de listas de control de acceso para proteger archivos UFS” de \*Guía de administración del sistema: servicios de seguridad\*](#).

## Archivo de configuración `submit.cf` de la versión 8.12 de sendmail

A partir de la versión 8.12, sendmail incluye un archivo de configuración adicional, `/etc/mail/submit.cf`. Este archivo, `submit.cf`, se utiliza para ejecutar sendmail en modo de programa de envío de correo, en lugar de ejecutarlo en modo de daemon. El modo de programa de envío de correo, a diferencia del modo de daemon, no requiere el privilegio root, por lo que este nuevo paradigma proporciona una mejor seguridad.

Consulte la lista siguiente de funciones para `submit.cf`:

- sendmail usa `submit.cf` para ejecutarse en modo de programa de envío de correo (MSP), que envía mensajes de correo electrónico y puede ser iniciado por programas (como `mailx`) y por usuarios. Consulte las descripciones de la opción `-Ac` y la opción `-Am` en la página del comando man [sendmail\(1M\)](#).
- `submit.cf` se utiliza en los siguientes modos de operación:
  - `-bm`, que es el modo de operación predeterminado
  - `-bs`, que utiliza la entrada estándar para ejecutar SMTP
  - `-bt`, que es el modo de prueba que se utiliza para resolver direcciones
- sendmail, al utilizar `submit.cf`, no se ejecuta como un daemon de SMTP.
- sendmail, al utilizar `submit.cf`, utiliza `/var/spool/clientmqueue`, la cola de correo exclusiva del cliente, que contiene mensajes que no se han entregado al daemon sendmail. Los mensajes en la cola exclusiva del cliente son entregados por el “daemon” del cliente, que realmente actúa como un ejecutor de colas de clientes.
- De manera predeterminada, sendmail utiliza `submit.cf` periódicamente para ejecutar la cola MSP (también conocida como la cola exclusiva del cliente), `/var/spool/clientmqueue`.

```
/usr/lib/sendmail -Ac -q15m
```

Tenga en cuenta lo siguiente:

- A partir de la versión Solaris 9, `submit.cf` se proporciona automáticamente.
- `submit.cf` no requiere planificación ni procedimientos preliminares antes de la instalación de Solaris 9 o una versión más reciente.

- A menos que especifique un archivo de configuración, sendmail utiliza automáticamente `submit.cf` según sea necesario. Básicamente, sendmail sabe qué tareas son adecuadas para `submit.cf` y qué tareas son adecuadas para `sendmail.cf`.

## Funciones que distinguen `sendmail.cf` de `submit.cf`

El archivo de configuración `sendmail.cf` es para el modo de daemon. Al utilizar este archivo, sendmail actúa como un agente de transferencia de correo (MTA), que es iniciado por root.

```
/usr/lib/sendmail -L sm-mta -bd -qlh
```

Consulte la siguiente lista de otras funciones distintivas para `sendmail.cf`:

- De manera predeterminada, `sendmail.cf` acepta las conexiones SMTP en los puertos 25 y 587.
- De manera predeterminada, `sendmail.cf` ejecuta la cola principal, `/var/spool/mqueue`.

## Cambios funcionales de la versión 8.12 de sendmail

Con la adición de `submit.cf`, se produjeron los siguientes cambios funcionales:

- A partir de la versión 8.12 de sendmail, sólo root puede ejecutar la cola de correo. Para obtener más información, consulte los cambios que se describen en la página del comando `man mailq(1)`. Para obtener más información sobre las tareas, consulte [“Administración de los directorios de la cola \(mapa de tareas\)” en la página 324](#).
- El modo de programa de envío de correo se ejecuta sin el privilegio root, que puede impedir que sendmail tenga acceso a determinados archivos (como los archivos `.forward`). Por lo tanto, la opción `-bv` para sendmail podría dar al usuario una salida engañosa. No hay ninguna solución disponible.
- Antes de la versión 8.12 de sendmail, si no ejecutaba sendmail en modo de daemon, sólo impedía la entrega de correo entrante. A partir de la versión 8.12 de sendmail, si no ejecuta el daemon sendmail con la configuración predeterminada, también impide la entrega de correo saliente. El ejecutor de colas de clientes (también conocido como el programa de envío de correo) debe poder enviar el correo al daemon en el puerto SMTP local. Si el ejecutor de colas de clientes intenta abrir una sesión SMTP con el host local y el daemon no está escuchando en el puerto SMTP, el correo permanece en la cola. La configuración predeterminada ejecuta un daemon, por lo que este problema no se produce si está utilizando la configuración predeterminada. Sin embargo, si ha deshabilitado el daemon, consulte [“Cómo gestionar la entrega de correo mediante una configuración alternativa de `sendmail.cf`” en la página 312](#) para conocer una manera de resolver este problema.

## Opciones de línea de comandos descartadas o adicionales de la versión 8.12 de sendmail

En la siguiente tabla, se describen las opciones de línea de comandos descartadas o adicionales para sendmail. Otras opciones de línea de comandos se describen en la página del comando man [sendmail\(1M\)](#).

TABLA 14-19 Opciones de línea de comandos descartadas o adicionales de la versión 8.12 de sendmail

Opción	Descripción
-Ac	Indica que desea utilizar el archivo de configuración, <code>submit.cf</code> , incluso si el modo de operación no indica un envío de correo inicial. Para obtener más información sobre <code>submit.cf</code> , consulte “ <a href="#">Archivo de configuración submit.cf de la versión 8.12 de sendmail</a> ” en la página 389.
-Am	Indica que desea utilizar el archivo de configuración, <code>sendmail.cf</code> , incluso si el modo de operación indica un envío de correo inicial. Para obtener más información, consulte “ <a href="#">Archivo de configuración submit.cf de la versión 8.12 de sendmail</a> ” en la página 389.
-bP	Indica que está imprimiendo el número de entradas en cada cola.
-G	Indica que el mensaje que se está enviando desde la línea de comandos es para la retransmisión, y no para el envío inicial. El mensaje se rechaza si las direcciones no están completas. No se realiza ninguna canonización. Como se señala en las notas de la versión que forman parte de la distribución de sendmail en <a href="http://ftp.sendmail.org">ftp://ftp.sendmail.org</a> , es posible que los mensajes que no están formados correctamente se rechacen en futuras versiones.
-L <i>etiqueta</i>	Establece el identificador que se utiliza para los mensajes syslog como la <i>etiqueta</i> proporcionada.
-q[!]I <i>subcadena</i>	Procesa sólo los trabajos que contienen esta <i>subcadena</i> de uno de los destinatarios. Cuando ! se agrega, la opción sólo procesa los trabajos que no tienen esta <i>subcadena</i> de uno de los destinatarios.
-q[!]R <i>subcadena</i>	Procesa sólo los trabajos que contienen esta <i>subcadena</i> del ID de cola. Cuando ! se agrega, la opción sólo procesa los trabajos que no tienen esta <i>subcadena</i> del ID de cola.
-q[!]S <i>subcadena</i>	Procesa sólo los trabajos que contienen esta <i>subcadena</i> del remitente. Cuando ! se agrega, la opción sólo procesa los trabajos que no tienen esta <i>subcadena</i> del remitente.
-qf	Procesa los mensajes guardados en la cola una vez, sin usar la llamada del sistema <code>fork</code> , y ejecuta el proceso en primer plano. Consulte la página del comando man <a href="#">fork(2)</a> .
-qG <i>nombre</i>	Procesa sólo los mensajes en el grupo de colas <i>nombre</i> .
-q <i>tiempo</i>	Procesa los mensajes guardados en la cola en un intervalo específico de tiempo con un solo secundario que se bifurca para cada cola. El secundario permanece inactivo entre las ejecuciones de colas. Esta nueva opción es similar a <i>-qtiempo</i> , que periódicamente bifurca un secundario para procesar la cola.
-U	Como se señala en las notas de la versión que forman parte de la distribución de sendmail en <a href="http://ftp.sendmail.org">ftp://ftp.sendmail.org</a> , esta opción no está disponible a partir de la versión 8.12. Los agentes de usuario de correo deben utilizar el argumento -G.

# Argumentos adicionales para las opciones PidFile y ProcessTitlePrefix de la versión 8.12 de sendmail

En la siguiente tabla, se describen los argumentos procesados con macro adicionales para las opciones PidFile y ProcessTitlePrefix. Para obtener más información sobre estas opciones, consulte la página del comando man [sendmail\(1M\)](#).

TABLA 14-20 Argumentos para las opciones PidFile y ProcessTitlePrefix

Macro	Descripción
`\${daemon_addr}`	Proporciona la dirección del daemon (por ejemplo, 0.0.0.0)
`\${daemon_family}`	Proporciona la familia del daemon (por ejemplo, inet e inet6)
`\${daemon_info}`	Proporciona información sobre el daemon (por ejemplo, SMTP+queueing@00:30:00)
`\${daemon_name}`	Proporciona el nombre del daemon (por ejemplo, MSA)
`\${daemon_port}`	Proporciona el puerto del daemon (por ejemplo, 25)
`\${queue_interval}`	Proporciona el intervalo de ejecución de cola (por ejemplo, 00:30:00)

# Macros definidas adicionales de la versión 8.12 de sendmail

En la siguiente tabla, se describen las macros adicionales que se reservan para ser utilizadas por el programa sendmail. Los valores de las macros se asignan internamente. Para obtener más información, consulte la página del comando man [sendmail\(1M\)](#).

TABLA 14-21 Macros definidas adicionales para sendmail

Macro	Descripción
`\${addr_type}`	Identifica la dirección actual como una dirección de destinatario o remitente del sobre.
`\${client_resolve}`	Contiene el resultado de la llamada resolver para `\${client_name}`: OK, FAIL, FORGED o TEMP.
`\${deliveryMode}`	Especifica el modo de entrega actual que sendmail utiliza, en lugar del valor de la opción DeliveryMode.
`\${dsn_notify}`,`\${dsn_envid}`,`\${dsn_ret}`	Contiene los valores de parámetros DSN correspondientes.



TABLA 14–21    Macros definidas adicionales para sendmail    (Continuación)

Macro	Descripción
<code>\${if_addr}</code>	Proporciona la dirección de la interfaz para la conexión entrante si la interfaz no pertenece a la red de bucle de retorno. Esta macro es especialmente útil para el hospedaje virtual.
<code>\${if_addr_out}</code> , <code>\${if_name_out}</code> , <code>\${if_family_out}</code>	Evita la reutilización de <code>\${if_addr}</code> . Contiene los siguientes valores respectivamente:  La dirección de la interfaz para la conexión saliente  El nombre de host de la interfaz para la conexión saliente  La familia de la interfaz para la conexión saliente
<code>\${if_name}</code>	Proporciona el nombre de host de la interfaz para la conexión entrante y es especialmente útil para el hospedaje virtual.
<code>\${load_avg}</code>	Comprueba e informa el número medio actual de trabajos en la cola de ejecución.
<code>\${msg_size}</code>	Contiene el valor del tamaño del mensaje ( <code>SIZE=parameter</code> ) en un diálogo ESMTP antes de que el mensaje se recopile. A partir de ese momento, la macro almacena el tamaño del mensaje según lo calculado por sendmail y se utiliza en <code>check_compat</code> . Para obtener información sobre <code>check_compat</code> , consulte la <a href="#">Tabla 14–25</a> .
<code>\${nrcpts}</code>	Contiene el número de destinatarios validados.
<code>\${ntries}</code>	Contiene el número de intentos de entrega.
<code>\${rcpt_mailer}</code> , <code>\${rcpt_host}</code> , <code>\${rcpt_addr}</code> , <code>\${mail_mailer}</code> , <code>\${mail_host}</code> , <code>\${mail_addr}</code>	Contiene los resultados del análisis de los argumentos RCPT y MAIL, que es el tripló (RHS) del lado derecho resuelto del agente de entrega de correo ( <code>##mailer</code> ), el host ( <code>\$@host</code> ) y el usuario ( <code>\$:addr</code> ).

## Macros adicionales de la versión 8.12 de sendmail

En esta sección, puede encontrar una tabla que describe las macros adicionales que se utilizan para crear el archivo de configuración de sendmail.

TABLA 14–22    Macros adicionales utilizadas para crear el archivo de configuración de sendmail

Macro	Descripción
LOCAL_MAILER_EOL	Sustituye la cadena de fin de línea predeterminada para la aplicación de correo local.
LOCAL_MAILER_FLAGS	Agrega el encabezado Return-Path: de manera predeterminada.
MAIL_SETTINGS_DIR	Contiene la ruta (incluida la barra diagonal final) para el directorio de configuración de correo.
MODIFY_MAILER_FLAGS	Mejora el *_MAILER_FLAGS. Esta macro establece, agrega o elimina indicadores.
RELAY_MAILER_FLAGS	Define indicadores adicionales para la aplicación de correo de retransmisión.

## Macros MAX adicionales de la versión 8.12 de sendmail

Use las siguientes macros para configurar el número máximo de comandos que se pueden recibir antes de que sendmail lentifique su entrega. Puede definir estas macros MAX en el tiempo de compilación. Los valores máximos en la siguiente tabla también representan los valores predeterminados actuales.

TABLA 14–23    Macros MAX adicionales

Macro	Valor máximo	Comandos comprobados por cada macro
MAXBADCOMMANDS	25	Comandos desconocidos
MAXNOOPCOMMANDS	20	NOOP, VERB, ONEX, XUSR
MAXHELOCOMMANDS	3	HELO, EHLO
MAXVRFYCOMMANDS	6	VRFY, EXPN
MAXETRNCOMMANDS	8	ETRN

**Nota** – Puede deshabilitar la comprobación de una macro estableciendo el valor de la macro en cero.

# Macros de configuración m4 revisadas y adicionales de la versión 8.12 de sendmail

Esta sección contiene una tabla de macros de configuración m4 revisadas y adicionales para sendmail. Utilice la siguiente sintaxis para declarar estas macros.

```
symbolic-name('value')
```

Si necesita crear un nuevo archivo `sendmail.cf`, consulte [“Modificación de la configuración de sendmail” en la página 303](#) en el [Capítulo 13, “Servicios de correo \(tareass\)”](#).

TABLA 14–24 Macros de configuración m4 revisadas y adicionales para sendmail

Macro m4	Descripción
FEATURE()	Para obtener detalles, consulte <a href="#">“Cambios en la declaración FEATURE() de la versión 8.12 de sendmail” en la página 395</a> .
LOCAL_DOMAIN()	Esta macro agrega entradas a la clase <code>w</code> ( <code>\$=w</code> ).
MASQUERADE_EXCEPTION()	Una nueva macro que define hosts o subdominios que no se pueden enmascarar.
SMART_HOST()	Esta macro ahora puede usarse para direcciones entre corchetes, como <code>user@[host]</code> .
VIRTUSER_DOMAIN() o VIRTUSER_DOMAIN_FILE()	Cuando estas macros se utilizan, incluya <code>#{VirtHost}</code> en <code>\$=R</code> . Como recordatorio, <code>\$=R</code> es el conjunto de nombres de host que tienen permitido realizar la retransmisión.

## Cambios en la declaración FEATURE() de la versión 8.12 de sendmail

Consulte las tablas siguientes para obtener información sobre los cambios específicos realizados en las declaraciones `FEATURE()`.

Para utilizar los nombres de `FEATURE` revisados y nuevos, use la sintaxis siguiente.

```
FEATURE('name', 'argument')
```

Si necesita crear un nuevo archivo `sendmail.cf`, consulte [“Modificación de la configuración de sendmail” en la página 303](#) en el [Capítulo 13, “Servicios de correo \(tareass\)”](#).

TABLA 14–25 Declaraciones FEATURE ( ) revisadas y adicionales

Nombre de FEATURE ( )	Descripción
compat_check	<p>Argumento: consulte el ejemplo en el siguiente párrafo.</p> <p>Esta nueva FEATURE ( ) le permite buscar una clave en el mapa de acceso que consta de la dirección del remitente y la dirección del destinatario. Esta FEATURE ( ) está delimitada por la siguiente cadena: &lt;@&gt;. <i>emisor@sdomain</i>&lt;@&gt;<i>destinatario @rdomain</i> es un ejemplo.</p>
delay_checks	<p>Argumento: friend, que permite realizar una prueba spam-friend o hater, que permite realizar una prueba spam-hater.</p> <p>Una nueva FEATURE ( ) que retrasa todas las comprobaciones. Al utilizar FEATURE ( 'delay_checks' ), los conjuntos de reglas check_mail y check_relay no se llaman cuando un cliente se conecta o ejecuta un comando MAIL respectivamente. En cambio, estos conjuntos de reglas son llamados por el conjunto de reglas check_rcpt. Para obtener detalles, consulte el archivo /etc/mail/cf/README.</p>
dnsbl	<p>Argumento: esta FEATURE ( ) acepta un máximo de dos argumentos:</p> <ul style="list-style-type: none"><li>■ Nombre del servidor DNS</li><li>■ Mensaje de rechazo</li></ul> <p>Una nueva FEATURE ( ) que se puede incluir varias veces para comprobar los valores devueltos para búsquedas de DNS. Tenga en cuenta que esta FEATURE ( ) permite especificar el comportamiento de errores de consulta temporales.</p>
enhdnsbl	<p>Argumento: nombre de dominio.</p> <p>Una nueva FEATURE ( ) que es una versión mejorada de dnsbl, que le permite comprobar los valores devueltos para búsquedas de DNS. Para obtener más información, consulte /etc/mail/cf/README.</p>
generics_entire_domain	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE ( ) que también puede utilizar para aplicar genericstable a subdominios de \$=G.</p>
ldap_routing	<p>Argumento: para ver detalles, consulte las notas de la versión en <a href="http://www.sendmail.org">http://www.sendmail.org</a>.</p> <p>Una nueva FEATURE ( ) que implementa el enrutamiento de direcciones LDAP.</p>
local_lmtp	<p>Argumento: nombre de ruta de una aplicación de correo compatible con LMTP. El valor predeterminado es mail.local, que es compatible con LMTP en esta versión de Solaris.</p> <p>Una FEATURE ( ) que ahora establece el tipo de código de diagnóstico de notificación de estado de entrega (DSN) para la aplicación de correo local en el valor adecuado de SMTP.</p>

TABLA 14–25 Declaraciones FEATURE() revisadas y adicionales (Continuación)

Nombre de FEATURE()	Descripción
local_no_masquerade	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que puede utilizar para evitar el enmascaramiento de la aplicación de correo local.</p>
lookupdotdomain	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que también puede utilizar para buscar <i>.domain</i> en el mapa de acceso.</p>
nocanonicalfy	<p>Argumento: canonicalfy_hosts o nada.</p> <p>Una FEATURE() que ahora incluye las siguientes características.</p> <p>Permite una lista de dominios, especificada por CANONIFY_DOMAIN o CANONIFY_DOMAIN_FILE, que se transferirán a los operadores \$[ y \$] para la canonización.</p> <p>Permite que las direcciones que sólo tienen un nombre de host, como &lt;user@host&gt;, sean canonizadas si canonicalfy_hosts se especifica como su parámetro.</p> <p>Agrega un punto final a las direcciones con más de un componente.</p>
no_default_msa	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que desactiva la configuración predeterminada de sendmail de los archivos de configuración generados por m4 para “escuchar” en varios puertos diferentes, una implementación de RFC 2476.</p>
nouucp	<p>Argumento: reject, que no permite el token ! o nospecial, que permite el token !.</p> <p>Una FEATURE() que determina si se debe permitir el token ! en la parte local de una dirección.</p>
nullclient	<p>Argumento: ninguno.</p> <p>Una FEATURE() que ahora proporciona los conjuntos de reglas completos de una configuración normal, lo que permite la realización de controles contra el correo no deseado.</p>
preserve_local_plus_detail	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que permite mantener la parte +detail de la dirección cuando sendmail pasa la dirección al agente de entrega local.</p>
preserve_luser_host	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que permite conservar el nombre del host receptor si se utiliza LUSER_RELAY.</p>
queugroup	<p>Argumento: ninguno.</p> <p>Una nueva FEATURE() que le permite seleccionar un grupo de colas que se basa en la dirección de correo electrónico completa o en el dominio del destinatario.</p>

TABLA 14–25 Declaraciones FEATURE ( ) revisadas y adicionales (Continuación)

Nombre de FEATURE ( )	Descripción
relay_mail_from	Argumento: el dominio ( <i>dominio</i> ) es un argumento opcional.  Una nueva FEATURE ( ) que permite retransmitir si el remitente del correo aparece como RELAY en el mapa de acceso y está etiquetado con la línea del encabezado From: . Si se indica el argumento <i>domain</i> opcional, la parte del dominio del remitente del correo también se comprueba.
virtuser_entire_domain	Argumento: ninguno.  Una FEATURE ( ) que ahora puede utilizar para aplicar $\$=\{\text{VirtHost}\}$ , una nueva clase para comparar entradas virtusertable que pueden ser rellenas por VIRTUSER_DOMAIN o VIRTUSER_DOMAIN_FILE.  FEATURE (‘virtuser_entire_domain’) también puede aplicar la clase $\$=\{\text{VirtHost}\}$ a subdominios completos.

Las siguientes declaraciones FEATURE ( ) ya no son admitidas.

TABLA 14–26 Declaraciones FEATURE ( ) no admitidas

Nombre de FEATURE ( )	Sustitución
rbl	FEATURE (‘dnsbl’) y FEATURE (‘enhdnsbl’) reemplazan esta FEATURE ( ), que ha sido eliminada.
remote_mode	MASQUERADE_AS (‘\$S’) reemplaza a FEATURE (‘remote_mode’) en /etc/mail/cf/subsidiary.mc. \$S es el valor SMART_HOST en sendmail.cf.
sun_reverse_alias_files	FEATURE (‘genericstable’).
sun_reverse_alias_nis	FEATURE (‘genericstable’).
sun_reverse_alias_nisplus	FEATURE (‘genericstable’).

## Cambios en la declaración MAILER ( ) de la versión 8.12 de sendmail

La declaración MAILER ( ) especifica la compatibilidad con agentes de entrega. Para declarar un agente de entrega, utilice la siguiente sintaxis.

MAILER (‘*symbolic-name*’)

Tenga en cuenta los siguientes cambios.

- En esta nueva versión de sendmail, la declaración MAILER('smtp') ahora incluye una aplicación de correo adicional, dsmtplib, que proporciona entrega a petición utilizando el indicador de aplicación de correo F=%. La definición de la aplicación de correo dsmtplib utiliza la nueva DSMTP\_MAILER\_ARGS, que se establece de manera predeterminada en IPC \$h.
- Los números para conjuntos de reglas utilizados por MAILER se han eliminado. Ahora no tiene ningún orden requerido para enumerar MAILER, excepto MAILER('uucp'), que debe seguir a MAILER('smtp') si uucp-dom y uucp-uudom se utilizan.

Para obtener más información sobre los servicios de envío de correo, consulte [“Servicios de envío de correo y sendmail” en la página 344](#). Si necesita crear un nuevo archivo sendmail.cf, consulte [“Modificación de la configuración de sendmail” en la página 303](#) en el [Capítulo 13](#), [“Servicios de correo \(tarear\)”](#).

## Indicadores de agente de entrega adicionales de la versión 8.12 de sendmail

En la siguiente tabla, se describen indicadores de agente de entrega adicionales, que, de manera predeterminada, no están establecidos. Estos indicadores de un solo carácter son booleanos. Puede establecer o anular un indicador mediante su inclusión o exclusión en la instrucción F= del archivo de configuración, como se muestra en el siguiente ejemplo.

```
Mlocal,      P=/usr/lib/mail.local, F=lsDFMAw5:/|@qSXfmnz9, S=10/30, R=20/40,
Mprog,       P=/bin/sh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
Msmtp,       P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
Mesmtplib,   P=[IPC], F=mDFMuXa, S=11/31, R=21, E=\r\n, L=990,
Msmtp8,      P=[IPC], F=mDFMuX8, S=11/31, R=21, E=\r\n, L=990,
Mrelay,      P=[IPC], F=mDFMuXa8, S=11/31, R=61, E=\r\n, L=2040,
```

**TABLA 14-27** Indicadores de aplicación de correo adicionales

Indicador	Descripción
%	Los servicios de envío de correo que utilizan este indicador no intentan la entrega al destinatario inicial de un mensaje ni a ejecuciones de colas, a menos que el mensaje en cola se seleccione utilizando una solicitud ETRN o una de las siguientes opciones de cola: -qI, -qR o -qS.
1	Este indicador deshabilita la capacidad de la aplicación de correo de enviar caracteres nulos (por ejemplo, \0).
2	Este indicador deshabilita el uso de ESMTP y requiere que SMTP se utilice en su lugar.
6	Este indicador permite que los servicios de envío de correo filtren encabezados a 7 bits.

# Ecuaciones adicionales para agentes de entrega de la versión 8.12 de sendmail

En la siguiente tabla, se describen ecuaciones adicionales que puede utilizar con el comando de definición de agente de entrega M. La siguiente sintaxis muestra cómo anexas nuevas ecuaciones o nuevos argumentos a las ecuaciones que ya existen en el archivo de configuración.

*Magent-name, equate, equate, ...*

El ejemplo siguiente incluye la nueva ecuación W=. Esta ecuación especifica el tiempo máximo que se va a esperar para que la aplicación de correo regrese después de que todos los datos se han enviado.

Msmtp, P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990, W=2m

Al modificar la definición de un valor de la configuración m4, utilice la sintaxis que se proporciona en el ejemplo siguiente.

```
define('SMTP_MAILER_MAXMSG', '1000')
```

El ejemplo anterior establece un límite de 1000 en el número de mensajes que se entregan por conexión en una aplicación de correo smtp.

Si necesita crear un nuevo archivo sendmail.cf, consulte [“Modificación de la configuración de sendmail” en la página 303 en el Capítulo 13, “Servicios de correo \(tareass\)”](#).

**Nota** – Normalmente, puede modificar las definiciones de ecuación en el directorio mailer sólo cuando realiza ajustes.

TABLA 14–28 Ecuaciones adicionales para agentes de entrega

Ecuación	Descripción
/=	Argumento: ruta a un directorio  Especifica un directorio al cual aplicar chroot() antes de que la aplicación de correo se ejecute
m=	Argumento: cualquiera de los siguientes valores m4 que se han definido previamente con la rutina define() SMTP_MAILER_MAXMSG, para la aplicación de correo smtp LOCAL_MAILER_MAXMSG, para la aplicación de correo local RELAY_MAILER_MAXMSG, para la aplicación de correo relay  Limita el número de mensajes que se entregan por conexión en una aplicación de correo smtp, local o relay



TABLA 14–28 Ecuaciones adicionales para agentes de entrega (Continuación)

Ecuación	Descripción
W=	Argumento: un incremento de tiempo  Especifica el tiempo máximo de espera para que la aplicación de correo regrese después de que todos los datos se han enviado

## Funciones de cola adicionales de la versión 8.12 de sendmail

La siguiente lista proporciona información sobre las funciones de cola adicionales.

- Esta versión admite varios directorios de cola. Para utilizar varias colas, incluya un valor de la opción `QueueDirectory` en el archivo de configuración que termine con un asterisco (\*), tal como se muestra en el ejemplo siguiente.  
  
`O QueueDirectory=/var/spool/mqueue/q*`  
  
El valor de la opción, `/var/spool/mqueue/q*`, utiliza todos los directorios (o enlaces simbólicos a directorios) que empiezan con "q" como directorios de cola. No cambie la estructura del directorio de cola mientras `sendmail` se está ejecutando. Las ejecuciones de cola crean un proceso independiente para ejecutar cada cola, a menos que el indicador detallado (-v) se utilice en una ejecución de cola no daemon. Los elementos nuevos se asignan aleatoriamente a una cola.
- El nuevo sistema de nomenclatura de archivos de cola utiliza nombres de archivos que están garantizados como exclusivos por 60 años. Este sistema permite que los ID de cola se asignen sin complejos bloqueos de sistemas de archivos y simplifica el movimiento de elementos en cola entre colas.
- A partir de la versión 8.12, sólo root puede ejecutar la cola de correo. Para obtener más información, consulte los cambios que se describen en la página del comando `man mailq(1)`. Para obtener más información sobre las tareas, consulte [“Administración de los directorios de la cola \(mapa de tareas\)” en la página 324](#).
- Para permitir la división de sobres, los nombres de archivos de cola ahora tienen 15 caracteres de longitud, en lugar de 14 caracteres de longitud. Los sistemas de archivos con un límite de nombre de 14 caracteres ya no se admiten.

Para obtener información sobre las tareas, consulte [“Administración de los directorios de la cola \(mapa de tareas\)” en la página 324](#).

## Cambios en LDAP de la versión 8.12 de sendmail

En la siguiente lista, se describen los cambios efectuados en el uso del protocolo ligero de acceso a directorios (LDAP) con `sendmail`.

- LDAPROUTE\_EQUIVALENT ( ) y LDAPROUTE\_EQUIVALENT\_FILE ( ) permiten especificar nombres de host equivalentes, que son reemplazados por el nombre de dominio de enmascaramiento para búsquedas de enrutamiento LDAP. Para obtener más información, consulte /etc/mail/cf/README.
- Como se señala en las notas de la versión que forman parte de la distribución sendmail en <ftp://ftp.sendmail.org>, el mapa LDAPX se ha renombrado a LDAP. Utilice la siguiente sintaxis para LDAP.

Kldap ldap options

- Esta versión admite la devolución de varios valores para una sola consulta LDAP. Coloque los valores que se van a devolver en una cadena separada por comas con la opción -v, tal como se muestra.
- Kldap ldap -v"mail,more-mail"
- Si no hay atributos LDAP especificados en una declaración de mapa LDAP, se devuelven todos los atributos que se encuentran en la comparación.
  - Esta versión de sendmail impide que las comas en las cadenas de valores y claves en cola de las especificaciones del archivo de alias LDAP dividan una sola entrada en varias entradas.
  - Esta versión de sendmail tiene una nueva opción para mapas LDAP. La opción -Vseparator permite especificar un separador de modo que una consulta pueda devolver un atributo y un valor que estén separados por un separador (separator) relevante.
  - Además de utilizar el token %s para analizar una especificación de filtro LDAP, puede utilizar el nuevo token, %0, para codificar la memoria intermedia de clave. El token %0 aplica un significado literal a caracteres especiales LDAP.

El ejemplo siguiente muestra cómo estos tokens difieren para una consulta “\*”.

TABLA 14-29 Comparación de tokens

Especificación de mapa LDAP	Especificación equivalente	Resultado
-k"uid=%s"	-k"uid=*"	Coincide con cualquier registro que tiene un atributo de usuario
-k"uid=%0"	-k"uid=\2A"	Coincide con un usuario que tiene el nombre “*”

En la siguiente tabla, se describen indicadores de mapa LDAP adicionales.

TABLA 14-30 Indicadores de mapa LDAP adicionales

Indicador	Descripción
- 1	Requiere que se devuelva una sola coincidencia. Si se devuelve más de una coincidencia, los resultados equivalen a ningún registro encontrado.

TABLA 14–30 Indicadores de mapa LDAP adicionales (Continuación)

Indicador	Descripción
-r never always search find	Establece la opción de eliminación de referencia de alias de LDAP.
-Z size	Limita el número de coincidencias que se devuelven.

## Cambio en la aplicación de correo integrada de la versión 8.12 de sendmail

La antigua aplicación de correo integrada [TCP] no está disponible. Utilice la aplicación de correo integrada P=[IPC] en su lugar. La aplicación de correo integrada ([IPC]) de comunicaciones entre procesos ahora permite la entrega a un socket de dominio UNIX en los sistemas que lo admiten. Puede utilizar esta aplicación de correo con agentes de entrega LMTP que escuchan en un socket especificado. Un ejemplo de aplicación de correo podría ser similar al siguiente.

```
Mexecmail, P=[IPC], F=lsDFMmqSXzA5@/:|, E=\r\n,
S=10, R=20/40, T=DNS/RFC822/X-Unix, A=FILE /var/run/lmtpd
```

El primer argumento de aplicación de correo en la aplicación de correo [IPC] ahora se comprueba para determinar si contiene un valor legítimo. En la siguiente tabla, se proporcionan los valores posibles para el primer argumento de aplicación de correo.

TABLA 14–31 Valores posibles para el primer argumento de aplicación de correo

Valor	Descripción
A=FILE	Se utiliza para la entrega de socket de dominio de UNIX
A=TCP	Se utiliza para conexiones TCP/IP
A=IPC	Ya no está disponible como un primer argumento de aplicación de correo

## Conjuntos de reglas adicionales de la versión 8.12 de sendmail

En la siguiente tabla, se muestran los conjuntos de reglas adicionales y se describe qué hacen los conjuntos de reglas.

TABLA 14–32 Conjuntos de reglas nuevos

Conjunto	Descripción
check_eoh	Correlaciona la información recopilada entre encabezados y comprueba si faltan encabezados. Este conjunto de reglas se utiliza con el mapa de almacenamiento de macros y se llama después de que todos los encabezados se han recopilado.
check_etrn	Utiliza el comando ETRN (como check_rcpt utiliza RCPT).
check_expn	Utiliza el comando EXPN (como check_rcpt utiliza RCPT).
check_vrfy	Utiliza el comando VRFY (como check_rcpt utiliza RCPT).

En la siguiente lista, se describen las funciones de conjuntos de reglas adicionales.

- Los conjuntos de reglas con número también tienen nombre, pero aún se puede acceder a ellos por sus números.
- El comando del archivo de configuración del encabezado H permite que se especifique un conjunto de reglas predeterminado para las comprobaciones de encabezados. Este conjunto de reglas sólo se llama si al encabezado individual no se le ha asignado su propio conjunto de reglas.
- Los comentarios en conjuntos de reglas (es decir, texto entre paréntesis) no se eliminan si la versión del archivo de configuración es nueve o superior. Por ejemplo, la siguiente regla coincide con la entrada token (1), pero no coincide con la entrada token.  
  
R\$+ (1)            \$@ 1
- sendmail acepta el comando RSET del SMTP, incluso cuando rechaza comandos debido a los envoltorios TCP o al conjunto de reglas check\_relay.
- Recibirá una advertencia si define la opción OperatorChars varias veces. Además, no establezca la opción OperatorChars después de definir los conjuntos de reglas.
- El nombre del conjunto de reglas, así como sus líneas, se ignoran si se declara un conjunto de reglas no válido. Las líneas del conjunto de reglas no se agregan a S0.

## Cambios en los archivos de la versión 8.12 de sendmail

Observe los siguientes cambios.

- A partir de la versión Solaris 10, para admitir un sistema de archivos /usr de sólo lectura, el contenido del directorio /usr/lib/mail se ha trasladado al directorio /etc/mail/cf. Para obtener detalles, consulte [“Contenido del directorio /etc/mail/cf” en la página 357](#). No obstante, tenga en cuenta que las secuencias de comandos de shell /usr/lib/mail/sh/check-hostname y /usr/lib/mail/sh/check-permissions ahora se encuentran en el directorio /usr/sbin. Consulte [“Otros archivos utilizados para servicios](#)

de correo” en la página 360. Por razones de compatibilidad de retroceso, los enlaces simbólicos hacen referencia a las nuevas ubicaciones de los archivos.

- El nuevo nombre para `/usr/lib/mail/cf/main-v7sun.mc` es `/etc/mail/cf/cf/main.mc`.
- El nuevo nombre para `/usr/lib/mail/cf/subsidiary-v7sun.mc` es `/etc/mail/cf/cf/subsidiary.mc`.
- El archivo `helpfile` ahora se encuentra en `/etc/mail/helpfile`. El nombre anterior (`/etc/mail/sendmail.hf`) tiene un enlace simbólico que hace referencia al nuevo nombre.
- El archivo `trusted-users` ahora se encuentra en `/etc/mail/trusted-users`. Durante una actualización, si se detecta el nombre anterior (`/etc/mail/sendmail.ct`), pero no el nombre nuevo, se crea un enlace físico del nombre anterior al nombre nuevo. De lo contrario, no se efectúa ningún cambio. El contenido predeterminado es `root`.
- El archivo `local-host-names` ahora se encuentra en `/etc/mail/local-host-names`. Durante una actualización, si se detecta el nombre anterior (`/etc/mail/sendmail.cw`), pero no el nombre nuevo, se crea un enlace físico del nombre anterior al nombre nuevo. De lo contrario, no se efectúa ningún cambio. El contenido predeterminado tiene una longitud de cero.

## Versión 8.12 de sendmail y direcciones IPv6 en configuración

A partir de la versión 8.12 de sendmail, las direcciones IPv6 que se utilizan en la configuración deben tener la etiqueta IPv6: como prefijo para identificar la dirección correctamente. Si no puede identificar una dirección IPv6, no se utilizó una etiqueta de prefijo.



## **P A R T E V**

### **Redes en serie (temas)**

Esta sección acerca de redes en serie proporciona información sobre la descripción general, las tareas y la referencia de PPP y UUCP.





## Solaris PPP 4.0 (descripción general)

---

En esta sección se tratan temas de redes en serie. Redes en serie hace referencia al uso de una interfaz en serie, como un puerto RS-232 o V.35 para conectar dos o más equipos para transferencia de datos. A diferencia de las interfaces LAN, como Ethernet, estas interfaces se utilizan para conectar sistemas separados por grandes distancias. PPP (Protocolo punto a punto) y UUCP (copia de UNIX a UNIX) son tecnologías distintas que pueden utilizarse para implementar redes en serie. Cuando una interfaz en serie está configurada para red, está disponible para varios usuarios, de la misma forma que cualquier otra interfaz de red, como Ethernet.

En este capítulo, se presenta Solaris PPP 4.0. Esta versión de PPP habilita dos equipos en diferentes ubicaciones físicas para comunicarse entre sí mediante PPP a través de diversos medios. A partir de la versión de Solaris 9, Solaris PPP 4.0 se incluye como parte de la instalación base.

Se explican los siguientes temas:

- “Conceptos básicos de Solaris PPP 4.0” en la página 409
- “Configuraciones y terminología de PPP” en la página 413
- “Autenticación PPP” en la página 419
- “Compatibilidad para usuarios de DSL a través de PPPoE” en la página 422

### Conceptos básicos de Solaris PPP 4.0

Solaris PPP 4.0 implementa el Protocolo punto a punto (PPP), un protocolo de enlace de datos que es un miembro del conjunto de protocolos TCP/IP. PPP describe cómo se transmiten los datos entre dos equipos de punto final a través de medios de comunicación, como líneas telefónicas.

Desde principios de 1990, PPP ha sido un estándar de Internet ampliamente utilizado para el envío de datagramas a través de un enlace de comunicaciones. El grupo de trabajo de punto a punto del Grupo Especial sobre Ingeniería de Internet (IETF, Internet Engineering Task Force)

describe el estándar de PPP en RFC 1661. PPP se utiliza comúnmente cuando los equipos remotos llaman a un proveedor de servicios de Internet (ISP) o a un proveedor corporativo configurado para recibir llamadas entrantes.

Solaris PPP 4.0 se basa en el PPP-2.4 de la Universidad Nacional de Australia (ANU, Australian National University) disponible públicamente e implementa el estándar de PPP. Se admiten enlaces de PPP síncronos y asíncronos.

## Compatibilidad de Solaris PPP 4.0

Varias versiones de PPP estándar están disponibles y se utilizan ampliamente en toda la comunidad de Internet. PPP-2.4 de ANU es una opción muy utilizada para Linux, Tru64, UNIX y las tres principales variantes de BSD:

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 brinda funciones ampliamente configurables de PPP-2.4 de ANU para equipos que ejecutan el sistema operativo Solaris. Los equipos que ejecutan Solaris PPP 4.0 pueden configurar fácilmente enlaces de PPP a cualquier equipo que ejecuta una implementación de PPP estándar.

Algunas implementaciones de PPP que no se basan en ANU que interoperan correctamente con Solaris PPP 4.0 incluyen lo siguiente:

- Solaris PPP (también conocido como asppp) disponible desde la versión Solaris 2.4 hasta la versión Solaris 8
- Solstice PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0 (síncrono)

## Cómo determinar qué versión de Solaris PPP se debe usar

La implementación de PPP que se admite es Solaris PPP 4.0. La versión Solaris 9 y las versiones subsiguientes no incluyen el software de Solaris PPP asíncrono anterior (asppp). Para obtener más información, consulte lo siguiente:

- El [Capítulo 23, “Migración de Solaris PPP asíncrono a Solaris PPP 4.0 \(tareas\)”](#)
- La Colección de administración del sistema Solaris, en <http://docs.sun.com>

## ¿Por qué utilizar Solaris PPP 4.0?

Si actualmente utiliza `asppp`, considere la posibilidad de migrar a Solaris PPP 4.0. Tenga en cuenta las siguientes diferencias entre las dos tecnologías de Solaris PPP:

- **Modos de transferencia**

`asppp` admite sólo comunicaciones asíncronas. Solaris PPP 4.0 admite comunicaciones síncronas y asíncronas.

- **Proceso de configuración**

La configuración de `asppp` necesita la configuración del archivo de configuración `asppp.cf`, tres archivos de UUCP y el comando `ifconfig`. Además, debe preconfigurar interfaces para todos los usuarios que posiblemente inicien sesión en el equipo.

La configuración de Solaris PPP 4.0 necesita opciones de definición para los archivos de configuración de PPP o la emisión del comando `pppd` con opciones. También puede utilizar una combinación del archivo de configuración y los métodos de línea de comandos. Solaris PPP crea y elimina interfaces de manera dinámica. No tiene que configurar directamente las interfaces de PPP para cada usuario.

- **Funciones de Solaris PPP 4.0 no disponibles desde `asppp`**

- Autenticación MS-CHAPv1 y MS-CHAPv2
- PPP a través de Ethernet (PPPoE) para admitir puentes de Línea de abonado digital asimétrica (ADSL)
- Autenticación PAM
- Módulos de conexión
- Direcciones IPv6
- Compresión de datos que utiliza compresión Deflate o BSD
- Compatibilidad de devolución de llamada por parte del cliente de Microsoft

## Ruta de actualización de Solaris PPP 4.0

Si convierte una configuración de `asppp` existente para Solaris PPP 4.0, puede utilizar la secuencia de comandos de traducción que se proporciona con esta versión. Para obtener instrucciones completas, consulte [“Cómo convertir de `asppp` a Solaris PPP 4.0” en la página 555](#).

## Dónde ir para obtener más información acerca de PPP

Muchos recursos con información sobre PPP se pueden encontrar impresos y en línea. Las siguientes subsecciones brindan algunas sugerencias.

## Manuales de referencia profesional sobre PPP

Para obtener más información sobre implementaciones de PPP muy utilizadas, incluido PPP de ANU, consulte los siguientes manuales:

- Carlson, James. *PPP Design, Implementation, and Debugging*. 2nd ed. (Diseño, implementación y depuración de PPP 2.ª edición). Addison-Wesley, 2000.
- Sun, Andrew. *Using and Managing PPP* (Uso y gestión de PPP). O'Reilly & Associates, 1999.

## Sitios web sobre PPP

Vaya a los siguientes sitios web para obtener información general sobre PPP:

- Para obtener información técnica, preguntas más frecuentes, discusiones sobre la administración del sistema Solaris y versiones anteriores de PPP, vaya al recurso de administradores del sistema de Sun Microsystems, <http://www.sun.com/bigadmin/home/index.html>.
- Para configuración de módem y consejos acerca de diversas implementaciones de PPP, consulte el sitio web de Gestión de proyecto de red y desarrollo de software de consultoría de Stokely: <http://www.stokely.com/unix.serial.port.resources/ppp.slip.html>.

## Solicitudes de comentarios (RFC) sobre PPP

Algunas solicitudes de comentarios de Internet útiles sobre PPP incluyen lo siguientes:

- 1661 y 1662, que describen las principales características de PPP
- 1334, que describe protocolos de autenticación, como el Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación por desafío mutuo (CHAP)
- 1332, RFC informativa que describe PPP a través de Ethernet (PPPoE)

Para obtener copias de RFC de PPP, especifique el número de la RFC en la página web RFC de IETF en <http://www.ietf.org/rfc.html>.

## Páginas del comando man sobre PPP

Para obtener información técnica acerca de la implementación de Solaris PPP 4.0, consulte las siguientes páginas del comando man:

- [pppd\(1M\)](#)
- [chat\(1M\)](#)
- [pppstats\(1M\)](#)
- [pppoec\(1M\)](#)
- [pppoed\(1M\)](#)
- [sppptun\(1M\)](#)
- [snoop\(1M\)](#)

También, consulte la página del comando man para [pppdump\(1M\)](#). Puede buscar páginas del comando man relacionadas con PPP mediante el comando `man`.

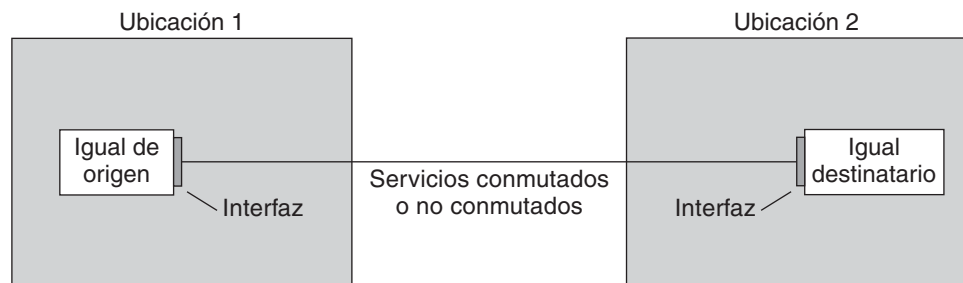
# Configuraciones y terminología de PPP

Esta sección presenta configuraciones de PPP. Esta sección también define los términos que se utilizan en esta guía.

Solaris PPP 4.0 admite un número de configuraciones.

- Acceso conmutado o configuraciones *de marcación telefónica*
- Configuraciones de *línea arrendada* o conexión fija

FIGURA 15-1 Partes del enlace de PPP



La figura anterior muestra un enlace de PPP básico. El enlace tiene las siguientes partes:

- Dos equipos, normalmente en distintas ubicaciones físicas, denominados *iguales*. Un igual podría ser un equipo personal, una estación de trabajo de ingeniería, un servidor grande o incluso un enrutador comercial, según los requisitos del sitio.
- Interfaz en serie en cada igual. En equipos que ejecutan Solaris, esta interfaz podría ser cua, hihp u otra interfaz, según si configura PPP asíncrono o síncrono.
- Enlace físico, como un cable de serie, una conexión de módem o una línea arrendada de un proveedor de red, como una línea T1 o T3.

## Descripción general de PPP de marcación telefónica

La configuración de PPP más utilizada es el *enlace por marcación telefónica*. En un enlace por marcación telefónica, el igual local *llama* al igual remoto para establecer la conexión y ejecutar PPP. En el proceso de marcación telefónica, el igual local llama al número de teléfono del igual remoto para iniciar el enlace.

Un escenario de marcación telefónica común incluye un equipo que llama a un igual en un ISP, configurado para recibir llamadas entrantes. Otro escenario es un sitio corporativo donde un equipo local transmite datos a través de un enlace de PPP para un igual en otro edificio.

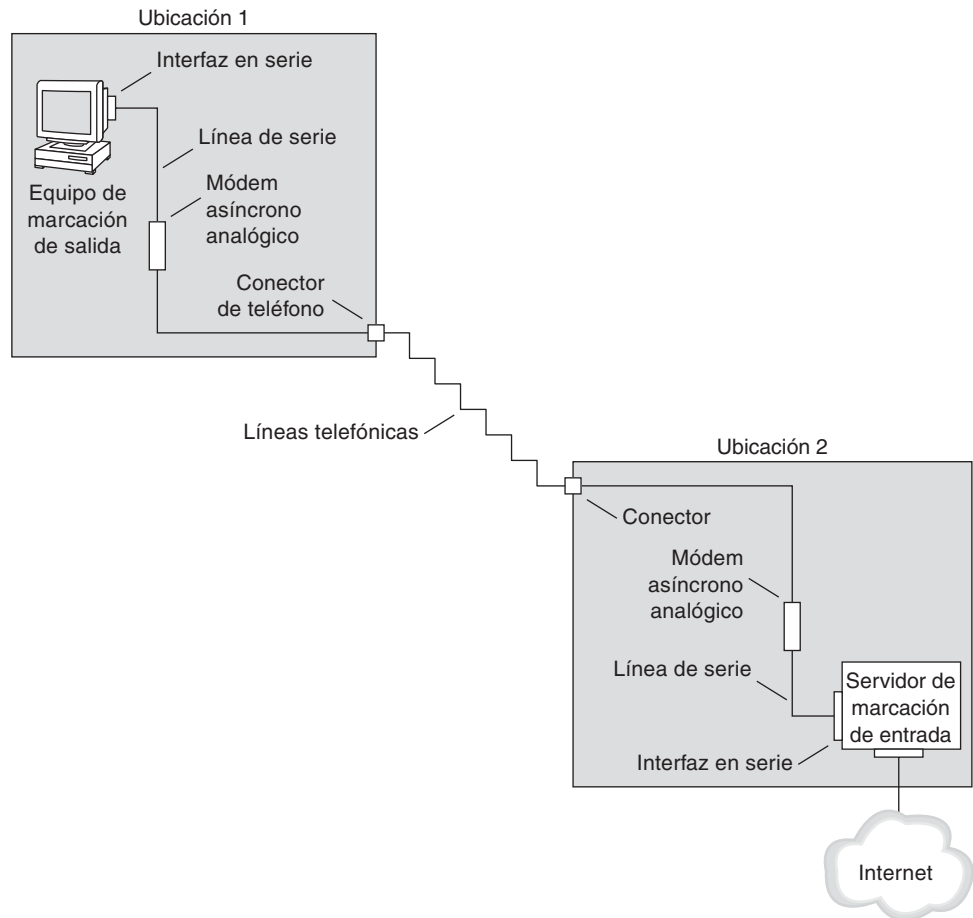
En esta guía, al igual local que inicia la conexión por marcación telefónica se lo denomina *equipo de marcación de salida*. Al igual que recibe la llamada entrante se lo denomina como *servidor de marcación de entrada*. Este equipo es en realidad el igual de destino del equipo de marcación de salida y es posible o no que sea un servidor verdadero.

PPP no es un protocolo cliente-servidor. Algunos documentos de PPP utilizan los términos "cliente" y "servidor" para referirse al establecimiento de la llamada telefónica. Un servidor de marcación de entrada no es un servidor verdadero, como un servidor de archivos o un servidor de nombres. El servidor de marcación de entrada es un término de PPP muy utilizado, debido a que los equipos de marcación de entrada, por lo general, "sirven" accesibilidad de red a más de un equipo de marcación de salida. No obstante, el servidor de marcación de entrada es el igual de destino del equipo de marcación de salida.

## **Partes de un enlace de PPP por marcación telefónica**

Consulte la siguiente figura.

FIGURA 15-2 Enlace de PPP por marcación telefónica analógico básico



La configuración de Ubicación 1, el lado de marcación de salida del enlace, se compone de los siguientes elementos:

- Equipo de marcación de salida, normalmente, un equipo personal o una estación de trabajo en el hogar de un individuo.
- Interfaz en serie en el equipo de marcación de salida. `/dev/cua/a` o `/dev/cua/b` es la interfaz en serie estándar para llamadas salientes en equipos que ejecutan el software de Solaris.
- Módem asíncrono o adaptador de terminal (TA) RDSI que está conectado a un conector de teléfono.
- Líneas telefónicas y servicios de una compañía telefónica.

La configuración de Ubicación 2, el lado de marcación de entrada del enlace, se compone de los siguientes elementos:

- Conector de teléfono o conector similar, que está conectado a la red de teléfono
- Módem asíncrono o adaptador de terminal RDSI
- Interfaz en serie en el servidor de marcación de entrada, ya sea `ttya` o `ttyb` para las llamadas entrantes
- Servidor de marcación de entrada, que está conectado a una red, como una intranet corporativa, o en la instancia de un ISP, Internet global

## Uso de adaptadores de terminal RDSI con un equipo de marcación de salida

Los adaptadores de terminal RSDI poseen una velocidad superior a los módems, pero los adaptadores de terminal se configuran básicamente de la misma manera. La diferencia principal en la configuración de un adaptador de terminal RDSI está en la secuencia de comandos de chat, que requiere comandos específicos para el fabricante del adaptador de terminal. Consulte [“Secuencia de comandos de chat para adaptador de terminal RDSI externo” en la página 528](#) para obtener información sobre secuencias de comandos de chat para adaptadores de terminal RDSI.

## Qué sucede durante comunicaciones de marcación telefónica

Los archivos de configuración de PPP de los iguales de marcación de salida y de marcación de entrada contienen instrucciones para la configuración del enlace. El siguiente proceso se produce cuando se inicia el enlace por marcación telefónica.

1. El usuario o el proceso en el equipo de marcación de salida ejecuta el comando `pppd` para iniciar el enlace.
2. El equipo de marcación de salida lee sus archivos de configuración de PPP. El equipo de marcación de salida envía instrucciones a través de la línea de serie al módem, incluido el número de teléfono del servidor de marcación de entrada.
3. El módem marca el número de teléfono para establecer una conexión telefónica con el módem del servidor de marcación de entrada.

Las series de cadenas de texto que el equipo de marcación de salida envía al módem y al servidor de marcación de entrada se encuentran en un archivo llamado *secuencia de comandos de chat*. Si es necesario, el equipo de marcación de salida envía comandos al servidor de marcación de entrada para que invoque PPP en el servidor.

4. El módem conectado al servidor de marcación de entrada inicia una negociación de enlace con el módem del equipo de marcación de salida.
5. Cuando la negociación módem a módem se completa, el módem en el equipo de marcación de salida muestra "CONECTAR".



- 6. El PPP en ambos iguales ingresa a la fase *Establecer*, donde el Protocolo de control de enlace (LCP) negocia parámetros de enlace básicos y el uso de autenticación.
- 7. Si es necesario, los iguales se autentican recíprocamente.
- 8. Los Protocolos de control de red (NCP) de PPP negocian el uso de protocolos de red, como IPv4 o IPv6.

El equipo de marcación de salida puede ejecutar `telnet` o un comando similar para un host que se puede alcanzar mediante el servidor de marcación de entrada.

## Descripción general de PPP de línea arrendada

Una configuración de PPP de *línea arrendada*, de conexión fija, implica dos iguales conectados mediante un enlace. Este enlace consiste en un servicio digital conmutado o no conmutado arrendado de un proveedor. Solaris PPP 4.0 funciona a través de cualquier medio de línea arrendada de punto a punto de dúplex completo. Normalmente, una compañía alquila un enlace de conexión fija de un proveedor de red para conectarse a un ISP u otro sitio remoto.

## Comparación de enlaces de líneas arrendadas y por marcación telefónica

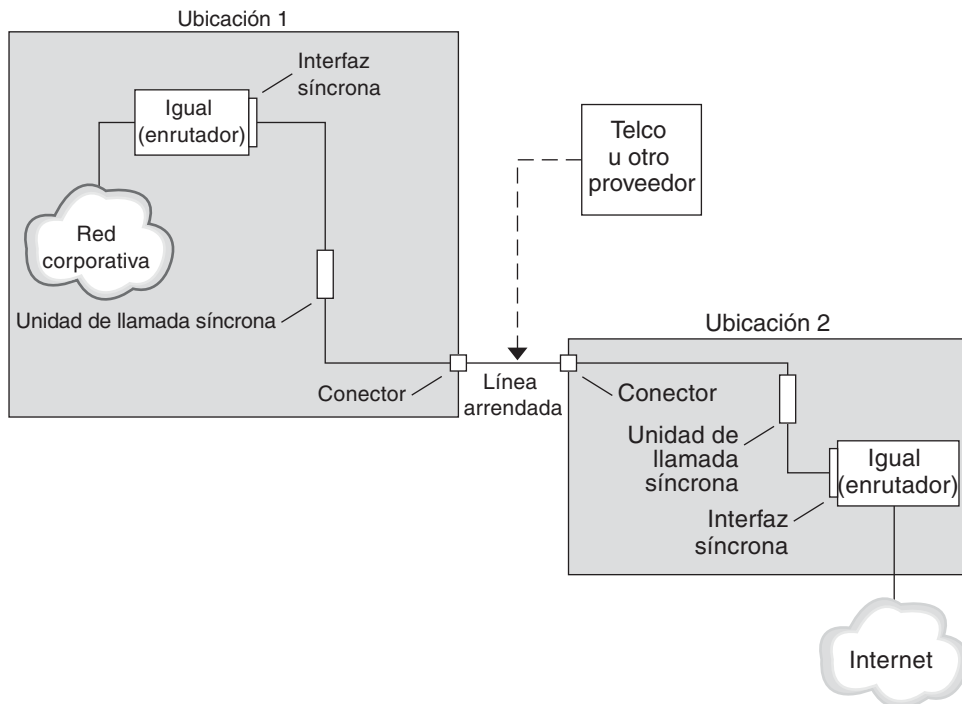
En los enlaces de líneas arrendadas y por marcación telefónica participan dos iguales que se conectan por un medio de comunicación. La siguiente tabla hace un resumen de las diferencias entre los tipos de enlace.

Línea arrendada	Línea por marcación telefónica
Siempre conectada, a menos que un administrador del sistema o un fallo en la alimentación eléctrica la desconecten.	Iniciada a petición, cuando un usuario intenta llamar a un igual remoto.
Utiliza comunicaciones síncronas y asíncronas. Para comunicaciones asíncronas, se utiliza por lo general un módem de larga distancia.	Utiliza comunicaciones asíncronas.
Alquilado de un proveedor.	Utiliza líneas telefónicas existentes.
Requiere unidades síncronas.	Utiliza módems menos costosos.
Requiere puertos síncronos, que son comunes en la mayoría de los sistemas SPARC. Sin embargo, los puertos síncronos no son comunes en los sistemas x86 ni en los sistemas SPARC más recientes.	Utiliza interfaces en serie estándar que se incluyen en la mayoría de los equipos.

## Partes de un enlace de PPP de línea arrendada

Consulte la siguiente figura.

FIGURA 15-3 Configuración de línea arrendada básica



El enlace de línea arrendada contiene las siguientes partes:

- **Dos iguales**, cada igual en un extremo del enlace. Cada igual puede ser una estación de trabajo o un servidor. Con frecuencia el igual cumple la función de enrutador entre la red o Internet, y el igual opuesto.
- **Interfaz síncrona en cada igual**. Algunos equipos que ejecutan el software de Solaris necesitan que adquiera una tarjeta de interfaz síncrona, como HSI/P, para conectarse a una línea arrendada. Otros equipos, como las estaciones de trabajo UltraSPARC, poseen interfaces síncronas incorporadas.
- **Unidad digital síncrona CSU/DSU en cada igual**, que conecta el puerto síncrono a la línea arrendada.

Es posible que una CSU esté incorporada en la DSU, sea de su propiedad o esté arrendada, según su ubicación. La DSU le brinda a un equipo que ejecuta Solaris una interfaz en serie síncrona estándar. Con Frame Relay, el Dispositivo de acceso Frame Relay (FRAD) realiza la adaptación de interfaz en serie.

- **Línea arrendada**, que proporciona servicios digitales conmutados o no conmutados. Algunos ejemplos son SONET/SDH, Frame Relay PVC y T1.

## Qué sucede durante comunicaciones de línea arrendada

En la mayoría de los tipos de líneas arrendadas, los iguales en realidad no se llaman entre sí. En su lugar, una compañía adquiere un servicio de línea arrendada para conectarse explícitamente entre dos ubicaciones fijas. A veces, los dos iguales en cada extremo de la línea arrendada se encuentran en diferentes ubicaciones físicas de la misma compañía. Otro escenario es una compañía que configura un enrutador en una línea arrendada conectada a un ISP.

Las líneas arrendadas se utilizan con menos frecuencia que los enlaces por marcación telefónica, aunque los enlaces de conexión fija son más fáciles de configurar. Los enlaces de conexión fija no requieren secuencias de comandos de chat. La autenticación no se utiliza con frecuencia porque ambos iguales ya se conocen cuando una línea está arrendada. Después de que los dos iguales inicien PPP a través de un enlace, el enlace permanece activo. Un enlace de línea arrendada permanece activo a menos que se produzca un fallo en la línea o el igual finalice el enlace explícitamente.

Un igual en una línea arrendada que ejecuta Solaris PPP 4.0 utiliza la mayoría de los mismos archivos de configuración que definen un enlace por marcación telefónica.

Se produce el siguiente proceso para iniciar la comunicación a través de la línea arrendada:

1. Cada equipo de igual ejecuta el comando `pppd` como parte del proceso de arranque u otra secuencia de comandos administrativa.
2. Los iguales leen sus archivos de configuración de PPP.
3. Los iguales negocian parámetros de comunicaciones.
4. Se establece un enlace de IP.

## Autenticación PPP

*Autenticación* es el proceso que verifica que el usuario sea quien dice ser. La secuencia de inicio de sesión de UNIX es una forma sencilla de autenticación:

1. El comando `login` solicita al usuario un nombre y una contraseña.
2. `login` intenta autenticar al usuario buscando el nombre de usuario y la contraseña que se introdujeron en la base de datos de contraseñas.

3. Si la base de datos contiene el nombre de usuario y la contraseña, se *autentica* al usuario y se le brinda acceso al sistema. Si la base de datos no contiene el nombre de usuario y la contraseña, se deniega el acceso al sistema.

De manera predeterminada, Solaris PPP 4.0 no solicita autenticación en equipos que no tienen una ruta predeterminada especificada. Por lo tanto, un equipo local sin una ruta predeterminada no autentica a emisores de llamadas remotos. Por el contrario, si un equipo tiene una ruta predeterminada definida, el equipo remoto siempre autentica a emisores de llamadas remotos.

Puede utilizar protocolos de autenticación PPP para verificar la identidad de los emisores de llamadas que intentan establecer un enlace de PPP a su equipo. Por el contrario, debe configurar la información de autenticación PPP si el equipo local debe llamar a iguales que autentican a emisores de llamadas.

## Autenticadores y autenticados

El equipo que llama en un enlace de PPP se considera el *autenticado* porque el emisor de llamada debe demostrar su identidad al igual remoto. El igual se considera el *autenticador*. El autenticador busca la identidad del emisor de llamada en los archivos de PPP adecuados para el protocolo de seguridad y autentica o no al emisor.

Normalmente configura la autenticación PPP para un enlace por marcación telefónica. Cuando se inicia la llamada, el equipo de marcación de salida es el autenticado. El servidor de marcación de entrada es el autenticador. El servidor tiene una base de datos en forma de un archivo *secrets*. Este archivo enumera todos los usuarios a los que se les otorga permiso para configurar un enlace de PPP en el servidor. Considere a estos usuarios como *emisores de llamadas de confianza*.

Algunos equipos de marcación de salida requieren que iguales remotos proporcionen información de autenticación al responder la llamada del equipo de marcación de salida. Entonces se invierten los roles: el igual remoto se convierte en el autenticado y el equipo de marcación de salida en el autenticador.

---

**Nota** – PPP 4.0 no impide la autenticación por parte de iguales de línea arrendada, pero la autenticación no se utiliza con frecuencia en enlaces de líneas arrendadas. La naturaleza de los contratos de líneas arrendadas normalmente implica que los participantes en los extremos de la línea se conocen. Ambos participantes generalmente son de confianza. Sin embargo, ya que la autenticación PPP no es tan difícil de administrar, debe considerar seriamente la implementación de autenticación para líneas arrendadas.

---

## Protocolos de autenticación PPP

Los protocolos de autenticación PPP son: Protocolo de autenticación de contraseña (PAP) y Protocolo de autenticación por desafío mutuo (CHAP). Cada protocolo utiliza una base de datos *secrets* que contiene información de identificación o *credenciales de seguridad*, para cada emisor de llamada al que se le permite establecer un enlace con el equipo local. Para obtener una explicación detallada de PAP, consulte [“Protocolo de autenticación de contraseña \(PAP\)” en la página 532](#). Para una explicación de CHAP, consulte [“Protocolo de autenticación por desafío mutuo \(CHAP\)” en la página 535](#).

## ¿Por qué utilizar autenticación PPP?

Proporcionar autenticación en un enlace de PPP es opcional. Además, aunque la autenticación verifica que un igual es de confianza, la autenticación PPP no proporciona confidencialidad de datos. Para cuestiones de confidencialidad, utilice un software de cifrado, como IPsec, PGP, SSL, Kerberos y Solaris Secure Shell.

---

**Nota** – Solaris PPP 4.0 no implementa el Protocolo de control de cifrado (ECP) de PPP, que se describe en RFC 1968.

---

Considere la posibilidad de implementar la autenticación PPP en las siguientes situaciones:

- La compañía acepta llamadas entrantes de usuarios a través de la red telefónica conmutada pública.
- La política de seguridad de la empresa requiere que los usuarios proporcionen credenciales de autenticación al acceder a la red a través de un cortafuegos de la empresa o durante transacciones de seguridad.
- Desea autenticar a los emisores de llamadas según una base de datos de contraseñas de UNIX estándar, como `/etc/passwd`, NIS, NIS+, LDAP o PAM. Utilice la autenticación PAP para este escenario.
- Los servidores de marcación de entrada de la compañía también proporcionan la conexión a Internet de la red. Utilice la autenticación PAP para este escenario.
- La línea de serie es menos segura que la base de datos de contraseñas del equipo o las redes en cualquiera de los extremos del enlace. Utilice la autenticación CHAP para este escenario.

## Compatibilidad para usuarios de DSL a través de PPPoE

Muchos proveedores de red e individuos que trabajan desde casa utilizan tecnología de Línea de suscripción digital (DSL, Digital Subscriber Line) para proporcionar rápido acceso a la red. Para admitir usuarios de DSL, Solaris PPP 4.0 incluye la función PPP a través de Ethernet (PPPoE). La tecnología PPPoE permite que varios hosts ejecuten sesiones de PPP a través de un enlace Ethernet para uno o más destinos.

Si uno de los siguientes factores se aplica a su situación, debe utilizar PPPoE:

- Admite usuarios de DSL, posiblemente se lo incluya a usted. Es posible que el proveedor de servicios de DSL requiera que los usuarios configuren un túnel PPPoE para recibir servicios a través de línea DSL.
- Su sitio es un ISP que intenta ofrecer PPPoE a los clientes.

Esta sección presenta términos asociados con PPPoE y una descripción general de la topología de PPPoE básica.

## Descripción general de PPPoE

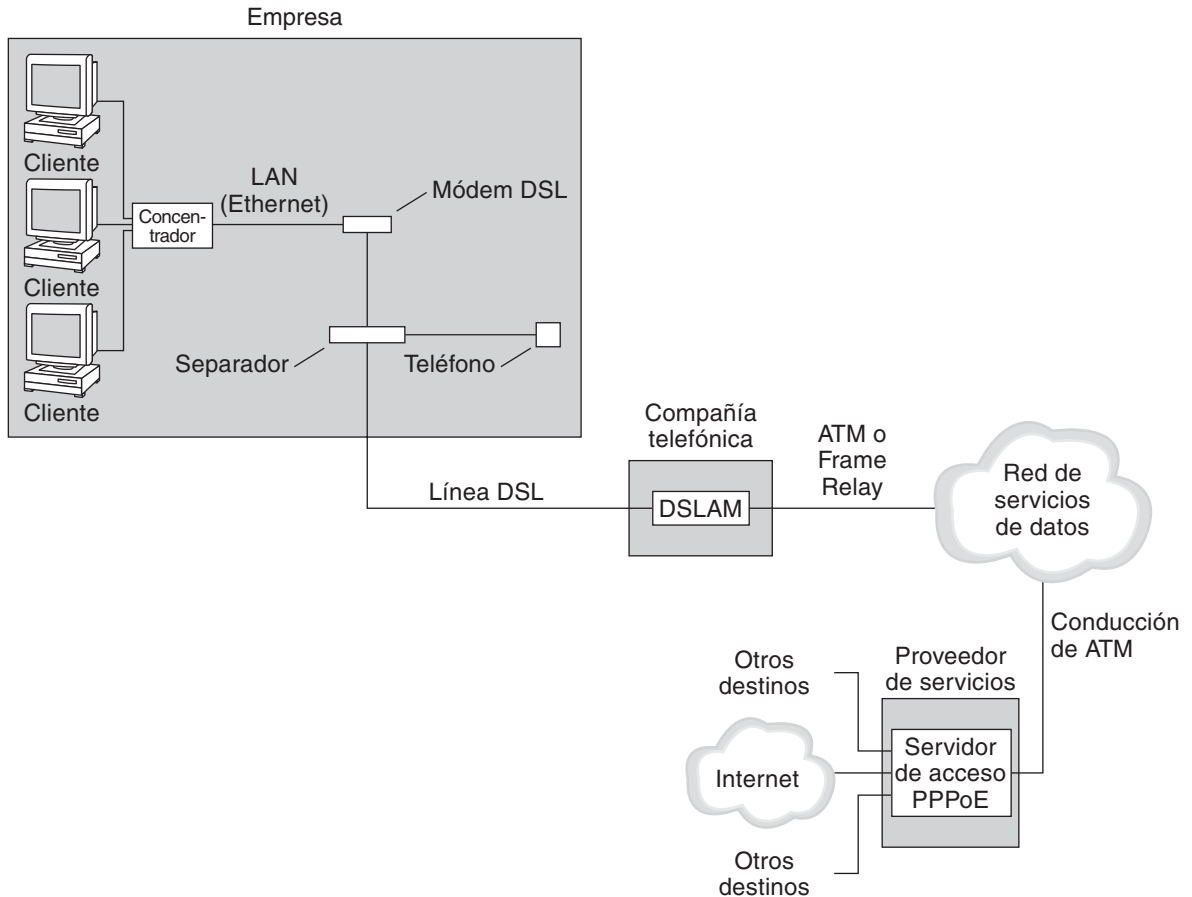
*PPPoE* es un protocolo de propiedad de RedBack Networks. PPPoE es un protocolo de detección en lugar de otra versión de PPP estándar. En un escenario de PPPoE, un equipo que inicia comunicaciones de PPP primero debe ubicar, o *detectar*, a un igual que ejecuta PPPoE. El protocolo de PPPoE utiliza paquetes de difusión Ethernet para localizar al igual.

Después del proceso de detección, PPPoE configura un túnel basado en Ethernet del host de inicio, o *cliente PPPoE*, al igual, el *servidor de acceso PPPoE*. *Establecimiento de túneles* es la práctica de ejecución de un protocolo encima de otro. Al utilizar PPPoE, Solaris PPP 4.0 crea un túnel de PPP a través de Ethernet IEEE 802.2, ambos son protocolos de enlace de datos. La conexión de PPP que se obtiene como resultado se comporta como un enlace dedicado entre el cliente PPPoE y el servidor de acceso. Para obtener información detallada sobre PPPoE, consulte [“Creación de túneles PPPoE para compatibilidad de DSL” en la página 541](#).

## Partes de una configuración de PPPoE

Tres participantes intervienen en una configuración de PPPoE: un consumidor, una compañía telefónica y un proveedor de servicios, como muestra la siguiente figura.

FIGURA 15-4 Los participantes de un túnel PPPoE



## Consumidores de PPPoE

Como administrador del sistema, puede ayudar a los consumidores con sus configuraciones de PPPoE. Un tipo común de consumidor de PPPoE es una persona que necesita ejecutar PPPoE a través de una línea DSL. Otro consumidor de PPPoE es una compañía que compra una línea DSL a través de la cual los empleados pueden ejecutar túneles PPPoE, como se ilustra en la figura anterior.

El motivo principal para que un consumidor corporativo utilice PPPoE es para ofrecer comunicaciones de PPP a través de un dispositivo DSL de alta velocidad a varios hosts. Con frecuencia, un único cliente PPPoE tiene un *módem DSL* individual. O bien, es posible que un grupo de clientes en un concentrador comparta un módem DSL también conectado al concentrador mediante una línea Ethernet.

---

**Nota** – Los dispositivos DSL son técnicamente puentes, no módems. Sin embargo, ya que en la práctica común se hace referencia a estos dispositivos como módems, esta guía utiliza el término "módem DSL".

---

PPPoE ejecuta PPP a través de un túnel en la línea Ethernet conectada al módem DSL. Esa línea está conectada a un separador que, a su vez, se conecta a una línea telefónica.

## PPPoE en una compañía telefónica

La compañía telefónica es la capa intermedia del escenario de PPPoE. La compañía telefónica divide la señal que se recibe a través de la línea de teléfono mediante un dispositivo que se denomina *Multiplexor de acceso a la línea digital de abonado (DSLAM)*. DSLAM desglosa las señales en cables independientes, cables analógicos para el servicio telefónico y cables digitales para PPPoE. Desde DSLAM, los cables digitales extienden el túnel a través de una red de datos de ATM al ISP.

## PPPoE en un proveedor de servicios

El ISP recibe la transmisión de PPPoE de la red de datos de ATM a través de un puente. En el ISP, un servidor de acceso que ejecuta PPPoE actúa como el igual para el enlace de PPP. El servidor de acceso es muy similar en su función al servidor de marcación de entrada que se presentó en la [Figura 15–2](#), pero el servidor de acceso no utiliza módems. El servidor de acceso convierte sesiones de PPPoE individuales en tráfico IP normal, por ejemplo, acceso a Internet.

Si es un administrador del sistema para un proveedor ISP, es posible que sea responsable de la configuración y el mantenimiento de un servidor de acceso.

## Seguridad en un túnel PPPoE

El túnel PPPoE es intrínsecamente inseguro. Puede utilizar PAP o CHAP para proporcionar autenticación de usuario para el enlace de PPP que se ejecuta a través del túnel.



## Planificación del enlace de PPP (tareas)

La configuración de un enlace de PPP implica una serie de tareas discretas, que incluye tareas de planificación y otras actividades que no están relacionadas con PPP. En este capítulo se explica cómo planificar los enlaces de PPP más comunes, para la autenticación y para PPPoE.

Los capítulos de tareas que siguen al [Capítulo 16, “Planificación del enlace de PPP \(tareas\)”](#) utilizan configuraciones de ejemplo para ilustrar cómo configurar un enlace específico. Estas configuraciones de ejemplo se presentan en este capítulo.

En los temas que se tratan, se incluye lo siguiente:

- “Planificación de un enlace de PPP por marcación telefónica” en la página 426
- “Planificación de un enlace de línea arrendada” en la página 430
- “Planificación para autenticación en un enlace” en la página 433
- “Planificación de compatibilidad de DSL a través de un túnel PPPoE” en la página 438

## Planificación de PPP general (mapa de tareas)

PPP requiere tareas de planificación antes de que pueda configurar el enlace. Además, si desea utilizar un establecimiento de túneles PPPoE, primero tiene que configurar el enlace de PPP y, a continuación, proporcionar el establecimiento de túneles. El siguiente mapa de tareas enumera las tareas de planificación que se tratan en este capítulo. Es posible que necesite utilizar sólo la tarea general para el tipo de enlace que se va a configurar. O es posible que requiera la tarea para el enlace, la autenticación y, posiblemente, PPPoE.

TABLA 16-1 Mapa de tareas para planificación de PPP

Tarea	Descripción	Para obtener instrucciones
Plan para enlace de PPP por marcación telefónica	Reunir información necesaria para configurar un equipo de marcación de salida o un servidor de marcación de entrada	“Planificación de un enlace de PPP por marcación telefónica” en la página 426

TABLA 16-1 Mapa de tareas para planificación de PPP (Continuación)

Tarea	Descripción	Para obtener instrucciones
Plan para un enlace de línea arrendada	Reunir información necesaria para configurar un cliente en una línea arrendada	<a href="#">“Planificación de un enlace de línea arrendada” en la página 430</a>
Plan para la autenticación en el enlace de PPP	Reunir información necesaria para configurar autenticación PAP o CHAP en el enlace de PPP	<a href="#">“Planificación para autenticación en un enlace” en la página 433</a>
Plan para un túnel PPPoE	Reunir información necesaria para configurar un túnel PPPoE a través del cual se puede ejecutar un enlace de PPP	<a href="#">“Planificación de compatibilidad de DSL a través de un túnel PPPoE” en la página 438</a>

## Planificación de un enlace de PPP por marcación telefónica

Los enlaces por marcación telefónica son los enlaces de PPP más usados. Esta sección incluye la siguiente información:

- Información de planificación para un enlace por marcación telefónica
- Explicación del enlace de ejemplo que se utilizará en el [Capítulo 17, “Configuración de un enlace de PPP por marcación telefónica \(tareas\)”](#)

Normalmente, sólo configura el equipo en un solo extremo del enlace de PPP por marcación telefónica, el equipo de marcación de salida o el servidor de marcación de entrada. Para una introducción al PPP por marcación telefónica, consulte [“Descripción general de PPP de marcación telefónica” en la página 413](#).

### Antes de configurar el equipo de marcación de salida

Antes de configurar un equipo de marcación de salida, recopile la información que se menciona en la siguiente tabla.

**Nota** – La información de planificación en esta sección no incluye información para recopilar sobre autenticación o PPPoE. Para obtener detalles sobre la planificación de autenticación, consulte [“Planificación para autenticación en un enlace” en la página 433](#). Para la planificación de PPPoE, consulte [“Planificación de compatibilidad de DSL a través de un túnel PPPoE” en la página 438](#).

TABLA 16-2 Información para un equipo de marcación de salida

Información	Acción
Velocidad máxima de módem	Consulte la documentación proporcionada por el fabricante del módem.

**TABLA 16-2** Información para un equipo de marcación de salida (Continuación)

Información	Acción
Comandos de conexión de módem (comandos AT)	Consulte la documentación proporcionada por el fabricante del módem.
Nombre que se utilizará para el servidor de marcación de entrada en el otro extremo del enlace	Cree cualquier nombre que lo ayude a identificar el servidor de marcación de entrada.
Secuencia de inicio de sesión solicitada por el servidor de marcación de entrada	Póngase en contacto con el administrador del servidor de marcación de entrada o consulte la documentación del ISP si el servidor de marcación de entrada se encuentra en el ISP.

## Antes de configurar el servidor de marcación de entrada

Antes de configurar un servidor de marcación de entrada, recopile la información que se muestra en la siguiente tabla.

**Nota** – La información de planificación en esta sección no incluye información para recopilar sobre autenticación o PPPoE. Para obtener detalles sobre la planificación de autenticación, consulte [“Planificación para autenticación en un enlace” en la página 433](#). Para planificación de PPPoE, consulte [“Planificación de compatibilidad de DSL a través de un túnel PPPoE” en la página 438](#).

**TABLA 16-3** Información para un servidor de marcación de entrada

Información	Acción
Velocidad máxima de módem	Consulte la documentación proporcionada por el fabricante del módem.
Nombres de usuario de personas a las que se les permite llamar al servidor de marcación de entrada	Obtenga los nombres de los posibles usuarios antes de configurar sus directorios principales, como se ha explicado en <a href="#">“Cómo configurar usuarios del servidor de marcación de entrada” en la página 454</a> .
Dirección IP dedicada para comunicaciones de PPP	Obtenga una dirección de la persona responsable de delegar direcciones IP en la compañía.

## Ejemplo de una configuración para PPP de marcación telefónica

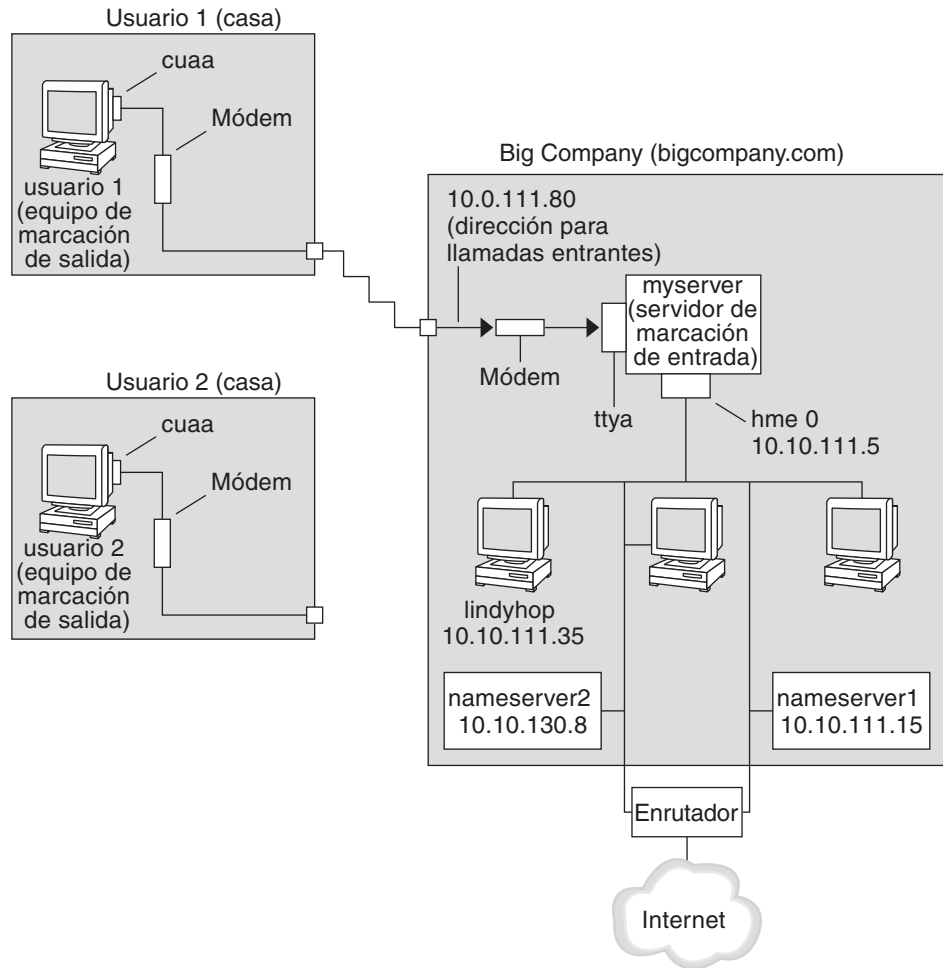
Las tareas que se presentarán en el [Capítulo 17, “Configuración de un enlace de PPP por marcación telefónica \(tareas\)”](#) cumplen los requisitos de una compañía pequeña para permitir que los empleados trabajen en sus casas algunos días de la semana. Algunos empleados necesitan tener el SO Solaris en los equipos de sus hogares. Esos trabajadores también necesitan iniciar sesión de manera remota en sus equipos de trabajo en la intranet corporativa.

Las tareas configuran un enlace por marcación telefónica básico con las siguientes funciones:

- Los equipos de *marcación de salida* se encuentran en las casas de los empleados que necesitan llamar a la intranet corporativa.
- El servidor de *marcación de entrada* es un equipo en la intranet corporativa que está configurado para recibir llamadas entrantes de los empleados.
- El inicio de sesión de estilo UNIX se utiliza para autenticar el equipo de marcación de salida. La política de seguridad de la compañía no requiere métodos de autenticación de Solaris PPP 4.0 más estrictos.

En la siguiente figura, se muestra el enlace que se configura en el [Capítulo 17, “Configuración de un enlace de PPP por marcación telefónica \(tareas\)”](#).

FIGURA 16-1 Enlace por marcación telefónica de ejemplo



En esta figura, un host remoto llama mediante su módem a través de la línea telefónica a la intranet de Big Company. Otro host está configurado para llamar a Big Company, pero actualmente está inactivo. Las llamadas de usuarios remotos se contestan en el orden que las recibió el módem que está conectado al servidor de marcación de entrada en Big Company. Una conexión de PPP se establece entre los iguales. El equipo de marcación de salida puede entonces iniciar sesión de manera remota en un equipo host en la intranet.

## Dónde ir para obtener más información sobre PPP de marcación telefónica

Consulte lo siguiente:

- Para configurar un equipo de marcación de salida, consulte la [Tabla 17–2](#).
- Para configurar un equipo de marcación de entrada, consulte la [Tabla 17–3](#).
- Para obtener una descripción general de enlaces por marcación telefónica, consulte “Descripción general de PPP de marcación telefónica” en la página 413.
- Para obtener información detallada sobre comandos y archivos de PPP, consulte “Uso de opciones de PPP en archivos y en la línea de comandos” en la página 509.

## Planificación de un enlace de línea arrendada

La configuración de un enlace de línea arrendada implica la configuración del igual en un extremo de un servicio conmutado o no conmutado arrendado de un proveedor.

Esta sección incluye la siguiente información:

- Información de planificación para un enlace de línea arrendada
- Explicación del enlace de ejemplo que se muestra en la [Figura 16–2](#)

Para obtener una introducción a los enlaces de líneas arrendadas, consulte “Descripción general de PPP de línea arrendada” en la página 417. Para tareas sobre la configuración de la línea arrendada, consulte el [Capítulo 18](#), “Configuración de un enlace de PPP de línea arrendada (tareas)”.

## Antes de configurar el enlace de línea arrendada

Cuando la compañía alquila un enlace de línea arrendada de un proveedor de red, normalmente configura sólo el sistema en su extremo del enlace. Otro administrador mantiene al igual en el otro extremo del enlace. Esta persona puede ser un administrador del sistema en una ubicación remota en la compañía o un administrador del sistema en un ISP.

## Hardware necesario para un enlace de línea arrendada

Además de los medios de enlace, su extremo del enlace requiere el siguiente hardware:

- Interfaz síncrona para su sistema
- Una unidad síncrona (CSU/DSU)
- Su sistema

Algunos proveedores de red incluyen un enrutador, una interfaz síncrona y una CSU/DSU como parte del equipo local del cliente (CPE). Sin embargo, el equipo necesario varía según el proveedor y cualquier restricción gubernamental en su configuración regional. El proveedor de red puede dar información sobre la unidad que se necesita si este equipo no se proporciona con la línea arrendada.

## Información que se recopilará para el enlace de línea arrendada

Antes de configurar el igual local, es posible que necesite recopilar los elementos que se enumeran en la siguiente tabla.

**TABLA 16-4** Planificación para un enlace de línea arrendada

Información	Acción
Nombre del dispositivo de la interfaz	Consulte la documentación de la tarjeta de interfaz.
Instrucciones de configuración para la tarjeta de interfaz síncrona	Consulte la documentación de la tarjeta de interfaz. Necesita esta información para configurar la interfaz HSI/P. Es posible que no necesite configurar otros tipos de tarjetas de interfaz.
(Opcional) Dirección IP del igual remoto	Consulte la documentación del proveedor de servicios. Como alternativa, póngase en contacto con el administrador del sistema del igual remoto. Esta información sólo es necesaria si la dirección IP no se negocia entre los dos iguales.
(Opcional) Nombre de igual remoto	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del igual remoto.
(Opcional) Velocidad del enlace	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del igual remoto.
(Opcional) Compresión que utiliza el igual remoto	Consulte la documentación del proveedor de servicios. Como alternativa, puede ponerse en contacto con el administrador del sistema del igual remoto.

## Ejemplo de una configuración para un enlace de línea arrendada

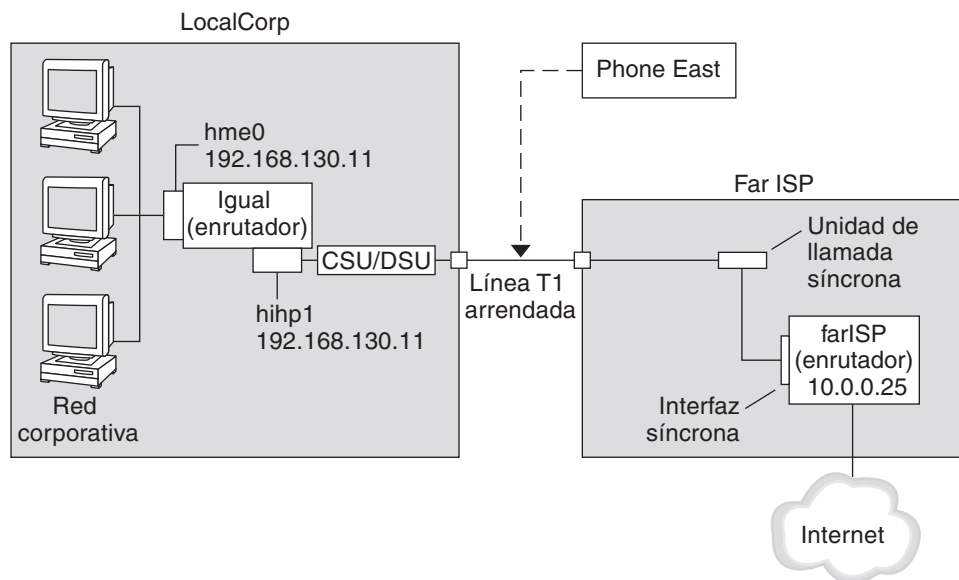
Las tareas del [Capítulo 18, “Configuración de un enlace de PPP de línea arrendada \(tareas\)”](#) muestran cómo implementar el objetivo de una empresa mediana (LocalCorp) para proporcionar acceso a Internet a sus empleados. Actualmente, los equipos de los empleados están conectados a una intranet corporativa privada.

LocalCorp requiere transacciones rápidas y acceso a los muchos recursos de Internet. La organización firma un contrato con Far ISP, un proveedor de servicios que permite a LocalCorp configurar su propia línea arrendada para Far ISP. A continuación, LocalCorp arrenda una línea T1 de Phone East, una compañía telefónica. Phone East coloca la línea arrendada entre LocalCorp y Far ISP. A continuación, Phone East proporciona una CSU/DSU que ya está configurada para LocalCorp.

Las tareas configuran un enlace de línea arrendada con las siguientes características.

- LocalCorp ha configurado un sistema como un enrutador de puerta de enlace, que reenvía paquetes a través de la línea arrendada a hosts en Internet.
- Far ISP también ha configurado un igual como un enrutador al cual las líneas arrendadas de clientes están conectadas.

FIGURA 16-2 Ejemplo de una configuración de línea arrendada



En la figura, un enrutador se configura para PPP en LocalCorp. El enrutador se conecta a la intranet corporativa a través de su interfaz hme0. La segunda conexión es a través de la interfaz HSI/P (hihp1) del equipo a la unidad digital CSU/DSU. CSU/DSU se conecta a la línea arrendada instalada. El administrador en LocalCorp configura la interfaz HSI/P y los archivos de PPP. El administrador escribe `/etc/init.d/pppd` para iniciar el enlace entre LocalCorp y Far ISP.



## Donde ir para obtener más información sobre líneas arrendadas

Consulte lo siguiente:

- [Capítulo 18, “Configuración de un enlace de PPP de línea arrendada \(tareas\)”](#)
- [“Descripción general de PPP de línea arrendada” en la página 417](#)

## Planificación para autenticación en un enlace

Esta sección contiene información de planificación para proporcionar autenticación en el enlace de PPP. El [Capítulo 19, “Configuración de autenticación PPP \(tareas\)”](#) contiene tareas para implementar la autenticación PPP en el sitio.

PPP ofrece dos tipos de autenticación, PAP, que se describe en detalle en [“Protocolo de autenticación de contraseña \(PAP\)” en la página 532](#) y CHAP, que se describe en [“Protocolo de autenticación por desafío mutuo \(CHAP\)” en la página 535](#).

Antes de configurar la autenticación en un enlace, debe seleccionar qué protocolo de autenticación se adapta mejor a la política de seguridad del sitio. A continuación, configure el archivo secrets y los archivos de configuración de PPP para los equipos de marcación de entrada o los equipos de marcación de salida de los emisores de llamadas, o ambos tipos de equipos. Para obtener información sobre el protocolo de autenticación apropiado para su sitio, consulte [“¿Por qué utilizar autenticación PPP?” en la página 421](#).

Esta sección incluye la siguiente información:

- Información de planificación para autenticación PAP y CHAP
- Explicaciones de escenarios de autenticación de ejemplo que se muestran en la [Figura 16–3](#) y la [Figura 16–4](#)

Para tareas sobre la configuración de autenticación, consulte el [Capítulo 19, “Configuración de autenticación PPP \(tareas\)”](#).

## Antes de configurar la autenticación PPP

La configuración de la autenticación en el sitio debe ser una parte integral de la estrategia de PPP general. Antes de implementar la autenticación, debe ensamblar el hardware, configurar el software y probar el enlace.

TABLA 16-5 Requisitos previos antes de configurar la autenticación

Información	Para obtener instrucciones
Tareas para configurar un enlace por marcación telefónica	<a href="#">Capítulo 17, “Configuración de un enlace de PPP por marcación telefónica (tareas)”</a> .
Tareas para probar el enlace	<a href="#">Capítulo 21, “Resolución de problemas comunes de PPP (tareas)”</a> .
Requisitos de seguridad para su sitio	Su política de seguridad corporativa. Si no tiene una política, la configuración de autenticación PPP le ofrece una oportunidad de crear una política de seguridad.
Sugerencias sobre si desea utilizar PAP o CHAP en su sitio	<a href="#">“¿Por qué utilizar autenticación PPP?” en la página 421</a> . Para obtener información más detallada sobre estos protocolos, consulte <a href="#">“Autenticación de emisores de llamadas en un enlace” en la página 532</a> .

## Ejemplos de configuraciones de autenticación PPP

Esta sección contiene ejemplos de autenticación que se utilizarán en los procedimientos del [Capítulo 19, “Configuración de autenticación PPP \(tareas\)”](#).

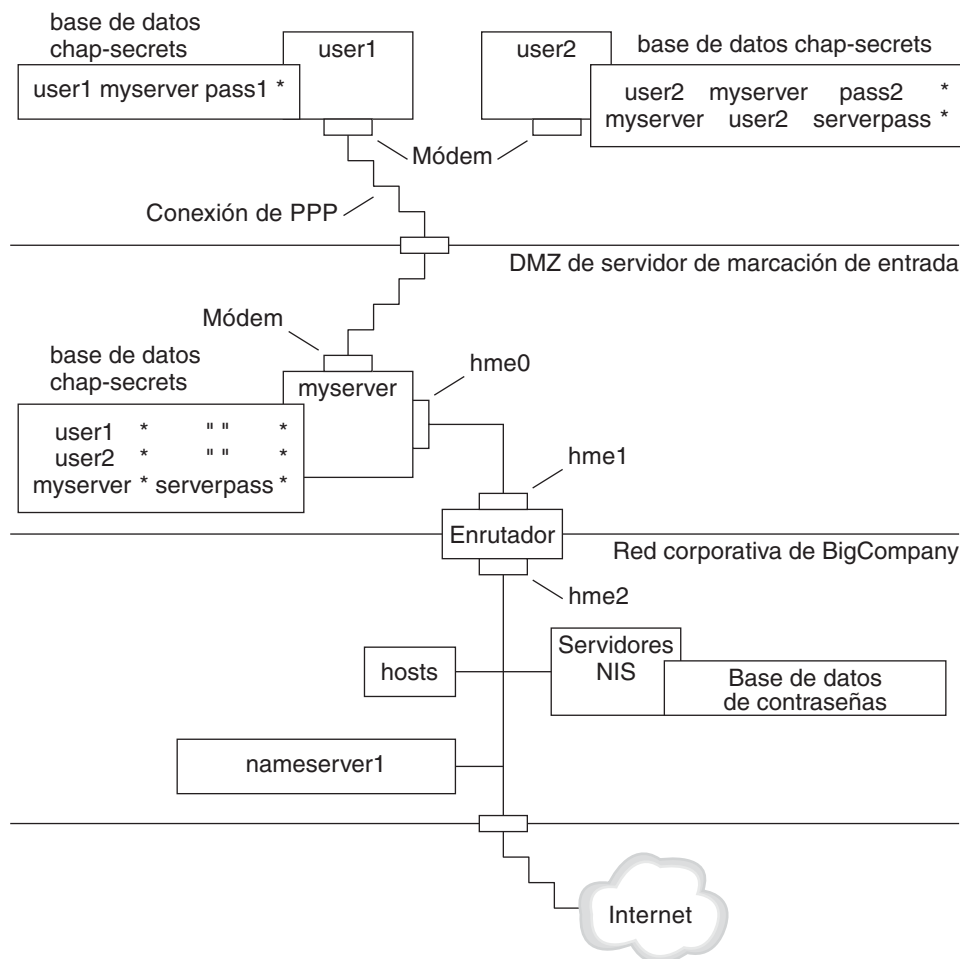
- [“Ejemplo de una configuración mediante autenticación PAP” en la página 434](#)
- [“Ejemplo de una configuración mediante autenticación CHAP” en la página 436](#)

### Ejemplo de una configuración mediante autenticación PAP

Las tareas en [“Configuración de autenticación PAP” en la página 466](#) muestran cómo configurar la autenticación PAP a través del enlace de PPP. Los procedimientos utilizan como ejemplo un escenario de PAP que se creó para la compañía ficticia "Big Company" en [“Ejemplo de una configuración para PPP de marcación telefónica” en la página 428](#).

Big Company desea permitir que los usuarios trabajen desde casa. Los administradores del sistema desean una solución segura para las líneas de serie al servidor de marcación de entrada. El inicio de sesión de estilo UNIX que utiliza la base de datos de contraseñas NIS ha resultado útil en el pasado para la red de Big Company. Los administradores del sistema desean un esquema de autenticación como UNIX para las llamadas que ingresan a la red a través del enlace de PPP. Por lo tanto, los administradores implementan el siguiente escenario que utiliza autenticación PAP.

FIGURA 16-3 Ejemplo de un escenario de autenticación PAP (al trabajar desde casa)



Los administradores del sistema crean una DMZ de marcación de entrada que está separada del resto de la red corporativa por un enrutador. El término DMZ proviene del término militar "zona desmilitarizada". La DMZ es una red aislada que se configura por cuestiones de seguridad. La DMZ normalmente contiene los recursos que una compañía ofrece al público, como servidores web, servidores FTP anónimos, bases de datos y servidores de módem. Los diseñadores de red con frecuencia ubican la DMZ entre un cortafuegos y la conexión de Internet de la compañía.

Los únicos ocupantes de la DMZ que se ilustra en la [Figura 16-3](#) son el servidor de marcación de entrada myserver y el enrutador. El servidor de marcación de entrada requiere que los emisores de llamadas proporcionen credenciales de PAP, incluidos los nombres de usuario y las contraseñas, al configurar el enlace. Además, el servidor de marcación de entrada utiliza la

opción login de PAP. Por lo tanto, los nombres de usuario y las contraseñas de PAP de los emisores de llamadas deben corresponderse exactamente con los nombres de usuario y las contraseñas de UNIX en la base de datos de contraseñas del servidor de marcación de entrada.

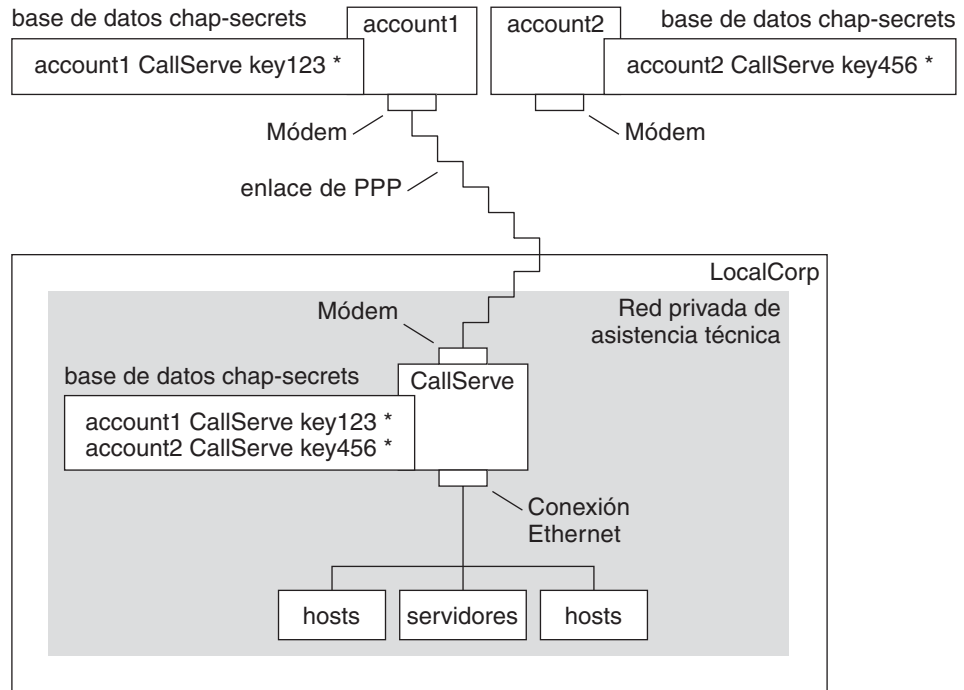
Después de que se establece el enlace de PPP, los paquetes del emisor de llamada se reenvían al enrutador. El enrutador reenvía la transmisión a su destino en la red corporativa o en Internet.

## **Ejemplo de una configuración mediante autenticación CHAP**

Las tareas de [“Configuración de autenticación CHAP” en la página 474](#) muestran cómo configurar la autenticación CHAP. Los procedimientos utilizan como ejemplo un escenario de CHAP que se creará para la compañía ficticia LocalCorp que se presentó en [“Ejemplo de una configuración para un enlace de línea arrendada” en la página 431](#).

LocalCorp proporciona conectividad a Internet a través de una línea arrendada a un ISP. El departamento de asistencia técnica dentro de LocalCorp genera un tráfico de red pesado. Por lo tanto, la asistencia técnica requiere su propia red privada aislada. Los técnicos de campo del departamento viajan mucho y necesitan poder acceder a la red de asistencia técnica desde ubicaciones remotas para obtener información de resolución de problemas. Para proteger la información confidencial en la base de datos de la red privada, se debe autenticar a los emisores de llamadas remotos antes de otorgarles permiso para iniciar sesión.

Por lo tanto, los administradores del sistema implementan el siguiente escenario de autenticación CHAP para una configuración de PPP de marcación telefónica.

**FIGURA 16-4** Ejemplo de un escenario de autenticación CHAP (llamada a una red privada)

El único enlace de la red de asistencia técnica al mundo exterior es la línea de serie al extremo del enlace del servidor de marcación de entrada. Los administradores del sistema configuran el equipo portátil de cada representante del servicio de campo para PPP con seguridad de CHAP, incluido un secreto de CHAP. La base de datos chap-secrets en el servidor de marcación de entrada contiene las credenciales de CHAP para todos equipos a los que se les permite llamar a la red de asistencia técnica.

## Dónde ir para obtener más información sobre autenticación

Elija entre las siguientes opciones:

- Consulte [“Configuración de autenticación PAP”](#) en la página 466.
- Consulte [“Configuración de autenticación CHAP”](#) en la página 474.
- Consulte [“Autenticación de emisores de llamadas en un enlace”](#) en la página 532 y la página del comando `man pppd(1M)`.

# Planificación de compatibilidad de DSL a través de un túnel PPPoE

Algunos proveedores de DSL necesitan que configure un túnel PPPoE para su sitio a fin de poder ejecutar PPP a través de líneas DSL de proveedores y redes digitales de alta velocidad. Para obtener una descripción general de PPPoE, consulte [“Compatibilidad para usuarios de DSL a través de PPPoE” en la página 422](#).

En un túnel PPPoE intervienen tres participantes: un consumidor, una compañía telefónica y un ISP. Puede configurar PPPoE para consumidores, como clientes PPPoE en su compañía o consumidores en sus hogares, o bien configurar PPPoE en un servidor en un ISP.

Esta sección contiene información de planificación para ejecutar PPPoE en los clientes y servidores de acceso. Contiene los temas siguientes:

- Información de planificación para los host PPPoE y el servidor de acceso
- Explicación del escenario PPPoE que se presenta en [“Ejemplo de una configuración para un túnel PPPoE” en la página 440](#)

Para tareas sobre la configuración de un túnel PPPoE, consulte el [Capítulo 20, “Configuración de un túnel PPPoE \(tareas\)”](#).

## Antes de configurar un túnel PPPoE

Las actividades de preconfiguración varían según si se configura el lado del cliente o el lado del servidor del túnel. En cualquier caso, el usuario o la organización deben establecer un contrato con una compañía telefónica. La compañía telefónica proporciona las líneas DSL para los clientes y algún tipo de establecimiento de puentes, y posiblemente una conducción ATM para servidores de acceso. En la mayoría de los contratos, la compañía telefónica ensambla los equipos en su sitio.

## Antes de configurar un cliente PPPoE

Las implementaciones de un cliente PPPoE constan generalmente de los siguientes equipos:

- Equipo personal u otro sistema que utiliza una persona
- Módem DSL, que generalmente la compañía telefónica o el proveedor de acceso a Internet se encargan de la instalación
- (Opcional) Un concentrador, si participa más de un cliente, ya que se aplica para consumidores de DSL corporativos
- (Opcional) Un separador, generalmente lo instala el proveedor

Es posible realizar diferentes configuraciones de DSL, según las necesidades del usuario o de la empresa y los servicios que ofrece el proveedor.

TABLA 16-6 Planificación de clientes PPPoE

Información	Acción
Si configura un cliente PPPoE principal para una persona o para usted, obtenga información de configuración que esté fuera del ámbito de PPPoE.	Pregunte a la compañía telefónica o ISP acerca de los procedimientos de configuración necesarios.
Si configura clientes de PPPoE en un sitio corporativo, recopile los nombres de los usuarios a los que se les asigna sistemas cliente PPPoE. Si configura clientes PPPoE remotos, es posible que sea responsable de proporcionar a los usuarios información acerca de cómo agregar equipos DSL domésticos.	Solicite a la administración de su compañía una lista de usuarios autorizados.
Averigüe qué interfaces están disponibles en el cliente PPPoE.	Ejecute el comando <code>ifconfig</code> -a en cada equipo para los nombres de interfaz.
(Opcional) Obtenga la contraseña para el cliente PPPoE.	Pregunte a los usuarios sus contraseñas predilectas. O bien, asigne contraseñas a los usuarios. Tenga en cuenta que esta contraseña se utiliza para autenticación de enlaces, no para inicio de sesión de UNIX.

## Antes de configurar un servidor PPPoE

La planificación para un servidor de acceso PPPoE implica trabajar con la compañía telefónica que proporciona la conexión a su red de servicio de datos. La compañía telefónica instala sus líneas, generalmente conducciones ATM, en su sitio y proporciona algún tipo de establecimiento de puentes a su servidor de acceso. Debe configurar las interfaces Ethernet que acceden a los servicios que ofrece su compañía. Por ejemplo, necesita configurar interfaces para el acceso a Internet, como también interfaces Ethernet del puente de la compañía telefónica.

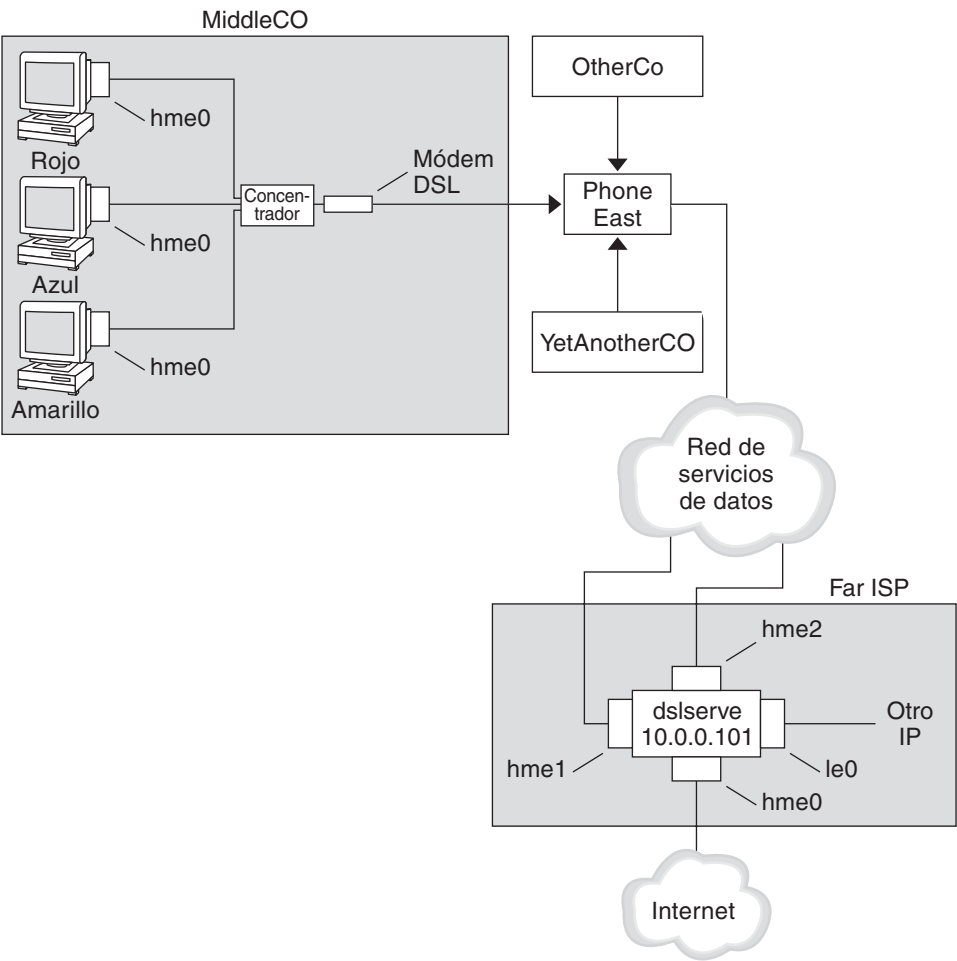
TABLA 16-7 Planificación de un servidor de acceso PPPoE

Información	Acción
Interfaces que se utilizan para líneas de red de servicio de datos	Ejecute el comando <code>ifconfig</code> -a para identificar las interfaces.
Tipos de servicios que se proporcionan de un servidor PPPoE	Pregunte a la administración y a los planificadores de redes acerca de los requisitos y solicite sugerencias.
(Opcional) Tipos de servicios para proporcionar a los consumidores	Pregunte a la administración y a los planificadores de redes acerca de los requisitos y solicite sugerencias.
(Opcional) Nombres de host y contraseñas para clientes remotos	Pregunte a los planificadores de redes y a otras personas de su sitio encargadas de las negociaciones de contratos. Los nombres de host y las contraseñas se utilizan para autenticación PAP o CHAP, no para inicio de sesión de UNIX.

# Ejemplo de una configuración para un túnel PPPoE

Esta sección contiene un ejemplo de un túnel PPPoE, que se utiliza como una ilustración para las tareas del [Capítulo 20, “Configuración de un túnel PPPoE \(tareas\)”](#). Aunque la ilustración muestra todos los participantes en el túnel, sólo administra un extremo, ya sea el lado del cliente o del servidor.

FIGURA 16-5 Ejemplo de un túnel PPPoE





En el ejemplo, MiddleCo desea proporcionar a los empleados acceso a Internet de alta velocidad. MiddleCo vende un paquete DSL de Phone East, que, a su vez, establece un contrato con el proveedor de servicios Far ISP. Far ISP ofrece Internet y otros servicios IP para clientes que compran DSL de Phone East.

## Ejemplo de una configuración de cliente PPPoE

MiddleCo vende un paquete de Phone East que proporciona una línea DSL para el sitio. El paquete incluye una conexión autenticada dedicada al ISP para clientes PPPoE de MiddleCo. El administrador del sistema conecta a los posibles clientes PPPoE a un concentrador. Los técnicos de Phone East conectan el concentrador a sus equipos DSL.

## Ejemplo de una configuración de servidor PPPoE

Para implementar los acuerdos comerciales que FarISP tiene con Phone East, el administrador del sistema en FarISP configura el servidor de acceso `dslserve`. Este servidor tiene las siguientes cuatro interfaces:

- `eri0` – Interfaz de red primaria que se conecta a la red local
- `hme0` – Interfaz a través de la que FarISP proporciona servicio de Internet para sus clientes
- `hme1` – Interfaz contratada por MiddleCo para túneles PPPoE autenticados
- `hme2` – Interfaz contratada por otros clientes para sus túneles PPPoE

## Dónde obtener más información sobre PPPoE

Elija entre las siguientes opciones:

- Consulte [“Configuración del cliente PPPoE” en la página 482](#).
- Consulte [“Configuración de un servidor de acceso PPPoE” en la página 485](#).
- Consulte [“Creación de túneles PPPoE para compatibilidad de DSL” en la página 541](#) y las páginas del comando `man pppoe(1M)`, `pppoe(1M)` y `sppptun(1M)`.



## Configuración de un enlace de PPP por marcación telefónica (tareas)

En este capítulo se explican las tareas que deben realizarse para configurar el enlace de PPP más común, el enlace por marcación telefónica. Los temas principales incluyen lo siguiente:

- “Configuración del equipo de marcación de salida” en la página 444
- “Configuración del servidor de marcación de entrada” en la página 451
- “Llamada al servidor de marcación de entrada” en la página 457

### Tareas principales para configuración de enlace de PPP por marcación telefónica (mapa de tareas)

Se configura el enlace de PPP por marcación telefónica al configurar módems, modificar archivos de base de datos de red y modificar archivos de configuración de PPP que se describen en la [Tabla 22-1](#).

La siguiente tabla muestra las principales tareas para configurar ambas partes de un enlace de PPP por marcación telefónica. Normalmente, se configura solamente un extremo del enlace, el equipo de marcación de salida o el servidor de marcación de entrada.

**TABLA 17-1** Mapa de tareas para configuración de enlace de PPP por marcación telefónica

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de iguales, los números de teléfono de destino y la velocidad del módem.	<a href="#">“Planificación de un enlace de PPP por marcación telefónica” en la página 426</a>
2. Configurar el equipo de marcación de salida	Configurar el PPP en el equipo que realiza la llamada a través del enlace.	<a href="#">Tabla 17-2</a>
3. Configurar el servidor de marcación de entrada	Configurar el PPP en el equipo que recibe llamadas entrantes.	<a href="#">Tabla 17-3</a>

TABLA 17-1 Mapa de tareas para configuración de enlace de PPP por marcación telefónica (Continuación)

Tarea	Descripción	Para obtener instrucciones
4. Llamar al servidor de marcación de entrada	Escribir el comando pppd para iniciar comunicaciones.	“Cómo llamar al servidor de marcación de entrada” en la página 457

## Configuración del equipo de marcación de salida

Las tareas de esta sección explican cómo configurar un equipo de marcación de salida. Las tareas utilizan como ejemplo el escenario de marcación de entrada desde el hogar que se presentó en la [Figura 16-1](#). Puede realizar las tareas de la compañía antes de pasarlas al equipo para un posible usuario. Como alternativa, puede indicar a los usuarios con experiencia acerca de la configuración de los equipos de sus hogares. Cualquier persona que configure un equipo de marcación de salida debe tener permiso root para ese equipo.

### Tareas para la configuración de un equipo de marcación de salida (mapa de tareas)

TABLA 17-2 Mapa de tareas para configuración de equipo de marcación de salida

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de iguales, los números de teléfono de destino y la velocidad del módem.	“Planificación de un enlace de PPP por marcación telefónica” en la página 426
2. Configurar el módem y el puerto de serie	Configurar el módem y el puerto de serie.	“Cómo configurar el módem y el puerto de serie (equipo de marcación de salida)” en la página 446
3. Configurar la comunicación de línea de serie	Configurar las características de la transmisión a través de la línea de serie.	“Cómo definir comunicaciones a través de la línea de serie” en la página 447
4. Definir la conversación entre el equipo de marcación de salida y el igual	Recopilar datos de comunicaciones para utilizar al crear la secuencia de comandos de chat.	“Cómo crear las instrucciones para llamar a un igual” en la página 448
5. Configurar información sobre un igual particular	Configurar opciones de PPP para llamar a un servidor de marcación de entrada individual.	“Cómo definir la conexión con un igual individual” en la página 449
6. Llamar al igual	Escribir el comando pppd para iniciar comunicaciones.	“Cómo llamar al servidor de marcación de entrada” en la página 457

## Archivos de plantilla de PPP de marcación telefónica

Solaris PPP 4.0 proporciona archivos de plantilla. Cada plantilla contiene opciones comunes para un determinado archivo de configuración de PPP. La siguiente tabla muestra las plantillas de ejemplo que se pueden utilizar para la configuración de un enlace por marcación telefónica y sus archivos equivalentes de Solaris PPP 4.0.

Archivo de plantilla	Archivo de configuración de PPP	Para obtener instrucciones
/etc/ppp/options.tpl	/etc/ppp/options	<a href="#">“Plantilla /etc/ppp/options.tpl” en la página 514</a>
/etc/ppp/options.ttya.tpl	/etc/ppp/options. <i>nombre de tty</i>	<a href="#">“Archivo de plantilla options.ttya.tpl” en la página 517</a>
/etc/ppp/myisp-chat.tpl	Archivo con el nombre de su elección que contiene la secuencia de comandos de chat	<a href="#">“Plantilla de secuencia de comandos de chat /etc/ppp/myisp-chat.tpl” en la página 524</a>
/etc/ppp/peers/myisp.tpl	/etc/ppp/peers/ <i>nombre de igual</i>	<a href="#">“Archivo de plantilla /etc/ppp/peers/myisp.tpl” en la página 520</a>

Si decide utilizar uno de los archivos de plantilla, asegúrese de cambiar el nombre de la plantilla a su archivo de configuración de PPP equivalente. La única excepción es la plantilla de archivo de chat /etc/ppp/myisp-chat.tpl. Puede seleccionar cualquier nombre para la secuencia de comandos de chat.

## Configuración de dispositivos en el equipo de marcación de salida

La primera tarea para la configuración de un equipo de PPP de marcación de salida es configurar los dispositivos en la línea de serie: el módem y el puerto de serie.

**Nota** – Las tareas que se aplican a un módem, por lo general, se aplican a un adaptador de terminal (TA) RDSI.

Antes de poder realizar el siguiente procedimiento, debe haber hecho lo siguiente.

- Instalado la versión de Solaris en los equipos de marcación de salida
- Determinado la velocidad de módem óptima
- Decidido qué puerto de serie desea utilizar en el equipo de marcación de salida
- Obtenido la contraseña root para el equipo de marcación de salida

Para obtener información de planificación, consulte la [Tabla 16–2](#).

## ▼ **Cómo configurar el módem y el puerto de serie (equipo de marcación de salida)**

### **1 Programe el módem.**

Aunque existe una gran variedad de tipos de módem, la mayoría de los módems se envían con la configuración adecuada para Solaris PPP 4.0. La lista siguiente muestra la configuración de parámetros básica para módems que utilizan Solaris PPP 4.0.

- **DCD:** seguir instrucciones del proveedor
- **DTR:** establecer en bajo para que el módem finalice la llamada y esté listo para establecer una comunicación
- **Control de flujo:** establecer a RTS/CTS para control de flujo de hardware dúplex completo
- **Secuencias de atención:** deshabilitar

Si tiene problemas para configurar el enlace y sospecha que el módem es el culpable, consulte primero la documentación del fabricante del módem. Además, varios sitios web ofrecen ayuda con la programación del módem. Por último, puede buscar algunas sugerencias para solucionar problemas del módem en [“Cómo diagnosticar problemas del módem”](#) en la [página 498](#).

### **2 Conecte los cables del módem al puerto de serie del equipo de marcación de salida y al conector de teléfono.**

### **3 Conviértase en superusuario en el equipo de marcación de salida o adopte un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

### **4 Ejecute el comando `/usr/sadm/bin/smc`, como se explica en [“Configuración de terminales y módems con la herramienta Serial Ports \(descripción general\)”](#) de *Guía de administración del sistema: Administración avanzada*. Este comando abre Solaris Management Console.**

Utilice Solaris Management Console para realizar lo siguiente.

#### **a. Seleccionar el puerto en el que se ha conectado el módem.**

#### **b. Especificar la dirección del módem como sólo marcación de salida.**

Puede configurar el módem como bidireccional. Sin embargo, la opción de sólo marcación de salida es más segura contra posibles intrusos.

---

**Nota** – Puede establecer la velocidad de transferencia de datos y el tiempo de espera de `/usr/sadm/bin/smc`. Sin embargo, el daemon `pppd` ignora estos valores.

---

- 5 Haga clic en OK para realizar los cambios.

## Configuración de comunicaciones en el equipo de marcación de salida

Los procedimientos de esta sección muestran cómo configurar comunicaciones a través de la línea de serie del equipo de marcación de salida. Antes de poder utilizar estos procedimientos, debe haber configurado el módem y el puerto de serie como se describe en [“Cómo configurar el módem y el puerto de serie \(equipo de marcación de salida\)” en la página 446](#).

Las siguientes tareas muestran cómo habilitar el equipo de marcación de salida para iniciar comunicaciones con éxito con el servidor de marcación de entrada. Las comunicaciones se inician como se definió en las opciones de los archivos de configuración de PPP. Necesita crear los siguientes archivos:

- `/etc/ppp/options`
- `/etc/ppp/options.nombre de tty`
- Secuencia de comandos de chat
- `/etc/ppp/peers/nombre de igual`

Solaris PPP 4.0 proporciona plantillas para los archivos de configuración de PPP, que puede personalizar según sus necesidades. Consulte [“Archivos de plantilla de PPP de marcación telefónica” en la página 445](#) para obtener información detallada acerca de esos archivos.

## ▼ Cómo definir comunicaciones a través de la línea de serie

- 1 **Conviértase en superusuario en el equipo de marcación de salida o adopte un rol equivalente.**  
 Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Cree un archivo denominado `/etc/ppp/options` con la siguiente entrada:**  
**lock**  
 El archivo `/etc/ppp/options` se utiliza para definir parámetros globales que se aplican a todas las comunicaciones por el equipo local. La opción `lock` habilita el bloqueo de estilo UUCP del formato `/var/spool/locks/LK.xxx.yyy.zzz`.

---

**Nota** – Si el equipo de marcación de salida no tiene el archivo `/etc/ppp/options`, sólo el superusuario puede ejecutar el comando `pppd`. Sin embargo, `/etc/ppp/options` puede estar vacío.

---

Para obtener una descripción completa de `/etc/ppp/options`, vaya a [“Archivo de configuración /etc/ppp/options” en la página 514](#).

- 3 (Opcional) Cree un archivo denominado `/etc/ppp/options.nombre de tty` para definir cómo se deben iniciar las comunicaciones desde un puerto de serie específico.**

En el siguiente ejemplo, se muestra un archivo `/etc/ppp/options.nombre de tty` para el puerto con el nombre del dispositivo `/dev/cua/a`.

```
# cat /etc/ppp/options.cua.a
crtscts
```

La opción PPP `crtscts` indica al daemon `pppd` que active el control de flujo de hardware para el puerto de serie `a`.

Para obtener más información sobre el archivo `/etc/ppp/options.ttyname`, vaya a [“Archivo de configuración /etc/ppp/options.nombre de tty” en la página 515](#).

- 4 Establezca la velocidad del módem, como se describe en [“Cómo establecer la velocidad del módem” en la página 453](#).**

## ▼ **Cómo crear las instrucciones para llamar a un igual**

Antes de que el equipo de marcación de salida pueda iniciar un enlace de PPP, debe recopilar información sobre el servidor de marcación de entrada que se convertirá en el igual. A continuación, podrá utilizar esta información para crear la secuencia de comandos de chat que describe la conversación real entre el equipo de marcación de salida y el igual.

- 1 Determine la velocidad a la que el módem del equipo de marcación de salida necesita ejecutarse.**

Para obtener más información, consulte [“Configuración de velocidad del módem para un enlace por marcación telefónica” en la página 522](#).

- 2 Obtenga la siguiente información a partir del sitio del servidor de marcación de entrada.**

- Número de teléfono del servidor
- Protocolo de autenticación que se utiliza, si corresponde
- Secuencia de inicio de sesión que requiere el igual para la secuencia de comandos de chat

- 3 Obtenga los nombres y las direcciones IP de los servidores de nombre en el sitio del servidor de marcación de entrada.**



#### 4 En una secuencia de comandos de chat, proporcione instrucciones para iniciar llamadas al igual particular.

Por ejemplo, podría crear la siguiente secuencia de comandos de chat `/etc/ppp/mychat` para llamar al servidor de marcación de entrada `myserver`.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M552=255
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in. Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

La secuencia de comandos contiene instrucciones para llamar a un servidor de marcación de entrada de Solaris que requiere una secuencia de inicio de sesión. Para obtener una descripción de cada instrucción, consulte [“Secuencia de comandos de chat básica mejorada para un inicio de sesión de estilo UNIX” en la página 526](#). Para obtener detalles completos sobre la creación de una secuencia de comandos de chat, lea la sección [“Definición de la conversación en el enlace por marcación telefónica” en la página 522](#).

---

**Nota** – No invoque la secuencia de comandos de chat directamente. En su lugar, utilice el nombre de archivo de la secuencia de comandos de chat como un argumento para el comando `chat` que invoca la secuencia de comandos.

---

Si un igual ejecuta Solaris o un sistema operativo similar, considere utilizar la secuencia de comandos de chat anterior como una plantilla para los equipos de marcación de salida.

## ▼ Cómo definir la conexión con un igual individual

### 1 Conviértase en superusuario en el equipo de marcación de salida o adopte un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Actualice las bases de datos de DNS creando el siguiente archivo `/etc/resolv.conf`:**

```
domain bigcompany.com
nameserver 10.10.111.15
nameserver 10.10.130.8
```

**dominio bigcompany.com**

Especifica que el dominio de DNS del igual es bigcompany.com.

**servidor de nombres 10.10.111.15 y servidor de nombres 10.10.130.8**

Enumera las direcciones IP de los servidores de nombres en bigcompany.com.

**3 Edite el archivo `/etc/nsswitch.conf` para que la base de datos de DNS busque primero la información del host.**

```
hosts:      dns [NOTFOUND=return] files
```

**4 Cree un archivo para el igual.**

Por ejemplo, se crearía el siguiente archivo para definir el servidor de marcación de entrada myserver:

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

`/dev/cua/a`

Especifica que el dispositivo `/dev/cua/a` se debe utilizar como la interfaz en serie para llamadas a myserver.

`57600`

Define la velocidad del enlace.

`noipdefault`

Especifica que para las transacciones con el igual myserver el equipo de marcación de salida tiene inicialmente una dirección IP de 0.0.0.0. myserver asigna una dirección IP al equipo de marcación de salida para cada sesión de marcación telefónica.

`idle 120`

Indica que el enlace debe entrar en tiempo de espera tras un período de inactividad de 120 segundos.

`noauth`

Especifica que el igual myserver no necesita proporcionar credenciales de autenticación al negociar la conexión con el equipo de marcación de salida.

```
connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
```

Especifica la opción connect y sus argumentos, que incluyen el número de teléfono del igual, y la secuencia de comandos de chat `/etc/ppp/mychat` con instrucciones de llamada.

- Véase también** La siguiente lista proporciona referencias a la información relacionada.
- Para configurar otro equipo de marcación de salida, consulte [“Cómo configurar el módem y el puerto de serie \(equipo de marcación de salida\)”](#) en la página 446.
  - Para probar la conectividad del módem llamando a otro equipo, consulte las páginas del comando `man cu(1C)` y `tip(1)`. Estas utilidades pueden ayudarlo a probar si el módem está configurado correctamente. Asimismo, emplee estas utilidades para probar si puede establecer una conexión con otro equipo.
  - Para obtener más información sobre opciones y archivos de configuración, consulte [“Uso de opciones de PPP en archivos y en la línea de comandos”](#) en la página 509.
  - Para configurar un servidor de marcación de entrada, consulte [“Configuración de dispositivos en el servidor de marcación de entrada”](#) en la página 452.

## Configuración del servidor de marcación de entrada

Las tareas de esta sección son para configurar el servidor de marcación de entrada. El servidor de marcación de entrada es un equipo de igual que recibe la llamada a través del enlace de PPP desde el equipo de marcación de salida. Las tareas muestran cómo configurar el servidor de marcación de entrada `myserver` que se presentó en la [Figura 16–1](#).

### Tareas para la configuración de un servidor de marcación de entrada (mapa de tareas)

TABLA 17–3 Mapa de tareas para configuración de servidor de marcación de entrada

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace, como los nombres de host de iguales, los números de teléfono de destino y la velocidad del módem.	<a href="#">“Planificación de un enlace de PPP por marcación telefónica”</a> en la página 426
2. Configurar el módem y el puerto de serie	Configurar el módem y el puerto de serie.	<a href="#">“Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada)”</a> en la página 452
3. Configurar información de igual de llamada	Configurar los entornos de usuario y las opciones de PPP para cada equipo de marcación de salida al que se le permite llamar al servidor de marcación de entrada.	<a href="#">“Cómo configurar usuarios del servidor de marcación de entrada”</a> en la página 454
4. Configurar la comunicación de línea de serie	Configurar las características de la transmisión a través de la línea de serie.	<a href="#">“Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada)”</a> en la página 456

## Configuración de dispositivos en el servidor de marcación de entrada

El siguiente procedimiento explica cómo configurar el módem y el puerto de serie en el servidor de marcación de entrada.

Antes de realizar el siguiente procedimiento, debe haber completado las siguientes actividades en el servidor de marcación de entrada de igual:

- Instalado la versión de Solaris
- Determinado la velocidad de módem óptima
- Decidido qué puerto de serie utilizar

### ▼ Cómo configurar el módem y el puerto de serie (servidor de marcación de entrada)

- 1 Programe el módem como se indica en la documentación del fabricante del módem.

Para obtener otras sugerencias, consulte [“Cómo configurar el módem y el puerto de serie \(equipo de marcación de salida\)”](#) en la página 446.

- 2 Conecte el módem al puerto de serie del servidor de marcación de entrada.

- 3 Conviértase en superusuario en el servidor de marcación de entrada o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 4 Configure el puerto de serie mediante el comando `/usr/sadm/bin/smc` para Solaris Management Console, como se describe en [“Configuración de terminales y módems con la herramienta Serial Ports \(descripción general\)”](#) de *Guía de administración del sistema: Administración avanzada*.

Utilice Solaris Management Console para realizar lo siguiente:

- a. Seleccionar el puerto de serie en el que se ha conectado el módem.
- b. Especificar la dirección del módem como sólo marcación de entrada.

---

**Nota** – Solaris PPP 4.0 no admite comunicaciones bidireccionales para un módem.

---

- c. Haga clic en OK para realizar los cambios.

## ▼ Cómo establecer la velocidad del módem

El siguiente procedimiento explica cómo establecer la velocidad del módem para un servidor de marcación de entrada. Para obtener sugerencias sobre velocidades a utilizar con equipos de Sun Microsystems, consulte [“Configuración de velocidad del módem para un enlace por marcación telefónica” en la página 522](#).

- 1 **Inicie sesión en el servidor de marcación de entrada.**
- 2 **Utilice el comando `tip` para acceder al módem.**  
Las instrucciones para usar `tip` para establecer la velocidad del módem están en la página del comando `man tip(1)`.
- 3 **Configure el módem para una velocidad DTE fija.**
- 4 **Bloquee el puerto de serie a esa velocidad mediante `ttymon o /usr/sadm/bin/smc` como se ha explicado en [“Configuración de terminales y módems con la herramienta Serial Ports \(descripción general\)” de \*Guía de administración del sistema: Administración avanzada\*](#).**

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- [“Cómo configurar el módem y el puerto de serie \(servidor de marcación de entrada\)” en la página 452](#)
- [“Cómo configurar usuarios del servidor de marcación de entrada” en la página 454](#)

## Configuración de usuarios del servidor de marcación de entrada

Parte del proceso de configuración de un servidor de marcación de entrada incluye información de configuración acerca de cada emisor de llamada remoto conocido.

Antes de iniciar los procedimientos de esta sección, debe haber hecho lo siguiente:

- Obtenido los nombres de usuarios de UNIX para todos los usuarios autorizados a iniciar sesión desde equipos de marcación de salida remotos.
- Configurado el módem y la línea de serie, como se describe en [“Cómo configurar el módem y el puerto de serie \(servidor de marcación de entrada\)” en la página 452](#).
- Dedicado una dirección IP para asignar a las llamadas entrantes procedentes de usuarios remotos. Considere la posibilidad de crear una dirección IP entrante dedicada si el número de posibles emisores de llamadas supera el número de módems y puertos de serie del servidor de marcación de entrada. Para obtener información completa sobre la creación de direcciones IP dedicadas, vaya a [“Creación de un esquema de direccionamiento IP para emisores de llamadas” en la página 538](#).

## ▼ Cómo configurar usuarios del servidor de marcación de entrada

**1 Conviértase en superusuario en el servidor de marcación de entrada o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Cree una cuenta nueva en el servidor de marcación de entrada para cada usuario de PPP remoto.**

Puede utilizar Solaris Management Console para crear un usuario nuevo. El comando `/usr/sadm/bin/smc` abre Solaris Management Console. Para obtener instrucciones sobre la creación de un usuario nuevo mediante Solaris Management Console, consulte [“Configuración de cuentas de usuario \(mapa de tareas\)” de Guía de administración del sistema: administración básica](#).

**3 Utilice Solaris Management Console para asignar parámetros para el usuario nuevo.**

Por ejemplo, la siguiente tabla muestra los parámetros de una cuenta denominada `pppuser` para `user1` en el equipo de marcación de salida `myhome`.

Parámetro	Valor	Definición
Nombre de usuario	<code>pppuser</code>	El nombre de cuenta de usuario del usuario remoto. Este nombre de cuenta debe corresponderse con el nombre de cuenta otorgado en la secuencia de inicio de sesión de la secuencia de comandos de chat. Por ejemplo, <code>pppuser</code> es el nombre de cuenta que se encuentra en la secuencia de comandos de chat en <a href="#">“Cómo crear las instrucciones para llamar a un igual” en la página 448</a> .
Shell de inicio de sesión	<code>/usr/bin/pppd</code>	El shell de inicio de sesión predeterminado para el usuario remoto. El shell de inicio de sesión <code>/usr/bin/pppd</code> restringe inicialmente al emisor de llamada a un entorno de PPP dedicado.
Cree una ruta de directorio principal	<code>/export/home/pppuser</code>	El directorio principal <code>/export/home/pppuser</code> se establece cuando el emisor de llamada inicia sesión correctamente en el servidor de marcación de entrada.

- 4 Cree para cada emisor de llamada un archivo `$HOME/.ppprc` que contenga varias opciones específicas de la sesión de PPP del usuario.

Por ejemplo, puede crear el siguiente archivo `.ppprc` para `pppuser`.

```
# cat /export/home/pppuser/.ppprc
noccp
```

`noccp` desactiva el control de compresión del enlace.

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- [“Cómo configurar usuarios del servidor de marcación de entrada” en la página 454.](#)
- [“Cómo definir comunicaciones a través de la línea de serie \(servidor de marcación de entrada\)” en la página 456.](#)

## Configuración de comunicaciones a través del servidor de marcación de entrada

La siguiente tarea muestra cómo habilitar el servidor de marcación de entrada para abrir comunicaciones con cualquier equipo de marcación de salida. Las opciones definidas en los siguientes archivos de configuración de PPP determinan cómo están establecidas las comunicaciones.

- `/etc/ppp/options`
- `/etc/ppp/options.nombre de tty`

Para obtener información detallada acerca de estos archivos, consulte [“Uso de opciones de PPP en archivos y en la línea de comandos” en la página 509.](#)

Antes de continuar, debe haber hecho lo siguiente:

- Configurado el puerto de serie y el módem en el servidor de marcación de entrada, como se describe en [“Cómo configurar el módem y el puerto de serie \(servidor de marcación de entrada\)” en la página 452.](#)
- Configurado información sobre los posibles usuarios del servidor de marcación de entrada, como se describe en [“Cómo configurar usuarios del servidor de marcación de entrada” en la página 454.](#)

# ▼ Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada)

**1 Conviértase en superusuario en el servidor de marcación de entrada o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Cree el archivo `/etc/ppp/options` con la siguiente entrada.**

**`nodefaultroute`**

`nodefaultroute` indica que ninguna sesión `pppd` en el sistema local puede establecer una ruta predeterminada sin privilegios `root`.

---

**Nota** – Si el servidor de marcación de entrada no tiene un archivo `/etc/ppp/options`, sólo el superusuario puede ejecutar el comando `pppd`. Sin embargo, el archivo `/etc/ppp/options` puede estar vacío.

---

**3 Cree el archivo `/etc/options.nombre de tty` para definir cómo las llamadas que se reciben a través del puerto de serie `nombre de tty` se deben gestionar.**

El siguiente archivo `/etc/options.ttya` define cómo el puerto de serie del servidor de marcación de entrada `/dev/ttya` debe manejar llamadas entrantes.

**`:10.0.0.80`**

**`xonxoff`**

**`:10.0.0.80`** Asigna la dirección IP 10.0.0.80 a todos los iguales que llaman a través del puerto de serie `ttya`

**`xonxoff`** Permite que la línea de serie gestione las comunicaciones de módems con control de flujo de software habilitado

**Véase también** Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace por marcación telefónica. La siguiente lista proporciona referencias a la información relacionada.

- Para probar la conectividad del módem llamando a otro equipo, consulte las páginas del comando `man cu(1C)` y `tip(1)`. Estas utilidades pueden ayudarlo a probar si el módem está configurado correctamente. Asimismo, emplee estas utilidades para probar si puede establecer una conexión con otro equipo.
- Para configurar más opciones del servidor de marcación de entrada, consulte [“Configuración del servidor de marcación de entrada” en la página 451](#).



- Para configurar más equipos de marcación de salida, consulte [“Configuración del equipo de marcación de salida” en la página 444](#).
- Para que el equipo remoto llame al servidor de marcación de entrada, consulte [“Llamada al servidor de marcación de entrada” en la página 457](#).

## Llamada al servidor de marcación de entrada

Establece un enlace de PPP por marcación telefónica haciendo que el equipo de marcación de salida llame al servidor de marcación de entrada. Puede indicar al equipo de marcación de salida que llame al servidor especificando la opción `demand` en los archivos de configuración de PPP locales. Sin embargo, el método más común para establecer el enlace es que el usuario ejecute el comando `pppd` en el equipo de marcación de salida.

Antes de continuar con la tarea siguiente, debe haber hecho una o ambas de las siguientes acciones:

- Configurado el equipo de marcación de salida, como se describe en [“Configuración del equipo de marcación de salida” en la página 444](#)
- Configurado el servidor de marcación de entrada, como se describe en [“Configuración del servidor de marcación de entrada” en la página 451](#)

### ▼ Cómo llamar al servidor de marcación de entrada

- 1 Inicie sesión en el equipo de marcación de salida utilizando la cuenta de usuario común, no `root`.

- 2 Llame al servidor de marcación de entrada ejecutando el comando `pppd`.

Por ejemplo, el siguiente comando inicia un enlace entre el equipo de marcación de salida y el servidor de marcación de entrada `myserver`:

```
% pppd 57600 call myserver
```

**pppd** Inicia la llamada invocando el daemon `pppd`

**57600** Ajusta la velocidad de la línea entre el host y el módem

**call myserver** Invoca la opción `call` de `pppd`. `pppd` luego lee las opciones del archivo `/etc/ppp/peers/myserver` que se ha creado en [“Cómo definir la conexión con un igual individual” en la página 449](#)

- 3 Póngase en contacto con un host en la red del servidor, por ejemplo, el host `Lindyhop` que se muestra en la [Figura 16–1](#):

```
ping lindyhop
```

Si el enlace no funciona correctamente, consulte el [Capítulo 21, “Resolución de problemas comunes de PPP \(tareas\)”](#).

#### **4 Termine la sesión de PPP:**

```
% kill -x pppd
```

**Véase también** Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace por marcación telefónica. La siguiente lista proporciona referencias a la información relacionada.

- Para que los usuarios empiecen a trabajar en sus equipos de marcación de salida, consulte [“Cómo llamar al servidor de marcación de entrada” en la página 457](#).
- Para solucionar problemas en el enlace, consulte el [Capítulo 21, “Resolución de problemas comunes de PPP \(tareas\)”](#).
- Para obtener más información sobre los archivos y las opciones que se utilizan en este capítulo, consulte [“Uso de opciones de PPP en archivos y en la línea de comandos” en la página 509](#).

## Configuración de un enlace de PPP de línea arrendada (tareas)

En este capítulo se explica cómo configurar un enlace de PPP que utiliza una línea arrendada entre iguales. Las secciones principales incluyen lo siguiente:

- “Configuración de dispositivos síncronos en la línea arrendada” en la página 460
- “Configuración de un equipo en la línea arrendada” en la página 461

## Configuración de una línea arrendada (mapa de tareas)

Los enlaces de líneas arrendadas son relativamente fáciles de configurar en comparación con los enlaces por marcación telefónica. En la mayoría de los casos, no tiene que configurar la CSU/DSU, los servicios de marcación ni la autenticación. Si necesita configurar la CSU/DSU, consulte la documentación del fabricante para obtener ayuda para esta tarea compleja.

El mapa de tareas en la siguiente tabla describe todas las tareas relacionadas con la configuración de un enlace de línea arrendada básico.

**Nota** – Algunos tipos de líneas arrendadas exigen CSU/DSU para “marcar” la dirección del igual opuesto. Por ejemplo, Frame Relay utiliza Circuitos virtuales conmutados (SVCs) o servicio conmutado 56.

TABLA 18-1 Mapa de tareas para configuración del enlace de línea arrendada

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los datos que se necesitan antes de configurar el enlace.	<a href="#">Tabla 16-4</a>
2. Configurar el hardware de la línea arrendada	Integrar CSU/DSU con la tarjeta de interfaz síncrona.	<a href="#">“Cómo configurar dispositivos síncronos” en la página 460</a>

TABLA 18-1 Mapa de tareas para configuración del enlace de línea arrendada (Continuación)

Tarea	Descripción	Para obtener instrucciones
3. Configurar la tarjeta de interfaz, si es necesario	Configurar la secuencia de comandos de interfaz que se debe utilizar cuando se inicia la línea arrendada.	<a href="#">“Cómo configurar dispositivos síncronos” en la página 460</a>
4. Configurar la información sobre el igual remoto	Definir cómo deben funcionar las comunicaciones entre el equipo local y el igual remoto.	<a href="#">“Cómo configurar un equipo en una línea arrendada” en la página 462</a>
5. Iniciar la línea arrendada	Configurar el equipo para iniciar PPP a través de la línea arrendada como parte del proceso de arranque.	<a href="#">“Cómo configurar un equipo en una línea arrendada” en la página 462</a>

## Configuración de dispositivos síncronos en la línea arrendada

La tarea en esta sección implica la configuración del equipo requerido por la topología de la línea arrendada que se presenta en [“Ejemplo de una configuración para un enlace de línea arrendada” en la página 431](#). Los dispositivos síncronos necesarios para conectarse a la línea arrendada incluyen la interfaz y el módem.

### Requisitos previos para configuración de dispositivos síncronos

Antes de poder realizar el siguiente procedimiento, debe tener los siguientes elementos:

- Una línea arrendada activa instalada en su sitio por el proveedor
- Una unidad síncrona (CSU/DSU)
- Versión de Solaris instalada en el sistema
- Una tarjeta de interfaz síncrona del tipo requerido por el sistema

### ▼ Cómo configurar dispositivos síncronos

- 1 Instale físicamente la tarjeta de interfaz en el local, si es necesario.**  
Siga las instrucciones de la documentación del fabricante.
- 2 Conecte los cables de la CSU/DSU a la interfaz.**  
Si es necesario, conecte cables de la CSU/DSU al conector de la línea arrendada o a un conector similar.
- 3 Configure la CSU/DSU como se indica en la documentación del fabricante o del proveedor de red.**

---

**Nota** – Es posible que el proveedor de quien obtuvo la línea arrendada le proporcione y configure la CSU/DSU para su enlace.

---

**4 Configure la tarjeta de interfaz, si es necesario, como se indica en la documentación de la interfaz.**

La configuración de la tarjeta de interfaz implica la creación de una secuencia de comandos de inicio para la interfaz. El enrutador en LocalCorp en la configuración de línea arrendada que se muestra en la [Figura 16–2](#) utiliza una tarjeta de interfaz HSI/P.

La siguiente secuencia de comandos, `hsi - conf`, inicia la interfaz HSI/P.

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null

hihp1          Indica que HSI/P es el puerto síncrono utilizado
speed=1536000  Indica la velocidad de la CSU/DSU
```

**Véase también** Para configurar el equipo local en la línea arrendada, consulte [“Cómo configurar un equipo en una línea arrendada” en la página 462](#).

## Configuración de un equipo en la línea arrendada

La tarea en esta sección explica cómo configurar un enrutador para que funcione como el igual local en el extremo de una línea arrendada. La tarea utiliza la línea arrendada que se presentó en [“Ejemplo de una configuración para un enlace de línea arrendada” en la página 431](#) como ejemplo.

### Requisitos previos para la configuración del equipo local en una línea arrendada

Antes de poder realizar el siguiente procedimiento, debe haber realizado lo siguiente:

- Instalado y configurado el dispositivo síncrono para el enlace, como se describe en [“Configuración de dispositivos síncronos en la línea arrendada” en la página 460](#)
- Obtenido la contraseña root para el equipo local en la línea arrendada
- Configurado el equipo local para que se ejecute como enrutador en la red o redes para utilizar los servicios del proveedor de la línea arrendada

## ▼ Cómo configurar un equipo en una línea arrendada

**1 Conviértase en superusuario en el equipo local (enrutador) o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

**2 Agregue una entrada para el igual remoto en el archivo /etc/hosts del enrutador.**

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1      localhost
192.168.130.10 local2-peer    loghost
192.168.130.11 local1-net
10.0.0.25      farISP
```

El archivo /etc/hosts de ejemplo es para el enrutador local en LocalCorp ficticio. Tenga en cuenta la dirección IP y el nombre de host para el igual remoto farisp en el proveedor de servicios.

**3 Cree el archivo /etc/ppp/peers/nombre de igual para mantener información sobre el igual del proveedor.**

Para este ejemplo de enlace de línea arrendada, puede crear el archivo /etc/ppp/peers/farISP.

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
nopcomp
novj
noaccomp
```

La siguiente tabla explica las opciones y los parámetros que se utilizan en /etc/ppp/peers/farISP.

Opción	Definición
init '/etc/ppp/conf_hsi'	Inicia el enlace. init configura la interfaz HSI utilizando los parámetros en la secuencia de comandos /etc/ppp/conf_hsi.

Opción	Definición
local	Indica al daemon pppd que no cambie el estado de la señal de Terminal de datos listo (DTR, Data Terminal Ready). También le indica a pppd que ignore la señal de entrada de Detección de portadora de datos (DCD, Data Carrier Detect).
/dev/hihpl	Proporciona el nombre de dispositivo de interfaz síncrona.
sync	Establece la codificación síncrona para el enlace.
noauth	Establece que el sistema local no necesita solicitar autenticación del igual. Sin embargo, el igual aún puede solicitar autenticación.
192.168.130.10:10.0.0.25	Define las direcciones IP del igual local y el igual remoto, separado por dos puntos.
passive	Indica al daemon pppd en el equipo local que pase a modo silencioso después de emitir un número máximo de solicitudes de configuración de LCP y espere a que el igual inicie actividad.
persist	Indica al daemon pppd que intente reiniciar el enlace después de que finaliza una conexión.
noccp, nopcomp, novj, noaccomp	Desactiva el Protocolo de control de compresión (CCP), la compresión de campo de protocolo, la compresión de Van Jacobson y la compresión de direcciones y de campo de control respectivamente. Estas formas de compresión aceleran las transmisiones en un enlace por marcación telefónica, pero podrían disminuir la velocidad de la línea arrendada.

4 Cree una secuencia de comandos de inicialización denominada demand, que crea el enlace de PPP como parte del proceso de arranque.

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /var/run/ppp-demand.pid ] &&
    /usr/bin/kill -s 0 '/bin/cat /var/run/ppp-demand.pid'
then
    :
else
    /usr/bin/pppd call farISP
fi
```

La secuencia de comandos demand contiene los comandos pppd para establecer un enlace de línea arrendada. La siguiente tabla explica el contenido de \$PPPDIR/demand.

Ejemplo de código	Explicación
if [ -f /var/run/ppp-demand.pid ] && /usr/bin/kill -s 0 '/bin/cat /var/run/ppp-demand.pid'	Estas líneas comprueban si pppd se está ejecutando. Si pppd se está ejecutando, no es necesario iniciarlo.
/usr/bin/pppd call farISP	Esta línea inicia pppd. pppd lee las opciones de /etc/ppp/options. La opción call farISP en la línea de comandos hace que también se lea /etc/ppp/peers/farISP.

La secuencia de comandos de inicio de Solaris PPP 4.0 `/etc/rc2.d/s47pppd` invoca la secuencia de comandos `demand` como parte del proceso de arranque. Las siguientes líneas en `/etc/rc2.d/s47pppd` buscan la presencia de un archivo que se denomina `$PPPDIR/demand`.

```
if [ -f $PPPDIR/demand ]; then
    . $PPPDIR/demand
fi
```

Si se encuentra, `$PPPDIR/demand` se ejecuta. Durante el curso de la ejecución de `$PPPDIR/demand`, se establece el enlace.

---

**Nota** – Para llegar a equipos que se encuentran fuera de la red local, debe hacer que los usuarios ejecuten `telnet`, `ftp`, `rsh` o comandos similares.

---

**Véase también** Si ha seguido todos los procedimientos de este capítulo, ha completado la configuración del enlace de línea arrendada. La siguiente lista proporciona referencias a la información relacionada.

- Para encontrar información sobre la resolución de problemas, consulte [“Resolución de problemas de línea arrendada” en la página 506](#).
- Para obtener más información sobre los archivos y las opciones que se utilizan en este capítulo, consulte [“Uso de opciones de PPP en archivos y en la línea de comandos” en la página 509](#).



## Configuración de autenticación PPP (tareas)

Este capítulo contiene tareas para configuración de autenticación PPP. En los temas que se tratan se incluye lo siguiente:

- “Configuración de autenticación PAP” en la página 466
- “Configuración de autenticación CHAP” en la página 474

Los procedimientos muestran cómo implementar la autenticación a través de un enlace por marcación telefónica, porque es más probable que los enlaces por marcación telefónica estén configurados para la autenticación que los enlaces de líneas arrendadas. Puede configurar la autenticación a través de líneas arrendadas si la autenticación es requerida por la política de seguridad corporativa. Para la autenticación de líneas arrendadas, use las tareas de este capítulo como directrices.

Si desea utilizar la autenticación PPP, pero no está seguro de qué protocolo debe utilizar, consulte la sección “¿Por qué utilizar autenticación PPP?” en la página 421. Para obtener más información sobre la autenticación PPP, consulte la página del comando `man pppd(1M)` y “Autenticación de emisores de llamadas en un enlace” en la página 532.

## Configuración de autenticación PPP (mapa de tareas)

Esta sección contiene mapas de tareas para ayudarlo a acceder rápidamente a los procedimientos para la autenticación PPP.

TABLA 19-1 Mapa de tareas para autenticación general de PPP

Tarea	Descripción	Para obtener instrucciones
Configurar autenticación PAP	Utilizar estos procedimientos para habilitar la autenticación PAP en un servidor de marcación de entrada y un equipo de marcación de salida.	“Configuración de autenticación PAP (mapas de tareas)” en la página 466

TABLA 19-1 Mapa de tareas para autenticación general de PPP (Continuación)

Tarea	Descripción	Para obtener instrucciones
Configurar autenticación CHAP	Utilizar estos procedimientos para habilitar la autenticación CHAP en un servidor de marcación de entrada y un equipo de marcación de salida.	<a href="#">“Configuración de autenticación CHAP (mapas de tareas)” en la página 474</a>

## Configuración de autenticación PAP

Las tareas de esta sección explican cómo implementar la autenticación en un enlace de PPP mediante el Protocolo de autenticación de contraseña (PAP). Las tareas utilizan el ejemplo que se muestra en [“Ejemplos de configuraciones de autenticación PPP” en la página 434](#) para ilustrar un escenario de trabajo de PAP para un enlace por marcación telefónica. Utilice las instrucciones como base para la implementación de la autenticación PAP en el sitio.

Antes de poder realizar los siguientes procedimientos debe haber hecho lo siguiente:

- Configurado y probado el enlace por marcación telefónica entre un servidor de marcación de entrada y equipos de marcación de salida que pertenecen a emisores de llamadas de confianza.
- En condiciones ideales, para la autenticación del servidor de marcación de entrada, haber obtenido permiso de superusuario para el equipo donde la base de datos de contraseñas de red se administra, por ejemplo, en LDAP, NIS o archivos locales.
- Obtenido autoridad de superusuario para el equipo local, ya sea servidor de marcación de entrada o equipo de marcación de salida.

## Configuración de autenticación PAP (mapas de tareas)

Utilice los mapas de tareas siguientes para acceder rápidamente a tareas relacionadas de PAP con el servidor de marcación de entrada y los emisores de llamadas de confianza en equipos de marcación de salida.

TABLA 19-2 Mapa de tareas para autenticación PAP (servidor de marcación de entrada)

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los nombres de usuario y otros datos necesarios para la autenticación.	<a href="#">“Planificación para autenticación en un enlace” en la página 433</a>
2. Actualizar la base de datos de contraseñas, si es necesario	Asegurarse de que todos los posibles emisores de llamadas estén en la base de datos de contraseñas del servidor.	<a href="#">“Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada)” en la página 467</a>
3. Crear la base de datos de PAP	Crear credenciales de seguridad para todos los posibles emisores de llamadas en /etc/ppp/pap-secrets.	<a href="#">“Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada)” en la página 467</a>

TABLA 19-2 Mapa de tareas para autenticación PAP (servidor de marcación de entrada) (Continuación)

Tarea	Descripción	Para obtener instrucciones
4. Modificar los archivos de configuración de PPP	Agregar opciones específicas para PAP a los archivos <code>/etc/ppp/options</code> y <code>/etc/ppp/peers/nombre de igual</code> .	“Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada)” en la página 469

TABLA 19-3 Mapa de tareas para autenticación PAP (equipo de marcación de salida)

Tarea	Descripción	Para obtener instrucciones
1. Recopilar información de preconfiguración	Recopilar los nombres de usuario y otros datos necesarios para la autenticación.	“Planificación para autenticación en un enlace” en la página 433
2. Crear la base de datos de PAP para el equipo del emisor de llamada de confianza	Crear credenciales de seguridad para un emisor de llamada de confianza y, si es necesario, credenciales de seguridad para otros usuarios que llaman al equipo de marcación de salida, en <code>/etc/ppp/pap-secrets</code> .	“Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza” en la página 471
3. Modificar los archivos de configuración de PPP	Agregar opciones específicas para PAP a los archivos <code>/etc/ppp/options</code> y <code>/etc/ppp/peers/nombre de igual</code> .	“Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida)” en la página 473

## Configuración de autenticación PAP en el servidor de marcación de entrada

Para configurar la autenticación PAP, debe realizar lo siguiente:

- Crear una base de datos de credenciales de PAP
- Modificar archivos de configuración de PPP para compatibilidad de PAP

### ▼ Cómo crear una base de datos de credenciales de PAP (servidor de marcación de entrada)

Este procedimiento modifica el archivo `/etc/ppp/pap-secrets`, que contiene las credenciales de seguridad de PAP que se utilizan para autenticar los emisores de llamadas en el enlace. `/etc/ppp/pap-secrets` debe existir en ambos equipos en un enlace de PPP.

El ejemplo de configuración de PAP que se presentó en la [Figura 16-3](#) utiliza la opción `login` de PAP. Si planea utilizar esta opción, puede que también necesite actualizar la base de datos de contraseñas de red. Para obtener más información sobre la opción `login`, consulte “Uso de la opción `login` con `/etc/ppp/pap-secrets`” en la página 535.

- 1 **Arme una lista de todos los posibles emisores de llamadas de confianza. Los emisores de llamadas de confianza son personas a las que se debe otorgar el permiso de llamar al servidor de marcación de entrada desde sus equipos remotos.**
- 2 **Verifique que cada emisor de confianza ya tenga un nombre de usuario y una contraseña de UNIX en la base de datos de contraseñas del servidor de marcación de entrada.**

---

**Nota** – La verificación es importante para el ejemplo de configuración de PAP, que utiliza la opción login de PAP para autenticar a los emisores de llamadas. Si decide no implementar login para PAP, los nombres de usuario de PAP de los emisores de llamadas no tienen que corresponderse con sus nombres de usuario de UNIX. Para obtener más información sobre `/etc/ppp/pap-secrets` estándar, consulte [“Archivo `/etc/ppp/pap-secrets`” en la página 532](#).

---

Realice las siguientes acciones si un posible emisor de llamada no tiene un nombre de usuario y una contraseña de UNIX:

- a. **Confirme con sus gestores que emisores de llamadas que no conoce personalmente tienen permiso de acceso al servidor de marcación de entrada.**
  - b. **Cree nombres de usuario y contraseñas de UNIX para estos emisores de llamadas de manera que se guíen por la política de seguridad corporativa.**
- 3 **Conviértase en superusuario en el servidor de marcación de entrada o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 4 **Edite el archivo `/etc/ppp/pap-secrets`.**

Esta versión proporciona un archivo `pap-secrets` en `/etc/ppp` que contiene comentarios sobre cómo utilizar la autenticación PAP, pero no contiene opciones. Puede agregar las siguientes opciones al final de los comentarios.

```
user1      myserver      ""          *
user2      myserver      ""          *
myserver   user2         serverpass  *
```

Para utilizar la opción login de `/etc/ppp/pap-secrets`, debe escribir el nombre de usuario de UNIX de cada emisor de llamada de confianza. Siempre que un juego de comillas dobles (“”) aparece en el tercer campo, la contraseña para el emisor de llamada se consulta en la base de datos de contraseñas del servidor.

La entrada `myserver * serverpass *` contiene el nombre de usuario y la contraseña de PAP para el servidor de marcación de entrada. En la [Figura 16–3](#), el emisor de llamada de confianza `user2` necesita autenticación de iguales remotos. Por lo tanto, el archivo `/etc/ppp/pap-secrets` de `myserver` contiene credenciales de PAP para utilizarlas cuando haya un enlace establecido con `user2`.

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- “Modificación de archivos de configuración de PPP para PAP (servidor de marcación de entrada)” en la página 469
- “Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)” en la página 470

## Modificación de archivos de configuración de PPP para PAP (servidor de marcación de entrada)

Las tareas de esta sección explican cómo actualizar cualquier archivo de configuración de PPP existente para admitir la autenticación PAP en el servidor de marcación de entrada.

### ▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (servidor de marcación de entrada)

El procedimiento usa como ejemplos los archivos de configuración de PPP que se presentaron en “Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada)” en la página 456.

#### 1 Inicie sesión como superusuario en el servidor de marcación de entrada o adopte un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “Configuración de RBAC (mapa de tareas)” de *Guía de administración del sistema: servicios de seguridad*.

#### 2 Agregue opciones de autenticación al archivo `/etc/ppp/options`.

Por ejemplo, debe agregar las opciones en negrita para un archivo `/etc/ppp/options` existente para implementar la autenticación PAP:

```
lock
auth
login
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

`auth` Especifica que el servidor debe autenticar a los emisores de llamadas antes de establecer el enlace.

`login` Especifica que el emisor de llamada remoto se debe autenticar mediante el uso de servicios de autenticación de usuarios de UNIX.

<code>nodedefaultroute</code>	Indica que ninguna sesión de <code>pppd</code> en el sistema local puede establecer una ruta predeterminada sin privilegios <code>root</code> .
<code>proxyarp</code>	Agrega una entrada a la tabla de Protocolo de resolución de direcciones (ARP) del sistema que especifica la dirección IP del igual y la dirección Ethernet del sistema. Con esta opción, el igual parece estar en el Ethernet local para otros sistemas.
<code>ms-dns 10.0.0.1</code>	Habilita <code>pppd</code> para proporcionar una dirección de Servidor de nombres de dominio (DNS), <code>10.0.0.1</code> , para el cliente.
<code>idle 120</code>	Especifica que los usuarios inactivos se desconectan después de dos minutos.

- 3 En el archivo `/etc/ppp/options.cua.a`, agregue la siguiente dirección para el usuario `cua/a`.  
`:10.0.0.2`
- 4 En el archivo `/etc/ppp/options.cua.b`, agregue la siguiente dirección para el usuario `cua/b`.  
`:10.0.0.3`
- 5 En el archivo `/etc/ppp/pap-secrets`, agregue la siguiente entrada.  

*	*	""	*
---	---	----	---

---

**Nota** – La opción `login`, como se ha descrito anteriormente, proporciona la autenticación de usuario necesaria. Esta entrada en el archivo `/etc/ppp/pap-secrets` es la forma estándar de habilitar PAP con la opción `login`.

---

**Véase también** Para configurar credenciales de autenticación PAP para los emisores de llamadas de confianza del servidor de marcación de entrada, consulte [“Configuración de autenticación PAP para emisores de llamadas de confianza \(equipos de marcación de salida\)”](#) en la página 470.

## Configuración de autenticación PAP para emisores de llamadas de confianza (equipos de marcación de salida)

Esta sección contiene tareas para configuración de autenticación PAP en los equipos de marcación de salida de emisores de llamadas de confianza. Como administrador del sistema, puede configurar la autenticación PAP en los sistemas antes de la distribución a los posibles emisores de llamadas. O bien, si los emisores de llamadas remotos ya tienen sus equipos, puede asignarles a estos las tareas de esta sección.

La configuración de PAP para emisores de llamadas de confianza incluye dos tareas:

- Configuración de las credenciales de seguridad de PAP de los emisores de llamadas.
- Configuración de los equipos de marcación de salida de los emisores de llamadas para admitir autenticación PAP.

## ▼ **Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza**

Este procedimiento muestra cómo configurar credenciales de PAP para dos emisores de llamadas de confianza, uno de los cuales necesita credenciales de autenticación de iguales remotos. Los pasos del procedimiento dan por sentado que usted, el administrador del sistema, crea las credenciales de PAP en los equipos de marcación de salida de emisores de llamadas de confianza.

### **1 Conviértase en superusuario en un equipo de marcación de salida o adopte un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

Con el ejemplo de configuración de PAP que se presentó en la [Figura 16–3](#), asuma que el equipo de marcación de salida pertenece a user1.

### **2 Modifique la base de datos pap-secrets para el emisor de llamada.**

Esta versión proporciona un archivo `/etc/ppp/pap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones a este archivo `/etc/ppp/pap-secrets`.

```
user1    myserver  pass1    *
```

Tenga en cuenta que la contraseña de user1 pass1 se transmite en formato ASCII legible a través del enlace. myserver es el nombre del emisor de llamada user1 para el igual.

### **3 Conviértase en superusuario en otro equipo de marcación de salida o adopte un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

Con el ejemplo de autenticación PAP, asuma que este equipo de marcación de salida pertenece al emisor de llamada user2.

**4 Modifique la base de datos pap-secrets para el emisor de llamada.**

Puede agregar las siguientes opciones al final del archivo `/etc/ppp/pap-secrets` existente.

```
user2      myserver  pass2      *
myserver   user2     serverpass *
```

En este ejemplo, `/etc/ppp/pap-secrets` tiene dos entradas. La primera entrada contiene las credenciales de seguridad de PAP que `user2` pasa al servidor de marcación de entrada `myserver` para la autenticación.

`user2` requiere credenciales de PAP del servidor de marcación de entrada como de la negociación de enlace. Por lo tanto, `/etc/ppp/pap-secrets` también contiene credenciales de PAP que se esperan de `myserver` en la segunda línea.

---

**Nota** – Porque la mayoría de los ISP no proporcionan credenciales de autenticación, es posible que el escenario anterior no sea realista para comunicaciones con un ISP.

---

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- [“Cómo crear una base de datos de credenciales de PAP \(servidor de marcación de entrada\)” en la página 467](#)
- [“Cómo configurar credenciales de autenticación PAP para los emisores de llamadas de confianza” en la página 471](#)

# **Modificación de archivos de configuración de PPP para PAP (equipo de marcación de salida)**

Las siguientes tareas explican cómo actualizar los archivos de configuración de PPP existentes para admitir la autenticación PAP en los equipos de marcación de salida de emisores de llamadas de confianza.

El procedimiento utiliza los siguientes parámetros para configurar la autenticación PAP en el equipo de marcación de salida que pertenece a `user2`, que se presentó en la [Figura 16–3](#). `user2` requiere emisores de llamadas entrantes para autenticar, incluidas las llamadas de `myserver` de marcación de entrada.



## ▼ Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP (equipo de marcación de salida)

Este procedimiento usa como ejemplos los archivos de configuración de PPP que se presentaron en [“Cómo definir comunicaciones a través de la línea de serie” en la página 447](#). El procedimiento configura el equipo de marcación de salida que pertenece a user2, como se muestra en la [Figura 16–3](#).

### 1 Inicie sesión en el equipo de marcación de salida como superusuario.

### 2 Modifique el archivo `/etc/ppp/options`.

El siguiente archivo `/etc/ppp/options` contiene opciones para compatibilidad de PAP, que se muestran en negrita.

```
# cat /etc/ppp/options
lock
name user2
auth
require-pap
```

`name user2` Establece user2 como nombre de PAP del usuario en el equipo local. Si se utiliza la opción `login`, el nombre de PAP debe ser el mismo que el nombre de usuario de UNIX del usuario en la base de datos de contraseñas.

`auth` Indica que el equipo de marcación de salida debe autenticar a los emisores de llamadas antes de establecer el enlace.

---

**Nota** – Este equipo de marcación de salida demanda autenticación de sus iguales, aunque la mayoría de los equipos de marcación de salida no realizan esta demanda. Cualquiera de los casos es aceptable.

---

`require-pap` Solicita credenciales de PAP de los iguales.

### 3 Cree un archivo `/etc/ppp/peers/nombre de igual del equipo remoto myserver`.

En el siguiente ejemplo, se muestra cómo agregar compatibilidad de PAP al archivo `/etc/ppp/peers/myserver` existente que se creó en [“Cómo definir la conexión con un igual individual” en la página 449](#).

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

Las nuevas opciones en negrita agregan requisitos de PAP para iguales myserver.

- user user2
- Define user2 como el nombre de usuario del equipo local.
- remotename myserver
- Define myserver como un igual que requiere credenciales de autenticación del equipo local.

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- Para probar la configuración de autenticación PAP mediante una llamada al servidor de marcación de entrada, consulte [“Cómo llamar al servidor de marcación de entrada” en la página 457](#).
- Para obtener más información acerca de la autenticación PAP, consulte [“Protocolo de autenticación de contraseña \(PAP\)” en la página 532](#).

## Configuración de autenticación CHAP

Las tareas de esta sección explican cómo implementar la autenticación en un enlace de PPP mediante el Protocolo de autenticación por desafío mutuo (CHAP). Las tareas utilizan el ejemplo que se muestra en la [Figura 16–4](#) para ilustrar un escenario de trabajo de CHAP para acceso telefónico a una red privada. Utilice las instrucciones como base para la implementación de la autenticación CHAP en el sitio.

Antes de poder realizar los siguientes procedimientos, debe haber hecho lo siguiente:

- Configurado y probado el enlace por marcación telefónica entre un servidor de marcación de entrada y equipos de marcación de salida que pertenecen a emisores de llamadas de confianza.
- Obtenido permiso de superusuario para el equipo local, ya sea servidor de marcación de entrada o equipo de marcación de salida.

## Configuración de autenticación CHAP (mapas de tareas)

TABLA 19–4 Mapa de tareas para autenticación CHAP (servidor de marcación de entrada)

Tarea	Descripción	Para obtener instrucciones
1. Asignar secretos de CHAP a todos los emisores de llamadas de confianza	Crear o hacer que los emisores de llamadas creen sus secretos de CHAP.	<a href="#">“Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)” en la página 476</a>

TABLA 19-4 Mapa de tareas para autenticación CHAP (servidor de marcación de entrada) (Continuación)

Tarea	Descripción	Para obtener instrucciones
2. Crear la base de datos chap-secrets	Agregar las credenciales de seguridad para todos los emisores de llamadas de confianza al archivo <code>/etc/ppp/chap-secrets</code> .	<a href="#">“Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)” en la página 476</a>
3. Modificar los archivos de configuración de PPP	Agregar opciones específicas para CHAP a los archivos <code>/etc/ppp/options</code> y <code>/etc/ppp/peers/nombre de igual</code> .	<a href="#">“Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada)” en la página 477</a>

TABLA 19-5 Mapa de tareas para autenticación CHAP (equipo de marcación de salida)

Tarea	Descripción	Para obtener instrucciones
1. Crear la base de datos de CHAP para el equipo del emisor de llamada de confianza	Crear credenciales de seguridad para un emisor de llamada de confianza y, si es necesario, credenciales de seguridad para otros usuarios que llaman al equipo de marcación de salida, en <code>/etc/ppp/chap-secrets</code> .	<a href="#">“Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)” en la página 476</a>
2. Modificar los archivos de configuración de PPP	Agregar opciones específicas para CHAP al archivo <code>/etc/ppp/options</code> .	<a href="#">“Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida)” en la página 480</a>

## Configuración de autenticación CHAP en el servidor de marcación de entrada

La primera tarea en la configuración de autenticación CHAP es modificar el archivo `/etc/ppp/chap-secrets`. Este archivo contiene las credenciales de seguridad de CHAP, incluido el secreto de CHAP, que se utilizan para autenticar a los emisores de llamadas en el enlace.

---

**Nota** – Los mecanismos de autenticación UNIX o PAM no funcionan con CHAP. Por ejemplo, no puede utilizar la opción `login` de PPP, como se describe en [“Cómo crear una base de datos de credenciales de PAP \(servidor de marcación de entrada\)” en la página 467](#). Si el escenario de autenticación requiere autenticación PAM o de estilo UNIX, seleccione PAP en su lugar.

---

El siguiente procedimiento implementa la autenticación CHAP para un servidor de marcación de entrada en una red privada. El enlace de PPP es la única conexión con el mundo exterior. Los únicos emisores de llamadas que tienen acceso a la red son aquellos a los que los gestores de red les han otorgado permiso, incluido, posiblemente, el administrador del sistema.

## ▼ **Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)**

**1 Arme una lista que contenga los nombres de usuario de todos los emisores de llamadas de confianza.**

Los emisores de llamadas de confianza incluyen a todas las personas a las que se les otorgó permiso para llamar a la red privada.

**2 Asigne a cada usuario un secreto de CHAP.**

---

**Nota** – Asegúrese de elegir un buen secreto de CHAP que no sea fácil de adivinar. No hay ninguna otra restricción en el contenido del secreto de CHAP.

---

El método para asignar secretos de CHAP depende de la política de seguridad del sitio. O bien, se tiene la responsabilidad de crear los secretos o los emisores de llamadas deben crear sus propios secretos. Si no es responsable de la asignación de secretos de CHAP, asegúrese de obtener los secretos de CHAP creados por o para emisores de llamadas de confianza.

**3 Conviértase en superusuario en el servidor de marcación de entrada o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**4 Modifique el archivo `/etc/ppp/chap-secrets`.**

Esta versión incluye un archivo `/etc/ppp/chap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones para el servidor `CallServe` al final del archivo `/etc/ppp/chap-secrets` existente.

```
account1 CallServe key123 *
account2 CallServe key456 *
```

`key123` es el secreto de CHAP para emisores de llamadas de confianza `account1`.

`key456` es el secreto de CHAP para emisores de llamadas de confianza `account2`.

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- [“Cómo crear una base de datos de credenciales de CHAP \(servidor de marcación de entrada\)” en la página 476](#)
- [“Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP \(servidor de marcación de entrada\)” en la página 477](#)
- [“Configuración de autenticación CHAP para emisores de llamadas de confianza \(equipos de marcación de salida\)” en la página 478](#)

## Modificación de archivos de configuración de PPP para CHAP (servidor de marcación de entrada)

La tarea de esta sección explica cómo actualizar archivos de configuración de PPP existentes para admitir la autenticación CHAP en el servidor de marcación de entrada.

### ▼ Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (servidor de marcación de entrada)

**1** Inicie sesión en el servidor de marcación de entrada como superusuario.

**2** Modifique el archivo `/etc/ppp/options`.

Agregue las opciones que se muestran en negrita para compatibilidad de CHAP.

```
# cat /etc/ppp/options
lock
nodefaultroute
name CallServe
auth
```

`name CallServe` Define *CallServe* como nombre de usuario de CHAP en el equipo local, en esta instancia, el servidor de marcación de entrada.

`auth` Hace que el equipo local autentique a los emisores de llamadas antes de establecer el enlace.

**3** Cree el resto de los archivos de configuración de PPP para admitir a los emisores de llamadas de confianza.

Consulte “Cómo configurar usuarios del servidor de marcación de entrada” en la página 454 y “Cómo definir comunicaciones a través de la línea de serie (servidor de marcación de entrada)” en la página 456.

**Véase también** Para configurar las credenciales de autenticación CHAP para emisores de llamadas de confianza, consulte “Cómo crear una base de datos de credenciales de CHAP (servidor de marcación de entrada)” en la página 476.

## Configuración de autenticación CHAP para emisores de llamadas de confianza (equipos de marcación de salida)

Esta sección contiene tareas para configuración de autenticación CHAP en los equipos de marcación de salida de emisores de llamadas de confianza. En función de la política de seguridad del sitio, tanto usted como los emisores de llamadas de confianza pueden ser responsables de la configuración de autenticación CHAP.

Para que los emisores de llamadas remotos configuren CHAP, asegúrese de que los secretos de CHAP locales de los emisores coincidan con los secretos de CHAP equivalentes de los emisores de llamadas en el archivo `/etc/ppp/chap-secrets` del servidor de marcación de entrada. A continuación, proporcione a los emisores de llamadas las tareas de esta sección para la configuración de CHAP.

La configuración de CHAP para emisores de llamadas de confianza incluye dos tareas:

- Creación de credenciales de seguridad de CHAP de emisores de llamadas.
- Configuración de los equipos de marcación de salida de los emisores de llamadas para admitir autenticación CHAP.

### ▼ Cómo configurar credenciales de autenticación CHAP para los emisores de llamadas de confianza

Este procedimiento muestra cómo configurar credenciales de CHAP para dos emisores de llamadas de confianza. Los pasos del procedimiento dan por sentado que usted, el administrador del sistema, crea las credenciales de CHAP en los equipos de marcación de salida de emisores de llamadas de confianza.

#### 1 Conviértase en superusuario en un equipo de marcación de salida o adopte un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

Con el ejemplo de configuración de CHAP en [“Ejemplo de una configuración mediante autenticación CHAP” en la página 436](#), asuma que el equipo de marcación de salida pertenece a un emisor de llamada de confianza `account1`.

**2 Modifique la base de datos chap-secrets para el emisor de llamada account1.**

Esta versión incluye un archivo `/etc/ppp/chap-secrets` que contiene comentarios útiles, pero no contiene opciones. Puede agregar las siguientes opciones al archivo `/etc/ppp/chap-secrets` existente.

```
account1 CallServe key123 *
```

`CallServe` es el nombre del igual que `account1` está intentando alcanzar. `key123` es el secreto de CHAP que se utilizará para enlaces entre `account1` y `CallServer`.

**3 Conviértase en superusuario en otro equipo de marcación de salida o adopte un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

Asuma que este equipo pertenece al emisor de llamada `account2`.

**4 Modifique la base de datos `/etc/ppp/chap-secrets` para el emisor de llamada account2.**

```
account2 CallServe key456 *
```

Ahora, `account2` tiene el secreto `key456` como sus credenciales de CHAP para utilizar a través de enlaces con el igual `CallServe`.

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- [“Cómo crear una base de datos de credenciales de CHAP \(servidor de marcación de entrada\)” en la página 476](#)
- [“Cómo configurar credenciales de autenticación CHAP para los emisores de llamadas de confianza” en la página 478](#)

## Adición de CHAP para los archivos de configuración (equipo de marcación de salida)

Para obtener más información sobre la autenticación CHAP, consulte [“Protocolo de autenticación por desafío mutuo \(CHAP\)” en la página 535](#). La siguiente tarea configura el equipo de marcación de salida que pertenece al emisor de llamada `account1`, que se presenta en [“Ejemplo de una configuración mediante autenticación CHAP” en la página 436](#).

## ▼ **Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP (equipo de marcación de salida)**

- 1 **Inicie sesión en el equipo de marcación de salida como superusuario.**
- 2 **Asegúrese de que el archivo `/etc/ppp/options` tenga las siguientes opciones.**

```
# cat /etc/ppp/options
lock
nodefaultroute
```

- 3 **Cree un archivo `/etc/ppp/peers/nombre de igual` para el equipo remoto CallServe.**

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

La opción `user account1` establece `account1` como nombre de usuario de CHAP que se otorgará a `CallServe`. Para obtener una descripción de las otras opciones en el archivo anterior, consulte el archivo similar `/etc/ppp/peers/myserver` en [“Cómo definir la conexión con un igual individual” en la página 449](#).

**Véase también** Para probar la autenticación CHAP mediante una llamada al servidor de marcación de entrada, consulte [“Cómo llamar al servidor de marcación de entrada” en la página 457](#).



## Configuración de un túnel PPPoE (tareas)

Este capítulo contiene tareas para configurar los participantes en cualquiera de los extremos del túnel PPPoE: el cliente PPPoE y el servidor de acceso PPPoE. Los temas específicos incluyen lo siguiente:

- “Tareas principales para la configuración de un túnel PPPoE (mapas de tareas)” en la página 481
- “Configuración del cliente PPPoE” en la página 482
- “Configuración de un servidor de acceso PPPoE” en la página 485

Las tareas utilizan el escenario que se presentó en “Planificación de compatibilidad de DSL a través de un túnel PPPoE” en la página 438 como un ejemplo. Para obtener una descripción general de PPPoE, consulte “Compatibilidad para usuarios de DSL a través de PPPoE” en la página 422.

### Tareas principales para la configuración de un túnel PPPoE (mapas de tareas)

En las siguientes tablas, se enumeran las tareas principales para la configuración de clientes PPPoE y el servidor de acceso PPPoE. Para implementar PPPoE en su sitio, necesita configurar sólo el extremo de su túnel PPPoE, ya sea el lado del cliente o del servidor de acceso.

TABLA 20-1 Mapa de tareas para configuración de un cliente PPPoE

Tarea	Descripción	Para obtener instrucciones
1. Configurar una interfaz para PPPoE	Definir la interfaz Ethernet que se utilizará para el túnel PPPoE.	“Cómo configurar una interfaz para un cliente PPPoE” en la página 483
2. Configurar la información sobre el servidor de acceso PPPoE	Definir los parámetros para el servidor de acceso en el extremo del proveedor de servicios del túnel PPPoE.	“Cómo definir un igual de servidor de acceso PPPoE” en la página 483

TABLA 20-1 Mapa de tareas para configuración de un cliente PPPoE (Continuación)

Tarea	Descripción	Para obtener instrucciones
3. Configurar los archivos de configuración de PPP	Definir los archivos de configuración de PPP para el cliente, si no lo ha hecho aún.	<a href="#">“Cómo definir comunicaciones a través de la línea de serie” en la página 447</a>
4. Crear el túnel	Llamar al servidor de acceso.	<a href="#">“Cómo definir un igual de servidor de acceso PPPoE” en la página 483</a>

TABLA 20-2 Mapa de tareas para configuración de un servidor de acceso PPPoE

Tarea	Descripción	Para obtener instrucciones
1. Configurar un servidor de acceso PPPoE	Definir la interfaz Ethernet que se utilizará para el túnel PPPoE y definir los servicios que ofrece el servidor de acceso.	<a href="#">“Cómo configurar un servidor de acceso PPPoE” en la página 485</a>
2. Configurar los archivos de configuración de PPP	Definir los archivos de configuración de PPP para el cliente, si no lo ha hecho aún.	<a href="#">“Configuración de comunicaciones a través del servidor de marcación de entrada” en la página 455</a>
3. (Opcional) Limitar el uso de una interfaz	Usar las opciones de PPPoE y autenticación PAP para restringir el uso de una interfaz Ethernet en particular para determinados clientes.	<a href="#">“Cómo restringir el uso de una interfaz a clientes específicos” en la página 487</a>

## Configuración del cliente PPPoE

Para proporcionar PPP a sistemas cliente a través de DSL, primero debe configurar PPPoE en la interfaz que está conectada al módem o concentrador. Luego necesita cambiar los archivos de configuración de PPP para definir el servidor de acceso en el extremo opuesto de PPPoE.

### Requisitos previos para la configuración del cliente PPPoE

Antes de poder configurar el cliente PPPoE, debe haber hecho lo siguiente:

- Instalado la versión de Solaris en los equipos cliente para utilizar el túnel PPPoE.
- Contactado al proveedor de servicios para obtener información acerca de su servidor de acceso PPPoE.
- Logrado que la compañía telefónica o el proveedor de servicios conecten los dispositivos que utilizan los equipos cliente. Esos dispositivos incluyen, por ejemplo, el módem DSL y el separador, que es posible que de eso se encargue la compañía telefónica.

## ▼ Cómo configurar una interfaz para un cliente PPPoE

Utilice este procedimiento para definir la interfaz Ethernet que se utilizará para el túnel PPPoE.

### 1 Conviértase en superusuario en el cliente PPPoE o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Agregue el nombre de la interfaz Ethernet con la conexión DSL para el archivo `/etc/ppp/pppoe.if`.

Por ejemplo, agregue la siguiente entrada a `/etc/ppp/pppoe.if` para un cliente PPPoE que utiliza `hme0` como la interfaz de red que está conectada al módem DSL.

```
hme0
```

Para obtener más información sobre `/etc/ppp/pppoe.if`, vaya a [“Archivo `/etc/ppp/pppoe.if`” en la página 542](#).

### 3 Configure la interfaz para utilizar PPPoE.

```
# /etc/init.d/pppd start
```

### 4 (Opcional) Verifique que la interfaz esté conectada para PPPoE.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
```

También puede utilizar el comando `/usr/sbin/sppptun` para conectar manualmente interfaces para PPPoE. Para obtener instrucciones, consulte [“Comando `/usr/sbin/sppptun`” en la página 542](#).

## ▼ Cómo definir un igual de servidor de acceso PPPoE

Define el servidor de acceso en el archivo `/etc/ppp/peers/nombre de igual`. Muchas de las opciones que se utilizan para el servidor de acceso también se utilizan para definir el servidor de marcación de entrada en un escenario de marcación telefónica. Para obtener una explicación detallada de `/etc/ppp/peers/nombre de igual`, consulte [“Archivo `/etc/ppp/peers/nombre de igual`” en la página 519](#).

### 1 Conviértase en superusuario en el cliente PPPoE o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Defina el servidor de acceso PPPoE del proveedor de servicios en el archivo**

***/etc/ppp/peers/nombre de igual.***

Por ejemplo, el siguiente archivo, `/etc/ppp/peers/dslserve`, define el servidor de acceso `dslserve` en Far ISP que se presenta en [“Ejemplo de una configuración para un túnel PPPoE” en la página 440.](#)

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoc hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Para obtener una definición de las opciones de este archivo, vaya a [“Archivo para definir un igual de servidor de acceso /etc/ppp/peers/nombre de igual” en la página 549.](#)

**3 Modifique los archivos de configuración de PPP en el cliente PPPoE.**

- a. Configure `/etc/ppp/options` como se describe en las instrucciones para la configuración de un equipo de marcación de salida en [“Configuración del equipo de marcación de salida” en la página 444.](#)
- b. Cree un archivo `/etc/ppp/options.sppptun`. `/etc/ppp/options.sppptun` define opciones de PPP para el puerto de serie al cual está conectada la interfaz (la cual está conectada para PPPoE).

Puede utilizar cualquiera de las opciones que están disponibles para el archivo `/etc/ppp/options.nombre de tty` según lo descrito en el [“Archivo de configuración /etc/ppp/options.nombre de tty” en la página 515.](#) Debe dar al archivo el nombre `/etc/ppp/options.sppptun` porque `sppptun` es el nombre de dispositivo especificado en la configuración de `pppd`.

**4 Asegúrese de que todos los usuarios puedan iniciar PPP en el cliente.**

```
# touch /etc/ppp/options
```

**5 Pruebe si PPP puede ejecutar la línea DSL.**

```
% pppd debug updetach call dslserve
```

`dslserve` es el nombre que se asigna al servidor de acceso de ISP que se muestra en [“Ejemplo de una configuración para un túnel PPPoE” en la página 440.](#) La opción `debug updetach` provoca que la información de depuración se muestre en una ventana de terminal.

Si PPP se ejecuta correctamente, la salida de terminal muestra cuando el enlace se vuelve activo. Si PPP todavía no se ejecuta, intente el siguiente comando para ver si los servidores se ejecutan correctamente:

```
# /usr/lib/inet/pppoc -i hme0
```

---

**Nota** – Los usuarios de clientes PPPoE configurados pueden iniciar la ejecución de PPP a través de una línea DSL al escribir lo siguiente:

```
% pppd call ISP-server-name
```

Entonces los usuarios pueden ejecutar una aplicación o un servicio.

---

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- Consulte [“Configuración del cliente PPPoE”](#) en la página 482.
- Consulte [“Creación de túneles PPPoE para compatibilidad de DSL”](#) en la página 541.
- Consulte el [Capítulo 21](#), [“Resolución de problemas comunes de PPP \(tareas\)”](#).
- Consulte [“Configuración de un servidor de acceso PPPoE”](#) en la página 485.

## Configuración de un servidor de acceso PPPoE

Si su compañía es un proveedor de servicios, puede ofrecer Internet y otros servicios a los clientes que lleguen a su sitio mediante conexiones DSL. El procedimiento implica determinar qué interfaces en el servidor deben formar parte del túnel PPPoE y definir qué servicios estarán disponibles para los usuarios.

### ▼ Cómo configurar un servidor de acceso PPPoE

Utilice este procedimiento para definir la interfaz Ethernet que se utilizará para el túnel PPPoE y para configurar los servicios que ofrece el servidor de acceso.

#### 1 Conviértase en superusuario en el servidor de acceso o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)”](#) de *Guía de administración del sistema: servicios de seguridad*.

- 2 Agregue el nombre de las interfaces Ethernet dedicadas a los túneles PPPoE para el archivo `/etc/ppp/pppoe.if`.**

Por ejemplo, debe utilizar el siguiente archivo `/etc/ppp/pppoe.if` para el servidor de acceso `dsldslserve` que se muestra en [“Ejemplo de una configuración para un túnel PPPoE” en la página 440](#).

```
# cat /etc/ppp/pppoe.if
hme1
hme2
```

- 3 Defina los servicios globales que proporciona el servidor de acceso en el archivo `/etc/ppp/pppoe`.**

El siguiente archivo `/etc/ppp/pppoe` enumera los servicios que proporciona el servidor de acceso `dsldslserve`, que se mostró en la [Figura 16–5](#).

```
device hme1,hme2
service internet
    pppd "proxyarp 192.168.1.1:"
service debugging
    pppd "debug proxyarp 192.168.1.1:"
```

En el ejemplo de archivo, el servicio de Internet se anuncia para las interfaces Ethernet de `dsldslserve` `hme1` y `hme2`. La depuración está activada para enlaces de PPP en las interfaces Ethernet.

- 4 Configure los archivos de configuración de PPP de la misma manera que lo haría para un servidor de marcación de entrada.**

Para obtener más información, consulte [“Creación de un esquema de direccionamiento IP para emisores de llamadas” en la página 538](#).

- 5 Inicie el daemon `pppoed`.**

```
# /etc/init.d/pppd start
```

`pppd` también conecta las interfaces que se enumeran en `/etc/ppp/pppoe.if`.

- 6 (Opcional) Verifique que las interfaces en el servidor estén conectadas para PPPoE.**

```
# /usr/sbin/sppptun query
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

El ejemplo anterior muestra que las interfaces `hme1` y `hme2` están conectadas para PPPoE. También puede utilizar el comando `/usr/sbin/sppptun` para conectar manualmente interfaces para PPPoE. Para obtener instrucciones, consulte [“Comando `/usr/sbin/sppptun`” en la página 542](#).

## ▼ Cómo modificar un archivo `/etc/ppp/pppoe` existente

- 1 **Conviértase en superusuario en el servidor de acceso o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Modifique `/etc/ppp/pppoe`, según sea necesario.**

- 3 **Haga que el daemon `pppoed` reconozca los nuevos servicios.**

```
# pkill -HUP pppoed
```

## ▼ Cómo restringir el uso de una interfaz a clientes específicos

El siguiente procedimiento muestra cómo restringir una interfaz a un grupo de clientes PPPoE. Antes de realizar esta tarea, debe obtener las direcciones MAC Ethernet reales de los clientes a los que les asigna la interfaz.

---

**Nota** – Algunos sistemas le permiten cambiar la dirección MAC de la interfaz Ethernet. Debe considerar esta capacidad como una comodidad, no como una medida de seguridad.

---

En el ejemplo que se muestra en [“Ejemplo de una configuración para un túnel PPPoE” en la página 440](#), se muestran los pasos sobre cómo reservar una de las interfaces `ds1serve`, `hme1`, para clientes en `MiddleCo`.

- 1 **Configure la interfaz del servidor de acceso y defina los servicios, como se muestra en [“Cómo configurar un servidor de acceso PPPoE” en la página 485](#).**

- 2 **Cree entradas para los clientes en la base de datos `/etc/ethers` del servidor.**

A continuación, se muestra una entrada para clientes Rojo, Azul, Amarillo.

```
8:0:20:1:40:30 redether
8:0:20:1:40:10 yellowether
8:0:20:1:40:25 blueether
```

El ejemplo asigna los nombres simbólicos `redether`, `yellowether` y `blueether` para las direcciones Ethernet de clientes Rojo, Amarillo y Azul. La asignación de nombres simbólicos para las direcciones MAC es opcional.

### 3 Restrinja los servicios que se proporcionan en una interfaz específica definiendo la siguiente información en el archivo `/etc/ppp/pppoe.dispositivo`.

En este archivo, *dispositivo* es el nombre del dispositivo que se va a definir.

```
# cat /etc/ppp/pppoe.hme1
service internet
    pppd "name dslserve-hme1"
        clients redether,yellowether,blueether
```

`dslserve-hme1` es el nombre del servidor de acceso, que se utiliza para hacer coincidir entradas en el archivo `pap-secrets`. La opción `clients` restringe el uso de la interfaz `hme1` a los clientes con los nombres Ethernet simbólicos `redether`, `yellowether` y `blueether`.

Si no definió nombres simbólicos para las direcciones MAC del cliente en `/etc/ethers`, puede utilizar las direcciones numéricas como argumentos para la opción `clients`. Se permiten comodines.

Por ejemplo, puede especificar la dirección numérica `clients 8:0:20::*:*`. Mediante el uso de comodines, todas las direcciones que coinciden en `/etc/ethers` son aceptadas.

### 4 Cree el archivo `/etc/ppp/pap-secrets` para el servidor de acceso:

Red	<code>dslserve-hme1</code>	<code>redpasswd</code>	*
Blue	<code>dslserve-hme1</code>	<code>bluepasswd</code>	*
Yellow	<code>dslserve-hme1</code>	<code>yellowpasswd</code>	*

Las entradas son los nombres y las contraseñas de PAP de clientes autorizados a ejecutar PPP a través de la interfaz `hme1` de `dslserve`.

Para obtener más información sobre la autenticación PAP, consulte [“Configuración de autenticación PAP” en la página 466](#).

**Véase también** La siguiente lista proporciona referencias a la información relacionada.

- Para obtener más información sobre PPPoE, consulte [“Creación de túneles PPPoE para compatibilidad de DSL” en la página 541](#).
- Para solucionar problemas de PPPoE y PPP, consulte [“Resolución de problemas relacionados con PPP y PPPoE” en la página 493](#).
- Para configurar un cliente PPPoE, consulte [“Configuración del cliente PPPoE” en la página 482](#).
- Para configurar la autenticación PAP para un cliente, consulte [“Configuración de autenticación PAP para emisores de llamadas de confianza \(equipos de marcación de salida\)” en la página 470](#).
- Para configurar la autenticación PAP en un servidor, consulte [“Configuración de autenticación PAP en el servidor de marcación de entrada” en la página 467](#).



## Resolución de problemas comunes de PPP (tareas)

---

Este capítulo contiene información para solucionar problemas comunes que se producen con Solaris PPP 4.0. Contiene los temas siguientes:

- “Herramientas para resolución de problemas de PPP” en la página 490
- “Resolución de problemas relacionados con PPP y PPPoE” en la página 493
- “Resolución de problemas de línea arrendada” en la página 506
- “Diagnóstico y resolución de problemas de autenticación” en la página 507

Las fuentes *PPP Design, Implementation, and Debugging* por James Carlson y el sitio web de la Universidad Nacional de Australia (ANU, Australian National University) también detallan sugerencias para la resolución de problemas de PPP. Para obtener más información, consulte “Manuales de referencia profesional sobre PPP” en la página 412 y “Sitios web sobre PPP” en la página 412.

## Resolución de problemas de PPP (mapa de tareas)

Utilice el siguiente mapa de tareas para acceder rápidamente a sugerencias y resolución de problemas de PPP comunes.

TABLA 21-1 Mapa de tareas para resolución de problemas de PPP

Tarea	Definición	Para obtener instrucciones
Obtener información de diagnóstico sobre el enlace de PPP	Utilizar herramientas de diagnóstico de PPP para obtener resultados para la resolución de problemas.	<a href="#">“Cómo obtener información de diagnóstico de pppd” en la página 491</a>
Obtener información de depuración para el enlace de PPP	Utilizar el comando <code>pppd debug</code> con el fin de generar un resultado para la resolución de problemas.	<a href="#">“Cómo activar la depuración de PPP” en la página 492</a>

TABLA 21-1 Mapa de tareas para resolución de problemas de PPP (Continuación)

Tarea	Definición	Para obtener instrucciones
Solucionar problemas generales con la capa de red	Identificar y solucionar problemas de PPP relacionados con la red mediante una serie de comprobaciones.	<a href="#">“Cómo diagnosticar problemas de red” en la página 494</a>
Solucionar problemas de comunicaciones generales	Identificar y solucionar problemas de comunicaciones que afectan al enlace de PPP.	<a href="#">“Cómo diagnosticar y solucionar problemas de comunicaciones” en la página 496</a>
Solucionar problemas de configuración	Identificar y solucionar problemas en los archivos de configuración de PPP.	<a href="#">“Cómo diagnosticar problemas con la configuración de PPP” en la página 498</a>
Solucionar problemas relacionados con el módem	Identificar y corregir problemas del módem.	<a href="#">“Cómo diagnosticar problemas del módem” en la página 498</a>
Solucionar problemas relacionados con la secuencia de comandos de chat	Identificar y solucionar problemas de la secuencia de comandos de chat en un equipo de marcación de salida.	<a href="#">“Cómo obtener información de depuración para secuencias de comandos de chat” en la página 500</a>
Solucionar problemas de velocidad de la línea de serie	Identificar y solucionar problemas de velocidad de la línea en un servidor de marcación de entrada.	<a href="#">“Cómo diagnosticar y solucionar problemas de velocidad de línea de serie” en la página 503</a>
Solucionar problemas comunes de las líneas arrendadas	Identificar y solucionar los problemas de rendimiento de una línea arrendada.	<a href="#">“Resolución de problemas de línea arrendada” en la página 506</a>
Solucionar problemas relacionados con la autenticación	Identificar y solucionar problemas relacionados con las bases de datos de autenticación.	<a href="#">“Diagnóstico y resolución de problemas de autenticación” en la página 507</a>
Solucionar problemas de áreas para PPPoE	Utilizar herramientas de diagnóstico de PPP para obtener una solución para identificar y solucionar problemas de PPPoE.	<a href="#">“Cómo obtener información de diagnóstico para PPPoE” en la página 504</a>

## Herramientas para resolución de problemas de PPP

Los enlaces de PPP generalmente tienen tres áreas principales de fallo:

- Fallo del enlace que se establecerá
- Bajo rendimiento del enlace durante el uso regular
- Problemas que pueden rastrearse en las redes en cualquier lado del enlace

La manera más sencilla de averiguar si PPP funciona es ejecutar un comando a través del enlace. Ejecute un comando como ping o traceroute para un host en la red del igual. A continuación,

observe los resultados. Sin embargo, debe utilizar herramientas de depuración de PPP y UNIX para supervisar el rendimiento de un enlace establecido o para solucionar un enlace problemático.

Esta sección explica cómo obtener información de diagnóstico de `pppd` y sus archivos de registro asociados. El resto de las secciones de este capítulo describen problemas habituales con PPP que puede detectar y solucionar con la ayuda de las herramientas de resolución de problemas de PPP.

## ▼ Cómo obtener información de diagnóstico de `pppd`

El siguiente procedimiento muestra cómo visualizar la operación actual de un enlace en el equipo local.

### 1 Conviértase en superusuario en el equipo local o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de \*Guía de administración del sistema: servicios de seguridad\*](#).

### 2 Ejecute `pppd` con el dispositivo serie configurado para PPP como el argumento:

```
# pppd cua/b debug updetach
```

Los siguientes ejemplos muestran las pantallas que se obtienen como resultado de un enlace por marcación telefónica y un enlace de línea arrendada cuando `pppd` se ejecuta en primer plano. Si ejecuta `pppd debug` en segundo plano, el resultado que se obtiene se envía al archivo `/etc/ppp/connect-errors`.

#### Ejemplo 21–1 Resultado de un enlace por marcación telefónica que funciona correctamente

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <-> /dev/cua/b
sent [LCP ConfReq id=0x7b <asynmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 6
2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 6 2004 09:36:22)
rcvd [LCP ConfRej id=0x7b <asynmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
2004 09:38:33)"]
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
```

```
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
Oct 6 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>]
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>]
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local IP address 10.0.0.2
remote IP address 10.0.0.1
```

## Ejemplo 21–2 Resultado de un enlace de línea arrendada que funciona correctamente

```
# pppd /dev/se_hdlc1 default-asynctmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <-> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ 0f 01>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ 0f 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ 0f 01>]
local IP address 10.0.0.2
remote IP address 10.0.0.1
```

## ▼ Cómo activar la depuración de PPP

La siguiente tarea muestra cómo utilizar el comando `pppd` para obtener información de depuración.

---

**Nota** – Sólo necesita realizar del paso 1 al paso 3 una vez para cada host. A partir de ese momento, puede continuar con el paso 4 para activar la depuración para el host.

---

**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)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Cree un archivo de registro para mantener los resultados de pppd.**

```
# touch /var/log/pppdebug
```

**3 Agregue las siguientes utilidades syslog para pppd en /etc/syslog.conf.**

```
daemon.debug;local2.debug          /var/log/pppdebug
```

**4 Reinicie syslogd.**

```
# pkill -HUP -x syslogd
```

**5 Active la depuración para llamadas a un igual específico mediante la siguiente sintaxis de pppd.**

```
# pppd debug call peer-name
```

*nombre de igual* debe ser el nombre de un archivo en el directorio /etc/ppp/peers.

**6 Visualice los contenidos del archivo de registro.**

```
# tail -f /var/log/pppdebug
```

Para obtener un ejemplo de un archivo de registro, consulte el [Paso 3](#).

## Resolución de problemas relacionados con PPP y PPPoE

Consulte las siguientes secciones para obtener información sobre cómo resolver problemas relacionados con PPP y PPPoE.

- “Cómo diagnosticar problemas de red” en la página 494
- “Problemas de red comunes que afectan el PPP” en la página 495
- “Cómo diagnosticar y solucionar problemas de comunicaciones” en la página 496
- “Problemas de comunicaciones generales que afectan PPP” en la página 497
- “Cómo diagnosticar problemas con la configuración de PPP” en la página 498
- “Problemas de configuración de PPP comunes” en la página 498
- “Cómo diagnosticar problemas del módem” en la página 498
- “Cómo obtener información de depuración para secuencias de comandos de chat” en la página 500
- “Problemas de secuencia de comandos de chat comunes” en la página 500
- “Cómo diagnosticar y solucionar problemas de velocidad de línea de serie” en la página 503
- “Cómo obtener información de diagnóstico para PPPoE” en la página 504

## ▼ Cómo diagnosticar problemas de red

Si el enlace de PPP pasa a ser activo pero sólo se puede establecer contacto con pocos hosts remotos, se puede tratar de un problema de red. El siguiente procedimiento le muestra cómo aislar y solucionar problemas de red que afectan a un enlace de PPP.

### 1 Conviértase en superusuario en el equipo local o asuma un rol equivalente.

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Cierre el enlace problemático.

### 3 Deshabilite cualquier protocolo opcional en los archivos de configuración agregando las siguientes opciones para la configuración de PPP:

```
noccp novj nopcomp noaccomp default-asynmap
```

Estas opciones proporcionan el PPP no comprimido más simple que está disponible. Intente invocar estas opciones como argumentos para `pppd` en la línea de comandos. Si puede acceder a hosts que antes eran inaccesibles, agregue las opciones en cualquiera de las siguientes ubicaciones.

- `/etc/ppp/peers/nombre de igual`, después de la opción `call`
- `/etc/ppp/options` y asegúrese de que las opciones se apliquen globalmente

### 4 Llame al igual remoto. A continuación, habilite las funciones de depuración.

```
% pppd debug call peer-name
```

### 5 Obtenga registros detallados del programa de chat mediante la opción `-v` de chat.

Por ejemplo, utilice el siguiente formato en cualquier archivo de configuración de PPP:

```
connect 'chat -v -f /etc/ppp/chatfile'
```

`/etc/ppp/chatfile` representa el nombre del archivo de chat.

### 6 Intente recrear el problema mediante Telnet u otras aplicaciones para llegar a los hosts remotos.

Observe los registros de depuración. Si aún no puede alcanzar los hosts remotos, es posible que el problema de PPP esté relacionado con la red.

### 7 Verifique que las direcciones IP de los hosts remotos sean direcciones de Internet registradas.

Algunas organizaciones asignan direcciones IP internas que son conocidas en la red local, pero que no se pueden enrutar a Internet. Si los hosts remotos se encuentran dentro de la compañía, debe configurar un servidor de traducción de dirección de red (NAT) o servidor proxy para acceder a Internet. Si los hosts remotos no están en la compañía, debe informar el problema a la organización remota.

**8 Examine las tablas de enrutamiento.**

- a. Compruebe las tablas de enrutamiento en el equipo local y en el igual.
- b. Compruebe las tablas de enrutamiento de cualquier enrutador que se encuentre en la ruta desde el igual hasta el servidor remoto. Compruebe también las tablas de enrutamiento de cualquier enrutador que se encuentre en la ruta de retorno al igual.

Asegúrese de que los enrutadores intermedios no se hayan configurado incorrectamente. Con frecuencia el problema se encuentra en la ruta de retorno al igual.

**9 (Opcional) Si el equipo es un enrutador, compruebe las características opcionales.**

```
# ndd -set /dev/ip ip_forwarding 1
```

Para obtener más información acerca de `ndd`, consulte la página del comando `man ndd(1M)`.

En la versión Solaris 10, puede usar `routeadm(1M)` en lugar de `ndd(1M)`.

```
# routeadm -e ipv4-forwarding -u
```

---

**Nota** – El comando `ndd` no es persistente. Los valores establecidos con este comando se pierden cuando el sistema se reinicia. El comando `routeadm` es persistente. Los valores establecidos con este comando se mantienen después de que se reinicia el sistema.

---

**10 Compruebe las estadísticas que se obtienen de `netstat -s` y herramientas similares.**

Para obtener detalles completos sobre `netstat`, consulte la página del comando `man netstat(1M)`.

- a. Ejecute estadísticas en el equipo local.
- b. Llame al igual.
- c. Observe las nuevas estadísticas generadas por `netstat -s`. Para obtener más información, consulte “[Problemas de red comunes que afectan el PPP](#)” en la página 495.

**11 Compruebe la configuración de DNS.**

Una configuración de servicio de nombres defectuosa hace que las aplicaciones fallen porque no se pueden resolver direcciones IP.

## Problemas de red comunes que afectan el PPP

Puede utilizar los mensajes que genera `netstat -s` para solucionar los problemas de red que se muestran en la siguiente tabla. Para obtener información de procedimiento relacionada, consulte “[Cómo diagnosticar problemas de red](#)” en la página 494.

TABLA 21-2 Problemas de red comunes que afectan el PPP

Mensaje	Problema	Solución
IP packets not forwardable	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.
ICMP input destination unreachable	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.
ICMP time exceeded	Dos enrutadores se envían la misma dirección de destino a cada uno, lo que provoca que el paquete vaya y vuelva hasta que el valor de tiempo de actividad (TTL) se excede.	Utilice traceroute para averiguar el origen del bucle de enrutamiento y, a continuación, póngase en contacto con el administrador del enrutador que presenta el error. Para obtener información sobre traceroute, consulte la página del comando <code>man traceroute(1M)</code> .
IP packets not forwardable	Falta una ruta en el host local.	Agregue la ruta faltante a la tabla de enrutamiento del host local.
ICMP input destination unreachable	Falta una ruta en el host local.	Agregue la ruta faltante a las tablas de enrutamiento del host local.

## ▼ Cómo diagnosticar y solucionar problemas de comunicaciones

Los problemas de comunicaciones se producen cuando los dos iguales no pueden establecer un enlace correctamente. Algunas veces, estos problemas son, en realidad, problemas de negociación causados por secuencias de comandos de chat configuradas incorrectamente. El siguiente procedimiento muestra cómo solucionar problemas de comunicación. Para solucionar problemas de negociación causados por una secuencia de comandos de chat defectuosa, consulte la [Tabla 21-5](#).

**1 Conviértase en superusuario en el equipo local o asuma un rol equivalente.**

Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte “[Configuración de RBAC \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Llame al igual.**

**3 Llame al igual remoto. A continuación, habilite las funciones de depuración.**

```
% pppd debug call peer-name
```

Es posible que necesite obtener información de depuración del igual para solucionar determinados problemas de comunicaciones.



- 4 Compruebe los registros resultantes para problemas de comunicación. Para obtener más información, consulte [“Problemas de comunicaciones generales que afectan PPP” en la página 497](#).

## Problemas de comunicaciones generales que afectan PPP

La siguiente tabla describe síntomas que están relacionados con el resultado del registro del procedimiento, [“Cómo diagnosticar y solucionar problemas de comunicaciones” en la página 496](#).

TABLA 21-3 Problemas de comunicaciones generales que afectan PPP

Síntoma	Problema	Solución
too many Configure-Requests	Un igual no puede escuchar a otro igual.	Compruebe si se presentan los siguientes problemas: <ul style="list-style-type: none"><li>■ El equipo o el módem pueden tener un cableado defectuoso.</li><li>■ Es posible que la configuración del módem tenga valores de bit incorrectos. O bien, es posible que la configuración haya afectado al control de flujo.</li><li>■ Es posible que se haya producido un fallo en la secuencia de comandos de chat. En esta situación, consulte la <a href="#">Tabla 21-5</a>.</li></ul>
El resultado pppd debug muestra que LCP se inicia, pero hay fallas en protocolos de alto nivel o se muestran errores de CRC.	El mapa de caracteres de control asíncrono (ACCM) se estableció de manera incorrecta.	Utilice la opción default -async para establecer ACCM según los valores predeterminados estándar de FFFFFFFF. Primero, intente usar default -async como una opción para pppd en la línea de comandos. Si el problema se soluciona, agregue default -async a /etc/ppp/options o a /etc/ppp/peers/ <i>nombre de igual</i> después de la opción de llamada.
El resultado pppd debug muestra que IPCP se inicia, pero finaliza inmediatamente.	Las direcciones IP pueden estar configuradas de forma incorrecta.	<ol style="list-style-type: none"><li>1. Compruebe la secuencia de comandos de chat para verificar si la secuencia de comandos tiene direcciones IP incorrectas.</li><li>2. Si la secuencia de comandos de chat es correcta, solicite registros de depuración para el igual y compruebe las direcciones IP en los registros del igual.</li></ol>
El enlace muestra un rendimiento muy bajo.	El módem podría estar configurado de manera incorrecta, con errores de configuración de control de flujo, errores de configuración de módem y tasas DTE configuradas de manera incorrecta.	Compruebe la configuración del módem. Ajuste la configuración si es necesario.

## ▼ Cómo diagnosticar problemas con la configuración de PPP

Algunos problemas de PPP se pueden rastrear en problemas de archivos de configuración de PPP. El siguiente procedimiento muestra cómo aislar y solucionar problemas de configuración generales.

- 1 Conviértase en superusuario en el equipo local o asuma un rol equivalente.**  
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 Llame al igual remoto. A continuación, habilite las funciones de depuración.**  
`% pppd debug call peer-name`
- 3 Compruebe el registro resultante para problemas de comunicación. Para obtener más información, consulte [“Problemas de configuración de PPP comunes” en la página 498](#).**

## Problemas de configuración de PPP comunes

La siguiente tabla describe síntomas que están relacionados con el resultado del registro del procedimiento, [“Cómo diagnosticar problemas con la configuración de PPP” en la página 498](#).

TABLA 21–4 Problemas de configuración de PPP comunes

Síntoma	Problema	Solución
El resultado <code>pppd debug</code> contiene el mensaje de error <code>Could not determine remote IP address</code> .	El archivo <code>/etc/ppp/peers/nombre de igual</code> no tiene una dirección IP para el igual. El igual no proporciona una dirección IP durante la negociación del enlace.	Proporcione una dirección IP para el igual en la línea de comando <code>pppd</code> o en <code>/etc/ppp/peers/nombre de igual</code> con el siguiente formato:  <code>:10.0.0.10</code>
El resultado <code>pppd debug</code> muestra que falló la compresión de datos de CCP. El resultado también indica que el enlace está caído.	Es posible que las configuraciones de compresión de PPP de los iguales estén en conflicto.	Deshabilite la compresión de CCP agregando la opción <code>noccp</code> a <code>/etc/ppp/options</code> en uno de los iguales.

## ▼ Cómo diagnosticar problemas del módem

Los módems pueden ser áreas de problemas principales para un enlace por marcación telefónica. El indicador más común de problemas con la configuración del módem es cuando

no hay respuesta del igual. Sin embargo, es posible que tenga dificultades para determinar si un problema de enlace es en realidad el resultado de problemas de configuración del módem.

Para obtener sugerencias de resolución de problemas del módem básicas, consulte [“Resolución de problemas de terminales y módems” de Guía de administración del sistema: Administración avanzada](#). La documentación y los sitios web de los fabricantes de módems contienen soluciones para problemas de sus respectivos equipos. El siguiente procedimiento ayuda a determinar si una configuración de módem defectuosa causa problemas de enlace.

- 1 **Llame al igual con la depuración activada, como se explica en [“Cómo activar la depuración de PPP” en la página 492](#).**

- 2 **Muestre el registro `/var/log/pppdebug` resultante para la configuración de un módem defectuosa.**

- 3 **Utilice `ping` para enviar paquetes de distintos tamaños a través del enlace.**

Para obtener detalles completos sobre `ping`, consulte la página del comando `man ping(1M)`.

Si se reciben paquetes pequeños, pero se descartan paquetes más grandes, se indican problemas del módem.

- 4 **Compruebe la existencia de errores en la interfaz `sppp0`:**

```
% netstat -ni
Name  Mtu  Net/Dest  Address      IpKts    Ierrs  OpKts    Oerrs  Collis  Queue
lo0    8232  127.0.0.0  127.0.0.1    826808   0      826808   0      0       0
hme0   1500  172.21.0.0 172.21.3.228 13800032 0      1648464  0      0       0
sppp0  1500  10.0.0.2   10.0.0.1     210      0      128     0      0       0
```

Si los errores de interfaz se incrementan con el tiempo, es posible que haya problemas en la configuración del módem.

#### Errores más frecuentes

Cuando se muestra el registro `/var/log/pppdebug` resultante, los siguientes síntomas en el resultado pueden indicar una configuración de módem defectuosa. El equipo local puede escuchar al igual, pero el igual no puede escuchar al equipo local.

- No se recibió ningún mensaje `"recvd"` del igual.
- El resultado contiene mensajes de LCP del igual, pero el enlace falla con mensajes `too many LCP Configure Requests` que se envían mediante el equipo local.
- El enlace finaliza con una señal `SIGHUP`.

## ▼ Cómo obtener información de depuración para secuencias de comandos de chat

Utilice el siguiente procedimiento para obtener información de depuración de chat y sugerencias para solucionar problemas comunes. Para obtener más información, consulte [“Problemas de secuencia de comandos de chat comunes” en la página 500](#).

- 1 **Conviértase en superusuario en el equipo de marcación de salida o adopte un rol equivalente.**  
Los roles incluyen autorizaciones y comandos con privilegios. Para obtener más información sobre los roles, consulte [“Configuración de RBAC \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 **Edita el archivo `/etc/ppp/peers/nombre de igual` para el igual al que se debe llamar.**
- 3 **Agregue `-v` como un argumento para el comando chat que se especifica en `connect`.**  
`connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"`
- 4 **Visualice errores de secuencia de comandos de chat en el archivo `/etc/ppp/connect-errors`.**

A continuación, se muestra el principal error que se produce con chat.

```
Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
```

En el ejemplo se muestra el tiempo de espera mientras se aguarda una cadena (CONNECT). Cuando chat falla, obtendrá el siguiente mensaje de pppd:

```
Connect script failed
```

## Problemas de secuencia de comandos de chat comunes

Las secuencias de comandos de chat son áreas propensas a errores para enlaces por marcación telefónica. La siguiente tabla muestra errores de secuencia de comandos de chat comunes y proporciona sugerencias para solucionar los errores. Para obtener información de procedimiento, consulte [“Cómo obtener información de depuración para secuencias de comandos de chat” en la página 500](#).

TABLA 21-5 Problemas de secuencia de comandos de chat comunes

Síntoma	Problema	Solución
El resultado <code>pppd debug</code> contiene <code>Connect script failed</code>	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña.  <code>ogin: user-name</code> <code>ssword: password</code>  Sin embargo, el igual al que intentó conectarse no muestra esta información.	<ol style="list-style-type: none"> <li>1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.</li> <li>2. Intente llamar al igual nuevamente.</li> <li>3. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.</li> </ol>
El registro <code>/usr/bin/chat -v</code> contiene <code>"expect (login:)" alarm read timed out</code>	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña.  <code>ogin: pppuser</code> <code>ssword: \q\U</code>  Sin embargo, el igual al que intenta conectarse no muestra esta información.	<ol style="list-style-type: none"> <li>1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.</li> <li>2. Intente llamar al igual nuevamente.</li> <li>3. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.</li> </ol>
El resultado <code>pppd debug</code> contiene <code>possibly looped-back</code>	El equipo local o su igual está bloqueado en la línea de comandos y no ejecuta PPP. Un nombre de inicio de sesión y una contraseña están configurados incorrectamente en la secuencia de comandos de chat.	<ol style="list-style-type: none"> <li>1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.</li> <li>2. Intente llamar al igual nuevamente.</li> <li>3. Si sigue recibiendo el mensaje, llame al ISP. Solicite la secuencia de inicio de sesión correcta.</li> </ol>
El resultado <code>pppd debug</code> muestra que se activa LCP, pero finaliza al poco tiempo de su activación.	Es posible que la contraseña en la secuencia de comandos de chat sea incorrecta.	<ol style="list-style-type: none"> <li>1. Asegúrese de que tiene la contraseña correcta para el equipo local.</li> <li>2. Compruebe la contraseña en la secuencia de comandos de chat. Corrija la contraseña si es incorrecta.</li> <li>3. Intente llamar al igual nuevamente.</li> <li>4. Si sigue recibiendo el mensaje, llame al ISP. Pida al ISP la secuencia de inicio de sesión correcta.</li> </ol>

TABLA 21-5 Problemas de secuencia de comandos de chat comunes (Continuación)

Síntoma	Problema	Solución
El texto del igual comienza con una tilde (~).	La secuencia de comandos de chat proporciona un nombre de usuario y una contraseña.  ogin: pppuser ssword: \q\U  Sin embargo, el igual al que intenta conectarse no muestra esta información.	1. Elimine el inicio de sesión y la contraseña de la secuencia de comandos de chat.  2. Intente llamar al igual nuevamente.  3. Si sigue recibiendo el mensaje, llame al ISP. Solicite la secuencia de inicio de sesión correcta.
El módem se bloquea.	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje CONNECT del igual:  CONNECT "	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del igual:  CONNECT \c  Finalice la secuencia de comandos de chat con ~\c.
El resultado pppd debug contiene LCP: timeout sending Config-Requests	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje CONNECT del igual:  CONNECT "	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del igual:  CONNECT \c  Finalice la secuencia de comandos de chat con ~\c.
El resultado pppd debug contiene Serial link is not 8-bit clean	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje CONNECT del igual:  CONNECT "	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del igual:  CONNECT \c  Finalice la secuencia de comandos de chat con ~\c.
El resultado pppd debug contiene Loopback detected	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje CONNECT del igual:  CONNECT "	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del igual:  CONNECT \c  Finalice la secuencia de comandos de chat con ~\c.

TABLA 21-5 Problemas de secuencia de comandos de chat comunes (Continuación)

Síntoma	Problema	Solución
El resultado pppd debug contiene SIGHUP	La secuencia de comandos de chat contiene la siguiente línea para forzar al equipo local a que espere el mensaje CONNECT del igual:  CONNECT "	Utilice la siguiente línea cuando desee que la secuencia de comandos de chat espere el mensaje CONNECT del igual:  CONNECT \c  Finalice la secuencia de comandos de chat con ~\c.

## ▼ Cómo diagnosticar y solucionar problemas de velocidad de línea de serie

Es posible que los servidores de marcación de entrada tengan problemas debido a una configuración de velocidad conflictiva. El siguiente procedimiento lo ayuda a aislar la causa del problema de enlace para velocidades de línea de serie conflictivas.

Los siguientes comportamientos provocan problemas de velocidad:

- Invocó PPP a través de un programa, como `/bin/login`, y especificó la velocidad de la línea.
- Inició PPP desde `mgetty` y accidentalmente proporcionó la tasa de bits.

pppd cambia la velocidad que se estableció originalmente para la línea por la velocidad establecida por `/bin/login` o `mgetty`. Como resultado, la línea falla.

**1 Inicie sesión en el servidor de marcación de entrada. Llame al igual con la depuración habilitada.**

Si necesita instrucciones, consulte [“Cómo activar la depuración de PPP” en la página 492](#).

**2 Visualice el registro `/var/log/pppdebug` resultante.**

Compruebe el resultado del siguiente mensaje:

LCP too many configure requests

Este mensaje indica que las velocidades de las líneas de serie que se configuraron para PPP podrían estar en conflicto.

**3 Compruebe si PPP se invoca a través de un programa, como `/bin/login`, y la velocidad de línea que se estableció.**

En esta situación, pppd cambia la velocidad de línea que se configuró originalmente por la velocidad especificada en `/bin/login`.

- 4 Compruebe si un usuario inició PPP desde el comando `mgetty` y especificó accidentalmente una tasa de bits.

Esta acción también hace que las velocidades de línea de serie entren en conflicto.

- 5 Solucione el problema de velocidad de línea de serie conflictiva como se indica a continuación:

- a. Bloquee la velocidad DTE del módem.
- b. No utilice velocidades automáticas.
- c. No cambie la velocidad de línea después de la configuración.

## ▼ Cómo obtener información de diagnóstico para PPPoE

Puede utilizar PPP y utilidades UNIX estándar para identificar problemas de PPPoE. Cuando sospecha que PPPoE es la causa de los problemas de un enlace, utilice las siguientes herramientas de diagnóstico para obtener información de resolución de problemas.

- 1 Conviértase en superusuario en el equipo que ejecuta el túnel PPPoE, ya sea cliente PPPoE o servidor de acceso PPPoE.
- 2 Active la depuración, como se explica en el procedimiento [“Cómo activar la depuración de PPP” en la página 492](#).
- 3 Visualice el contenido del archivo de registro `/var/log/pppdebug`.

En el siguiente ejemplo, se muestra parte de un archivo de registro que se generó para un enlace con un túnel PPPoE.

```
Sep 6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
pppoe.so loaded.
Sep 6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
2.4.0b1 (Sun Microsystems, Inc.,
Sep 5 2001 10:42:05) started by troot, uid 0
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
'/usr/lib/inet/pppoc
-v hme0' started (pid 100564)
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
<--> /dev/sppptun
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
is apparently empty
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
is apparently empty
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
[LCP ConfReq id=0xef <mru 1492>
asynctest 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep 6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
```



```
[LCP ConfReq id=0x2a <mru 1402>
asynccmap 0x0 <magic 0x9985f048><pcomp><acomp>
```

Si el resultado de la depuración no lo ayuda a aislar el problema, continúe con este procedimiento.

#### 4 Obtenga mensajes de diagnóstico de PPPoE.

```
# pppd connect "/usr/lib/inet/pppoe -v interface-name"
```

pppoe envía información de diagnóstico a `stderr`. Si ejecuta `pppd` en primer plano, se muestra un resultado en la pantalla. Si `pppd` se ejecuta en segundo plano, el resultado se envía a `/etc/ppp/connect-errors`.

En el siguiente ejemplo, se muestran los mensajes que se generan al negociar el túnel PPPoE.

```
Connect option: '/usr/lib/inet/pppoe -v hme0' started (pid 100564)
/usr/lib/inet/pppoe: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoe: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoe: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoe: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoe
/usr/lib/inet/pppoe: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoe: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoe: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoe: Received Active Discovery Session-confirmation from
8:0:20:cd:c1:2/hme0:pppoe
/usr/lib/inet/pppoe: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoe: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoe: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoe: connected
```

Si los mensajes de diagnóstico no lo ayudan a aislar el problema, continúe con este procedimiento.

#### 5 Ejecute snoop. A continuación, guarde el rastreo en un archivo.

Para obtener información sobre `snoop`, consulte la página del comando `man snoop(1M)`.

```
# snoop -o pppoe-trace-file
```

#### 6 Visualice el archivo de rastreo snoop.

```
# snoop -i pppoe-trace-file -v pppoe
```

```
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
```

```

PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = 0x00000002
PPPoE:
.
.
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18

```

## Resolución de problemas de línea arrendada

El problema más común con las líneas arrendadas es el bajo rendimiento. En la mayoría de los casos, necesita trabajar con la compañía telefónica para solucionar el problema.

TABLA 21-6 Problemas comunes de línea arrendada

Síntoma	Problema	Solución
El enlace no se inicia.	Esto se puede deber a violaciones bipolares de CSU (CSU BPV). Uno de los extremos del enlace está configurado para líneas AMI. El otro extremo está configurado para sustitución bipolar de 8 ceros (B8Zs) ESE.	Si reside en los Estados Unidos o en Canadá, puede solucionar directamente este problema desde el menú de CSU/DSU. Consulte la documentación del fabricante de CSU/DSU para obtener detalles. En otras configuraciones regionales, es posible que el proveedor sea el responsable de solucionar CSU BPVs.
El enlace tiene un bajo rendimiento.	El resultado pppd debug muestra errores de CRC cuando el tráfico sostenido está en el enlace. Es posible que la línea tenga problemas de sincronización a causa de configuraciones incorrectas entre la compañía telefónica y la red.	Póngase en contacto con la compañía telefónica para asegurarse de que la "sincronización de bucle" esté en uso. En algunas líneas arrendadas no estructuradas, es posible que tenga que proporcionar la sincronización. Los usuarios de Estados Unidos deben utilizar la sincronización de bucle.

## Diagnóstico y resolución de problemas de autenticación

La siguiente tabla describe soluciones para problemas de autenticación generales.

TABLA 21-7 Problemas de autenticación generales

Síntoma	Problema	Solución
El resultado pppd debug muestra el mensaje Peer is not authorized to use remote address <i>dirección</i> .	Utiliza autenticación PAP y la dirección IP para el igual remoto no está en el archivo <code>/etc/ppp/pap-secrets</code> .	Agregue un asterisco (*) después de la entrada para el igual en el archivo <code>/etc/ppp/pap-secrets</code> .
El resultado pppd debug muestra que LCP se inicia, pero finaliza su actividad al poco tiempo de su inicio.	Es posible que la contraseña no sea correcta en la base de datos para un protocolo de seguridad específico.	Compruebe la contraseña para el igual en el archivo <code>/etc/ppp/pap-secrets</code> o <code>/etc/ppp/chap-secrets</code> .



## Solaris PPP 4.0 (referencia)

---

Este capítulo proporciona información conceptual detallada sobre Solaris PPP 4.0. Los temas incluyen lo siguiente:

- “Uso de opciones de PPP en archivos y en la línea de comandos” en la página 509
- “Configuración de opciones específicas de usuarios” en la página 518
- “Especificación de información para comunicación con el servidor de marcación de entrada” en la página 519
- “Configuración de velocidad del módem para un enlace por marcación telefónica” en la página 522
- “Definición de la conversación en el enlace por marcación telefónica” en la página 522
- “Autenticación de emisores de llamadas en un enlace” en la página 532
- “Creación de un esquema de direccionamiento IP para emisores de llamadas” en la página 538
- “Creación de túneles PPPoE para compatibilidad de DSL” en la página 541

### Uso de opciones de PPP en archivos y en la línea de comandos

Solaris PPP 4.0 contiene una gran cantidad de opciones, que se utilizan para definir la configuración de PPP. Estas opciones se utilizan en los archivos de configuración de PPP o en la línea de comandos, o mediante el uso de una combinación de archivos y opciones de línea de comandos. Esta sección contiene información detallada sobre el uso de opciones de PPP en archivos de configuración y como argumentos para comandos de PPP.

### Dónde definir opciones de PPP

La configuración de Solaris PPP 4.0 es muy flexible. Puede definir opciones de PPP en las siguientes ubicaciones:

- Archivos de configuración de PPP
- Comandos de PPP que se emiten en la línea de comandos

■ Una combinación de ambos

La siguiente tabla enumera comandos y archivos de configuración de PPP.

TABLA 22-1 Resumen de comandos y archivos de configuración de PPP

Archivo o comando	Definición	Para obtener información
/etc/ppp/options	Un archivo que contiene características que se aplican de manera predeterminada a todos los enlaces de PPP del sistema, por ejemplo, si el equipo requiere que los iguales se autentiquen ellos mismos. Si este archivo está ausente, no se les permite a los usuarios que no son root utilizar PPP.	“Archivo de configuración /etc/ppp/options” en la página 514
/etc/ppp/options. <i>nombre de tty</i>	Un archivo que describe las características de todas las comunicaciones a través del puerto de serie <i>nombre de tty</i> .	“Archivo de configuración /etc/ppp/options. <i>nombre de tty</i> ” en la página 515
/etc/ppp/peers	Directorio que contiene, por lo general, información sobre pares con los que se conecta un equipo de marcación de salida. Los archivos de este directorio se utilizan con la opción <code>call</code> del comando <code>pppd</code> .	“Especificación de información para comunicación con el servidor de marcación de entrada” en la página 519
/etc/ppp/peers/ <i>nombre de igual</i>	Un archivo que contiene características del igual remoto <i>nombre de igual</i> . Las características típicas incluyen el número de teléfono del igual y una secuencia de comandos de chat para la negociación del enlace con el igual.	“Archivo /etc/ppp/peers/ <i>nombre de igual</i> ” en la página 519
/etc/ppp/pap-secrets	Un archivo que contiene las credenciales de seguridad necesarias para la autenticación Protocolo de autenticación de contraseña (PAP).	“Archivo /etc/ppp/pap-secrets” en la página 532
/etc/ppp/chap-secrets	Un archivo que contiene las credenciales de seguridad necesarias para la autenticación Protocolo de autenticación por desafío mutuo (CHAP).	“Archivo /etc/ppp/chap-secrets” en la página 536
~/.ppprc	Archivo en el directorio principal de un usuario de PPP. Se utiliza generalmente con servidores de marcación de entrada. Este archivo contiene información específica sobre la configuración de cada usuario.	“Configuración de \$HOME/.ppprc en un servidor de marcación de entrada” en la página 518
pppd <i>opciones</i>	Comando y opciones para iniciar un enlace de PPP y describir sus características.	“Cómo se procesan las opciones de PPP” en la página 511

Consulte la página del comando `man pppd(1M)` para obtener detalles sobre los archivos de PPP. `pppd(1M)` también incluye descripciones completas de todas las opciones que están disponibles para el comando `pppd`. Las plantillas de ejemplo para todos los archivos de configuración de PPP están disponibles en `/etc/ppp`.

## Cómo se procesan las opciones de PPP

1. El daemon `pppd` analiza lo siguiente:

Todas las operaciones de Solaris PPP 4.0 son gestionadas por el daemon `pppd`, que se inicia cuando el usuario ejecuta el comando `pppd`. Cuando un usuario llama a un igual remoto, se produce lo siguiente:

- `/etc/ppp/options`
  - `$HOME/.ppprc`
  - Los archivos que se abren mediante la opción `file` o `call` en `/etc/ppp/options` y `$HOME/.ppprc`
2. `pppd` analiza la línea de comandos para determinar el dispositivo en uso. El daemon aún no interpreta ninguna de las opciones que se encuentran.
  3. `pppd` intenta detectar el dispositivo serie que se utilizará mediante el uso de estos criterios:
    - Si un dispositivo serie se especifica en la línea de comandos o un archivo de configuración procesado anteriormente, `pppd` utiliza el nombre de ese dispositivo.
    - Si no hay ningún dispositivo serie con nombre, `pppd` busca la opción `notty`, `pty` o `socket` en la línea de comandos. Si se especifica una de estas opciones, `pppd` asume que no existe ningún nombre de dispositivo.
    - De lo contrario, si `pppd` descubre que la entrada estándar está conectada a `tty`, se utiliza el nombre de `tty`.
    - Si `pppd` no puede encontrar un dispositivo serie, `pppd` finaliza la conexión y emite un error.
  4. `pppd` después comprueba la existencia del archivo `/etc/ppp/options.nombre de tty`. Si se encuentra el archivo, `pppd` analiza el archivo.
  5. `pppd` procesa cualquier opción de la línea de comandos.
  6. `pppd` negocia el Protocolo de control de enlace (LCP) para configurar el enlace.
  7. (Opcional) Si se necesita autenticación, `pppd` lee `/etc/ppp/pap-secrets` o `/etc/ppp/chap-secrets` para autenticar al igual opuesto.

El archivo `/etc/ppp/peers/nombre de igual` se lee cuando el daemon `pppd` encuentra la opción `call nombre de igual` en la línea de comandos o en otros archivos de configuración.

# Cómo funcionan los privilegios de archivos de configuración de PPP

La configuración de Solaris PPP 4.0 incluye el concepto de *privilegios*. Los privilegios determinan la precedencia de las opciones de configuración, especialmente cuando la misma opción se invoca en más de una ubicación. Una opción que se invoca desde un origen privilegiado tiene más prioridad que la misma opción invocada desde un origen no privilegiado.

## Privilegios de usuarios

El único usuario con privilegios es el superusuario (root), con el UID de cero. Todos los demás usuarios no tienen privilegios.

## Privilegios de archivos

Los siguientes archivos de configuración tienen privilegios, independientemente de sus propietarios:

- /etc/ppp/options
- /etc/ppp/options.*nombre de tty*
- /etc/ppp/peers/*nombre de igual*

El archivo \$HOME/.ppprc es propiedad del usuario. Las opciones que se leen desde \$HOME/.ppprc y desde la línea de comandos tienen privilegios sólo si el usuario que invoca pppd es root.

Los argumentos que siguen a la opción `file` tienen privilegios.

## Efectos de privilegios de opciones

Algunas opciones necesitan que el usuario que invoca o el origen tengan privilegios para poder funcionar. A las opciones que se invocan en la línea de comandos se les asignan los privilegios del usuario que ejecuta el comando pppd. Estas opciones no tienen privilegios, a menos que el usuario que invoca pppd esté en root.

Opción	Estado	Explicación
domain	Con privilegios	Requiere privilegios para su uso.
linkname	Con privilegios	Requiere privilegios para su uso.
noauth	Con privilegios	Requiere privilegios para su uso.
nopam	Con privilegios	Requiere privilegios para su uso.
pam	Con privilegios	Requiere privilegios para su uso.



Opción	Estado	Explicación
plugin	Con privilegios	Requiere privilegios para su uso.
privgroup	Con privilegios	Requiere privilegios para su uso.
allow-ip direcciones	Con privilegios	Requiere privilegios para su uso.
name nombre de host	Con privilegios	Requiere privilegios para su uso.
plink	Con privilegios	Requiere privilegios para su uso.
noplink	Con privilegios	Requiere privilegios para su uso.
plumbed	Con privilegios	Requiere privilegios para su uso.
proxyarp	Tiene privilegios si noproxyarp se ha especificado	No se puede sustituir por un uso sin privilegios.
defaultroute	Con privilegios si nodefault route está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
disconnect	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
bsdcomp	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	El usuario sin privilegios no puede especificar un tamaño de código mayor al que el usuario con privilegios ha especificado.
deflate	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	El usuario sin privilegios no puede especificar un tamaño de código mayor al que el usuario con privilegios ha especificado.
connect	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
init	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
pty	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.
welcome	Con privilegios si está establecido en un archivo con privilegios o por un usuario con privilegios	No se puede sustituir por un usuario sin privilegios.

Opción	Estado	Explicación
<i>nombre de tty</i>	Con privilegios si se estableció en un archivo con privilegios	Abierto con permisos root, independientemente de quién invoca pppd.
	Sin privilegios si se estableció en un archivo sin privilegios	Abierto con los privilegios del usuario que invoca pppd.

## Archivo de configuración /etc/ppp/options

Utiliza el archivo /etc/ppp/options para definir opciones globales para todas las comunicaciones de PPP en el equipo local. /etc/ppp/options es un archivo con privilegios. /etc/ppp/options debe pertenecer a root aunque pppd no aplica esta regla. Las opciones que define en /etc/ppp/options tienen precedencia sobre las definiciones de las mismas opciones en todos los demás archivos y la línea de comandos.

Entre las opciones típicas que puede usar en /etc/ppp/options, se incluyen las siguientes:

- **lock** – Habilita el bloqueo de archivos de estilo UUCP
- **noauth** – Indica que el equipo no autentica a los emisores de llamadas

**Nota** – El software de Solaris PPP 4.0 no incluye un archivo /etc/ppp/options predeterminado. pppd no requiere el archivo /etc/ppp/options para funcionar. Si un equipo no tiene un archivo /etc/ppp/options, sólo root puede ejecutar pppd en ese equipo.

Debe crear /etc/ppp/options mediante un editor de texto, como se muestra en “[Cómo definir comunicaciones a través de la línea de serie](#)” en la [página 447](#). Si un equipo no requiere opciones globales, puede crear un archivo /etc/ppp/options vacío. Entonces, root y los usuarios comunes pueden ejecutar pppd en el equipo local.

### Plantilla /etc/ppp/options.tpl

/etc/ppp/options.tpl contiene comentarios útiles sobre el archivo /etc/ppp/options y tres opciones comunes para el archivo global /etc/ppp/options.

```
lock
nodefaultroute
noproxyarp
```

Opción	Definición
lock	Habilita el bloqueo de archivos de estilo UUCP
nodefaultroute	Especifica que no se definió ninguna ruta predeterminada

Opción	Definición
noproxyarp	No permite proxyarp

Para usar `/etc/ppp/options.tmpl` como el archivo de opciones globales, cambie el nombre de `/etc/ppp/options.tmpl` a `/etc/ppp/options`. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

## ¿Dónde encontrar ejemplos de los archivos `/etc/ppp/options`?

Para encontrar ejemplos del archivo `/etc/ppp/options`, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte [“Cómo definir comunicaciones a través de la línea de serie” en la página 447](#).
- Para un servidor de marcación de entrada, consulte [“Cómo definir comunicaciones a través de la línea de serie \(servidor de marcación de entrada\)” en la página 456](#).
- Para compatibilidad de PAP en un servidor de marcación de entrada, consulte [“Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP \(servidor de marcación de entrada\)” en la página 469](#).
- Para compatibilidad de PAP en un equipo de marcación de salida, consulte [“Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP \(equipo de marcación de salida\)” en la página 473](#).
- Para compatibilidad de CHAP en un servidor de marcación de entrada, consulte [“Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP \(servidor de marcación de entrada\)” en la página 477](#).

## Archivo de configuración `/etc/ppp/options.nombre de tty`

Puede configurar las características de comunicaciones en la línea de serie en el archivo `/etc/ppp/options.nombre de tty`. `/etc/ppp/options.nombre de tty` es un archivo con privilegios que lee `pppd` después de analizar cualquier archivo existente `/etc/ppp/options` y `$HOME/.ppprc`. De lo contrario, `pppd` lee `/etc/ppp/options.nombre de tty` después de analizar `/etc/ppp/options`.

`nombre de tty` se utiliza tanto para enlaces por marcación telefónica como también para enlaces de líneas arrendadas. `nombre de tty` representa un determinado puerto de serie en un equipo, como `cua/a` o `cua/b`, donde es posible que un módem o un adaptador de terminal RDSI estén conectados.

Al asignar un nombre al archivo `/etc/ppp/options.nombre de tty`, sustituya la barra diagonal (/) en el nombre del dispositivo con un punto (.). Por ejemplo, el archivo `options` para el dispositivo `cua/b` debe llamarse `/etc/ppp/options.cua.b`.

---

**Nota** – Solaris PPP 4.0 no requiere un archivo `/etc/ppp/options.nombre de tty` para funcionar correctamente. Es posible que el servidor tenga sólo una línea de serie para PPP. Además, el servidor requiere algunas opciones. En esta instancia, puede especificar cualquier opción requerida en otro archivo de configuración o en la línea de comandos.

---

## Uso de `/etc/ppp/options.nombre de tty` en un servidor de marcación de entrada

Para un enlace por marcación telefónica, es posible que elija crear archivos `/etc/ppp/options.nombre de tty` individuales para cada puerto de serie en un servidor de marcación de entrada con un módem conectado. Entre las opciones típicas, se incluyen las siguientes:

- Dirección IP requerida por el servidor de marcación de entrada

Establezca esta opción si requiere que los emisores de llamadas en el puerto de serie *nombre de tty* utilicen una dirección IP específica. Su espacio de dirección puede tener un número limitado de direcciones IP disponibles para PPP en comparación con el número de posibles emisores de llamadas. En esta situación, considere la posibilidad de asignar una dirección IP a cada interfaz en serie que se utiliza para PPP en el servidor de marcación de entrada. Esta asignación implementa un direccionamiento dinámico para PPP.

- `asynmap valor de mapa`

La opción `asynmap` asigna caracteres de control que no se pueden recibir a través de la línea de serie mediante el módem específico o adaptador de terminal RDSI. Cuando se utiliza la opción `xonxoff`, `pppd` establece automáticamente un `asynmap` de `0xa0000`.

*valor de mapa*, en formato hexadecimal, indica los caracteres de control que son problemáticos.

- `init "chat -U -f /etc/ppp/mychat"`

La opción `init` indica al módem que inicie comunicaciones a través de la línea de serie utilizando la información del comando `chat -U`. El módem utiliza la cadena de chat en el archivo `/etc/ppp/mychat`.

- Parámetros de seguridad que se muestran en la página del comando `man pppd(1m)`

## Uso de `/etc/ppp/options.nombre de tty` en un equipo de marcación de salida

Para un sistema de marcación de salida, puede crear un archivo `/etc/ppp/options.nombre de tty` para el puerto de serie que está conectado al módem u optar por no utilizar `/etc/ppp/options.nombre de tty`.

**Nota** – Solaris PPP 4.0 no requiere un archivo `/etc/ppp/options.nombre de tty` para funcionar correctamente. Es posible que el equipo de marcación de salida tenga sólo una línea de serie para PPP. Además, es posible que el equipo de marcación de salida requiera algunas opciones. Puede especificar cualquier opción requerida en otro archivo de configuración o en la línea de comandos.

## Archivo de plantilla `options.ttya.tpl`

El archivo `/etc/ppp/options.ttya.tpl` contiene comentarios útiles sobre el archivo `/etc/ppp/options.nombre de tty`. La plantilla contiene tres opciones comunes para el archivo `/etc/ppp/options.nombre de tty`.

```
38400
asynmap 0xa0000
:192.168.1.1
```

Opción	Definición
38400	Utilice esta velocidad de transferencia para el puerto de ttya.
asynmap 0xa0000	Asigne el valor asynmap de 0xa0000 para que el equipo local pueda comunicarse con iguales con problemas.
:192.168.1.1	Asigne la dirección IP 192.168.1.1 a todos los iguales que llaman a través de un enlace.

Para usar `/etc/ppp/options.ttya.tpl` en el sitio, cambie el nombre de `/etc/ppp/options.tpl` a `/etc/ppp/options.nombre de ttya`. Reemplace *nombre de tty* con el nombre del puerto de serie con el módem. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

## ¿Dónde encontrar ejemplos de los archivos `/etc/ppp/options.nombre de tty`?

Para encontrar ejemplos de los archivos `/etc/ppp/options.nombre de tty`, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte [“Cómo definir comunicaciones a través de la línea de serie” en la página 447](#).
- Para un servidor de marcación de entrada, consulte [“Cómo definir comunicaciones a través de la línea de serie \(servidor de marcación de entrada\)” en la página 456](#).

## Configuración de opciones específicas de usuarios

Esta sección contiene información detallada sobre la configuración de usuarios en el servidor de marcación de entrada.

### Configuración de `$HOME/.ppprc` en un servidor de marcación de entrada

El archivo `$HOME/.ppprc` es para usuarios que configuran opciones de PPP preferidas. Como administrador, también puede configurar `$HOME/.ppprc` para los usuarios.

Las opciones en `$HOME/.ppprc` tienen privilegios sólo cuando el usuario que invoca el archivo tiene privilegios.

Cuando un emisor utiliza el comando `pppd` para iniciar una llamada, el archivo `.ppprc` es el segundo archivo que el daemon `pppd` comprueba.

Consulte “[Configuración de usuarios del servidor de marcación de entrada](#)” en la página 453 para obtener instrucciones acerca de la configuración de `$HOME/.ppprc` en el servidor de marcación de entrada.

### Configuración de `$HOME/.ppprc` en un equipo de marcación de salida

No se necesita el archivo `$HOME/.ppprc` en el equipo de marcación de salida para que Solaris PPP 4.0 funcione correctamente. Además, no necesita tener un archivo `$HOME/.ppprc` en el equipo de marcación de salida (excepto en circunstancias especiales). Cree uno o más archivos `.ppprc` si realiza lo siguiente:

- Permite que varios usuarios con diferentes necesidades de comunicación llamen a iguales remotos desde el mismo equipo. En tal caso, cree archivos `.ppprc` individuales en los directorios principales de cada usuario que debe realizar una llamada.
- Necesita especificar opciones que controlan problemas específicos de su enlace, como la inhabilitación de la compresión de Van Jacobson. Consulte *PPP Design, Implementation, and Debugging* de James Carlson y la página del comando `man pppd(1M)` para recibir asistencia de resolución de problemas de enlace.

Debido a que el archivo `.ppprc` se utiliza la mayoría de las veces al configurar un servidor de marcación de entrada, consulte “[Cómo configurar usuarios del servidor de marcación de entrada](#)” en la página 454 para obtener instrucciones de configuración para `.ppprc`.

# Especificación de información para comunicación con el servidor de marcación de entrada

Para comunicarse con un servidor de marcación de entrada, necesita recopilar información sobre el servidor. Y, a continuación, editar algunos archivos. Lo más importante es que debe configurar los requisitos de comunicación de todos los servidores de marcación de entrada a los que el equipo de marcación de salida necesita llamar. Puede especificar opciones acerca de un servidor de marcación de entrada, como un número de teléfono de ISP, en el archivo `/etc/ppp/options.nombre de tty`. Sin embargo, el lugar óptimo para configurar información del igual se encuentra en los archivos `/etc/ppp/peers/nombre de igual`.

## Archivo `/etc/ppp/peers/nombre de igual`

---

**Nota** – No se necesita el archivo `/etc/ppp/peers/nombre de igual` en el equipo de marcación de salida para que Solaris PPP 4.0 funcione correctamente.

---

Utilice el archivo `/etc/ppp/peers/nombre de igual` para proporcionar información para comunicarse con un igual determinado. `/etc/ppp/peers/nombre de igual` permite a los usuarios comunes invocar opciones con privilegios preseleccionadas que a los usuarios no se les permite establecer.

Por ejemplo, un usuario sin privilegios no puede sustituir la opción `noauth` si `noauth` se especifica en el archivo `/etc/ppp/peers/nombre de igual`. Supongamos que el usuario desea configurar un enlace para `peerB`, que no proporciona credenciales de autenticación. Como superusuario, puede crear un archivo `/etc/ppp/peers/peerB` que incluye la opción `noauth`. `noauth` indica que el equipo local no autentica llamadas de `peerB`.

El daemon `pppd` lee `/etc/ppp/peers/nombre de igual` cuando `pppd` encuentra la siguiente opción:

```
call peer-name
```

Puede crear un archivo `/etc/ppp/peers/nombre de igual` para cada igual de destino con el que el equipo de marcación de salida necesita comunicarse. Esta práctica es particularmente útil para permitir que los usuarios comunes puedan invocar enlaces de marcación de salida sin la necesidad de privilegios root.

Las opciones típicas que especifica en `/etc/ppp/peers/nombre de igual` incluyen lo siguiente:

- **user nombre de usuario**

Proporcione *nombre de usuario* al servidor de marcación de entrada, como el nombre de inicio de sesión del equipo de marcación de salida, cuando realice autenticación con PAP o CHAP.

- remotename *nombre de igual*  
Utilice *nombre de igual* como el nombre del equipo de marcación de entrada. remotename se utiliza junto con la autenticación PAP o CHAP al explorar los archivos /etc/ppp/pap-secrets o /etc/ppp/chap-secrets.
- connect "chat *chat\_script* . . ."  
Establezca comunicación con el servidor de marcación de entrada mediante el uso de instrucciones de la secuencia de comandos de chat.
- noauth  
No autentique al igual *nombre de igual* al iniciar comunicaciones.
- noipdefault  
Defina la dirección IP inicial que se utiliza en la negociación con el igual en 0.0.0.0. Utilice noipdefault cuando configure un enlace para la mayoría de los ISP a fin de facilitar la negociación de IPCP entre los iguales.
- defaultroute  
Instale una ruta IPv4 predeterminada cuando se establece IP en el enlace.

Consulte la página del comando man [pppd\(1M\)](#) para obtener más opciones que se pueden aplicar a un igual de destino específico.

## Archivo de plantilla /etc/ppp/peers/myisp.tpl

El archivo /etc/ppp/peers/myisp.tpl contiene comentarios útiles sobre el archivo /etc/ppp/peers/*nombre de igual*. La plantilla concluye con opciones comunes que puede utilizar para un archivo /etc/ppp/peers/*nombre de igual*:

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

Opción	Definición
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"	Llame al igual mediante la secuencia de comandos de chat /etc/ppp/myisp-chat.
user myname	Utilice este nombre de cuenta para el equipo local. myname es el nombre de este equipo en el archivo /etc/ppp/pap-secrets del igual.



Opción	Definición
remotename myisp	Reconozca myisp como el nombre del igual en el equipo local del archivo <code>/etc/ppp/pap-secrets</code> .
noauth	No necesita que los iguales que llaman proporcionen credenciales de autenticación.
noipdefault	No utilice una dirección IP predeterminada para el equipo local.
defaultroute	Utilice la ruta predeterminada que se asignó al equipo local.
updetach	Errores de registro en los archivos de registro de PPP, en lugar de en la salida estándar.
noccp	No utilice la compresión de CCP.

Para usar `/etc/ppp/peers/myisp.tmpl` en su sitio, cambie el nombre de `/etc/ppp/peers/myisp.tmpl` a `/etc/ppp/peers/.nombre de igual`. Reemplace *nombre de igual* con el nombre del igual al que va a llamar. A continuación, modifique los contenidos del archivo según sea necesario en función del sitio.

## Dónde encontrar ejemplos de los archivos `/etc/ppp/peers/.nombre de igual`

Para encontrar ejemplos de los archivos `/etc/ppp/peers/.nombre de igual`, consulte lo siguiente:

- Para un equipo de marcación de salida, consulte [“Cómo definir la conexión con un igual individual” en la página 449](#).
- Para un equipo local en una línea arrendada, consulte [“Cómo configurar un equipo en una línea arrendada” en la página 462](#).
- Para compatibilidad de autenticación PAP en un equipo de marcación de salida, consulte [“Cómo agregar compatibilidad de PAP a los archivos de configuración de PPP \(equipo de marcación de salida\)” en la página 473](#).
- Para compatibilidad de autenticación CHAP en un equipo de marcación de salida, consulte [“Cómo agregar compatibilidad de CHAP a los archivos de configuración de PPP \(equipo de marcación de salida\)” en la página 480](#).
- Para compatibilidad de PPPoE en un sistema cliente, consulte [“Configuración del cliente PPPoE” en la página 482](#).

## Configuración de velocidad del módem para un enlace por marcación telefónica

Un problema grave en la configuración del módem es la determinación de la velocidad a la que el módem debería funcionar. Las siguientes directrices se aplican a los módems que se utilizan con equipos de Sun Microsystems:

- Sistemas SPARC anteriores: Consulte la documentación del hardware que acompaña al sistema. Muchos equipos SPARCstation requieren que la velocidad del módem no exceda 38.400 bps.
- Equipos UltraSPARC: Establezca la velocidad del módem en 115.200 bps, que es útil con los módems modernos y lo suficientemente rápida para un enlace por marcación telefónica. Si tiene previsto utilizar un adaptador de terminal RDSI de doble canal con compresión, deberá aumentar la velocidad del módem. El límite en un sistema UltraSPARC es 460.800 bps para un enlace asíncrono.

Para un *equipo de marcación de salida*, establezca la velocidad del módem en los archivos de configuración de PPP, como `/etc/ppp/peers/nombre de igual`, o mediante la especificación de la velocidad como una opción para `pppd`.

Para un *servidor de marcación de entrada*, necesita establecer la velocidad mediante el uso de la utilidad `ttymon` o Solaris Management Console, como se describe en “[Configuración de dispositivos en el servidor de marcación de entrada](#)” en la página 452.

## Definición de la conversación en el enlace por marcación telefónica

El equipo de marcación de salida y sus iguales remotos se comunican a través del enlace de PPP mediante la negociación y el intercambio de diversas instrucciones. Al configurar un equipo de marcación de salida, debe determinar qué instrucciones necesitan los módems locales y remotos. A continuación, cree un archivo denominado secuencia de comandos de chat que contenga estas instrucciones. En esta sección se trata información sobre la configuración de módems y la creación de secuencias de comandos de chat.

### Contenidos de la secuencia de comandos de chat

Cada igual remoto al que el equipo de marcación de salida necesita conectarse probablemente necesite su propia secuencia de comandos de chat.

---

**Nota** – Las secuencias de comandos de chat se utilizan, por lo general, sólo en enlaces por marcación telefónica. Los enlaces de líneas arrendadas no utilizan secuencias de comandos de chat, a menos que el enlace incluya una interfaz asíncrona que requiera configuración de inicio.

---

Los contenidos de la secuencia de comandos de chat están determinados por los requisitos del modelo del módem o adaptador de terminal RDSI, y el igual remoto. Estos contenidos aparecen como un conjunto de cadenas *expect-send*. El equipo de marcación de salida y sus iguales remotos intercambian las cadenas como parte del proceso de iniciación de comunicaciones.

Una cadena *expect* contiene caracteres que el equipo host de marcación de salida espera recibir del igual remoto para iniciar una conversación. Una cadena *send* contiene caracteres que el equipo de marcación de salida envía al igual remoto después de recibir la cadena "expect".

La información en la secuencia de comandos de chat, normalmente, incluye lo siguiente:

- Comandos del módem, conocidos, generalmente, como *comandos AT*, que permiten que el módem transmita datos por teléfono
- Número de teléfono del igual de destino  
Este número de teléfono podría ser el número que requiere el ISP o un servidor de marcación de entrada en un sitio corporativo, o un equipo individual.
- Valor de tiempo de espera, si es necesario
- Secuencia de inicio de sesión que se espera del igual remoto
- Secuencia de inicio de sesión que se envía mediante el equipo de marcación de salida

## Ejemplos de secuencias de comandos de chat

Esta sección contiene secuencias de comandos de chat que puede utilizar como una referencia para crear sus propias secuencias de comandos. La guía del fabricante del módem e información sobre el ISP y otros hosts de destino contienen requisitos de chat para el módem y los iguales de destino. Además, numerosos sitios web de PPP tienen secuencias de comandos de chat de ejemplo.

### Secuencia de comandos de chat de módem básica

A continuación se muestra una secuencia de comandos de chat básica que puede utilizar como una plantilla para crear sus propias secuencias de comandos de chat.

```
ABORT    BUSY
ABORT    'NO CARRIER'
REPORT   CONNECT
TIMEOUT  10
""       AT&F1M0&M5S2=255
```

```
SAY      "Calling myserver\n"
TIMEOUT 60
OK       "ATDT1-123-555-1212"
ogin:    pppuser
ssword:  \q\U
%        pppd
```

La siguiente tabla describe los contenidos de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
ABORT BUSY	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT 'NO CARRIER'	Aborta la transmisión si el módem informa ABORT 'NO CARRIER' durante la marcación. Este mensaje se debe, normalmente, a fallos en el marcado o en la negociación del módem.
REPORT CONNECT	Recopila la cadena CONNECT desde el módem. Imprime la cadena.
TIMEOUT 10	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
"" AT&F1M0&M5S2=255	M0 – Desactiva el altavoz durante la conexión.  &M5: hace que el módem requiera control de errores.  S2=255: deshabilita la secuencia de bloqueo TIES “+++”.
SAY "Calling myserver\n"	Muestra el mensaje Calling myserver en el equipo local.
TIMEOUT 60	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
OK "ATDT1-123-555-1212"	Llama al igual remoto mediante el número de teléfono 123-555-1212.
ogin: pppuser	Inicia sesión con el igual mediante el inicio de sesión de estilo UNIX. Proporciona el nombre de usuario pppuser.
ssword: \q\U	\q: no inicia sesión si se depura con la opción -v.  \U: inserta en esta ubicación los contenidos de la cadena que se indica a continuación de -U, que se especifica en la línea de comandos. Normalmente, la cadena contiene la contraseña.
% pppd	Espera el indicador de shell % y ejecuta el comando pppd.

## Plantilla de secuencia de comandos de chat

### /etc/ppp/myisp-chat.tpl

Esta versión incluye /etc/ppp/myisp-chat.tpl, que puede modificar para su uso en el sitio. /etc/ppp/myisp-chat.tpl es similar a la secuencia de comandos de chat de módem básica, excepto que la plantilla no incluye una secuencia de inicio de sesión.

```
ABORT    BUSY
ABORT    'NO CARRIER'
REPORT   CONNECT
TIMEOUT  10
""       "AT&F1"
OK       "AT&C1&D2"
SAY      "Calling myisp\n"
TIMEOUT  60
OK       "ATDT1-123-555-1212"
CONNECT  \c
```

Contenidos de la secuencia de comandos	Explicación
ABORT BUSY	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT 'NO CARRIER	Aborta la transmisión si el módem informa ABORT 'NO CARRIER' durante la marcación. Este mensaje se debe, normalmente, a fallos en el marcado o en la negociación del módem.
REPORT CONNECT	Recopila la cadena CONNECT desde el módem. Imprime la cadena.
TIMEOUT 10	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
"" "AT&F1"	Restablece el módem a los valores predeterminados de fábrica.
OK "AT&C1&D2"	Restablece el módem de manera que, para &C1, DCD desde el módem sigue al proveedor. Si el lado remoto cuelga el teléfono por alguna razón, entonces DCD se pierde.  Para &D2, la transición alta a baja de DTR hace que el módem esté listo para establecer una comunicación o finalice una llamada.
SAY "Calling myisp\n"	Muestra el mensaje "Calling myisp" en el equipo local.
TIMEOUT 60	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
OK "ATDT1-123-555-1212"	Llama al igual remoto mediante el número de teléfono 123-555-1212.
CONNECT \c	Espera el mensaje CONNECT del módem del igual opuesto.

## Secuencia de comandos de chat de módem para llamar a un ISP

Utilice la siguiente secuencia de comandos de chat como una plantilla para llamar a un ISP desde un equipo de marcación de salida con un módem U.S. Robotics Courier.

```
ABORT    BUSY
ABORT    'NO CARRIER'
REPORT   CONNECT
TIMEOUT  10
""       AT&F1M0&M552=255
```

```
SAY      "Calling myisp\n"
TIMEOUT  60
OK       "ATDT1-123-555-1212"
CONNECT  \c
\r \d\c
SAY      "Connected; running PPP\n"
```

La siguiente tabla describe los contenidos de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
ABORT BUSY	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT 'NO CARRIER'	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
REPORT CONNECT	Recopila la cadena CONNECT desde el módem. Imprime la cadena.
TIMEOUT 10	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
"" AT&F1M0M0M0M0&M5S2=255	M0: desactiva el altavoz durante la conexión.  &M5: hace que el módem requiera control de errores.  S2=255: deshabilita la secuencia de bloqueo TIES “+++”.
SAY "Calling myisp\n"	Muestra el mensaje Calling myisp en el equipo local.
TIMEOUT 60	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
OK "ATDT1-123-555-1212"	Llama al igual remoto mediante el número de teléfono 123-555-1212.
CONNECT \c	Espera el mensaje CONNECT del módem del igual opuesto.
\r \d\c	Espera hasta el final del mensaje CONNECT.
SAY "Connected; running PPP\n"	Muestra el mensaje informativo Connected; running PPP en el equipo local.

## Secuencia de comandos de chat básica mejorada para un inicio de sesión de estilo UNIX

La siguiente secuencia de comandos de chat es una secuencia de comandos básica que se ha mejorado para llamar a un igual Solaris remoto u otro igual de tipo UNIX. Esta secuencia de comandos de chat se usa en [“Cómo crear las instrucciones para llamar a un igual” en la página 448](#).

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
```

```
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in. Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

La siguiente tabla explica los parámetros de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
TIMEOUT 10	Establece el tiempo de espera inicial en 10 segundos. La respuesta del módem debería ser inmediata.
ABORT BUSY	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT 'NO CARRIER'	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT ERROR	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
REPORT CONNECT	Recopila la cadena CONNECT desde el módem. Imprime la cadena.
"" AT&F1&M5S2=255	&M5: hace que el módem requiera control de errores. S2=255: deshabilita la secuencia de bloqueo TIES “+++”.
TIMEOUT 60	Restablece el tiempo de espera en 60 segundos para permitir más tiempo para la negociación del enlace.
OK ATDT1-123-555-1234	Llama al igual remoto mediante el número de teléfono 123-555-1212.
CONNECT \c	Espera el mensaje CONNECT del módem del igual opuesto.
SAY "Connected; logging in.\n"	Muestra el mensaje informativo Connected; logging in para proporcionar el estado de usuario.
TIMEOUT 5	Cambia el tiempo de espera para permitir una visualización rápida del indicador de inicio de sesión.

Contenidos de la secuencia de comandos	Explicación
ogin:--ogin: pppuser	Espera el indicador de inicio de sesión. Si no se recibe el indicador, se envía una DEVOLUCIÓN y se espera. A continuación, se envía el nombre de usuario pppuser al igual. La mayoría de los ISP hacen referencia a la secuencia que se indica a continuación como inicio de sesión de PAP. Sin embargo, el inicio de sesión de PAP no tiene ninguna relación con la autenticación PAP.
TIMEOUT 20	Cambia el tiempo de espera a 20 segundos para permitir una verificación de contraseña lenta.
ssword: \qmysecrerehere	Espera el indicador de contraseña del igual. Cuando se recibe el indicador, se envía la contraseña \qmysecrerehere. \q impide que la contraseña se escriba para los archivos de registro del sistema.
% " \c	Espera un indicador de shell del igual. La secuencia de comandos de chat utiliza el shell C. Cambia este valor si el usuario prefiere iniciar sesión con un shell diferente.
SAY "Logged in. Starting PPP on peer system.\n"	Muestra el mensaje informativo Logged in. Starting PPP on peer system para proporcionar un estado de usuario.
ABORT 'not found'	Aborta la transmisión si el shell encuentra errores.
"" "exec pppd"	Inicia pppd en el igual.
~ \c	Espera que PPP se inicie en el igual.

El inicio de PPP inmediatamente después de CONNECT \c se denomina con frecuencia *inicio de sesión de PAP* por los ISP, aunque el inicio de sesión de PAP, en realidad, no forma parte de la autenticación PAP.

La frase ogin: -ogin: pppuser indica al módem que envíe el nombre de usuario pppuser en respuesta al indicador de inicio de sesión del servidor de marcación de entrada. pppuser es un nombre de cuenta de usuario de PPP especial que se creó para user1 remoto en el servidor de marcación de entrada. Para obtener instrucciones sobre cómo crear cuentas de usuarios de PPP en un servidor de marcación de entrada, consulte [“Cómo configurar usuarios del servidor de marcación de entrada” en la página 454](#).

## Secuencia de comandos de chat para adaptador de terminal RDSI externo

La siguiente secuencia de comandos de chat se utiliza para llamar desde un equipo de marcación de salida con un adaptador de terminal RDSI. ZyXEL omni.net.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
```



```

ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"

```

La siguiente tabla explica los parámetros de la secuencia de comandos de chat.

Contenidos de la secuencia de comandos	Explicación
SAY "Calling the peer"	Muestra este mensaje en la pantalla del equipo de marcación de salida.
TIMEOUT 10	Establece el tiempo de espera inicial en 10 segundos.
ABORT BUSY	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT 'NO CARRIER'	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
ABORT ERROR	Aborta la transmisión si el módem recibe este mensaje del igual opuesto.
REPORT CONNECT	Recopila la cadena CONNECT desde el módem. Imprime la cadena.
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255	<p>Las letras en esta línea tienen el siguiente significado:</p> <ul style="list-style-type: none"> <li>■ &amp;F: usa los valores predeterminados de fábrica</li> <li>■ B40: realiza la conversión de PPP asíncrono</li> <li>■ S83.7=1: utiliza los datos a través del portador de voz</li> <li>■ &amp;K44: habilita la compresión de CCP</li> <li>■ &amp;J3: habilita MP</li> <li>■ X7: informa las velocidades de DCE</li> <li>■ S61.3=1: utiliza la fragmentación de paquetes</li> <li>■ S0=0: no hay respuesta automática</li> <li>■ S2=255: deshabilita el escape de TIES</li> </ul>
OK ATDI18882638234	Realiza una llamada RDSI. Para multivínculo, la segunda llamada se ubica en el mismo número de teléfono, que, generalmente, es lo que requieren la mayoría de los ISP. Si el igual remoto requiere un segundo número de teléfono diferente, se anexa "+ nnnn.". nnnn representa el segundo número de teléfono.
CONNECT \c	Espera el mensaje CONNECT del módem del igual opuesto.
\r \d\c	Espera hasta el final del mensaje CONNECT.

Contenidos de la secuencia de comandos	Explicación
SAY "Connected; running PPP\n"	Muestra este mensaje en la pantalla del equipo de marcación de salida.

Consulte la página del comando `man chat(1M)` para obtener descripciones de opciones y otra información detallada sobre la secuencia de comandos de chat. Para obtener una explicación de la cadena expect-send, consulte “[Campo Chat-Script en el archivo /etc/uucp/Systems](#)” en la [página 579](#).

### Para obtener más ejemplos de secuencias de comandos de chat

Un número de sitios web ofrece secuencias de comandos de chat de ejemplo y asistencia para la creación de secuencias de comandos de chat. Por ejemplo, consulte <http://ppp.samba.org/ppp/index.html>.

## Invocación de la secuencia de comandos de chat

Llama secuencias de comandos de chat mediante el uso de la opción `connect`. Puede utilizar `connect "chat . . ."` en cualquier archivo de configuración de PPP o en la línea de comandos.

Las secuencias de comandos de chat no son ejecutables, pero el programa invocado por `connect` debe ser ejecutable. Es posible que utilice la utilidad de chat como el programa que será invocado por `connect`. En esta instancia, si almacena la secuencia de comandos de chat en un archivo externo mediante la opción `-f`, el archivo de secuencia de comandos de chat no es ejecutable.

El programa chat que se describe en `chat(1m)` ejecuta la secuencia de comandos real. El daemon `pppd` invoca el programa chat siempre que `pppd` encuentra la opción `connect "chat . . ."`.

---

**Nota** – Puede utilizar cualquier programa externo, como Perl o Tcl, para crear secuencias de comandos de chat avanzadas. La utilidad chat se proporciona como una comodidad.

---

## ▼ Cómo invocar una secuencia de comandos de chat (tarea)

- 1 Cree la secuencia de comandos de chat como un archivo ASCII.
- 2 Invoque la secuencia de comandos de chat en cualquier archivo de configuración de PPP mediante la siguiente sintaxis:

```
connect 'chat -f /etc/ppp/chatfile'
```

El indicador -f indica que sigue un nombre de archivo. */etc/ppp/chatfile* representa el nombre del archivo de chat.

### 3 Otorgue permiso de lectura para el archivo de chat externo para el usuario que ejecuta el comando pppd.



**Precaución** – El programa de chat siempre se ejecuta con los privilegios del usuario, incluso si la opción connect 'chat ...' se invoca desde una fuente con privilegios. Por lo tanto, un archivo de chat independiente que se lee con la opción -f podrá ser leído por el usuario que invoca. Este privilegio puede ser un problema de seguridad si la secuencia de comandos de chat contiene contraseñas u otra información confidencial.

#### Ejemplo 22-1 Secuencia de comandos de chat en línea

Puede ubicar toda la conversación de secuencia de comandos de chat en una única línea, similar a lo siguiente:

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

La secuencia de comandos de chat completa sigue la palabra clave chat. La secuencia de comandos finaliza con "\c"'. Utiliza esta forma en cualquier archivo de configuración de PPP o en la línea de comandos como un argumento para pppd.

#### Más información Secuencia de comandos de chat en un archivo externo

Si la secuencia de comandos de chat necesaria para un igual determinado es extensa o complicada, considere la posibilidad de crear la secuencia de comandos como un archivo independiente. Los archivos de chat externos son fáciles de mantener y documentar. Puede agregar comentarios al archivo de chat si antepone el signo de almohadilla (#) a los comentarios.

El procedimiento [“Cómo crear las instrucciones para llamar a un igual” en la página 448](#) muestra el uso de una secuencia de comandos de chat contenida en un archivo externo.

## Creación de un archivo de chat que es ejecutable

Puede crear un archivo de chat que sea una secuencia de comandos ejecutable para que se ejecute automáticamente cuando se inicie el enlace por marcación telefónica. Por lo tanto, puede ejecutar comandos adicionales durante el inicio del enlace, como stty, para valores de paridad, además de los comandos que se incluyen en una secuencia de comandos de chat tradicional.

Esta secuencia de comandos de chat ejecutable se registra en un sistema de estilo UNIX antiguo que requiere 7 bits con paridad par. A continuación, el sistema cambia a 8 bits sin paridad al ejecutar PPP.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

## ▼ Cómo crear un programa de chat ejecutable

- 1 Utilice su editor de texto para crear un programa de chat ejecutable, como el ejemplo anterior.

- 2 Convierta el programa de chat en ejecutable.

```
# chmod +x /etc/ppp/chatprogram
```

- 3 Invoque el programa de chat.

```
connect /etc/ppp/chatprogram
```

Los programas de chat no tienen que estar ubicados dentro del sistema de archivos `/etc/ppp`. Puede almacenar los programas de chat en cualquier ubicación.

## Autenticación de emisores de llamadas en un enlace

En esta sección se explica cómo funcionan los protocolos de autenticación PPP y se explican las bases de datos que están asociadas a los protocolos de autenticación.

### Protocolo de autenticación de contraseña (PAP)

La autenticación PAP es parecida en operación al programa `login` de UNIX, aunque PAP no concede acceso shell al usuario. PAP utiliza los archivos de configuración de PPP y la base de datos de PAP en forma del archivo `/etc/ppp/pap-secrets` para configurar la autenticación. PAP también utiliza `/etc/ppp/pap-secrets` para definir credenciales de seguridad de PAP. Estas credenciales incluyen un nombre de igual, un "nombre de usuario" en lenguaje de PAP y una contraseña. Las credenciales de PAP también contienen información relacionada para cada emisor de llamada al que se le permite establecer un enlace con el equipo local. Los nombres de usuario y las contraseñas de PAP pueden ser idénticos o diferentes de los nombres de usuario y las contraseñas de UNIX en la base de datos de contraseñas.

#### Archivo `/etc/ppp/pap-secrets`

La base de datos de PAP se implementa en el archivo `/etc/ppp/pap-secrets`. Los equipos en ambos lados del enlace de PPP deben haber configurado correctamente las credenciales de PAP en sus archivos `/etc/ppp/pap-secrets` para una autenticación correcta. El emisor de llamada (autenticado) proporciona credenciales en las columnas `user` y `password` del archivo

/etc/ppp/pap-secrets o en el archivo +ua obsoleto. El servidor (autenticador) valida estas credenciales comparando la información en /etc/ppp/pap-secrets, a través de la base de datos passwd de UNIX o en la utilidad de PAM.

El archivo /etc/ppp/pap-secrets tiene la siguiente sintaxis.

```
myclient ISP-server mypassword *
```

Los parámetros tienen el siguiente significado.

myclient	Nombre de usuario de PAP del emisor de llamada. Con frecuencia, este nombre es idéntico al nombre de usuario de UNIX del emisor, especialmente si el servidor de marcación de entrada utiliza la opción login de PAP.
ISP-server	Nombre del equipo remoto, generalmente un servidor de marcación de entrada.
mypassword	Contraseña de PAP del emisor de llamada.
*	Dirección IP que está asociada con el emisor. Utilice un asterisco (*) para indicar cualquier dirección IP.

## Creación de contraseñas de PAP

Las contraseñas de PAP se envían a través del enlace *sin cifrar*, es decir, en formato ASCII legible. Para el emisor de llamada (autenticado), la contraseña de PAP se debe almacenar sin cifrar en cualquiera de las siguientes ubicaciones:

- En /etc/ppp/pap-secrets
- En otro archivo externo
- En una conducción con nombre a través de la función pap-secrets @
- Como una opción para pppd, en la línea de comandos o en un archivo de configuración de PPP
- A través del archivo +ua.

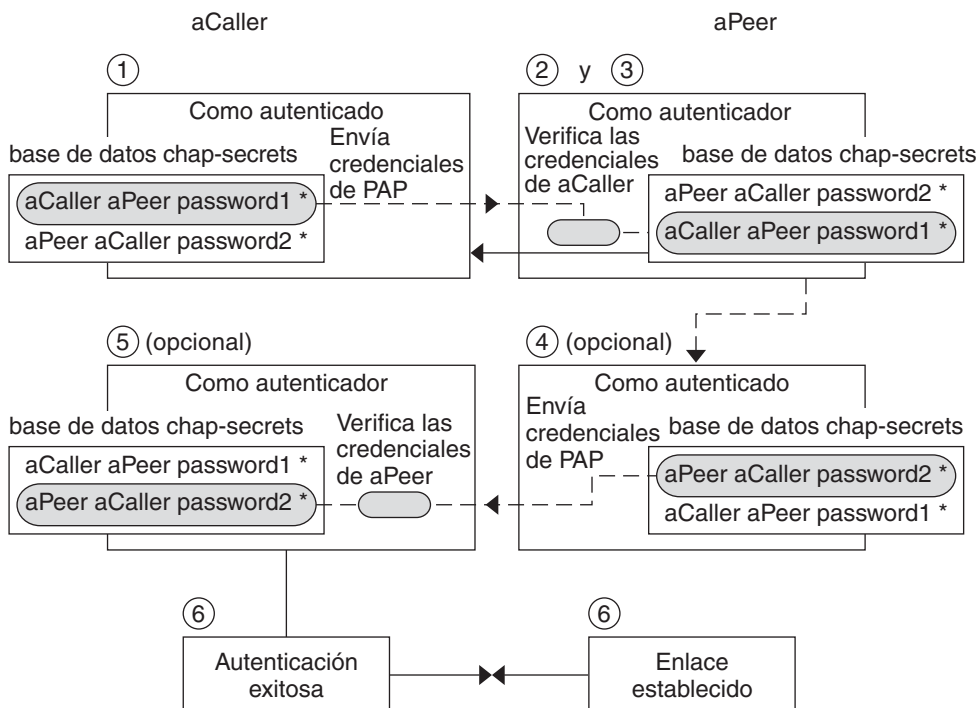
En el servidor (autenticador), la contraseña de PAP se puede ocultar al realizar una de las siguientes acciones:

- Especificar papcrypt y utilizar contraseñas a las que se les ha aplicado un algoritmo hash mediante crypt(3C) en el archivo pap-secrets.
- Especificar la opción login para pppd y omitir la contraseña del archivo pap-secrets colocando comillas dobles (") en la columna de contraseña. En esta instancia, la autenticación se realiza a través de la base de datos "passwd" de UNIX o el mecanismo pam(3pam).

## Qué sucede durante la autenticación PAP

La autenticación PAP se produce en la siguiente secuencia.

FIGURA 22-1 Proceso de autenticación PAP



1. El emisor de llamada (autenticado) llama al igual remoto (autenticador) y proporciona su nombre de usuario y contraseña de PAP como parte de la negociación del enlace.
2. El igual verifica la identidad del emisor en su archivo `/etc/ppp/pap-secrets`. Si el igual utiliza la opción `login` de PAP, el igual verifica el nombre de usuario y la contraseña del emisor de llamada en su base de datos de contraseñas.
3. Si la autenticación es correcta, el igual continúa la negociación del enlace con el emisor. Si la autenticación falla, el enlace se pierde.
4. (Opcional) Si el emisor de llamada autentica respuestas de iguales remotos, el igual remoto debe enviar sus propias credenciales de PAP al emisor. Por lo tanto, el igual remoto se convierte en el autenticado y el emisor en el autenticador.
5. (Opcional) El emisor de llamada original lee su propio `/etc/ppp/pap-secrets` para verificar la identidad del igual remoto.

**Nota** – Si el emisor de llamada original requiere credenciales de autenticación del igual remoto, el paso 1 y el paso 4 suceden en paralelo.

Si se autentica al igual, la negociación continúa. De lo contrario, el enlace se pierde.

6. La negociación entre el emisor de llamada y el igual continúa hasta que el enlace se establece correctamente.

Uso de la opción login con /etc/ppp/pap-secrets

Puede agregar la opción login para autenticar credenciales de PAP en cualquier archivo de configuración de PPP. Cuando se especifica login, por ejemplo, en /etc/ppp/options, pppd verifica que las credenciales de PAP del emisor existen en la base de datos de contraseñas. En el siguiente ejemplo, se muestra el formato de un archivo /etc/ppp/pap-secrets con la opción login.

```
joe      *   ""   *
sally    *   ""   *
sue      *   ""   *
```

Los parámetros tienen los siguientes significados.

Emisor de llamada	joe, sally y sue son los nombres de los emisores de llamadas autorizados.
Servidor	Asterisco (*), que indica que cualquier nombre de servidor es válido. La opción name no es necesaria en los archivos de configuración de PPP.
Contraseña	Comillas dobles, que indican que cualquier contraseña es válida.  Si una contraseña está en esta columna, la contraseña del igual debe coincidir con la contraseña de PAP y la base de datos passwd de UNIX.
Direcciones IP	Asterisco (*), que indica que se permite cualquier dirección IP.

Protocolo de autenticación por desafío mutuo (CHAP)

La autenticación CHAP utiliza la noción de *desafío y respuesta*, que significa que el igual (autenticador) exige al emisor (autenticado) que demuestre su identidad. El desafío incluye un número aleatorio y un ID único que genera el autenticador. El emisor de llamada debe utilizar el ID, el número aleatorio y sus credenciales de seguridad de CHAP para generar la respuesta adecuada (reconocimiento) para enviar al igual.

Las credenciales de seguridad de CHAP incluyen un nombre de usuario de CHAP y un "secreto" de CHAP. El secreto de CHAP es una cadena arbitraria conocida por el emisor y por el

igual antes de negociar un enlace de PPP. Configure credenciales de seguridad de CHAP en la base de datos de CHAP, `/etc/ppp/chap-secrets`.

### Archivo `/etc/ppp/chap-secrets`

La base de datos de CHAP se implementa en el archivo `/etc/ppp/chap-secrets`. Los equipos en ambos lados del enlace de PPP deben tener sus respectivas credenciales de PAP en sus archivos `/etc/ppp/chap-secrets` para una autenticación correcta.

---

**Nota** – A diferencia de PAP, el secreto compartido debe estar sin cifrar en ambos iguales. No puede utilizar `crypt`, `PAM` ni la opción `login` de PPP con CHAP.

---

El archivo `/etc/ppp/chap-secrets` tiene la siguiente sintaxis.

```
myclient myserver secret5748 *
```

Los parámetros tienen los siguientes significados:

<code>myclient</code>	Nombre de usuario de CHAP del emisor de llamada. Este nombre puede ser diferente o igual al nombre de usuario de UNIX del emisor de llamada.
<code>myserver</code>	Nombre del equipo remoto, generalmente un servidor de marcación de entrada.
<code>secret5748</code>	Secreto de CHAP del emisor de llamada.

---

**Nota** – A diferencia de las contraseñas de PAP, los secretos de CHAP nunca se envían a través del enlace. En su lugar, los secretos de CHAP se utilizan cuando los equipos locales procesan la respuesta.

---

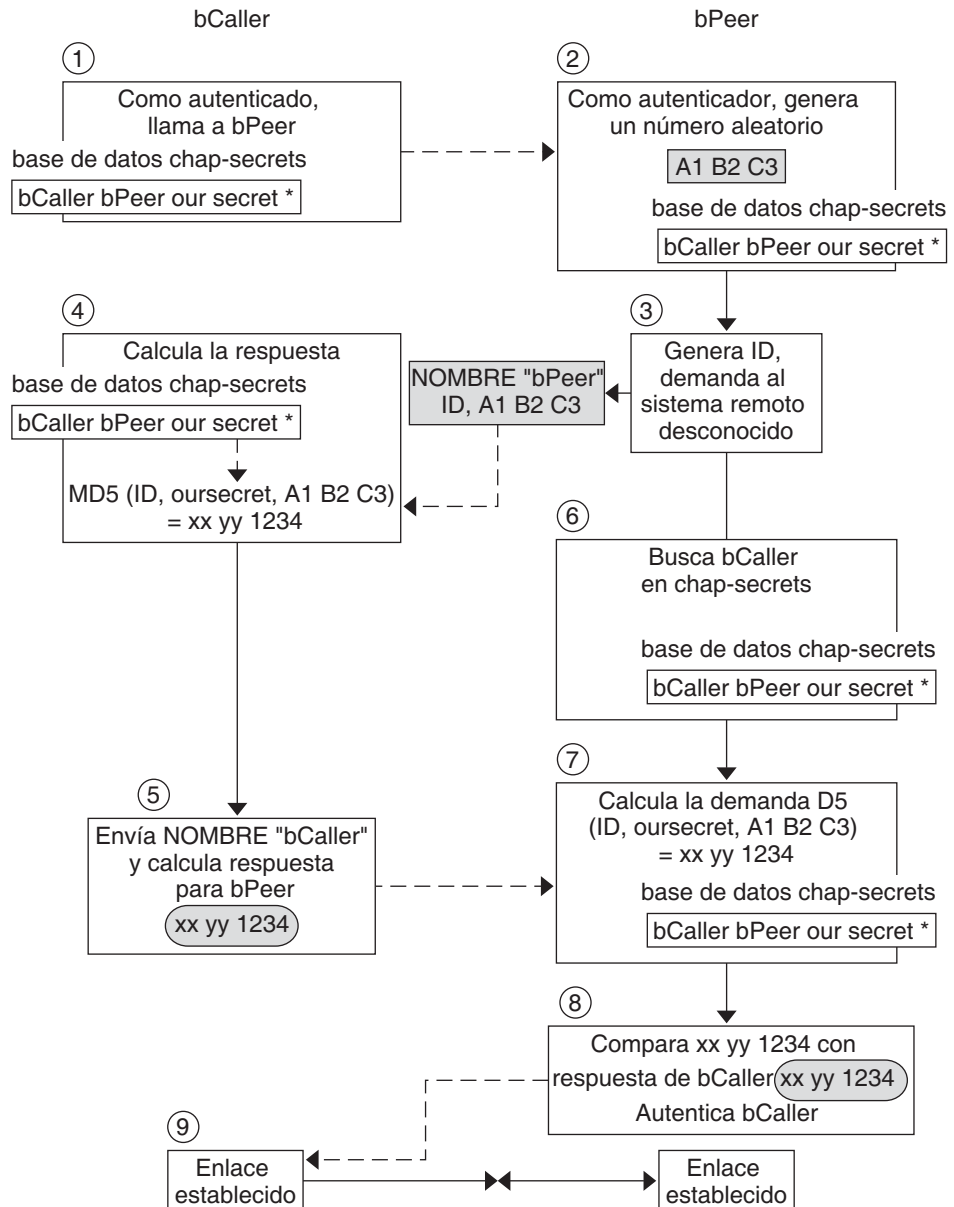
`*` Dirección IP que está asociada con el emisor. Utilice un asterisco (\*) para indicar cualquier dirección IP.

### Qué sucede durante la autenticación CHAP

La autenticación CHAP se produce en la siguiente secuencia.



FIGURA 22-2 Autenticación CHAP secuencia



1. Dos iguales que están por iniciar comunicaciones se ponen de acuerdo sobre un secreto que se utilizará para la autenticación durante la negociación del enlace de PPP.

2. Los administradores de ambos equipos agregan el secreto, los nombres de usuario de CHAP y otras credenciales de CHAP a la base de datos `/etc/ppp/chap-secrets` de sus respectivos equipos.
3. El emisor de llamada (autenticado) llama al igual remoto (autenticador).
4. El autenticador genera un número aleatorio y un ID, y envía esos datos al autenticado como una desafío.
5. El autenticado busca el nombre y secreto del igual en su base de datos `/etc/ppp/chap-secrets`.
6. El autenticado calcula una respuesta aplicando el algoritmo computacional MD5 al secreto y al desafío de número aleatorio del igual. A continuación, el autenticado envía los resultados como su respuesta al autenticador.
7. El autenticador busca el nombre y secreto del autenticado en su base de datos `/etc/ppp/chap-secrets`.
8. El autenticador calcula su propia figura aplicando MD5 al número que se generó como el desafío y el secreto para el autenticado en `/etc/ppp/chap-secrets`.
9. El autenticador compara sus resultados con la respuesta del emisor de llamada. Si los dos números son los mismos, el igual ha autenticado correctamente al emisor de llamada y la negociación del enlace continúa. De lo contrario, el enlace se pierde.

## Creación de un esquema de direccionamiento IP para emisores de llamadas

Considere la posibilidad de crear una o más direcciones IP para todas las llamadas entrantes en lugar de asignar una dirección IP única para cada usuario remoto. Las direcciones IP dedicadas son especialmente importantes si el número de posibles emisores de llamadas supera el número de puertos de serie y módems en el servidor de marcación de entrada. Puede implementar un número de diferentes escenarios, según las necesidades del sitio. Además, los escenarios no son mutuamente excluyentes.

## Asignación de direcciones IP dinámicas a emisores de llamadas

El direccionamiento dinámico implica la asignación a cada emisor de llamada de la dirección IP que está definida en `/etc/ppp/options.nombre de tty`. El direccionamiento dinámico se produce por puerto de serie. Cuando llega una llamada a través de una línea de serie, el emisor de llamada recibe la dirección IP del archivo `/etc/ppp/options.nombre de tty` para la interfaz en serie del emisor de llamada.

Por ejemplo, suponga que un servidor de marcación de entrada tiene cuatro interfaces de serie que proporcionan servicio por marcación telefónica para llamadas entrantes:

- Para el puerto de serie term/a, cree el archivo `/etc/ppp/options.term.a` con el siguiente registro:  
:10.1.1.1
- Para el puerto de serie term/b, cree el archivo `/etc/ppp/options.term.b` con la siguiente entrada:  
:10.1.1.2
- Para el puerto de serie term/c, cree el archivo `/etc/ppp/options.term.c` con la siguiente entrada:  
:10.1.1.3
- Para el puerto de serie term/d, cree el archivo `/etc/ppp/options.term.d` con la siguiente entrada:  
:10.1.1.4

Con el esquema de direccionamiento anterior, a una llamada entrante en la interfaz de serie `/dev/term/c` se le proporciona la dirección IP 10.1.1.3 durante la duración de la llamada. Después de que el primer emisor de llamada cuelga, a la llamada que llega después a través de una interfaz en serie `/dev/term/c` también se le proporciona la dirección IP 10.1.1.3.

Entre las ventajas del direccionamiento dinámico, se incluye lo siguiente:

- Puede realizar un seguimiento del uso de red de PPP en el puerto de serie.
- Puede asignar un número mínimo de direcciones IP para uso de PPP.
- Puede administrar el filtrado IP de una manera más simple.

## Asignación de direcciones IP estáticas a emisores de llamadas

Si su sitio implementa autenticación PPP, puede asignar direcciones IP *estáticas* específicas a emisores de llamadas individuales. En este escenario, cada vez que un equipo de marcación de salida llama al servidor de marcación de entrada, el emisor de llamada recibe la misma dirección IP.

Implementa direcciones estáticas en la base de datos `pap-secrets` o `chap-secrets`. Aquí se muestra un ejemplo de un archivo `/etc/ppp/pap-secrets` que define direcciones IP estáticas.

```
joe   myserver  joepasswd  10.10.111.240
sally myserver  sallypasswd 10.10.111.241
sue   myserver  suepasswd   10.10.111.242
```

Emisor de llamada	joe, sally y sue son los nombres de los emisores de llamadas autorizados.
Servidor	myserver indica el nombre del servidor.
Contraseña	joepasswd, sallypasswd y suepasswd indican las contraseñas para cada emisor de llamada.
Direcciones IP	10.10.111.240 y 10.10.111.241 y 10.10.111.242 son las direcciones IP asignadas a cada emisor de llamada.

Aquí se muestra un ejemplo de un archivo `/etc/ppp/chap-secrets` que define direcciones IP estáticas.

```
account1 myserver secret5748 10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Emisor de llamada	account1 y account2 indican los nombres de los emisores de llamadas.
Servidor	myserver indica el nombre del servidor para cada emisor de llamada.
Contraseña	secret5748 y secret91011 indican el secreto de CHAP para cada emisor de llamada.
Direcciones IP	10.10.111.244 y 10.10.111.245 son las direcciones IP para cada emisor de llamada.

## Asignación de direcciones IP por número de unidad sPPP

Si utiliza autenticación PAP o CHAP, puede asignar direcciones IP a los emisores de llamadas por número de unidad sPPP. A continuación se muestra un ejemplo de este uso.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

El signo más (+) indica que el número de unidad se agrega a la dirección IP. Tenga en cuenta lo siguiente:

- Las direcciones 10.10.111.240 a través de 10.10.111.255 se asignan a usuarios remotos.
- sPPP0 obtiene la dirección IP 10.10.111.240.
- sPPP1 obtiene la dirección IP 10.10.111.241 y así sucesivamente.

# Creación de túneles PPPoE para compatibilidad de DSL

Al utilizar PPPoE, puede proporcionar PPP a través de servicios digitales de alta velocidad a varios clientes que utilizan uno o más módems DSL. PPPoE implementa estos servicios mediante la creación de un túnel Ethernet a través de tres participantes: la empresa, la compañía telefónica y el proveedor de servicios.

- Para obtener una descripción general y una descripción sobre cómo funciona PPPoE, consulte “[Descripción general de PPPoE](#)” en la [página 422](#).
- Para tareas de configuración de túneles PPPoE, consulte el [Capítulo 20](#), “[Configuración de un túnel PPPoE \(tareas\)](#)”.

Esta sección contiene información detallada acerca de comandos y archivos de PPPoE, que se resume en la siguiente tabla.

TABLA 22-2 Comandos y archivos de configuración de PPPoE

Archivo o comando	Descripción	Para obtener instrucciones
<code>/etc/ppp/pppoe</code>	Un archivo que contiene características que se aplican de manera predeterminada a todos los túneles configurados por PPPoE en el sistema	“ <a href="#">Archivo <code>/etc/ppp/pppoe</code>”</a> en la <a href="#">página 544</a>
<code>/etc/ppp/pppoe.<i>dispositivo</i></code>	Un archivo que contiene características de una interfaz determinada utilizada por PPPoE para un túnel	“ <a href="#">Archivo <code>/etc/ppp/pppoe.<i>dispositivo</i></code>”</a> en la <a href="#">página 546</a>
<code>/etc/ppp/pppoe.if</code>	Archivo que muestra la interfaz Ethernet a través de la que se ejecuta el túnel configurado por PPPoE	“ <a href="#">Archivo <code>/etc/ppp/pppoe.if</code>”</a> en la <a href="#">página 542</a>
<code>/usr/sbin/sppptun</code>	Comando para configurar interfaces Ethernet implicadas en un túnel PPPoE	“ <a href="#">Comando <code>/usr/sbin/sppptun</code>”</a> en la <a href="#">página 542</a>
<code>/usr/lib/inet/pppoed</code>	Comando y opciones para utilizar PPPoE para configurar un túnel	“ <a href="#">Daemon <code>/usr/lib/inet/pppoed</code>”</a> en la <a href="#">página 543</a>

## Archivos para configuración de interfaces para PPPoE

Las interfaces que se utilizan en cualquier extremo del túnel PPPoE deben estar configuradas antes de que el túnel pueda admitir comunicaciones de PPP. Utilice los archivos `/usr/sbin/sppptun` y `/etc/ppp/pppoe.if` para este propósito. Debe utilizar estas herramientas para configurar interfaces Ethernet en todos los servidores de acceso PPPoE y clientes PPPoE de Solaris.

## Archivo `/etc/ppp/pppoe.if`

El archivo `/etc/ppp/pppoe.if` enumera los nombres de todas las interfaces Ethernet en un host que se utilizarán para los túneles PPPoE. Este archivo se procesa durante el inicio del sistema cuando las interfaces que se enumeran están conectadas para su uso en túneles PPPoE.

Necesita crear explícitamente `/etc/ppp/pppoe.if`. Escriba el nombre de una interfaz que se debe configurar para PPPoE en cada línea.

En el siguiente ejemplo se muestra un archivo `/etc/ppp/pppoe.if` para un servidor que ofrece tres interfaces para túneles PPPoE.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

Los clientes PPPoE normalmente sólo tienen una interfaz mencionada en `/etc/ppp/pppoe.if`.

## Comando `/usr/sbin/sppptun`

Puede utilizar el comando `/usr/sbin/sppptun` para conectar y desconectar manualmente las interfaces Ethernet que se utilizarán para túneles PPPoE. Por el contrario, `/etc/ppp/pppoe.if` sólo se lee cuando se inicia el sistema. Estas interfaces deben corresponderse con las interfaces enumeradas en `/etc/ppp/pppoe.if`.

`sppptun` conecta las interfaces Ethernet que se utilizan en túneles PPPoE de una manera similar al comando `ifconfig`. A diferencia de `ifconfig`, debe conectar las interfaces dos veces para admitir PPPoE debido a que participan dos números de protocolo Ethernet.

La sintaxis básica para `sppptun` es la siguiente:

```
# /usr/sbin/sppptun plumb pppoe device-name
device-name: pppoe
# /usr/sbin/sppptun plumb pppoe device-name
device-name: pppoe
```

En esta sintaxis, *nombre de dispositivo* es el nombre del dispositivo que se conectará para PPPoE.

La primera vez que emite el comando `sppptun`, el protocolo de detección `pppoed` se conecta en la interfaz. La segunda vez que ejecuta `sppptun`, el protocolo de sesión `pppoe` está conectado. `sppptun` imprime el nombre de la interfaz que se acaba de conectar. Este nombre se utiliza para desconectar la interfaz, cuando es necesario.

Para obtener más información, consulte la página del comando `man sppptun(1M)`.

## Ejemplos de comandos `sppptun` para administración de interfaces

En el siguiente ejemplo se muestra cómo conectar manualmente una interfaz para PPPoE mediante `/usr/sbin/sppptun`.

```
# /usr/sbin/sppptun plumb pppoe hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
hme0:pppoe
```

En este ejemplo se muestra cómo enumerar las interfaces en un servidor de acceso conectado para PPPoE.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

En este ejemplo se muestra cómo desconectar una interfaz.

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

## Comandos y archivos de servidor de acceso PPPoE

Un proveedor de servicios que ofrece servicios DSL o admite que los clientes puedan utilizar un servidor de acceso que ejecuta PPPoE. El cliente y el servidor de acceso PPPoE funcionan en la relación cliente-servidor tradicional. Esta relación es similar a la relación del equipo de marcación de salida y el servidor de marcación de entrada en un enlace por marcación telefónica. Un sistema PPPoE inicia comunicaciones y un sistema PPPoE responde. Por el contrario, el protocolo de PPP no tiene noción de la relación cliente-servidor. PPP considera ambos sistemas como iguales.

Los archivos y comandos para configurar un servidor de acceso PPPoE incluyen lo siguiente:

- “Comando `/usr/sbin/sppptun`” en la página 542
- “Daemon `/usr/lib/inet/pppoed`” en la página 543
- “Archivo `/etc/ppp/pppoe`” en la página 544
- “Archivo `/etc/ppp/pppoe.dispositivo`” en la página 546
- “Objeto compartido `pppoe.so`” en la página 549

### Daemon `/usr/lib/inet/pppoed`

El daemon `pppoed` acepta difusiones para servicios desde posibles clientes PPPoE. Además, `pppoed` negocia el lado del servidor del túnel PPPoE y ejecuta `pppd`, el daemon de PPP, a través del túnel.

Configura servicios `pppoed` en los archivos `/etc/ppp/pppoe` y `/etc/ppp/pppoe.dispositivo`. Si `/etc/ppp/pppoe` existe cuando se inicia el sistema, `pppoed` se ejecuta automáticamente. También puede ejecutar explícitamente el daemon `pppoed` en la línea de comandos si escribe `/usr/lib/inet/pppoed`.

## Archivo `/etc/ppp/pppoe`

El archivo `/etc/ppp/pppoe` describe los servicios que ofrece un servidor de acceso más las opciones que definen cómo PPP se ejecuta a través del túnel PPPoE. Puede definir servicios para interfaces individuales o globalmente, es decir, para todas las interfaces del servidor de acceso. El servidor de acceso envía la información en el archivo `/etc/ppp/pppoe`, en respuesta a una difusión de un posible cliente PPPoE.

La siguiente es la sintaxis básica de `/etc/ppp/pppoe`:

```
global-options
service service-name
    service-specific-options
    device interface-name
```

Los parámetros tienen los siguientes significados.

### *opciones globales*

Establece las opciones predeterminadas para el archivo `/etc/ppp/pppoe`. Estas opciones pueden ser cualquiera de las opciones disponibles a través de `pppoed` o `pppd`. Para ver una lista completa de opciones, consulte las páginas del comando `man pppoed(1M)` y `pppd(1M)`.

Por ejemplo, debe enumerar las interfaces Ethernet que están disponibles para el túnel PPPoE como parte de *opciones globales*. Si no define dispositivos en `/etc/ppp/pppoe`, los servicios no se ofrecen en ninguna interfaz.

Para definir `devices` como una opción global, utilice lo siguiente:

```
device interface <,interface>
```

*interfaz* especifica la interfaz donde el servicio está atento a posibles clientes PPPoE. Si más de una interfaz está asociada al servicio, separe cada nombre con una coma.

### *servicio nombre de servicio*

Inicia la definición del servicio *nombre de servicio*. *nombre de servicio* es una cadena que puede ser cualquier frase que sea apropiada para los servicios que se proporcionan.

### *opciones específicas de servicio*

Muestra las opciones de PPPoE y PPP específicas para este servicio.

### *device nombre de interfaz*

Especifica la interfaz donde el servicio previamente mencionado está disponible.

Para opciones adicionales para `/etc/ppp/pppoe`, consulte las páginas del comando `man pppoed(1M)` y `pppd(1M)`.



Es posible que un archivo `/etc/ppp/pppoe` típico se asemeje a lo siguiente.

**EJEMPLO 22-2** Archivo `/etc/ppp/pppoe` básico

```
device hme1,hme2,hme3
service internet
  pppd "name internet-server"
service intranet
  pppd "192.168.1.1:"
service debug
  device hme1
  pppd "debug name internet-server"
```

En este archivo, se aplican los siguientes valores.

<code>hme1,hme2,hme3</code>	Tres interfaces en el servidor de acceso que se utilizarán para túneles PPPoE.
<code>service internet</code>	Anuncia un servicio que se denomina <code>internet</code> para posibles clientes. El proveedor que ofrece el servicio determina también cómo <code>internet</code> está definido. Por ejemplo, un proveedor puede interpretar <code>internet</code> como distintos servicios IP, así como el acceso a Internet.
<code>pppd</code>	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca <code>pppd</code> . La opción <code>"name internet-server"</code> proporciona el nombre del equipo local, el servidor de acceso, como <code>internet-server</code> .
<code>service intranet</code>	Anuncia otro servicio que se denomina <code>intranet</code> para posibles clientes.
<code>pppd "192.168.1.1:"</code>	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca <code>pppd</code> . Cuando el emisor de llamada invoca <code>pppd</code> , <code>192.168.1.1</code> se establece como la dirección IP del equipo local, el servidor de acceso.
<code>service debug</code>	Anuncia un tercer servicio, la depuración, en las interfaces que se definen para PPPoE.
<code>device hme1</code>	Restringe la depuración para túneles PPPoE para <code>hme1</code> .
<code>pppd "debug name internet-server"</code>	Establece las opciones de línea de comandos que se utilizan cuando el emisor de llamada invoca <code>pppd</code> , en esta instancia, la depuración de PPP en

internet - server, el equipo local.

### Archivo `/etc/ppp/pppoe.dispositivo`

El archivo `/etc/ppp/pppoe.dispositivo` describe los servicios ofrecidos en una interfaz de un servidor de acceso PPPoE. `/etc/ppp/pppoe.dispositivo` también incluye opciones que definen cómo PPP se ejecuta a través del túnel PPPoE. `/etc/ppp/pppoe.dispositivo` es un archivo opcional, que funciona exactamente igual que `/etc/ppp/pppoe` global. Sin embargo, si `/etc/ppp/pppoe.dispositivo` se define para una interfaz, sus parámetros tienen precedencia para dicha interfaz sobre los parámetros globales que se definen en `/etc/ppp/pppoe`.

La sintaxis básica de `/etc/ppp/pppoe.dispositivo` es la siguiente:

```
service service-name
    service-specific-options
service another-service-name
    service-specific-options
```

La única diferencia entre esta sintaxis y la sintaxis de `/etc/ppp/pppoe` es que no puede utilizar la opción `device` que se muestra en [“Archivo `/etc/ppp/pppoe`” en la página 544](#).

### Complemento `pppoe.so`

`pppoe.so` es el archivo de objeto compartido PPPoE que debe ser invocado por clientes y servidores de acceso PPPoE. Este archivo limita MTU y MRU a 1492, filtra paquetes desde el controlador y negocia el túnel PPPoE junto con `pppoe`. En el lado del servidor de acceso, `pppoe.so` es invocado automáticamente por el daemon `pppd`.

### Uso de archivos PPPoE y PPP para configurar un servidor de acceso

Esta sección contiene ejemplos de todos los archivos que se utilizan para configurar un servidor de acceso. El servidor de acceso es de hosts múltiples. El servidor está conectado a tres subredes: `green`, `orange` y `purple`. `pppoe` se ejecuta como `root` en el servidor, que es el valor predeterminado.

Los clientes PPPoE pueden acceder a las redes de `orange` y `purple` a través de interfaces `hme0` y `hme1`. Los clientes inician sesión en el servidor mediante el inicio de sesión de UNIX estándar. El servidor autentica a los clientes mediante PAP.

La red `green` no se anuncia para los clientes. La única forma en que los clientes pueden acceder a `green` es especificar directamente `"green-net"` y proporcionar credenciales de autenticación CHAP. Además, sólo los clientes `joe` y `mary` tienen permiso para acceder a la red `green` mediante direcciones IP estáticas.

**EJEMPLO 22-3** Archivo para un servidor de acceso /etc/ppp/pppoe

```

service orange-net
    device hme0,hme1
    pppd "require-pap login name orange-server orange-server:"
service purple-net
    device hme0,hme1
    pppd "require-pap login name purple-server purple-server:"
service green-net
    device hme1
    pppd "require-chap name green-server green-server:"
nowildcard

```

Este ejemplo describe los servicios que están disponibles desde el servidor de acceso. La primera sección de servicio describe los servicios de la red orange.

```

service orange-net
    device hme0,hme1
    pppd "require-pap login name orange-server orange-server:"

```

Los clientes acceden a la red orange a través de interfaces hme0 y hme1. Las opciones que se brindan al comando pppd obligan al servidor a solicitar credenciales de PAP de clientes potenciales. Las opciones pppd establecen el nombre del servidor para orange-server, como se utiliza en el archivo pap-secrets.

La sección de servicio para la red purple es idéntica a la sección de servicio de la red orange a excepción de los nombres de servidor y de red.

La siguiente sección describe los servicios de la red green:

```

service green-net
    device hme1
    pppd "require-chap name green-server green-server:"
nowildcard

```

Esta sección restringe el acceso de cliente a la interfaz hme1. Las opciones que se brindan al comando pppd obligan al servidor que solicite credenciales de CHAP de clientes potenciales. Las opciones pppd también establecen el nombre de servidor para green-server, que se utilizará en el archivo chap-secrets. La opción nowildcard especifica que la existencia de la red "green" no se anuncia a los clientes.

Para este escenario de servidor de acceso que acabamos de debatir, es posible que configure el siguiente archivo /etc/ppp/options.

**EJEMPLO 22-4** Archivo para un servidor de acceso /etc/ppp/options

```

auth
proxyarp
nodefaulttroute
name no-service    # don't authenticate otherwise

```

La opción `name no-service` modifica el nombre de servidor que normalmente se busca durante la autenticación PAP o CHAP. El nombre predeterminado del servidor es el que se encuentra mediante el comando `/usr/bin/hostname`. La opción `name` en el ejemplo anterior cambia el nombre del servidor a `no-service`. No es muy posible que se encuentre el nombre `no-service` en un archivo `pap` o `chap-secrets`. Esta acción impide que un usuario al azar ejecute `pppd` y cambie las opciones `auth` y `name` establecidas en `/etc/ppp/options`. `pppd` falla debido a que no se pueden encontrar secretos para el cliente con un nombre de servidor de `no-service`.

El escenario de servidor de acceso utiliza el siguiente archivo `/etc/hosts`.

**EJEMPLO 22-5** Archivo para un servidor de acceso `/etc/hosts`

```
172.16.0.1    orange-server
172.17.0.1    purple-server
172.18.0.1    green-server
172.18.0.2    joes-pc
172.18.0.3    marys-pc
```

Aquí está el archivo `/etc/ppp/pap-secrets` que se utiliza para autenticación PAP para clientes que intentan acceder a las redes `orange` y `purple`.

**EJEMPLO 22-6** Archivo para un servidor de acceso `/etc/ppp/pap-secrets`

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

Aquí está el archivo `/etc/ppp/chap-secrets` que se utiliza para autenticación CHAP. Tenga en cuenta que sólo los clientes `joe` y `mary` se muestran en el archivo.

**EJEMPLO 22-7** Archivo para un servidor de acceso `/etc/ppp/chap-secrets`

```
joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

## Archivos y comandos de cliente PPPoE

Para ejecutar PPP a través de un módem DSL, un equipo debe convertirse en un cliente PPPoE. Debe conectar una interfaz para ejecutar PPPoE y, a continuación, utilizar la utilidad `pppoe` para "detectar" la existencia de un servidor de acceso. A partir de ese momento, el cliente puede crear el túnel PPPoE a través del módem DSL y ejecutar PPP.

El cliente PPPoE se relaciona con el servidor de acceso en el modelo cliente-servidor tradicional. El túnel PPPoE no es un enlace por marcación telefónica, pero está configurado y opera casi de la misma manera.

Los archivos y comandos para configurar un cliente PPPoE incluyen lo siguiente:

- “Comando `/usr/sbin/sppptun`” en la página 542
- “Utilidad `/usr/lib/inet/pppoe`” en la página 549
- “Objeto compartido `pppoe.so`” en la página 549
- “Archivo `/etc/ppp/peers/nombre de igual`” en la página 519
- “Archivo de configuración `/etc/ppp/options`” en la página 514

## Utilidad `/usr/lib/inet/pppoe`

La utilidad `/usr/lib/inet/pppoe` es responsable de negociar el lado del cliente de un túnel PPPoE. `pppoe` es similar a la utilidad `chat`. No invoca `pppoe` directamente. En su lugar, inicia `/usr/lib/inet/pppoe` como un argumento para la opción `connect` de `pppd`.

## Objeto compartido `pppoe.so`

`pppoe.so` es el objeto compartido PPPoE que debe ser cargado por PPPoE para proporcionar funciones PPPoE para acceder a servidores y clientes. El objeto compartido `pppoe.so` limita MTU y MRU 1492, filtra paquetes desde el controlador y gestiona mensajes PPPoE de tiempo de ejecución.

En el lado del cliente, `pppd` carga `pppoe.so` cuando el usuario especifica la opción `plugin pppoe.so`.

## Archivo para definir un igual de servidor de acceso `/etc/ppp/peers/nombre de igual`

Cuando define un servidor de acceso para que lo detecte `pppoe`, puede usar opciones que se apliquen a `pppoe` y al daemon `pppd`. Un archivo `/etc/ppp/peers/nombre de igual` de un servidor de acceso requiere los siguientes parámetros:

- `sppptun`: nombre para el dispositivo serie utilizado por el túnel PPPoE.
- `plugin pppoe.so`: indica a `pppd` que cargue el objeto compartido `pppoe.so`.
- `connect "/usr/lib/inet/pppoe dispositivo"`: inicia una conexión. `connect` luego invoca la utilidad `pppoe` a través de *dispositivo*, la interfaz que está conectada para PPPoE.

Los parámetros restantes del archivo `/etc/ppp/peers/nombre de igual` se deben aplicar al enlace de PPP en el servidor. Utilice las mismas opciones que usaría para `/etc/ppp/peers/nombre de igual` en un equipo de marcación de salida. Intente limitar el número de opciones al mínimo necesario para el enlace de PPP.

El siguiente ejemplo se presenta en “[Cómo definir un igual de servidor de acceso PPPoE](#)” en la página 483.

**EJEMPLO 22-8** /etc/ppp/peers/*nombre de igual* para definir un servidor de acceso remoto

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoc hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Este archivo define parámetros que se utilizarán al configurar un túnel PPPoE y un enlace de PPP para el servidor de acceso dslserve. Las opciones que se incluyen son las siguientes.

Opción	Descripción
sppptun	Define sppptun como nombre del dispositivo serie.
plugin pppoe.so	Indica a pppd que cargue el objeto compartido pppoe.so.
connect "/usr/lib/inet/pppoc hme0"	Ejecuta pppoc y designa hme0 como interfaz para el túnel PPPoE y el enlace de PPP.
noccp	Desactiva la compresión CCP en el enlace.  <b>Nota</b> – Muchos ISP utilizan sólo algoritmos de compresión de propietario. La desactivación del algoritmo CCP disponible públicamente ahorra tiempo de negociación y evita problemas de interoperabilidad frecuentes.
noauth	Evita que pppd exija credenciales de autenticación desde el servidor de acceso. La mayoría de proveedores de servicios de Internet no proporcionan credenciales de autenticación a los clientes.
user Red	Establece el nombre Red como nombre de usuario para el cliente, que es requerido para autenticación PAP por el servidor de acceso.
password redsecret	Define redsecret como la contraseña que se proporcionará al servidor de acceso para autenticación PAP.
noipdefault	Asigna 0.0.0.0 como la dirección IP inicial.
defaultroute	Indica a pppd que instale una ruta IPv4 predeterminada después de la negociación de IPCP. Debe incluir defaultroute en /etc/ppp/peers/ <i>nombre de igual</i> cuando el enlace es el enlace del sistema a Internet, lo que se aplica para un cliente PPPoE.

## Migración de Solaris PPP asíncrono a Solaris PPP 4.0 (tareas)

---

Las versiones anteriores del SO Solaris incluían una implementación de PPP diferente, Solaris PPP asíncrono (asppp). Si desea convertir a los iguales que ejecutan asppp a la nueva versión PPP 4.0, tendrá que ejecutar una secuencia de comandos de conversión. En este capítulo se tratan los siguientes temas de conversión de PPP:

- “[Antes de convertir archivos asppp](#)” en la página 551
- “[Ejecución de la secuencia de comandos de conversión asppp2pppd \(tareas\)](#)” en la página 554

El capítulo utiliza un ejemplo de configuración de asppp para explicar cómo realizar la conversión de PPP. Para obtener una descripción de las diferencias entre Solaris PPP 4.0 y asppp, vaya a “[Cómo determinar qué versión de Solaris PPP se debe usar](#)” en la página 410.

### Antes de convertir archivos asppp

Puede utilizar la secuencia de comandos de conversión `/usr/sbin/asppp2pppd` para convertir los archivos que componen una configuración asppp estándar.

- `/etc/asppp.cf`: archivo de configuración de PPP asíncrono
- `/etc/uucp/Systems`: archivo de UUCP que describe las características del igual remoto
- `/etc/uucp/Devices`: archivo de UUCP que describe el módem en el equipo local
- `/etc/uucp/Dialers`: archivo de UUCP que contiene la secuencia de comandos de inicio de sesión que utilizará el módem que se describe en el archivo `/etc/uucp/Devices`

Para obtener más información sobre asppp, consulte la *Colección de administración del sistema Solaris 8, volumen 3*, disponible en `http://docs.sun.com`.

### Ejemplo del archivo de configuración `/etc/asppp.cf`

El procedimiento que se muestra en “[Cómo convertir de asppp a Solaris PPP 4.0](#)” en la página 555 utiliza el siguiente archivo `/etc/asppp.cf`.

```
#
ifconfig ipdptp0 plumb mojava gobi up

path
  inactivity_timeout 120      # Approx. 2 minutes
  interface ipdptp0
  peer_system_name Pgobi      # The name we log in with (also in
                              # /etc/uucp/Systems
```

El archivo contiene los siguientes parámetros.

<code>ifconfig ipdptp0 plumb mojava gobi up</code>	Ejecuta el comando <code>ifconfig</code> para configurar un enlace desde una interfaz de PPP <code>ipdptp0</code> en el equipo local <code>mojava</code> hasta el igual remoto <code>gobi</code>
<code>inactivity_timeout 120</code>	Termina la línea después de dos minutos de inactividad
<code>interface ipdptp0</code>	Configura la interfaz <code>ipdptp0</code> en el equipo de marcación de salida para PPP asíncrono
<code>peer_system_name Pgobi</code>	Proporciona el nombre del igual remoto, <code>Pgobi</code>

## Ejemplo del archivo `/etc/uucp/Systems`

El procedimiento que se muestra en [“Cómo convertir de asppp a Solaris PPP 4.0” en la página 555](#) utiliza el siguiente archivo `/etc/uucp/Systems`.

```
#ident "@(#)Systems 1.5 92/07/14 SMI" /* from SVR4 bnu:Systems 2.4 */
#
# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojava word: sand
```

El archivo contiene los siguientes parámetros:

<code>Pgobi</code>	Utiliza <code>Pgobi</code> como el nombre de host del igual remoto.
<code>Any ACU</code>	Indica al módem en el equipo de marcación de salida <code>mojava</code> que establezca un enlace con un módem <code>Pgobi</code> en cualquier momento del día. Cualquier unidad de llamada automática (ACU) significa "buscar ACU en el archivo <code>/etc/uucp/Devices</code> ".
<code>38400</code>	Establece 38400 como la velocidad máxima del enlace.
<code>15551212</code>	Proporciona el número de teléfono de <code>Pgobi</code> .



`in:-in: mojave word: sand` Define la secuencia de comandos de inicio de sesión que requiere Pgobi para autenticar el equipo de marcación de salida `mojave`.

## Ejemplo del archivo `/etc/uucp/Devices`

El procedimiento que se muestra en [“Cómo convertir de asppp a Solaris PPP 4.0” en la página 555](#) utiliza el siguiente archivo `/etc/uucp/Devices`.

```
#ident "@(#)Devices 1.6 92/07/14 SMI" /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

El archivo admite cualquier módem Hayes que esté conectado al puerto de serie `cua/b`.

## Ejemplo del archivo `/etc/uucp/Dialers`

El procedimiento que se muestra en [“Cómo convertir de asppp a Solaris PPP 4.0” en la página 555](#) utiliza el siguiente archivo `/etc/uucp/Dialers`.

```
#
#      <Much information about modems supported by Oracle Solaris UUCP>

penril      =W-P      "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

```

ventel    =&-%      "" \r\p\r\c $ k\c ONLINE!
vadic     =K-K      "" \005\p *- \005\p- * \005\p- * D\p BER? \E\T\e \r\c LINE
develcon  ""        "" \pr\ps\c est:\007 \E\D\e \n\007
micom     ""        "" \s\c NAME? \D\r\c GO
direct
#
#
#
# Hayes Smartmodem -- modem should be set with the configuration
# switches as follows:
#
#      S1 - UP      S2 - UP      S3 - DOWN  S4 - UP
#      S5 - UP      S6 - DOWN    S7 - ?      S8 - DOWN
#
hayes     =, -,      "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

```

*<much more information about modems supported by Oracle Solaris UUCP>*

Este archivo contiene las secuencias de comandos de chat para todos los tipos de módems, incluido los módems Hayes que se admiten en el archivo /etc/uucp/Dialers.

## Ejecución de la secuencia de comandos de conversión asppp2pppd (tareas)

La secuencia de comandos /usr/sbin/asppp2pppd copia la información de PPP en /etc/asppp.cf y los archivos de UUCP relacionados con PPP para ubicaciones apropiadas en los archivos de Solaris PPP 4.0.

## Requisitos previos de la tarea

Antes de realizar la siguiente tarea, debe haber hecho lo siguiente:

- Instalado la versión de Solaris en el equipo que también tiene los archivos de configuración de UUCP y asppp.
- Convertido en superusuario en el equipo con los archivos de PPP, por ejemplo, el equipo mojave

## ▼ Cómo convertir de asppp a Solaris PPP 4.0

### 1 Inicie la secuencia de comandos de conversión.

```
# /usr/sbin/asppp2pppd
```

El proceso de conversión se inicia y le muestra la siguiente pantalla.

```
This script provides only a suggested translation for your existing aspppd
configuration. You will need to evaluate for yourself whether the translation
is appropriate for your operating environment.
Continue [Yn]?
```

### 2 Escriba "Y" para continuar.

Recibirá el siguiente resultado.

```
Chat cannot do echo checking; requests for this removed.
Adding 'noauth' to /etc/ppp/options
```

```
Preparing to write out translated configuration:
```

```
1 chat file:
  1. /etc/ppp/chat.Pgobi.hayes
2 option files:
  2. /etc/ppp/peers/Pgobi
  3. /etc/ppp/options
1 script file:
  4. /etc/ppp/demand
```

Los nuevos archivos de Solaris PPP 4.0 se han generado.

## ▼ Cómo ver los resultados de la conversión

Puede ver los archivos de Solaris PPP 4.0 que se crearon mediante la secuencia de comandos de conversión /usr/sbin/asppp2pppd al final del proceso de conversión. La secuencia de comandos muestra la siguiente lista de opciones.

```
Enter option number:
  1 - view contents of file on standard output
  2 - view contents of file using /usr/bin/less
  3 - edit contents of file using /usr/bin/vi
  4 - delete/undelete file from list
  5 - rename file in list
  6 - show file list again
  7 - escape to shell (or "!")
  8 - abort without saving anything
  9 - save all files and exit (default)
Option:
```

**1 Escriba 1 para ver los contenidos de los archivos en la pantalla.**

La secuencia de comandos solicita el número del archivo que desea ver.

File number (1 .. 4):

Los números se refieren a los archivos traducidos que se enumeran durante el proceso de conversión, como se muestra en el paso 2 anterior.

**2 Escriba 1 para ver el archivo de chat /etc/ppp/chat.Pgobi.hayes.**

```
File number (1 .. 4): 1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

La secuencia de comandos de chat contiene la información de "chat" del módem que aparece en la línea Hayes en el archivo de ejemplo /etc/uucp/Dialers./etc/ppp/chat.Pgobi.hayes también contiene la secuencia de inicio de sesión para Pgobi que aparece en el archivo de ejemplo /etc/uucp/Systems. La secuencia de comandos de chat se encuentra ahora en el archivo /etc/ppp/chat.Pgobi.hayes.

**3 Escriba 2 para ver el archivo de los iguales, /etc/ppp/peers/Pgobi.**

```
File number (1 .. 4): 2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T '15551212'"
user NeverAuthenticate
mojave:gobi
```

La información del puerto de serie (/dev/cua/b) se obtiene del archivo /etc/uucp/Devices. La velocidad del enlace, el tiempo de inactividad, la información de autenticación y los nombres de iguales se obtienen del archivo /etc/asppp.cf. "demand" hace referencia a la secuencia de comandos "demand", a la que se llama cuando el equipo de marcación de salida intenta conectarse con el igual Pgobi.

**4 Escriba 3 para ver el archivo /etc/ppp/options que se crea para el equipo de marcación de salida mojave.**

```
File number (1 .. 4): 3
#lock
noauth
```

La información de /etc/ppp/options se obtiene del archivo /etc/asppp.cf.

**5 Escriba 4 para ver los contenidos de la secuencia de comandos demand.**

```
File number (1 .. 4): 4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

Esta secuencia de comandos, cuando se invoca, ejecuta el comando `pppd` que luego lee `/etc/ppp/peers/Pgobi` para iniciar el enlace entre `mojave` y `Pgobi`.

- 6 Escriba 9 para guardar los archivos creados. A continuación, salga de la secuencia de comandos de conversión.**



## UUCP (descripción general)

---

En este capítulo, se introducen el programa de copia de UNIX a UNIX (UUCP) y sus daemons. Contiene los temas siguientes:

- “Configuraciones de hardware del UUCP” en la página 559
- “Software del UUCP” en la página 560
- “Archivos de base de datos del UUCP” en la página 563

El UUCP permite a los equipos transferir archivos e intercambiar correo entre ellos. El programa también permite a los equipos participar en redes de gran tamaño, como Usenet.

El SO Solaris proporciona la versión de utilidades básicas de red (BNU) del UUCP, también conocida como HoneyDanBer UUCP. El término *UUCP* indica el rango completo de utilidades y archivos que componen el sistema, del cual el programa *uucp* es sólo una parte. El rango de utilidades del UUCP abarca desde las utilidades que se utilizan para copiar archivos entre equipos (*uucp* y *uuto*) hasta las utilidades que se utilizan para iniciar sesión y ejecutar comandos de manera remota (*cu* y *uux*).

## Configuraciones de hardware del UUCP

El UUCP admite las siguientes configuraciones de hardware:

Enlaces directos	Puede crear un enlace directo a otro equipo colocando cables RS-232 entre los puertos de serie de los dos equipos. Los enlaces directos son útiles cuando dos equipos se comunican regularmente y están físicamente cerca, por ejemplo, dentro de 50 ft (15 m) entre ellos. Puede utilizar un módem de distancia limitada para aumentar esta distancia un poco.
Líneas telefónicas	Al usar una unidad de llamada automática (ACU), como un módem de alta velocidad, el equipo puede comunicarse con otros equipos por medio de líneas de teléfono estándar. El módem marca el número de teléfono

solicitado por el UUCP. El equipo destinatario debe tener un módem capaz de responder llamadas entrantes.

#### Red

El UUCP también puede comunicarse por medio de una red que ejecuta TCP/IP u otra familia de protocolos. Después de que su equipo se ha establecido como un host en una red, el equipo puede ponerse en contacto con cualquier otro host que está conectado a la red.

En este capítulo, se asume que el hardware del UUCP ya se ha ensamblado y configurado. Si necesita configurar un módem, consulte la [Guía de administración del sistema: administración básica](#) y los manuales que acompañan el módem para obtener ayuda.

## Software del UUCP

El software del UUCP se incluye automáticamente al ejecutar el programa de instalación de Solaris y al seleccionar toda la distribución. También puede agregar el software del UUCP mediante pkgadd. Los programas del UUCP se pueden dividir en tres categorías: daemons, programas administrativos y programas de usuario.

## Daemons del UUCP

El sistema del UUCP tiene cuatro daemons: uucico, uuxqt, uusched e in.uucpd. Estos daemons manejan las transferencias de archivos y las ejecuciones de comandos del UUCP. También se pueden ejecutar de forma manual desde el shell, si es necesario.

**uucico**      Selecciona el dispositivo que se utiliza para el enlace, establece el enlace al equipo remoto y realiza las comprobaciones requeridas de permisos y secuencias de inicio de sesión. Además, uucico transfiere archivos de datos, archivos ejecutables y resultados de registros, y notifica al usuario por correo cuando se completan las transferencias. uucico actúa como el "shell de inicio de sesión" para las cuentas de entrada del UUCP. Cuando el daemon uucico local llama a un equipo remoto, se comunica directamente con el daemon uucico remoto durante la sesión.

Después de que todos los archivos necesarios se han creado, los programas uucp, uuto y uux ejecutan el daemon uucico para ponerse en contacto con el equipo remoto. uusched y lutry ejecutan uucico. Consulte la página del comando [man uucico\(1M\)](#) para obtener detalles.

**uuxqt**      Ejecuta solicitudes de ejecución remota. Este daemon busca en el directorio de cola de impresión archivos ejecutables (siempre denominados *X.file*) que se han enviado desde un equipo remoto. Cuando un archivo *X.file* se encuentra, uuxqt lo abre para obtener la lista de los archivos de datos que son necesarios para la



ejecución. `uuxqt` después comprueba si los archivos de datos necesarios están disponibles y son accesibles. Si los archivos están disponibles, `uuxqt` comprueba el archivo `Permissions` para verificar si tiene permiso para ejecutar el comando solicitado. El daemon `uuxqt` es ejecutado por la secuencia de comandos de shell `uudemon.hour`, que es iniciada por `cron`. Consulte la página del comando `man uuxqt(1M)` para obtener detalles.

- `uusched` Programa el trabajo en cola en el directorio de cola de impresión. `uusched` se ejecuta inicialmente en el momento del inicio mediante la secuencia de comandos de shell `uudemon.hour`, que es iniciada por `cron`. Consulte la página del comando `man uusched(1M)` para obtener detalles. Antes de iniciar el daemon `uucico`, `uusched` selecciona al azar el orden en el que los equipos remotos se llaman.
- `in.uucpd` Admite conexiones del UUCP por medio de redes. El `inetd` en el host remoto invoca a `in.uucpd` cada vez que se establece una conexión del UUCP. `uucpd`, a continuación, solicita un nombre de inicio de sesión. `uucico` en el host que llama debe responder con un nombre de inicio de sesión. `in.uucpd`, a continuación, solicita una contraseña, a menos que no sea necesaria. Consulte la página del comando `man in.uucpd(1M)` para obtener detalles.

## Programas administrativos del UUCP

La mayoría de los programas administrativos del UUCP están en `/usr/lib/uucp`. La mayoría de los archivos de base de datos básicos están en `/etc/uucp`. La única excepción es `uulog`, que está en `/usr/bin`. El directorio principal del ID de inicio de sesión `uucp` es `/usr/lib/uucp`. Al ejecutar los programas administrativos mediante su `login`, utilice el ID de usuario `uucp`. El ID de usuario posee los programas y los archivos de datos en cola de impresión.

- `uulog` Muestra el contenido de los archivos de registro de un equipo especificado. Los archivos de registro se crean para cada equipo remoto con el que su equipo se comunica. Los archivos de registro registran cada uso de `uucp`, `uuto` y `uux`. Consulte la página del comando `man uucp(1C)` para obtener detalles.
- `uucleanup` Limpia el directorio de la cola de impresión. `uucleanup` es normalmente ejecutado desde la secuencia de comandos de shell `uudemon.cleanup`, que es iniciada por `cron`. Consulte la página del comando `man uucleanup(1M)` para obtener detalles.
- `Uutry` Prueba las capacidades de procesamiento de llamadas y realiza una depuración moderada. `Uutry` invoca el daemon `uucico` para establecer un enlace de comunicación entre su equipo y el equipo remoto que especifique. Consulte la página del comando `man Uutry(1M)` para obtener detalles.

**uucheck** Comprueba la presencia de directorios, programas y archivos de compatibilidad del UUCP. **uucheck** también puede comprobar determinadas partes del archivo `/etc/uucp/Permissions` para buscar errores sintácticos evidentes. Consulte la página del comando `man uucheck(1M)` para obtener detalles.

## Programas de usuario del UUCP

Los programas de usuario del UUCP están en `/usr/bin`. No es necesario un permiso especial para usar estos programas.

**cu** Conecta el equipo con un equipo remoto para que pueda iniciar sesión en ambos equipos al mismo tiempo. **cu** le permite transferir archivos o ejecutar comandos en cualquiera de los equipos sin necesidad de abandonar el enlace inicial. Consulte la página del comando `man cu(1C)` para obtener detalles.

**uucp** Permite copiar un archivo de un equipo a otro. **uucp** crea archivos de trabajo y archivos de datos, pone en cola trabajos para transferencia y llama al daemon `uucico`, que, a su vez, intenta ponerse en contacto con el equipo remoto. Consulte la página del comando `man uucp(1C)` para obtener detalles.

**uuto** Copia archivos del equipo local al directorio de cola de impresión público `/var/spool/uucppublic/receive` en el equipo remoto. A diferencia de **uucp**, que permite copiar un archivo en cualquier directorio accesible del equipo remoto, **uuto** coloca el archivo en un directorio de cola de impresión adecuado e indica al usuario remoto que recoja el archivo con `uupick`. Consulte la página del comando `man uuto(1C)` para obtener detalles.

**uupick** Recupera los archivos en `/var/spool/uucppublic/receive` cuando los archivos se transfieren a un equipo mediante **uuto**. Consulte la página del comando `man uuto(1C)` para obtener más información.

**uux** Crea los archivos de trabajo, de datos y ejecutables que son necesarios para ejecutar comandos en un equipo remoto. Consulte la página del comando `man uux(1C)` para obtener detalles.

**uustat** Muestra el estado de transferencias solicitadas (**uucp**, **uuto** o **uux**). **uustat** también proporciona un medio para controlar transferencias en cola. Consulte la página del comando `man uustat(1C)` para obtener detalles.

## Archivos de base de datos del UUCP

Una parte importante de la configuración del UUCP es la configuración de los archivos que componen la base de datos del UUCP. Estos archivos están en el directorio `/etc/uucp`. Debe editar estos archivos para configurar el UUCP o `asppp` en su equipo. Los archivos incluyen lo siguiente:

<code>Config</code>	Contiene una lista de parámetros variables. Estos parámetros se pueden definir manualmente para configurar la red.
<code>Devconfig</code>	Se utiliza para configurar las comunicaciones de red.
<code>Devices</code>	Se utiliza para configurar las comunicaciones de red.
<code>Dialcodes</code>	Contiene abreviaturas de código de marcación que se pueden utilizar en el campo de número de teléfono de las entradas del archivo <code>Systems</code> . Aunque no se requiere, <code>Dialcodes</code> puede ser utilizado por <code>asppp</code> y por el UUCP.
<code>Dialers</code>	Contiene cadenas de caracteres que son necesarias para negociar con módems y establecer conexiones con equipos remotos. <code>Dialers</code> es usado por <code>asppp</code> y por el UUCP.
<code>Grades</code>	Define niveles de trabajos, y los permisos que se relacionan con cada nivel de trabajo, que los usuarios pueden especificar para poner en cola trabajos en un equipo remoto.
<code>Limits</code>	Define el número máximo de comandos <code>uucico</code> , <code>uuxqt</code> y <code>uusched</code> simultáneos que se permiten en el equipo.
<code>Permissions</code>	Define el nivel de acceso que se otorga a hosts remotos que intentan transferir archivos o ejecutar comandos en el equipo.
<code>Poll</code>	Define los equipos que van a ser sondeados por el sistema y cuándo van a ser sondeados.
<code>Sysfiles</code>	Asigna varios o diferentes archivos que serán usados por <code>uucico</code> y <code>cu</code> como archivos <code>Systems</code> , <code>Devices</code> y <code>Dialers</code> .
<code>Sysname</code>	Permite definir un único nombre del UUCP para un equipo, además de su nombre de host TCP/IP.
<code>Systems</code>	<p>Contiene información que necesita el daemon <code>uucico</code>, <code>cu</code> y <code>asppp</code> para establecer un enlace con un equipo remoto. Esta información incluye lo siguiente:</p> <ul style="list-style-type: none"> <li>■ Nombre del host remoto</li> <li>■ Nombre del dispositivo de conexión asociado con el equipo remoto</li> <li>■ Hora en la que se puede acceder al host</li> <li>■ Número de teléfono</li> <li>■ ID de inicio de sesión</li> </ul>

- Contraseña

Otros archivos se pueden considerar parte de la base de datos auxiliar, pero no participan directamente en el establecimiento de un enlace ni en la transferencia de archivos.

## Configuración de archivos de base de datos del UUCP

La base de datos del UUCP consta de los archivos que se muestran en [“Archivos de base de datos del UUCP” en la página 563](#). Sin embargo, la configuración básica del UUCP sólo involucra los siguientes archivos críticos:

- /etc/uucp/Systems
- /etc/uucp/Devices
- /etc/uucp/Dialers

Debido a que asppp utiliza algunas de las bases de datos del UUCP, debe comprender, como mínimo, estos archivos de base de datos críticos si planea configurar asppp. Después de que estas bases de datos se configuran, la administración del UUCP es bastante sencilla. Normalmente, primero edita el archivo `Systems` y luego edita el archivo `Devices`. Por lo general, puede utilizar el archivo predeterminado `/etc/uucp/Dialers`, a menos que planea agregar marcadores que no están en el archivo predeterminado. Además, es posible que también desee utilizar los siguientes archivos para la configuración básica del UUCP y asppp:

- /etc/uucp/Sysfiles
- /etc/uucp/Dialcodes
- /etc/uucp/Sysname

Dado que estos archivos trabajan de forma estrecha entre ellos, debe comprender todo su contenido antes de realizar cambios. Un cambio en una entrada de un archivo puede exigir un cambio en una entrada relacionada de otro archivo. El resto de los archivos que aparecen en [“Archivos de base de datos del UUCP” en la página 563](#) no están tan críticamente entrelazados.

---

**Nota** – asppp utiliza sólo los archivos que se describen en esta sección. asppp no utiliza los otros archivos de base de datos del UUCP.

---

## Administración del UUCP (tareas)

En este capítulo, se explica cómo iniciar operaciones del UUCP después de modificar el archivo de base de datos que corresponde a sus equipos. El capítulo contiene información sobre procedimientos y resolución de problemas para configurar y mantener el UUCP en equipos que ejecutan el sistema operativo Solaris, como los siguientes:

- “Administración del UUCP (mapa de tareas)” en la página 565
- “Adición de inicios de sesión del UUCP” en la página 566
- “Inicio del UUCP” en la página 567
- “Ejecución del UUCP mediante TCP/IP” en la página 569
- “Seguridad y mantenimiento del UUCP” en la página 570
- “Resolución de problemas del UUCP” en la página 572

### Administración del UUCP (mapa de tareas)

En la siguiente tabla, se proporcionan referencias a los procedimientos que se cubren en este capítulo, además de una breve descripción de cada procedimiento.

TABLA 25-1 Mapa de tareas para la administración del UUCP

Tarea	Descripción	Para obtener instrucciones
Permitir que los equipos remotos tengan acceso al sistema	Edite el archivo <code>/etc/passwd</code> para agregar entradas con el fin de identificar los equipos que tienen permiso para acceder al sistema.	“Cómo agregar inicios de sesión del UUCP” en la página 566
Iniciar el UUCP	Utilice las secuencias de comandos de shell proporcionadas para iniciar el UUCP.	“Cómo iniciar el UUCP” en la página 568
Habilitar el UUCP para trabajar con TCP/IP	Edite los archivos <code>/etc/inetd.conf</code> y <code>/etc/uucp/Systems</code> para activar el UUCP para TCP/IP.	“Cómo activar el UUCP para TCP/IP” en la página 569

TABLA 25-1 Mapa de tareas para la administración del UUCP (Continuación)

Tarea	Descripción	Para obtener instrucciones
Solucionar algunos problemas comunes del UUCP	Utilice los pasos de diagnóstico para comprobar si existen módems o ACU con errores.	<a href="#">“Cómo comprobar si existen módems o ACU con errores” en la página 572</a>
	Utilice los pasos de diagnóstico para depurar transmisiones.	<a href="#">“Cómo depurar transmisiones” en la página 572</a>

# Adición de inicios de sesión del UUCP

Para que las solicitudes (uucico) entrantes del UUCP de los equipos remotos se administren correctamente, cada equipo debe tener un inicio de sesión en su sistema.

## ▼ Cómo agregar inicios de sesión del UUCP

Para permitir que un equipo remoto acceda al sistema, es necesario agregar una entrada al archivo `/etc/passwd` de la siguiente manera:

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).
- 2 Edite el archivo `/etc/passwd` y agregue la entrada para identificar el equipo que tiene permiso para acceder al sistema.**

Una entrada típica que puede incluir en el archivo `/etc/passwd` para un equipo remoto que tiene permitido acceder al sistema con una conexión del UUCP sería de la siguiente manera:

```
Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
```

Por convención, el nombre de inicio de sesión de un equipo remoto es el nombre de equipo precedido por la letra en mayúscula U. Tenga en cuenta que el nombre no debe exceder los ocho caracteres. De lo contrario, puede que tenga que truncar o abreviar el nombre.

La entrada anterior muestra que una solicitud de inicio de sesión por Ugobi es respondida por `/usr/lib/uucp/uucico`. El directorio principal es `/var/spool/uucppublic`. La contraseña se obtiene del archivo `/etc/shadow`. Debe coordinar la contraseña y el nombre de inicio de sesión con el administrador del UUCP del equipo remoto. El administrador remoto debe agregar una entrada adecuada, con el nombre de inicio de sesión y la contraseña sin cifrar, en el archivo `Systems` del equipo remoto.

### 3 Coordine el nombre del equipo con los administradores del UUCP de otros sistemas.

De forma similar, debe coordinar el nombre y la contraseña del equipo con los administradores del UUCP de todos los equipos que desea contactar por medio del UUCP.

## Inicio del UUCP

El UUCP incluye cuatro secuencias de comandos de shell que sondean equipos remotos, reprograman transmisiones y borran archivos de registro antiguos y transmisiones incorrectas. Las secuencias de comandos son las siguientes:

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

Estas secuencias de comandos de shell se deben ejecutar con regularidad para garantizar que el UUCP se ejecute sin problemas. El archivo `crontab` para ejecutar las secuencias de comandos se crea automáticamente en `/usr/lib/uucp/uudemon.crontab` como parte del proceso de instalación de Solaris si selecciona la instalación completa. De lo contrario, el archivo se crea al instalar el paquete del UUCP.

También puede ejecutar las secuencias de comandos de shell del UUCP manualmente. El siguiente es el archivo `uudemon.crontab` prototipo que puede personalizar para un equipo determinado:

```
#
#ident "@(#)uudemon.crontab 1.5 97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

---

**Nota** – De manera predeterminada, las operaciones del UUCP están deshabilitadas. Para habilitar el UUCP, edite la programación de tiempo y elimine el comentario de las líneas adecuadas en el archivo `uudemon.crontab`.

---

## ▼ Cómo iniciar el UUCP

Para activar el archivo `uudemon.crontab`, realice los siguientes pasos:

- 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

- 2 **Edite el archivo `/usr/lib/uucp/uudemon.crontab` y cambie las entradas según sea necesario.**

- 3 **Active el archivo `uudemon.crontab` mediante la ejecución de este comando:**

```
crontab < /usr/lib/uucp/uudemon.crontab
```

## Secuencia de comandos de shell `uudemon.poll`

La secuencia de comandos de shell `uudemon.poll` predeterminada lee el archivo `/etc/uucp/Poll` una vez por hora. Si algún equipo en el archivo `Poll` está programado para ser sondeado, un archivo de trabajo (`C.synxxx`) se coloca en el directorio `/var/spool/uucp/nombre de nodo`. *nombre de nodo* representa el nombre de nodo del UUCP del equipo.

La secuencia de comandos de shell está programada para ejecutarse una vez por hora, antes de `uudemon.hour`, para que los archivos de trabajo estén en su lugar cuando se llama a `uudemon.hour`.

## Secuencia de comandos de shell `uudemon.hour`

La secuencia de comandos de shell `uudemon.hour` predeterminada realiza lo siguiente:

- Llama al programa `uusched` para buscar en los directorios de cola de impresión archivos de trabajo (`C.`) que no han sido procesados. La secuencia de comandos programa estos archivos para transferirlos a un equipo remoto.
- Llama al daemon `uuxqt` para buscar en los directorios de cola de impresión archivos ejecutables (`X.`) que se transfirieron a su equipo y no se procesaron cuando se transfirieron.

De manera predeterminada, `uudemon.hour` se ejecuta dos veces por hora. Puede que desee que `uudemon.hour` se ejecute con más frecuencia si espera un elevado porcentaje de fallos de llamadas a equipos remotos.



## Secuencia de comandos de shell `uudemon . admin`

La secuencia de comandos de shell `uudemon . admin` predeterminada realiza lo siguiente:

- Ejecuta el comando `uustat` con las opciones `p` y `q`. La opción `q` informa sobre el estado de archivos de trabajo (C.), archivos de datos (D.) y archivos ejecutables (X.) que están en cola. La opción `p` imprime información de proceso de procesos de red que figuran en los archivos de bloqueo (`/var/spool/locks`).
- Envía información de estado resultante al inicio de sesión administrativo de `uucp` mediante `mail`.

## Secuencia de comandos de shell `uudemon . cleanup`

La secuencia de comandos de shell `uudemon . cleanup` predeterminada realiza lo siguiente:

- Recopila archivos de registro para equipos individuales del directorio `/var/uucp/.Log`, fusiona dichos archivos y coloca los archivos en el directorio `/var/uucp/.Old` con la otra información de registro antigua.
- Elimina archivos de trabajo (C.) de hace siete días o más antiguos, archivos de datos (D.) de hace siete días o más antiguos, y archivos ejecutables (X.) de hace dos días o más antiguos de los archivos de cola de impresión.
- Devuelve correo que no se puede entregar al remitente.
- Envía por correo un resumen de la información sobre el estado que se recopiló durante el día actual al inicio de sesión administrativo del UUCP (`uucp`).

## Ejecución del UUCP mediante TCP/IP

Para ejecutar el UUCP en una red TCP/IP, debe efectuar algunas modificaciones, como se describe en esta sección.

### ▼ Cómo activar el UUCP para TCP/IP

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Edite el archivo `/etc/uucp/Systems` para garantizar que las entradas tengan los siguientes campos:

*System-Name Time TCP Port networkname Standard-Login-Chat*

Una entrada típica sería similar a la siguiente:

```
rochester Any TCP - ur-seneca login: Umachine password: xxx
```

Tenga en cuenta que el campo *networkname* permite especificar de forma explícita el nombre de host del TCP/IP. Esta capacidad es importante para algunos sitios. En el ejemplo anterior, el sitio tiene el nombre de nodo *rochester* del UUCP, que es diferente del nombre de host *ur-seneca* del TCP/IP. Además, un equipo completamente diferente podría ejecutar el UUCP con facilidad y tener el nombre de host *rochester* para el TCP/IP.

El campo Port del archivo *Systems* debe tener la entrada *-*. Esta sintaxis equivale a enumerar la entrada como *uucp*. En casi todas las situaciones, el campo *networkname* es el mismo que el nombre del sistema, y el campo Port es *-*, que indica que se debe utilizar el puerto *uucp* estándar de la base de datos *services*. El daemon *in.uucpd* espera que el equipo remoto envíe su inicio de sesión y contraseña para la autenticación, y, además, el daemon *in.uucpd* los solicita, al igual que los comandos *getty* y *login*.

### 3 Edite el archivo */etc/inet/services* para configurar un puerto para el UUCP:

```
uucp 540/tcp uucpd # uucp daemon
```

No debería tener que cambiar la entrada. Sin embargo, si su equipo ejecuta NIS o NIS+ como servicio de nombres, debe cambiar la entrada */etc/nsswitch.conf* por */etc/services* para comprobar *files* en primer lugar y, a continuación, *nis* o *nisplus*.

### 4 Verifique que el UUCP esté habilitado.

```
# svcs network/uucp
```

El servicio UUCP es administrado por la utilidad de gestión de servicios. Para consultar el estado de este servicio, puede utilizar el comando *svcs*. 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*.

### 5 (Opcional) Si es necesario, habilite el UUCP escribiendo lo siguiente:

```
# inetadm -e network/uucp
```

## Seguridad y mantenimiento del UUCP

Una vez que ha configurado el UUCP, el mantenimiento es sencillo. En esta sección, se explican las tareas del UUCP en curso que se relacionan con la seguridad, el mantenimiento y la resolución de problemas.

## Configuración de la seguridad del UUCP

El archivo */etc/uucp/Permissions* predeterminado proporciona el mayor nivel de seguridad para los enlaces del UUCP. El archivo *Permissions* predeterminado no contiene entradas.

Puede configurar parámetros adicionales para cada uno de los equipos remotos para definir lo siguiente:

- Las maneras en las que el equipo remoto puede recibir archivos de su equipo.
- Los directorios para los cuales el equipo remoto leyó y escribió permisos.
- Los comandos que el equipo remoto puede utilizar para la ejecución remota.

Una entrada `Permissions` típica es de la siguiente manera:

```
MACHINE=datsum LOGNAME=Udatsum VALIDATE=datsum
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

Esta entrada permite que los archivos sean enviados hacia los directorios "comunes" del UUCP y que sean recibidos desde ellos, y no desde cualquier lugar en el sistema. La entrada también genera que el nombre de usuario del UUCP sea validado en el momento del inicio de sesión.

## Mantenimiento regular del UUCP

El UUCP no requiere demasiado mantenimiento. Sin embargo, debe asegurarse de que el archivo `crontab` esté en su lugar, como se describe en la sección [“Cómo iniciar el UUCP” en la página 568](#). Su preocupación debe ser el aumento de la cantidad de archivos de correo y el directorio público.

### Correo electrónico para el UUCP

Todos los mensajes de correo electrónico generados por secuencias de comandos y programas del UUCP son enviados al ID de usuario `uucp`. Si no inicia sesión con frecuencia como ese usuario, es posible que no se dé cuenta de que el correo se está acumulando y está consumiendo espacio en el disco. Para solucionar este problema, cree un alias en `/etc/mail/aliases` y redirija ese correo electrónico a `root` o a usted o a otras personas que sean responsables de mantener el UUCP. Recuerde ejecutar el comando `newaliases` después de modificar el archivo `aliases`.

### Directorio público del UUCP

El directorio `/var/spool/uucppublic` es el único lugar de cada sistema en el cual el UUCP puede copiar archivos de manera predeterminada. Cada usuario tiene permiso para cambiar a `/var/spool/uucppublic` y leer y escribir archivos en el directorio. Sin embargo, el bit de permanencia del directorio está establecido, por lo que el modo del directorio es `01777`. Como consecuencia, los usuarios no pueden eliminar archivos que se han copiado en él y que pertenecen a `uucp`. Sólo usted, como administrador del UUCP que inició sesión como `root` o `uucp`, puede eliminar archivos de este directorio. Para evitar la acumulación sin control de archivos en este directorio, debe asegurarse de eliminar archivos de él periódicamente.

Si este mantenimiento no es conveniente para los usuarios, debe alentarlos a que utilicen `uuto` y `uupick` en lugar de eliminar el bit de permanencia, que está establecido por motivos de seguridad. Consulte la página del comando `man uuto(1C)` para obtener instrucciones sobre cómo utilizar `uuto` y `uupick`. También puede restringir el modo del directorio a un único grupo de personas. Si no desea arriesgarse a que alguien llene su disco, incluso puede denegar el acceso del UUCP a él.

## Resolución de problemas del UUCP

Estos procedimientos describen cómo resolver problemas comunes del UUCP.

### ▼ Cómo comprobar si existen módems o ACU con errores

Puede verificar si los módems u otras ACU no están funcionando correctamente de varias maneras.

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Obtenga recuentos y motivos del error de contacto ejecutando el siguiente comando:

```
# uustat -q
```

#### 3 Llame por una línea en particular e imprima la información de depuración en el intento.

La línea se debe definir como `direct` en el archivo `/etc/uucp/Devices`. Debe agregar un número de teléfono al final de la línea de comandos si la línea está conectada a un marcador automático, o el dispositivo debe estar configurado como `direct`. Tipo:

```
# cu -d -lline
```

*line* es `/dev/cua/a`.

### ▼ Cómo depurar transmisiones

Si no puede ponerse en contacto con un equipo particular, puede comprobar las comunicaciones con ese equipo mediante `Uutry` y `uucp`.

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

## 2 Intente establecer contacto:

```
# /usr/lib/uucp/Uutry -r machine
```

Reemplace *equipo* con el nombre de host del equipo con el cual no puede establecer contacto. Este comando realiza lo siguiente:

- Inicia el daemon de transferencia (uucico) con depuración. Puede obtener más información sobre depuración si usted es root.
- Dirige la salida de depuración a */tmp/equipo*.
- Imprime la salida de depuración en el terminal mediante la ejecución de este comando:

```
# tail -f
```

Presione Control+C para finalizar la salida. Puede copiar la salida de */tmp/equipo* si desea guardar la salida.

## 3 Si Uutry no aísla el problema, intente poner en cola un trabajo:

```
# uucp -r file machine\!/dir/file
```

*archivo*            Utilice el nombre del archivo que desea transferir.

*equipo*            Utilice el nombre del equipo en el que desee copiar.

*/dir/archivo*      Especifique la ubicación del archivo para el otro equipo.

## 4 Use el siguiente comando:

```
# Uutry
```

Si aún no puede resolver el problema, es posible que tenga que llamar a su representante de asistencia técnica local. Guarde la salida de depuración, que puede ayudar a diagnosticar el problema.

---

**Nota** – También puede aumentar o disminuir el nivel de depuración proporcionado por Uutry por medio de la opción *-x n*. *n* indica el nivel de depuración. El nivel de depuración predeterminado para Uutry es 5.

El nivel de depuración 3 proporciona información básica sobre cuándo y cómo se establece la conexión, pero no proporciona mucha información sobre la transmisión. El nivel de depuración 9, sin embargo, proporciona información exhaustiva sobre el proceso de transmisión. Tenga en cuenta que la depuración se produce en ambos extremos de la transmisión. Si tiene previsto utilizar un nivel superior al 5 en un texto moderadamente extenso, póngase en contacto con el administrador de otro sitio y decida cuándo cambiar el nivel.

---

## Comprobación del archivo `/etc/uucp/Systems` del UUCP

Verifique que cuente con información actualizada en el archivo `Systems` si tiene problemas para ponerse en contacto con un equipo determinado. La información que puede estar desactualizada para un equipo es la siguiente:

- Número de teléfono
- ID de inicio de sesión
- Contraseña

## Comprobación de mensajes de error del UUCP

El UUCP tiene dos tipos de mensajes de error: `ASSERT` y `STATUS`.

- Cuando un proceso se cancela, los mensajes de error `ASSERT` se registran en `/var/uucp/.Admin/errors`. Estos mensajes incluyen el nombre de archivo, `sccsid`, el número de línea y el texto. Estos mensajes, por lo general, se generan a partir de problemas del sistema.
- Los mensajes de error `STATUS` se almacenan en el directorio `/var/uucp/.Status`. El directorio contiene un archivo separado para cada uno de los equipos remotos con los cuales su equipo intenta comunicarse. Estos archivos contienen información de estado sobre la comunicación que se intentó establecer y si la comunicación se ha realizado correctamente.

## Comprobación de información básica

Hay varios comandos disponibles para comprobar la información básica de la red:

- Utilice el comando `uuname` para enumerar los equipos con los cuales su equipo se puede poner en contacto.
- Utilice el comando `uulog` para visualizar el contenido de los directorios de registro de hosts particulares.
- Utilice el comando `uucheck -v` para comprobar la presencia de archivos y directorios que son necesarios para `uucp`. Este comando también comprueba el archivo `Permissions` y muestra información sobre los permisos que ha configurado.

## UUCP (referencia)

---

En este capítulo, se proporciona información de referencia para trabajar con el UUCP. Contiene los temas siguientes:

- “Archivo `/etc/uucp/Systems` del UUCP” en la página 575
- “Archivo `/etc/uucp/Devices` del UUCP” en la página 583
- “Archivo `/etc/uucp/Dialers` del UUCP” en la página 589
- “Otros archivos de configuración básica del UUCP” en la página 593
- “Archivo `/etc/uucp/Permissions` del UUCP” en la página 596
- “Archivo `/etc/uucp/Poll` del UUCP” en la página 605
- “Archivo `/etc/uucp/Config` del UUCP” en la página 605
- “Archivo `/etc/uucp/Grades` del UUCP” en la página 605
- “Otros archivos de configuración del UUCP” en la página 608
- “Archivos administrativos del UUCP” en la página 610
- “Mensajes de error del UUCP” en la página 612

### Archivo `/etc/uucp/Systems` del UUCP

El archivo `/etc/uucp/Systems` contiene la información que necesita el daemon `uucico` para establecer un enlace de comunicación a un equipo remoto. `/etc/uucp/Systems` es el primer archivo que necesita editar para configurar el UUCP.

Cada entrada del archivo `Systems` representa un equipo remoto con el cual se comunica el host. Un host determinado puede tener más de una entrada. Las entradas adicionales representan rutas de comunicación alternativas que se prueban en orden secuencial. Además, de manera predeterminada, el UUCP evita que cualquier equipo que no aparece en `/etc/uucp/Systems` inicie sesión en el host.

Al usar el archivo `Sysfiles`, puede definir varios archivos que se utilizarán como archivos `Systems`. Consulte “Archivo `/etc/uucp/Sysfiles` del UUCP” en la página 595 para obtener una descripción de `Sysfiles`.

A continuación, se muestra la sintaxis de una entrada en el archivo Systems:

System-Name    Time    Type    Speed    Phone    Chat Script

Consulte el ejemplo siguiente de una entrada en el archivo Systems.

**EJEMPLO 26-1**    Entrada en /etc/uucp/Systems

Arabian        Any    ACUEC   38400   111222   ogin: Puucp   ssword:beledi

Arabian	Entrada para el campo System-Name. Para obtener más información, consulte <a href="#">“Campo System-Name en el archivo /etc/uucp/Systems” en la página 576.</a>
Any	Entrada para el campo Time. Para obtener más información, consulte <a href="#">“Campo Time en el archivo /etc/uucp/Systems” en la página 577.</a>
ACUEC	Entrada para el campo Type. Para obtener más información, consulte <a href="#">“Campo Type en el archivo /etc/uucp/Systems” en la página 578.</a>
38400	Entrada para el campo Speed. Para obtener más información, consulte <a href="#">“Campo Speed en el archivo /etc/uucp/Systems” en la página 578.</a>
111222	Entrada para el campo Phone. Para obtener más información, consulte <a href="#">“Campo Phone en el archivo /etc/uucp/Systems” en la página 578.</a>
ogin: Puucp   ssword:beledi	Entrada para el campo Chat Script. Para obtener más información, consulte <a href="#">“Campo Chat-Script en el archivo /etc/uucp/Systems” en la página 579.</a>

## Campo System-Name en el archivo /etc/uucp/Systems

Este campo contiene el nombre del nodo del equipo remoto. En redes TCP/IP, este nombre puede ser el nombre de host del equipo o un nombre que se crea específicamente para las comunicaciones del UUCP por medio del archivo /etc/uucp/Sysname. Consulte [“Archivo /etc/uucp/Systems del UUCP” en la página 575.](#) En el [Ejemplo 26-1](#), el campo System-Name contiene una entrada para el host remoto Arabian.



## Campo Time en el archivo /etc/uucp/Systems

Este campo especifica el día de la semana y la hora del día en los que el equipo remoto se puede llamar. El formato del campo Time es el siguiente:

```
daytime[;retry]
```

### Parte *day* del campo Time

La parte *day* puede ser una lista que contiene algunas de las siguientes entradas.

Su Mo Tu We Th Fr Sa

Para días individuales.

Wk

Para cualquier día de la semana.

Any

Para cualquier día.

Never

El host nunca inicia una llamada al equipo remoto. La llamada debe ser iniciada por el equipo remoto. El host funciona en *modo pasivo*.

### Parte *time* del campo Time

El [Ejemplo 26-1](#) muestra Any en el campo Time, lo que indica que el host Arabian se puede llamar en cualquier momento.

La parte *time* debe ser un rango de horas que se especifican en una notación de 24 h, por ejemplo, 0800 - 1230 para el rango de 8:30 a. m. a 12:30 p. m. Si no hay ninguna parte *time* especificada, se asume que cualquier hora del día está permitida para la llamada.

Un rango de horas que abarca 0000 está permitido. Por ejemplo, 0800 - 0600 significa que todas las horas están permitidas, excepto las horas entre 6 a. m. y 8 a. m.

### Parte *retry* del campo Time

El subcampo *retry* permite especificar el tiempo mínimo (en minutos) antes de un reintento, después de un intento fallido. La espera predeterminada es de 60 min. El separador de subcampo es un punto y coma (;). Por ejemplo, Any; 9 se interpreta como que se puede llamar en cualquier momento, pero se debe esperar al menos 9 min antes de volver a intentar después de que se produce un fallo.

Si no especifica una entrada *retry*, se utiliza un algoritmo de interrupción exponencial. Esto significa que el UUCP se inicia con un tiempo de espera predeterminado que aumenta a medida que el número de intentos fallidos aumenta. Por ejemplo, suponga que el tiempo de reintento inicial es de 5 min. Si no se produce ninguna respuesta, el siguiente reintento es 10 min más tarde. El siguiente reintento es 20 min más tarde, y así sucesivamente hasta que se alcanza el

máximo tiempo de reintento de 23 h. Si *retry* se especifica, el valor especificado es siempre el tiempo de reintento. De lo contrario, se utiliza el algoritmo de interrupción.

## Campo Type en el archivo /etc/uucp/Systems

Este campo contiene el tipo de dispositivo que debe utilizarse para establecer el enlace de comunicación al equipo remoto. La palabra clave que se utiliza en este campo se compara con el primer campo de las entradas del archivo `Devices`.

### EJEMPLO 26-2 Palabra clave con el campo Type

Arabian Any ACUEC, g 38400 1112222 ogin: Puucp ssword:beledi

Puede definir el protocolo que se utiliza para ponerse en contacto con el sistema agregando el protocolo en el campo `Type`. El ejemplo anterior muestra la forma de agregar el protocolo `g` en el tipo de dispositivo `ACUEC`. Para obtener más información sobre protocolos, consulte [“Definiciones de protocolo en el archivo /etc/uucp/Devices” en la página 588](#).

## Campo Speed en el archivo /etc/uucp/Systems

Este campo, también conocido como el campo `Class`, especifica la velocidad de transferencia del dispositivo que se utiliza para establecer el enlace de comunicación. El campo de velocidad del UUCP puede contener una letra y una velocidad, como `C1200` o `D1200`, para diferenciar entre las clases de marcadores. Consulte [“Campo Class en el archivo /etc/uucp/Devices” en la página 585](#).

Algunos dispositivos se pueden utilizar a cualquier velocidad, por lo que la palabra clave `Any` se puede utilizar. Este campo debe coincidir con el campo `Class` en la entrada del archivo `Devices` relacionada.

### EJEMPLO 26-3 Entrada en el campo Speed

eagle Any ACU, g D1200 NY3251 ogin: nuucp ssword:Oakgrass

Si no se requiere información para este campo, utilice un guión (-) como marcador de posición para el campo.

## Campo Phone en el archivo /etc/uucp/Systems

Este campo permite especificar el número de teléfono, conocido como *token*, del equipo remoto para marcadores automáticos, conocidos como *selectores de puerto*. El número de teléfono

consta de una abreviatura alfabética opcional y una parte numérica. Si se utiliza una abreviatura, dicha abreviatura debe estar enumerada en el archivo `Dialcodes`.

#### EJEMPLO 26-4 Entrada en el campo Phone

nubian	Any	ACU	2400	<b>NY555-1212</b>	ogin: Puucp ssword:Passuan
eagle	Any	ACU, g	D1200	<b>NY=3251</b>	ogin: nuucp ssword:Oakgrass

En el campo Phone, un signo igual (=) indica a la ACU que espere un tono de marcación secundario antes de marcar el resto de los dígitos. Un guión (-) en la cadena indica a la ACU que pause 4 s antes de marcar el siguiente dígito.

Si su equipo se encuentra conectado a un selector de puerto, puede acceder a otros equipos que están conectados a dicho selector. Las entradas del archivo `Systems` para esos equipos remotos no deben tener un número de teléfono en el campo Phone. En cambio, este campo debe contener el token que se transferirá al conmutador. De esta forma, el selector de puerto sabe el equipo remoto con el que el host se desea comunicar. Por lo general, sólo sabe el nombre del sistema. La entrada del archivo `Devices` relacionada debe indicar \D al final de la entrada para asegurarse de que este campo no sea traducido mediante el archivo `Dialcodes`.

## Campo Chat-Script en el archivo /etc/uucp/Systems

Este campo, también conocido como el campo Login, contiene una cadena de caracteres denominada *chat-script*. La secuencia de comandos de chat contiene los caracteres que los equipos local y remoto se deben pasar entre ellos en la conversación inicial. Las secuencias de comandos de chat tienen el siguiente formato:

*expect send [expect send] ....*

*expect* representa la cadena que el host local espera recibir del host remoto para iniciar la conversación. *send* es la cadena que el host local envía después de que el host local recibe la cadena *expect* del host remoto. Una secuencia de comandos de chat puede tener más de una secuencia *expect-send*.

Una secuencia de comandos de chat básica puede contener lo siguiente:

- Indicador de inicio de sesión que el host local espera recibir del equipo remoto.
- Nombre de inicio de sesión que el host local envía al equipo remoto para iniciar la sesión.
- Indicador de contraseña que el host local espera recibir del equipo remoto.
- Contraseña que el host local envía al equipo remoto.

El campo *expect* puede estar compuesto por subcampos con el siguiente formato:

*expect[-send-expect]...*

El subcampo *-send* se envía si el subcampo *expect* anterior no se lee correctamente. El subcampo *-expect* que sigue al subcampo *-send* es la siguiente cadena esperada.

Por ejemplo, con cadenas `login - login`, el UUCP en el host local espera a `login`. Si el UUCP recibe a `login` del equipo remoto, el UUCP pasa al campo siguiente. Si el UUCP no recibe a `login`, el UUCP envía un retorno de carro y, a continuación, busca a `login` de nuevo. Si el equipo local inicialmente no espera ningún carácter, utilice los caracteres `""`, para la cadena `NULL`, en el campo *expect*. Todos los campos *send* se envían con un retorno de carro agregado, a menos que la cadena *send* termine con `\c`.

El siguiente es un ejemplo de una entrada del archivo `Systems` que utiliza una cadena *expect-send*:

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzyz
```

En este ejemplo, se indica al UUCP en el host local que envíe dos retornos de carro y que espere por `ogin:` (para `Login:`). Si `ogin:` no se recibe, envíe un `BREAK`. Cuando recibe `ogin:`, envíe el nombre de inicio de sesión `Puucpx`. Cuando recibe `ssword:` (para `Password:`), envíe la contraseña `xyzyz`.

En la siguiente tabla, se muestran algunos caracteres de escape útiles.

**TABLA 26-1** Caracteres de escape utilizados en el campo Chat-Script del archivo `Systems`

Carácter de escape	Significado
<code>\b</code>	Envía o espera un carácter de retroceso.
<code>\c</code>	Si se encuentra al final de una cadena, suprime el retorno de carro que normalmente se envía. De lo contrario, se ignora.
<code>\d</code>	Retrasa entre 1 s y 3 s antes de enviar más caracteres.
<code>\E</code>	Inicia la comprobación de eco. A partir de este punto, siempre que se transmite un carácter, el UUCP espera que se reciba el carácter antes de continuar las comprobaciones.
<code>\e</code>	Transmite la comprobación.
<code>\H</code>	Ignora un bloqueo del sistema. Utilice esta opción para módems con devolución de llamada.
<code>\K</code>	Envía un carácter de interrupción.
<code>\M</code>	Activa el indicador <code>CLOCAL</code> .
<code>\m</code>	Desactiva el indicador <code>CLOCAL</code> .
<code>\n</code>	Envía o espera un carácter de línea nueva.
<code>\N</code>	Envía un carácter nulo (ASCII NUL).

**TABLA 26-1** Caracteres de escape utilizados en el campo Chat-Script del archivo Systems  
(Continuación)

Carácter de escape	Significado
\p	Realiza una pausa de 1/4 s a 1/2 s aproximadamente.
\r	Envía o espera un retorno de carro.
\s	Envía o espera un carácter de espacio.
\t	Envía o espera un carácter de tabulación.
EOT	Envía un EOT, seguido de una línea nueva dos veces.
BREAK	Envía un carácter de interrupción.
\ddd	Envía o espera el carácter que está representado por los dígitos octales ( <i>ddd</i> ).

## Habilitación de devolución de llamada por medio de la secuencia de comandos de chat

Algunas empresas configuran servidores de marcación de entrada para administrar llamadas de equipos remotos. Por ejemplo, su compañía puede tener un servidor de marcación de entrada con un módem de devolución de llamada al que los empleados pueden llamar desde sus equipos domésticos. Después de que el servidor de marcación de entrada identifica el equipo remoto, el servidor de llamada entrante desconecta el enlace al equipo remoto y, a continuación, devuelve la llamada al equipo remoto. Luego, el enlace de comunicación se restablece.

Puede facilitar la devolución de llamada mediante la opción \H en la secuencia de comandos de chat del archivo Systems en el lugar donde la devolución de llamada debe producirse. Incluya la opción \H como parte de una cadena expect en el lugar donde se espera que el servidor de marcación de entrada se bloquee.

Por ejemplo, suponga que la secuencia de comandos de chat que llama al servidor de marcación de entrada contiene la siguiente cadena:

```
INITIATED\Hogin:
```

La utilidad de marcación del UUCP en el equipo local espera recibir los caracteres INITIATED del servidor de marcación de entrada. Después de que los caracteres INITIATED se han comparado, la utilidad de marcación borra los caracteres subsiguientes que la utilidad de marcación recibe hasta que el servidor de marcación de entrada se bloquea. La utilidad de marcación local espera hasta recibir la parte siguiente de la cadena expect, los caracteres ogin:, del servidor de marcación de entrada. Cuando recibe a ogin:, la utilidad de marcación continúa a lo largo de la secuencia de comandos de chat.

Una cadena de caracteres no necesita preceder ni seguir directamente a \H, como se muestra en la cadena de ejemplo anterior.

## Control de flujo de hardware en el archivo /etc/uucp/Systems

También puede utilizar la cadena pseudo-send `STTY=value` para definir las características del módem. Por ejemplo, `STTY=crtcts` habilita el control de flujo de hardware. STTY acepta todos los modos de stty. Consulte las páginas del comando man [stty\(1\)](#) y [termio\(7I\)](#) para obtener más información.

En el ejemplo siguiente, se habilita el control de flujo de hardware en una entrada del archivo Systems:

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtcts
```

Esta cadena pseudo-send también se puede utilizar en las entradas del archivo Dialers.

## Configuración de paridad en el archivo /etc/uucp/Systems

En algunas situaciones, tiene que restablecer la paridad porque el sistema al que llama comprueba la paridad del puerto y elimina la línea si es incorrecta. El pareado expect-send "" P\_ZERO establece el bit de orden superior (bit de paridad) en 0. Observe este pareado expect-send en el siguiente ejemplo:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

Los siguientes son pareados de paridad que pueden seguir al pareado expect-send "" P\_ZERO:

```
"" P_EVEN    Establece la paridad en par, que es la predeterminada
```

```
"" P_ODD     Establece la paridad en impar
```

```
"" P_ONE     Establece el bit de paridad en 1
```

Estos pareados de paridad se pueden insertar en cualquier lugar de la secuencia de comandos de chat. Los pareados de paridad se aplican a toda la información de la secuencia de comandos de chat que sigue a "" P\_ZERO, el pareado expect-send. Un pareado de paridad también se puede utilizar en las entradas del archivo Dialers. El ejemplo siguiente incluye el pareado de paridad "" P\_ONE:

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

# Archivo /etc/uucp/Devices del UUCP

El archivo /etc/uucp/Devices contiene información para todos los dispositivos que se pueden utilizar para establecer un enlace a un equipo remoto. Estos dispositivos incluyen ACU (que incluyen módems de alta velocidad), enlaces directos y conexiones de red.

Una entrada en el archivo /etc/uucp/Devices tiene la siguiente sintaxis:

```
Type Line Line2 Class Dialer-Token-Pairs
```

La siguiente es una entrada del archivo Devices para un módem V.32 bis de U.S. Robotics que está agregado al puerto A y que se está ejecutando a 38.400 bps.

```
ACUEC cua/a - 38400 usrv32bis-ec
```

ACUEC           Entrada en el campo Type. Para obtener más información, consulte [“Campo Type en el archivo /etc/uucp/Devices” en la página 583](#).

cua/a           Entrada en el campo Line. Para obtener más información, consulte [“Campo Line en el archivo /etc/uucp/Devices” en la página 585](#).

-               Entrada en el campo Line2. Para obtener más información, consulte [“Campo Line2 del archivo /etc/uucp/Devices” en la página 585](#).

38400           Entrada en el campo Class. Para obtener más información, consulte [“Campo Class en el archivo /etc/uucp/Devices” en la página 585](#).

usrv32bis-ec   Entrada en el campo Dialer-Token-Pairs. Para obtener más información, consulte [“Campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices” en la página 586](#).

Cada campo se describe en la siguiente sección.

## Campo Type en el archivo /etc/uucp/Devices

Este campo describe el tipo de enlace que el dispositivo establece. El campo Type del UUCP puede contener una de las palabras clave que se describen en las secciones a continuación.

### Palabra clave Direct

La palabra clave Direct aparece principalmente en las entradas para las conexiones del comando cu. Esta palabra clave indica que el enlace es un enlace directo a otro equipo o un selector de puerto. Cree una entrada separada para cada línea a la que desea hacer referencia por medio de la opción -l del comando cu.

## Palabra clave ACU

La palabra clave ACU indica que el enlace a un equipo remoto (ya sea mediante cu, UUCP, asppp o Solaris PPP 4.0) se realiza por medio de un módem. Este módem puede conectarse directamente al equipo o indirectamente por medio de un selector de puerto.

## Variable Port Selector

El selector de puerto es una variable que se reemplaza en el campo Type con el nombre de un selector de puerto. Los selectores de puerto son dispositivos que se adjuntan a una red que solicita el nombre de un módem que llama y, a continuación, otorgan acceso. El archivo /etc/uucp/Dialers contiene secuencias de comandos de emisor solamente para los selectores de puerto micom y develcon. Puede agregar sus propias entradas de selector de puerto al archivo Dialers. Consulte “[Archivo /etc/uucp/Dialers del UUCP](#)” en la página 589 para obtener más información.

## Variable System-Name

Esta variable se sustituye por el nombre de un equipo en el campo Type e indica que el enlace es un enlace directo a ese equipo particular. Este esquema de nomenclatura se utiliza para asociar la línea en esta entrada Devices con una entrada en /etc/uucp/Systems para el equipo *System-Name*.

## Campos Type en el archivo Devices y en el archivo Systems

El [Ejemplo 26–5](#) muestra una comparación de los campos de /etc/uucp/Devices y los campos de /etc/uucp/Systems. La palabra clave que se usa en el campo Type del archivo Devices se compara con el tercer campo de las entradas del archivo Systems. En el archivo Devices, el campo Type tiene la entrada ACUEC, que indica una unidad de llamada automática, en esta instancia, un módem V.32 bis. Este valor se compara con el campo Type del archivo Systems, que también contiene la entrada ACUEC. Consulte “[Archivo /etc/uucp/Systems del UUCP](#)” en la página 575 para obtener más información.

**EJEMPLO 26–5** Comparación de los campos Type en el archivo Devices y en el archivo Systems

A continuación se muestra un ejemplo de una entrada en el archivo Devices.

**ACUEC** cua/a - 38400 usrv32bis-ec

A continuación se muestra un ejemplo de una entrada en el archivo Systems.

Arabian Any **ACUEC** 38400 111222 ogin: Puucp ssword:beledi



## Campo Line en el archivo /etc/uucp/Devices

Este campo contiene el nombre del dispositivo de la línea (conocido como puerto) que está asociado con la entrada `Devices`. Si el módem que está asociado con una entrada concreta se adjuntara al dispositivo `/dev/cua/a` (puerto de serie A), el nombre que se introduciría en este campo sería `cua/a`. Un indicador de control de módem opcional, `M`, se puede utilizar en el campo `Line` para indicar que el dispositivo debe abrirse sin esperar a un portador. Por ejemplo:

`cua/a,M`

## Campo Line2 del archivo /etc/uucp/Devices

Este campo es un marcador de posición. Utilice siempre un guión (-) aquí. Los marcadores del tipo 801, que no son compatibles con el sistema operativo Solaris, utilizan el campo `Line2`. Los marcadores que no son del tipo 801, normalmente, no usan esta configuración, pero aún necesitan un guión en este campo.

## Campo Class en el archivo /etc/uucp/Devices

El campo `Class` contiene la velocidad del dispositivo si la palabra clave `ACU` o `Direct` se utiliza en el campo `Type`. Sin embargo, el campo `Class` puede contener una letra y una velocidad, como `C1200` o `D1200`, para diferenciar entre clases de marcadores, como `Centrex` o `Dimension PBX`.

Esta diferenciación es necesaria porque muchas oficinas más grandes pueden tener más de un tipo de red telefónica. Una red podría estar dedicada a atender sólo comunicaciones de oficina internas, mientras que otra red podría manejar las comunicaciones externas. En esta situación, debe distinguir las líneas que se deben utilizar para las comunicaciones internas y las líneas que se deben utilizar para las comunicaciones externas.

La palabra clave que se utiliza en el campo `Class` del archivo `Devices` se compara con el campo `Speed` del archivo `Systems`.

### EJEMPLO 26-6 Campo Class en el archivo Devices

`ACU cua/a - D2400 hayes`

Algunos dispositivos se pueden utilizar a cualquier velocidad, por lo que se puede utilizar la palabra clave `Any` en el campo `Class`. Si `Any` se utiliza, la línea coincide con cualquier velocidad solicitada en el campo `Speed` del archivo `Systems`. Si este campo es `Any` y el campo `Speed` del archivo `Systems` es `Any`, la velocidad predeterminada es 2400 bps.

# Campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices

El campo Dialer-Token-Pairs (DTP) contiene el nombre de un marcador y el token para pasarlo. El campo DTP tiene esta sintaxis:

*dialer token [dialer token]*

La parte *dialer* puede ser el nombre de un módem, un monitor de puerto o `direct` o `uudirect` para un dispositivo de enlace directo. Puede tener cualquier número de pares de marcador y token. Si la parte *dialer* no está presente, se toma de una entrada relacionada en el archivo `Systems`. La parte *token* se puede indicar inmediatamente después de la parte *dialer*.

El último par de marcador y token puede no estar presente, según el marcador asociado. En la mayoría de las situaciones, el último par contiene solamente una parte *dialer*. La parte *token* se recupera del campo `Phone` de la entrada del archivo `Systems` asociada.

Una entrada válida en la parte *dialer* puede estar definida en el archivo `Dialers` o puede ser uno de los tipos de marcador especiales. Estos tipos de marcador especiales se compilan con el software y, por lo tanto, están disponibles sin que haya entradas en el archivo `Dialers`. En la siguiente lista, se muestran los tipos de marcador especiales.

TCP	Red TCP/IP
TLI	Red de interfaz de nivel de transporte (sin STREAMS)
TLIS	Red de interfaz de nivel de transporte (con STREAMS)

Consulte “Definiciones de protocolo en el archivo /etc/uucp/Devices” en la [página 588](#) para obtener más información.

# Estructura del campo Dialer-Token-Pairs en el archivo /etc/uucp/Devices

El campo DTP se puede estructurar de cuatro maneras diferentes, según el dispositivo asociado con la entrada.

Consulte la primera manera en la que el campo DTP se puede estructurar:

**Módems conectados directamente:** si un módem está conectado directamente a un puerto en el equipo, el campo DTP de la entrada del archivo `Devices` tiene solamente un par. Este par sería, normalmente, el nombre del módem. Este nombre se utiliza para comparar la entrada del archivo `Devices` particular con una entrada en el archivo `Dialers`. Por lo tanto, el campo `Dialer` debe coincidir con el primer campo de la entrada de un archivo `Dialers`.

#### EJEMPLO 26-7 Campo Dialers para módems conectados directamente

```
Dialers hayes =, -, "" \\dA\pTE1V1X1Q0S2=255S12=255\r\c
\EATDT\T\r\c CONNECT
```

Tenga en cuenta que sólo la parte dialer (hayes) está presente en el campo DTP de la entrada del archivo Devices. Esto significa que el *token* que se pasará al marcador (en este caso, el número de teléfono) se toma del campo Phone de la entrada de un archivo Systems. (\T está implícito, como se describe en el [Ejemplo 26-9](#)).

Consulte la segunda y la tercera maneras en las que el campo DTP se puede estructurar:

- **Enlace directo:** para un enlace directo a un equipo particular, el campo DTP de la entrada asociada debería contener la palabra clave `direct`. Esta condición es verdadera para ambos tipos de entradas de enlace directo, `Direct` y `System-Name`. Consulte “[Campo Type en el archivo /etc/uucp/Devices](#)” en la [página 583](#).
- **Equipos en el mismo selector de puerto:** si un equipo con el que se desea comunicar se encuentra en el mismo conmutador del selector de puerto que su equipo, su equipo primero debe acceder al conmutador. Luego, el conmutador establece la conexión con el otro equipo. Este tipo de entrada tiene sólo un par. La parte *dialer* se utiliza para comparar la entrada de un archivo Dialers.

#### EJEMPLO 26-8 Campo Dialers del UUCP para equipos en el mismo selector de puerto

```
Dialers develcon , "" "" \pr\ps\c est:\007 \E\D\e \007
```

Tal como se indica, la parte *token* se deja en blanco. Esta designación indica que se recuperará del archivo Systems. La entrada del archivo Systems para este equipo contiene el token en el campo Phone, que se suele reservar para el número de teléfono del equipo. Consulte “[Archivo /etc/uucp/Systems del UUCP](#)” en la [página 575](#) para obtener detalles. Este tipo de DTP contiene un carácter de escape (\D), lo que asegura que el contenido del campo Phone no se interpreta como una entrada válida en el archivo Dialcodes.

Consulte la cuarta manera en la que el campo DTP se puede estructurar:

**Módems conectados al selector de puerto:** si un módem de alta velocidad está conectado a un selector de puerto, su equipo primero debe acceder al conmutador del selector de puerto. El conmutador establece la conexión con el módem. Este tipo de entrada necesita dos pares de marcador y token. La parte *dialer* de cada par (el quinto y el séptimo campos de la entrada) se utiliza para comparar entradas en el archivo Dialers, de la siguiente manera.

#### EJEMPLO 26-9 Campo Dialers del UUCP para módems conectados al selector de puerto

```
develcon "" "" \pr\ps\c est:\007 \E\D\e \007
ventel =&-% t"" \r\p\r\c $ <K\T%\r>\c ONLINE!
```

En el primer par, `devel` con `es` es el marcador y `vent` es el token que se pasa al conmutador Develcon para indicarle qué dispositivo, como un módem Ventel, se debe conectar al equipo. Este token es único para cada selector de puerto, ya que cada conmutador se puede configurar de forma distinta. Después de que el módem Ventel se ha conectado, se accede al segundo par. Ventel es el marcador, y el token se recupera del archivo `Systems`.

Dos caracteres de escape pueden aparecer en un campo DTP:

- `\T`: indica que el campo Phone (*token*) se debe traducir mediante el archivo `/etc/uucp/Dialcodes`. Este carácter de escape se coloca normalmente en el archivo `/etc/uucp/Dialers` para cada secuencia de comandos de emisor que está asociada con un módem, como Hayes y U.S. Robotics. Por lo tanto, la traducción no se produce hasta que se accede a la secuencia de comandos del emisor.
- `\D`: indica que el campo Phone (*token*) no se debe traducir mediante el archivo `/etc/uucp/Dialcodes`. Si no hay ningún carácter de escape especificado al final de una entrada `Devices`, `\D` se asume de manera predeterminada. `\D` también se utiliza en el archivo `/etc/uucp/Dialers` con entradas que están asociadas con conmutadores de red `devel` con y `micom`.

## Definiciones de protocolo en el archivo /etc/uucp/Devices

Puede definir el protocolo para utilizar con cada dispositivo en `/etc/uucp/Devices`. Esta especificación suele ser innecesaria debido a que puede utilizar el valor predeterminado o definir el protocolo con el sistema particular al que está llamando. Consulte “[Archivo /etc/uucp/Systems del UUCP](#)” en la [página 575](#) para obtener detalles. Si no especifica el protocolo, debe utilizar el siguiente formato:

*Type, Protocol [parameters]*

Por ejemplo, puede utilizar `TCP, te` para especificar el protocolo TCP/IP.

En la siguiente tabla, se muestran los protocolos disponibles para el archivo `Devices`.

**TABLA 26-2** Protocolos que se utilizan en `/etc/uucp/Devices`

Protocolo	Descripción
t	Este protocolo se utiliza normalmente para las transmisiones por medio de TCP/IP y otras conexiones fiables. t asume transmisiones libres de errores.
g	Este protocolo es un protocolo nativo del UUCP. g es lento, fiable y bueno para la transmisión por medio de líneas telefónicas ruidosas.

**TABLA 26-2** Protocolos que se utilizan en /etc/uucp/Devices (Continuación)

Protocolo	Descripción
e	Este protocolo asume la transmisión por medio de canales libres de errores que están orientados a los mensajes, en contraposición a los canales orientados a la secuencia de bytes, como TCP/IP.
f	Este protocolo se utiliza para la transmisión por medio de conexiones X.25. f se basa en el control de flujo de la secuencia de datos y está destinado para trabajar mediante enlaces que se pueden (casi) garantizar como libres de errores, específicamente, los enlaces X.25/PAD. Una suma de comprobación se aprueba por medio de un archivo completo solamente. Si un transporte falla, el receptor puede solicitar retransmisión o retransmisiones.

A continuación aparece un ejemplo que muestra una designación de protocolo para una entrada de dispositivo:

```
TCP,te - - Any TCP -
```

En este ejemplo, se indica que, para el dispositivo TCP, debe intentar utilizar el protocolo t. Si el otro extremo de la transmisión lo rechaza, utilice el protocolo e.

Ni e ni t son apropiados para utilizar mediante módems. Incluso si el módem garantiza una transmisión libre de errores, los datos aún se pueden perder entre el módem y la CPU.

## Archivo /etc/uucp/Dialers del UUCP

El archivo /etc/uucp/Dialers contiene instrucciones de marcación para los módems que se utilizan con más frecuencia. Es probable que no sea necesario cambiar ni agregar entradas en este archivo, a menos que planea utilizar un módem no estándar o planea personalizar el entorno del UUCP. No obstante, debe comprender lo que hay en el archivo y cómo se relaciona con los archivos Systems y Devices.

El texto especifica la conversación inicial que debe producirse en una línea antes de que la línea pueda ponerse disponible para la transferencia de datos. Esta conversación, conocida como secuencia de comandos de chat, suele ser una secuencia de cadenas ASCII que se transmite y se espera. Una secuencia de comandos de chat se suele utilizar para marcar un número de teléfono.

Como se muestra en los ejemplos en [“Archivo /etc/uucp/Devices del UUCP” en la página 583](#), el quinto campo en una entrada del archivo Devices es un índice en el archivo Dialers o un tipo de marcador especial, como TCP, TLI o TLI5. El daemon uucico intenta comparar el quinto campo del archivo Devices con el primer campo de cada entrada del archivo Dialers. Además, cada campo Devices impar, a partir de la séptima posición, se utiliza como un índice en el archivo Dialers. Si la comparación tiene éxito, la entrada Dialers se interpreta para realizar la conversación del marcador.

Cada entrada en el archivo `Dialers` tiene la siguiente sintaxis:

```
dialer substitutions expect-send
```

El ejemplo siguiente muestra la entrada de un módem V.32 bis de U.S. Robotics.

#### EJEMPLO 26-10 Entrada en el archivo /etc/uucp/Dialers

```
usrv32bis-e    =, -, ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

`usrv32bis-e`

Entrada en campo `Dialer`. El campo `Dialer` coincide con el quinto campo y con los campos impares adicionales en el archivo `Devices`.

`=, -, ""`

Entrada en el campo `Substitutions`. El campo `Substitutions` es una cadena de traducción. El primero de cada par de caracteres se asigna al segundo carácter del par. Esta asignación se utiliza normalmente para traducir = y - en lo que necesite el marcador para "esperar tono de marcación" y "pausar".

```
dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
```

Entrada en el campo `Expect-Send`. Los campos `Expect-Send` son cadenas de caracteres.

```
\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

Más información sobre el campo `Expect-Send`.

A continuación, se muestran entradas de ejemplo en el archivo `Dialers`, como se distribuyen al instalar el UUCP como parte del programa de instalación de Solaris.

#### EJEMPLO 26-11 Segmentos de /etc/uucp/Dialers

```
penril    =W-P ""    \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

```
ventel    =&-% ""    \r\p\r\c $ <K\T%\r>\c ONLINE!
```

```
vadic     =K-K ""    \005\p *- \005\p- * \005\p- * D\p BER? \E\T\e \r\c LINE
```

```
develcon  ""    ""    \pr\ps\c est:\007
```

```
\E\D\e \n\007 micom  ""    ""    \s\c NAME? \D\r\c GO
```

```
hayes     =, -, ""    \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

```
# Telebit TrailBlazer
```

```
tb1200    =W-, ""    \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
```

```
tb2400    =W-, ""    \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
```

```
tbfast     =W-, ""    \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST
```

```
# USRobotics, Codes, and DSI modems
```

**EJEMPLO 26-11** Segmentos de /etc/uucp/Dialers (Continuación)

```
dsi-ec =,-, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-, "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff

tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

En la siguiente tabla, se muestran los caracteres de escape que se utilizan normalmente en las cadenas de envío del archivo Dialers.

**TABLA 26-3** Caracteres de barra diagonal inversa para /etc/uucp/Dialers

Carácter	Descripción
\b	Envía o espera un carácter de retroceso.
\c	No hay una línea nueva ni un retorno de carro.
\d	Retrasa durante 2 s aproximadamente.
\D	Número de teléfono o token sin traducción de Dialcodes.
\e	Deshabilita la comprobación de eco.
\E	Habilita la comprobación de eco para dispositivos lentos.
\K	Inserta un carácter de interrupción.
\n	Envía una línea nueva.
\nnn	Envía un número octal. En la sección “ <a href="#">Archivo /etc/uucp/Systems del UUCP</a> ” en la página 575, se muestran los caracteres de escape adicionales que se pueden utilizar.
\N	Envía o espera un carácter nulo (ASCII NUL).
\p	Realiza una pausa de 12 s a 14 s aproximadamente.

TABLA 26-3 Caracteres de barra diagonal inversa para /etc/uucp/Dialers (Continuación)

Carácter	Descripción
\r	Regresa.
\s	Envía o espera un carácter de espacio.
\T	Número de teléfono o token con traducción de Dial codes.

Ésta es una entrada penril en el archivo Dialers:

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

En primer lugar, se establece el mecanismo de sustitución para el argumento de número de teléfono, de modo que cualquier = se reemplaza por una W (esperar tono de marcación) y cualquier - se reemplaza por una P (pausar).

El protocolo de enlace indicado por el resto de la línea funciona como se muestra:

- "": no espera nada, lo que significa que se debe continuar con el siguiente paso.
- \d: retrasa 2 s y luego envía un retorno de carro.
- >: espera un >.
- Q\c: envía una Q sin un retorno de carro.
- :: espera un :.
- \d-: retrasa 2 s y envía un - y un retorno de carro.
- >: espera un >.
- s\p9\c: envía una s, pausa y envía un 9 sin ningún retorno de carro.
- )-W\p\r\ds\p9\c-): espera un ). Si ) no se recibe, procesa la cadena entre los caracteres -, como se indica a continuación. Envía una W, pausa, envía un retorno de carro, retrasa, envía una s, pausa, envía un 9 sin un retorno de carro y, a continuación, espera el ).
- y\c: envía una y sin ningún retorno de carro.
- :: espera un :.
- \E\TP – \E habilita la comprobación de eco. A partir de este punto, siempre que se transmite un carácter, el UUCP espera que se reciba el carácter antes de continuar. A continuación, el UUCP envía el número de teléfono. \T significa que se debe tomar el número de teléfono que se pasa como un argumento. \T aplica la traducción de Dial codes y la traducción de la función del módem especificada por el campo 2 de esta entrada. A continuación, \T envía una P y un retorno de carro.
- >: espera un >.
- 9\c: envía un 9 sin una línea nueva.
- OK: espera la cadena OK.



## Habilitación del control de flujo de hardware en el archivo `/etc/uucp/Dialers`

También puede utilizar la cadena pseudo-send `STTY=`*value* para definir las características del módem. Por ejemplo, `STTY=crtscts` permite el control de flujo de hardware saliente. `STTY=crtsexoff` permite el control de flujo de hardware entrante. `STTY=crtscts, crtsexoff` permite el control de flujo de hardware entrante y saliente.

STTY acepta todos los modos de `stty`. Consulte las páginas del comando `man stty(1)` y `termio(7I)`.

En el ejemplo siguiente, se habilitaría el control de flujo de hardware en una entrada `Dialers`:

```
dsi =,-, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

Esta cadena pseudo-send también se puede utilizar en las entradas del archivo `Systems`.

## Configuración de paridad en el archivo `/etc/uucp/Dialers`

En algunas situaciones, tiene que restablecer la paridad porque el sistema al que llama comprueba la paridad del puerto y elimina la línea si es incorrecta. El pareado `expect-send P_ZERO` establece la paridad en cero:

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

Los siguientes son pareados de paridad que pueden seguir al pareado `expect-send`:

```
"" P_EVEN   Establece la paridad en par, que es la predeterminada
"" P_ODD    Establece la paridad en impar
"" P_ONE    Establece la paridad en uno
```

Esta cadena pseudo-send también se puede utilizar en las entradas del archivo `Systems`.

## Otros archivos de configuración básica del UUCP

Puede utilizar archivos de esta sección además de los archivos `Systems`, `Devices` y `Dialers` al realizar la configuración básica del UUCP.

# Archivo /etc/uucp/Dialcodes del UUCP

El archivo /etc/uucp/Dialcodes permite definir abreviaturas de código de marcación que se pueden utilizar en el campo Phone del archivo /etc/uucp/Systems. Puede utilizar el archivo Dialcodes con el fin de proporcionar información adicional sobre un número de teléfono básico utilizado por varios sistemas en el mismo sitio.

Cada entrada tiene la siguiente sintaxis:

Abbreviation	Dial-Sequence
Abbreviation	Este campo proporciona la abreviatura que se utiliza en el campo Phone del archivo Systems.
Dial-Sequence	Este campo proporciona la secuencia de marcación que se pasa al marcador cuando se accede a esa entrada particular del archivo Systems.

Compare los campos de los dos archivos. A continuación, se muestran los campos en el archivo Dialcodes.

**Abbreviation**   Dial-Sequence

A continuación, se muestran los campos en el archivo Systems.

System-Name   Time   Type   Speed   **Phone**   Chat   Script

En la tabla siguiente, se muestra el contenido de ejemplo para los campos de un archivo Dialcodes.

TABLA 26-4   Entradas en el archivo Dialcodes

Abreviatura	Secuencia de marcación
NY	1=212
jt	9+847

En la primera fila, NY es la abreviatura que aparece en el campo Phone del archivo Systems. Por ejemplo, el archivo Systems podría tener la siguiente entrada:

NY5551212

Cuando uucico lee NY en el archivo Systems, uucico busca en el archivo Dialcodes NY y obtiene la secuencia de marcación 1=212. 1=212 es la secuencia de marcación necesaria para cualquier llamada telefónica a Nueva York. Esta secuencia incluye el número 1, un "signo igual" (=) que significa pausar y esperar un tono de marcación secundario, y el código de área 212. uucico envía esta información al marcador y, a continuación, vuelve al archivo Systems para el resto del número de teléfono, 5551212.

La entrada `jt 9=847` - funcionaría con un campo `Phone`, como `jt7867`, en el archivo `Systems`. Cuando `uucico` lee la entrada que contiene `jt7867` en el archivo `Systems`, `uucico` envía la secuencia `9=847-7867` al marcador si el token del par de marcador y token es `\T`.

## Archivo `/etc/uucp/Sysfiles` del UUCP

El archivo `/etc/uucp/Sysfiles` le permite asignar distintos archivos que serán utilizados por `uucp` y `cu` como archivos `Systems`, `Devices` y `Dialers`. Para obtener más información sobre `cu`, consulte la página del comando `man cu(1C)`. Puede utilizar `Sysfiles` para lo siguiente:

- Diferentes archivos `Systems` para que las solicitudes de servicios de inicio de sesión se puedan realizar para direcciones diferentes que los servicios de `uucp`.
- Diferentes archivos `Dialers` para que pueda asignar diferentes protocolos de enlace a `cu` y `uucp`.
- Varios archivos `Systems`, `Dialers` y `Devices`. El archivo `Systems`, en particular, puede volverse grande, lo que hace que el archivo sea más adecuado para dividir en varios archivos más pequeños.

La sintaxis del archivo `Sysfiles` se muestra a continuación:

```
service=w systems=x:x dialers=y:y devices=z:z
```

- `w` Representa `uucico`, `cu` o ambos comandos separados por dos puntos
- `x` Representa uno o más archivos que se utilizarán como el archivo `Systems`, con cada nombre de archivo separado por dos puntos y leído en el orden que se presenta
- `y` Representa uno o más archivos que se utilizarán como el archivo `Dialers`
- `z` Representa uno o más archivos que se utilizarán como el archivo `Devices`

Se asume que cada nombre de archivo está relacionado con el directorio `/etc/uucp`, a menos que se proporcione una ruta de acceso completa.

El siguiente ejemplo, `/etc/uucp/Sysfiles`, define un archivo `Systems` local (`Local_Systems`) además del archivo `/etc/uucp/Systems` estándar:

```
service=uucico:cu systems=Systems :Local_Systems
```

Cuando esta entrada está en `/etc/uucp/Sysfiles`, tanto `uucico` como `cu` primero comprueban en el archivo `/etc/uucp/Systems` estándar. Si el sistema al que se llama no tiene una entrada en ese archivo o si las entradas en el archivo fallan, ambos comandos comprueban `/etc/uucp/Local_Systems`.

Como se especifica en la entrada anterior, `cu` y `uucico` comparten los archivos `Dialers` y `Devices`.

Cuando diferentes archivos `Systems` se definen para servicios de `uucico` y `cu`, su equipo almacena dos listas diferentes de `Systems`. Puede imprimir la lista de `uucico` utilizando el comando `uname` o la lista de `cu` utilizando el comando `uname -C`. El siguiente es otro ejemplo del archivo, que muestra que los archivos alternativos se consultan en primer lugar y los archivos predeterminados se consultan si es necesario:

```
service=uucico systems=Systems.cico:Systems
dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
devices=Devices.cu:Devices
```

## Archivo /etc/uucp/Sysname del UUCP

Cada equipo que utiliza el UUCP debe tener un nombre de identificación, a menudo conocido como el *nombre de nodo*. El nombre de nodo aparece en el archivo `/etc/uucp/Systems` del equipo remoto, junto con la secuencia de comandos de chat y otra información de identificación. Normalmente, el UUCP utiliza el mismo nombre de nodo devuelto por el comando `uname -n`, que también es utilizado por TCP/IP.

Puede especificar un nombre de nodo del UUCP independiente del nombre de host del TCP/IP mediante la creación del archivo `/etc/uucp/Sysname`. El archivo tiene una entrada de una línea que contiene el nombre de nodo del UUCP para el sistema.

## Archivo /etc/uucp/Permissions del UUCP

El archivo `/etc/uucp/Permissions` especifica los permisos que los equipos remotos tienen para el inicio de sesión, el acceso a archivos y la ejecución de comandos. Algunas opciones restringen la capacidad del equipo remoto de solicitar archivos y recibir archivos que el equipo local pone en cola. Hay otra opción disponible que especifica los comandos que un equipo remoto puede ejecutar en el equipo local.

## Entradas de estructuración del UUCP

Cada entrada es una línea lógica, con líneas físicas que terminan con una barra diagonal inversa (`\`) para indicar continuación. Las entradas están compuestas por opciones que están delimitadas por un espacio en blanco. Cada opción es un par de nombre y valor en el siguiente formato:

*nombre=valor*

*Valores* pueden ser listas separadas por dos puntos. No se permiten espacios en blanco dentro de una asignación de opción.

Las líneas de comentario comienzan con un signo de almohadilla (#) y ocupan toda la línea hasta un carácter de línea nueva. Las líneas en blanco se ignoran, incluso dentro de las entradas de varias líneas.

Los tipos de entrada del archivo `Permissions` son los siguientes:

- **LOGNAME:** especifica los permisos que entran en vigor cuando un equipo remoto inicia sesión en su equipo (es decir, llama a su equipo).

---

**Nota** – Cuando un equipo remoto lo llama, su identidad es cuestionable, a menos que el equipo remoto tenga un inicio de sesión único y una contraseña verificable.

---

- **MACHINE:** especifica permisos que entran en vigor cuando su equipo inicia sesión en un equipo remoto (es decir, llama a un equipo remoto).

Las entradas de **LOGNAME** contienen una opción **LOGNAME**. Las entradas de **MACHINE** contienen una opción **MACHINE**. Una entrada puede contener ambas opciones.

## Consideraciones del UUCP

Al utilizar el archivo `Permissions` para restringir el nivel de acceso que se otorga a equipos remotos, es conveniente tener en cuenta las siguientes consideraciones:

- Todos los ID de inicio de sesión utilizados por equipos remotos para iniciar sesión para comunicaciones del UUCP deben aparecer en una y sólo una entrada **LOGNAME**.
- Cualquier sitio que se llama con un nombre que no aparece en una entrada **MACHINE** tiene los permisos o las restricciones predeterminados que se indican a continuación:
  - Se ejecutan solicitudes locales de envío y recepción.
  - El equipo remoto puede enviar archivos al directorio `/var/spool/uucppublic` de su equipo.
  - Los comandos enviados por el equipo remoto para ejecutarse en su equipo deben ser uno de los comandos predeterminados, normalmente, `rmail`.

## Opción **REQUEST** del UUCP

Cuando un equipo remoto llama a su equipo y solicita recibir un archivo, esa solicitud se puede otorgar o rechazar. La opción **REQUEST** especifica si el equipo remoto puede solicitar configurar

transferencias de archivos desde su equipo. La cadena REQUEST=yes especifica que el equipo remoto puede solicitar transferir archivos desde su equipo. La cadena REQUEST=no especifica que el equipo remoto no puede solicitar recibir archivos desde su equipo. REQUEST=no, el valor predeterminado, se usa si la opción REQUEST no se especifica. La opción REQUEST puede aparecer en una entrada LOGNAME para que el equipo remoto lo llame o en una entrada MACHINE para que usted llame al equipo remoto.

## Opción SENDFILES del UUCP

Cuando un equipo remoto llama a su equipo y completa su trabajo, el equipo remoto puede intentar recuperar el trabajo que su equipo ha puesto en cola para él. La opción SENDFILES especifica si su equipo puede enviar el trabajo que está en cola para el equipo remoto.

La cadena SENDFILES=yes especifica que su equipo puede enviar el trabajo que está en cola para el equipo remoto si inició sesión con uno de los nombres de la opción LOGNAME. Esta cadena es *obligatoria* si ha introducido Never en el campo Time de /etc/uucp/Systems. Esta designación configura el equipo local en modo pasivo, pero no está permitido iniciar una llamada a ese equipo remoto particular. Consulte “[Archivo /etc/uucp/Systems del UUCP](#)” en la [página 575](#) para obtener más información.

La cadena SENDFILES=call especifica que los archivos que están en cola en su equipo se envían sólo cuando su equipo llama al equipo remoto. El valor call es el valor predeterminado para la opción SENDFILES. Esta opción sólo es significativa en entradas LOGNAME porque las entradas MACHINE se aplican cuando se envían llamadas a equipos remotos. Si la opción se utiliza con una entrada MACHINE, la opción se ignora.

## Opción MYNAME del UUCP

Esta opción permite designar un nombre de nodo único del UUCP para su equipo, además del nombre de host del TCP/IP, como lo devuelve el comando hostname. Por ejemplo, si asignó sin darse cuenta al host el mismo nombre que el de algún otro sistema, puede establecer la opción MYNAME del archivo Permissions. Suponga que desea que su organización sea conocida como widget. Si todos los módems están conectados a un equipo con el nombre de host gadget, puede tener una entrada en el archivo Permissions de gadget que se lee de la siguiente manera:

```
service=uucico systems=Systems.cico:Systems
dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
devices=Devices.cu:Devices
```

Ahora, el sistema world puede iniciar sesión en el equipo gadget como si estuviera iniciando sesión en widget. Para que el equipo world lo conozca también por el alias widget cuando lo llama, puede tener una entrada que lea de la siguiente manera:

```
MACHINE=world MYNAME=widget
```

También puede utilizar la opción MYNAME para fines de prueba, ya que esta opción permite que su equipo se llame a sí mismo. Sin embargo, debido a que esta opción se podría utilizar para enmascarar la identidad real de un equipo, debe utilizar la opción VALIDATE, como se describe en [“Opción VALIDATE del UUCP” en la página 602](#).

## Opciones READ y WRITE del UUCP

Estas opciones especifican las partes del sistema de archivos que uucico puede leer o escribir. Puede designar las opciones READ y WRITE con las entradas MACHINE o LOGNAME.

El valor predeterminado para las opciones READ y WRITE es el directorio uucppublic, como se muestra en las siguientes cadenas:

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

Las cadenas READ=/ y WRITE=/ especifican permiso para acceder a cualquier archivo al que puede acceder un usuario local con otros permisos.

El valor de estas entradas es una lista separada por dos puntos de nombres de ruta. La opción READ sirve para solicitar archivos y la opción WRITE sirve para depositar archivos. Uno de los valores debe ser el prefijo de cualquier nombre de ruta de acceso completa de un archivo que entra o sale. Para otorgar permiso para depositar archivos en /usr/news así como en el directorio público, utilice los siguientes valores con la opción WRITE:

```
WRITE=/var/spool/uucppublic:/usr/news
```

Si se utilizan las opciones READ y WRITE, se deben especificar todos los nombres de ruta porque los nombres de ruta no se agregan a la lista predeterminada. Por ejemplo, si el nombre de ruta /usr/news fuera la única ruta especificada en una opción WRITE, el permiso para depositar archivos en el directorio público sería denegado.

Preste atención a qué directorios permite que los sistemas remotos lean o escriban. Por ejemplo, el directorio /etc contiene muchos archivos del sistema esenciales. Los usuarios remotos no deben tener permiso para depositar archivos en ese directorio.

## Opciones NOREAD y NOWRITE del UUCP

Las opciones NOREAD y NOWRITE especifican excepciones a las opciones READ y WRITE, o valores predeterminados. La siguiente entrada permite leer cualquier archivo, excepto aquellos archivos en el directorio /etc (y sus subdirectorios). Recuerde que estas opciones son prefijos.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

Esta entrada permite escribir únicamente en el directorio /var/spool/uucppublic predeterminado. La opción NOWRITE funciona de la misma manera que la opción NOREAD. Puede utilizar las opciones NOREAD y NOWRITE en las entradas LOGNAME y MACHINE.

## Opción CALLBACK del UUCP

Puede utilizar la opción CALLBACK en las entradas LOGNAME para especificar que no ocurra ninguna transacción hasta que se devuelva la llamada al sistema que llama. Los motivos para configurar CALLBACK son los siguientes:

- Por motivos de seguridad: si le devuelve la llamada a un equipo, puede estar seguro de que es el equipo correcto.
- Por motivos contables: si realiza grandes transmisiones de datos, puede seleccionar el equipo que se factura para la llamada más larga.

La cadena CALLBACK=yes especifica que el equipo debe devolver la llamada al equipo remoto antes de que pueda ocurrir alguna transferencia de archivos.

El valor predeterminado para la opción CALLBACK es CALLBACK=no. Si define CALLBACK en yes, los permisos que afectan el resto de la conversación deben especificarse en la entrada MACHINE que corresponde al emisor. No especifique estos permisos en LOGNAME ni en la entrada LOGNAME que el equipo remoto puede haber definido para el host.

---

**Nota** – Si dos sitios tienen la opción CALLBACK definida mutuamente, nunca se inicia una conversación.

---

## Opción COMMANDS del UUCP



---

**Precaución** – La opción COMMANDS puede poner en peligro la seguridad del sistema. Utilice esta opción con mucho cuidado.

---



Puede utilizar la opción `COMMANDS` en las entradas `MACHINE` para especificar los comandos que un equipo remoto puede ejecutar en su equipo. El programa `uux` genera solicitudes de ejecución remota y pone en cola las solicitudes que se van a transferir al equipo remoto. Los archivos y comandos se envían al equipo de destino para la ejecución remota, que es una excepción a la regla que las entradas `MACHINE` aplican únicamente cuando su sistema realiza la llamada.

Tenga en cuenta que `COMMANDS` no se utiliza en una entrada `LOGNAME`. La opción `COMMANDS` en las entradas `MACHINE` define permisos de comandos si usted llama al sistema remoto o si el sistema remoto lo llama a usted.

La cadena `COMMANDS=rmail` especifica los comandos predeterminados que un equipo remoto puede ejecutar en su equipo. Si una cadena de comandos se utiliza en una entrada `MACHINE`, los comandos predeterminados se sobrescriben. Por ejemplo, la siguiente entrada sobrescribe la opción `COMMAND` predeterminada para que los equipos que se denominan `owl`, `raven`, `hawk` y `dove` ahora puedan ejecutar `rmail`, `rnews` y `lp` en su equipo.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

Además de los nombres especificados, puede tener nombres de ruta de acceso completa de comandos. Por ejemplo, la siguiente entrada especifica que el comando `rmail` utiliza la ruta de búsqueda predeterminada.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

La ruta de búsqueda predeterminada para el UUCP es `/bin` y `/usr/bin`. Cuando el equipo remoto especifica `rnews` o `/usr/local/rnews` para que el comando se ejecute, `/usr/local/rnews` se ejecuta independientemente de la ruta predeterminada. Del mismo modo, `/usr/local/lp` es el comando `lp` que se ejecuta.

La inclusión del valor `ALL` en la lista significa que se ejecuta cualquier comando de los equipos remotos que se especifican en la entrada. Si utiliza este valor, otorga a los equipos remotos acceso completo a su equipo.




---

**Precaución** – Este valor permite mucho más acceso que el que tienen los usuarios comunes. Debe utilizar este valor sólo cuando ambos equipos están en la misma ubicación, cuando ambos equipos están estrechamente conectados y cuando los usuarios son de confianza.

---

Ésta es la cadena con el valor `ALL` agregado:

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

Esta cadena ilustra dos puntos:

- El valor ALL puede aparecer en cualquier parte de la cadena.
- Los nombres de ruta que se especifican para rnews y lp se utilizan (en lugar de los predeterminados) si el comando solicitado no contiene los nombres de ruta de acceso completa para rnews o lp.

Debe utilizar la opción VALIDATE cada vez que se especifiquen comandos potencialmente peligrosos, como cat y uucp, con la opción COMMANDS. Cualquier comando que lee o escribe archivos es potencialmente peligroso para la seguridad local cuando el comando es ejecutado por el daemon de ejecución remota del UUCP (uuxqt).

## Opción VALIDATE del UUCP

Utilice la opción VALIDATE junto con la opción COMMANDS cada vez que especifique comandos que sean potencialmente peligrosos para la seguridad de su equipo. VALIDATE es simplemente un nivel adicional de seguridad además de la opción COMMANDS, aunque es una manera más segura de abrir el acceso a comandos que ALL.

VALIDATE proporciona un cierto grado de verificación de la identidad del emisor comprobando el nombre de host de un equipo que llama con el nombre de inicio de sesión que utiliza. La siguiente cadena garantiza que si un equipo que no sea widget ni gadget intenta iniciar sesión como Uwidget, la conexión se rechaza.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

La opción VALIDATE requiere que los equipos con privilegios tengan un inicio de sesión y una contraseña únicos para las transacciones del UUCP. Un aspecto importante de esta validación es que el inicio de sesión y la contraseña que están asociados con esta entrada están protegidos. Si un desconocido obtiene esa información, esa opción VALIDATE particular ya no puede considerarse segura.

Considere cuidadosamente a qué equipos remotos otorga inicios de sesión y contraseñas con privilegios para transacciones del UUCP. Proporcionar a un equipo remoto un inicio de sesión y una contraseña especiales con las capacidades de acceso a archivos y ejecución remota es como otorgar a cualquier usuario de dicho equipo un inicio de sesión y una contraseña comunes en su equipo. Por lo tanto, si no puede confiar en algún usuario del equipo remoto, no proporcione a ese equipo un inicio de sesión y una contraseña con privilegios.

La siguiente entrada LOGNAME especifica que si uno de los equipos remotos que afirma ser eagle, owl o hawk inicia sesión en su equipo, debe haber utilizado el inicio de sesión uucpfriend:

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

Si un desconocido obtiene la contraseña y el inicio de sesión uucpfriend, el enmascaramiento es sencillo.

No obstante, ¿en qué se relaciona esta entrada con la opción `COMMANDS`, que aparece sólo en las entradas `MACHINE`? Esta entrada enlaza la entrada `MACHINE` (y la opción `COMMANDS`) a una entrada `LOGNAME` que está asociada con un inicio de sesión con privilegios. Este enlace es necesario porque el daemon de ejecución no se ejecuta mientras el equipo remoto tiene una sesión iniciada. En realidad, el enlace es un proceso asíncrono que no sabe qué equipo envió la solicitud de ejecución. Por lo tanto, la verdadera pregunta es: ¿cómo sabe el equipo de dónde vinieron los archivos de ejecución?

Cada equipo remoto tiene su propio directorio de cola de impresión en el equipo local. Estos directorios de cola de impresión tienen permiso de escritura que se otorga únicamente a programas del UUCP. Los archivos de ejecución del equipo remoto se colocan en el directorio de cola de impresión después de que se transfieren a su equipo. Cuando el daemon uuxqt se ejecuta, puede utilizar el nombre del directorio de cola de impresión para buscar la entrada `MACHINE` en el archivo `Permissions` y obtener la lista `COMMANDS`. O bien si el nombre del equipo no aparece en el archivo `Permissions`, se utiliza la lista predeterminada.

En este ejemplo, se muestra la relación entre las entradas `MACHINE` y `LOGNAME`:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

El valor de la opción `COMMANDS` significa que los usuarios remotos pueden ejecutar `rmail` y `/usr/local/rnews`.

En la primera entrada, debe asumir que cuando desea llamar a uno de los equipos enumerados, en realidad, está llamando a `eagle`, `owl` o `hawk`. Por lo tanto, los archivos que se colocan en uno de los directorios de cola de impresión de `eagle`, `owl` o `hawk` son colocados allí por uno de esos equipos. Si un equipo remoto inicia sesión e indica que es uno de esos tres equipos, los archivos de ejecución también se colocan en el directorio de cola de impresión con privilegios. Por lo tanto, tiene que validar que el equipo tenga el inicio de sesión uucpz con privilegios.

## Entrada `MACHINE` para `OTHER` del UUCP

Es posible que desee especificar diferentes valores de opción para equipos remotos que no están mencionados en entradas `MACHINE` específicas. La necesidad puede surgir cuando muchos equipos llaman al host, y el conjunto de comandos cambia de vez en cuando. El nombre `OTHER` para el nombre de equipo se utiliza para esta entrada, como se muestra en este ejemplo:

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

Todas las demás opciones que están disponibles para la entrada MACHINE también se pueden establecer para los equipos que no están mencionados en otras entradas MACHINE.

## Combinación de entradas MACHINE y LOGNAME para el UUCP

Puede combinar las entradas MACHINE y LOGNAME en una sola entrada cuando las opciones comunes son las mismas. Por ejemplo, los siguientes dos conjuntos de entradas comparten las mismas opciones REQUEST, READ y WRITE:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

y

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Puede fusionar estas entradas, tal como se muestra:

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES=yes \
READ=/ WRITE=/
```

Combinar las entradas MACHINE y LOGNAME hace que el archivo Permissions sea más manejable y eficaz.

## Reenvío del UUCP

Al enviar archivos mediante una serie de equipos, los equipos intermediarios deben tener el comando uucp entre sus opciones COMMANDS. Si escribe el siguiente comando, la operación de reenvío funciona sólo si el equipo willow permite que el equipo oak ejecute el programa uucp.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

El equipo oak también debe permitir que su equipo ejecute el programa uucp. El equipo pine, como el último equipo designado, no tiene que permitir el comando uucp porque el equipo no está realizando ninguna operación de reenvío. Normalmente, los equipos no se configuran de esta manera.

## Archivo /etc/uucp/Poll del UUCP

El archivo /etc/uucp/Poll contiene información para sondear equipos remotos. Cada entrada del archivo Poll contiene el nombre de un equipo remoto para llamar, seguido por un carácter de tabulación o un espacio y, por último, las horas en las que el equipo debe ser llamado. El formato de las entradas en el archivo Poll es el siguiente:

*sys-name hour ...*

Por ejemplo, la entrada **eagle 0 4 8 12 16 20** proporciona sondeo del equipo eagle cada 4 h.

La secuencia de comandos `uudemon.poll` procesa el archivo Poll, pero, en realidad, no realiza el sondeo. La secuencia de comandos solamente configura un archivo de trabajo de sondeo (siempre denominado *C.archivo*) en el directorio de cola de impresión. La secuencia de comandos `uudemon.poll` inicia el programador, y el programador examina todos archivos de trabajo en el directorio de cola de impresión.

## Archivo /etc/uucp/Config del UUCP

El archivo /etc/uucp/Config permite sobrescribir ciertos parámetros manualmente. Cada entrada en el archivo Config tiene este formato:

*parameter=value*

Consulte el archivo Config que se proporciona con el sistema para obtener una lista completa de nombres de parámetros configurables.

La siguiente entrada Config establece el orden del protocolo predeterminado en Gge y cambia los valores predeterminados del protocolo G a 7 ventanas y paquetes de 512 bytes.

`Protocol=G(7,512)ge`

## Archivo /etc/uucp/Grades del UUCP

El archivo /etc/uucp/Grades contiene las definiciones de los niveles de trabajo que se pueden utilizar para poner en cola trabajos en un equipo remoto. Este archivo también contiene los permisos para cada nivel de trabajo. Cada entrada de este archivo representa una definición de un nivel de trabajo definido por el administrador que permite a los usuarios poner en cola trabajos.

Cada entrada en el archivo Grades tiene el siguiente formato:

*User-job-grade System-job-grade Job-size Permit-type ID-list*

Cada entrada contiene campos que están separados por un espacio en blanco. El último campo de la entrada está compuesto por subcampos que también están separados por espacios. Si una entrada ocupa más de una línea física, puede utilizar una barra diagonal inversa para continuar la entrada en la siguiente línea. Las líneas de comentario comienzan con un signo de almohadilla (#) y ocupan toda la línea. Las líneas en blanco siempre se ignoran.

## Campo User-job-grade del UUCP

Este campo contiene un nombre de nivel de trabajo de usuario definido por el administrador de hasta 64 caracteres.

## Campo System-job-grade del UUCP

Este campo contiene un nivel de trabajo de un solo carácter al cual *User-job-grade* está asignado. La lista válida de caracteres es A-Z, a-z, en donde A tiene la prioridad más alta y z la prioridad más baja.

## Relación entre niveles de trabajo de sistemas y usuarios

El nivel de trabajo de usuario se puede enlazar a más de un nivel de trabajo de sistema. Tenga en cuenta que el archivo Grades se busca secuencialmente para encontrar instancias de un nivel de trabajo de usuario. Por lo tanto, cualesquiera instancias de un nivel de trabajo de sistema deben aparecer en cumplimiento con la restricción sobre el máximo tamaño del trabajo.

Si bien no existe ningún número máximo para los niveles de trabajo de usuario, el número máximo de niveles de trabajo de sistema permitido es 52. El motivo es que más de un *User-job-grade* se puede asignar a un *System-job-grade*, pero cada *User-job-grade* debe estar en una línea diferente en el archivo. A continuación le mostramos un ejemplo:

```
mail N Any User Any netnews N Any User Any
```

Si realiza esta configuración en un archivo Grades, estos dos campos *User-job-grade* comparten el mismo *System-job-grade*. Debido a que los permisos para un *Job-grade* están asociados con un *User-job-grade* y no con un *System-job-grade*, dos *User-job-grade* pueden compartir el mismo *System-job-grade* y tener dos conjuntos diferentes de permisos.

## Nivel predeterminado

Puede definir el enlace de un *User-job-grade* predeterminado a un nivel de trabajo de sistema. Debe usar la palabra clave predeterminada como el nivel de trabajo de usuario en el campo *User-job-grade* del archivo Grades y el nivel de trabajo de sistema al que está enlazado. Las

restricciones y los campos de ID deben estar definidos como Any para que cualquier usuario y cualquier tamaño de trabajo se puedan poner en cola en este nivel. A continuación le mostramos un ejemplo:

default a Any User Any

Si no define el nivel de trabajo de usuario predeterminado, se utiliza el nivel predeterminado integrado Z. Debido a que el campo de restricción predeterminado es Any, no se comprueban varias instancias del nivel predeterminado.

## Campo Job-size del UUCP

Este campo especifica el tamaño máximo de trabajo que se puede introducir en la cola. *Job-size* es medido en bytes y puede ser una lista de las opciones que se describen en la siguiente lista.

<i>nnnn</i>	Número entero que especifica el tamaño máximo de trabajo para este nivel de trabajo
<i>n K</i>	Número decimal que representa el número de kilobytes (K es la abreviatura de kilobyte)
<i>n M</i>	Número decimal que representa el número de megabytes (M es la abreviatura de megabyte)
Any	Palabra clave que especifica que no existe un tamaño máximo de trabajo

Aquí se muestran algunos ejemplos:

- 5000 representa 5000 bytes
- 10K representa 10 Kbytes
- 2M representa 2 Mbytes

## Campo Permit-type del UUCP

Este campo contiene una palabra clave que indica cómo interpretar la lista de ID. En la siguiente tabla, se enumeran las palabras clave y sus significados.

TABLA 26-5 Campo Permit-type

Palabra clave	Contenido de la lista de ID
User	Nombres de inicio de sesión de usuarios que están autorizados a utilizar este nivel de trabajo
Non-user	Nombres de inicio de sesión de usuarios que no están autorizados a utilizar este nivel de trabajo

TABLA 26-5 Campo Permit-type (Continuación)

Palabra clave	Contenido de la lista de ID
Group	Nombres de grupos cuyos miembros están autorizados a utilizar este grupo
Non-group	Nombres de grupos cuyos miembros no están autorizados a utilizar este nivel de trabajo

## Campo ID-list del UUCP

Este campo contiene una lista de nombres de inicios de sesión o nombres de grupos a los cuales se va a permitir o rechazar la puesta en cola en este nivel de trabajo. Los nombres de la lista están separados por un espacio en blanco y terminan con un carácter de línea nueva. La palabra clave Any se utiliza para indicar que cualquier usuario puede poner en cola en este nivel de trabajo.

## Otros archivos de configuración del UUCP

En esta sección, se describen tres modificados con menos frecuencia que afectan el uso de las utilidades del UUCP.

### Archivo /etc/uucp/Devconfig del UUCP

El archivo /etc/uucp/Devconfig permite configurar dispositivos por servicio, como uucp o cu. Las entradas de Devconfig definen los módulos STREAMS que se utilizan para un dispositivo concreto. Estas entradas tienen el siguiente formato:

service= x device= y push= z[:z...]

x puede ser cu, uucico o ambos servicios separados por dos puntos. y es el nombre de una red y debe coincidir con una entrada en el archivo Devices. z es reemplazado por los nombres de los módulos STREAMS en el orden en que se van a insertar en la secuencia. Se pueden definir diferentes módulos y dispositivos para servicios cu y uucp.

Las entradas siguientes son para una red STARLAN y se utilizarían con más frecuencia en el archivo:

```
service=cu      device=STARLAN    push=ntty:tirdwr
service=uucico  device=STARLAN    push=ntty:tirdwr
```

Este ejemplo inserta ntty y, a continuación, tirdwr.



## Archivo `/etc/uucp/Limits` del UUCP

El archivo `/etc/uucp/Limits` controla el número máximo de comandos `uucico`, `uuxqt` y `uusched` simultáneos que se ejecutan en las redes del comando `uucp`. En la mayoría de las situaciones, los valores predeterminados son aceptables y no se necesitan cambios. Si desea cambiarlos, sin embargo, utilice cualquier editor de texto.

El formato del archivo `Limits` es el siguiente:

```
service=x max=y:
```

`x` puede ser `uucico`, `uuxqt` o `uusched`, e `y` es el límite que está permitido para ese servicio. Los campos pueden estar en cualquier orden y en minúsculas.

Las entradas siguientes se deben utilizar con más frecuencia en el archivo `Limits`:

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

El ejemplo permite que cinco comandos `uucico`, cinco `uuxqt` y dos `uusched` se ejecuten en el equipo.

## Archivo `remote.unknown` del UUCP

El otro archivo que afecta el uso de las utilidades de comunicación es el archivo `remote.unknown`. Este archivo es un programa binario que se ejecuta cuando un equipo que no se encuentra en ninguno de los archivos `Systems` inicia una conversación. Este programa registra el intento de conversación y elimina la conexión.



**Precaución** – Si cambia los permisos del archivo `remote.unknown` de modo que el archivo no se pueda ejecutar, el sistema acepta las conexiones de cualquier sistema.

---

Este programa se ejecuta cuando un equipo que no está en ninguno de los archivos `Systems` inicia una conversación. El programa registra el intento de conversación, pero no puede establecer una conexión. Si cambia los permisos de este archivo de manera que el archivo no se pueda ejecutar (`chmod 000 remote.unknown`), el sistema acepta cualquier solicitud de conversación. Este cambio no es trivial. Debe tener buenas razones para efectuar el cambio.

# Archivos administrativos del UUCP

Los archivos administrativos del UUCP se describen a continuación. Estos archivos se crean en directorios de cola de impresión para bloquear dispositivos, conservar datos temporales o mantener información acerca de ejecuciones o transferencias remotas.

- *Archivos de datos temporales* (TM): estos archivos de datos son creados por procesos del UUCP en el directorio de cola de impresión `/var/spool/uucp/x` cuando se recibe un archivo de otro equipo. El directorio *x* tiene el mismo nombre que el equipo remoto que envía el archivo. Los nombres de los archivos de datos temporales tienen el siguiente formato:  
  
`TM.pid.ddd`  
  
*pid* es un ID de proceso y *ddd* es un número secuencial de tres dígitos que comienza con 0. Cuando todo el archivo se recibe, el archivo `TM.pid.ddd` se mueve al nombre de ruta especificado en el archivo `C.sysnxxxx` (que se abarca más adelante) que generó la transmisión. Si el procesamiento se termina de modo anormal, el archivo `TM.pid.ddd` puede permanecer en el directorio *x*. Estos archivos deben ser eliminados automáticamente por `uucleanup`.
- *Archivos de bloqueo* (LCK): los archivos de bloqueo se crean en el directorio `/var/spool/locks` para cada dispositivo en uso. Los archivos de bloqueo evitan conversaciones duplicadas y varios intentos de utilizar el mismo dispositivo que llama. En la siguiente tabla, se muestran los distintos tipos de archivos de bloqueo del UUCP.

TABLA 26–6 Archivos de bloqueo del UUCP

Nombre de archivo	Descripción
LCK.sys	<i>sys</i> representa el nombre del equipo que está utilizando el archivo
LCK.dev	<i>dev</i> representa el nombre de un dispositivo que está utilizando el archivo
LCK.LOG	<i>LOG</i> representa un archivo de registro bloqueado del UUCP

Estos archivos pueden permanecer en el directorio de cola de impresión si el enlace de comunicaciones se elimina inesperadamente, como cuando un equipo falla. Un archivo de bloqueo se ignora (se elimina) una vez que el proceso principal ya no está activo. El archivo de bloqueo contiene el ID de proceso del proceso que ha creado el bloqueo.

- *Archivo de trabajo* (C.): los archivos de trabajo se crean en un directorio de cola de impresión cuando el trabajo, como transferencias de archivos o ejecuciones remotas de comandos, se ha puesto en cola para un equipo remoto. Los nombres de archivos de trabajo tienen el siguiente formato:  
  
`C.sysnxxxx`

*sys* es el nombre del equipo remoto, *n* es el carácter ASCII que representa el nivel (la prioridad) del trabajo y *xxxx* es el número de secuencia de trabajo de cuatro dígitos asignado por el UUCP. Los archivos de trabajo contienen la siguiente información:

- Nombre de ruta de acceso completa del archivo que se va a enviar o solicitar.
- Nombre de ruta de acceso completa del destino o el nombre de archivo o usuario.
- Nombre de inicio de sesión del usuario.
- Lista de opciones.
- Nombre de archivos de datos asociados en el directorio de cola de impresión. Si se especificó la opción *uucp -C* o *uuto -p*, se utiliza un nombre ficticio (*D. 0*).
- Bits de modo del archivo de origen.
- El nombre de inicio de sesión del usuario remoto que se notificará cuando termine la transferencia.
- *Archivo de datos (D.)*: los archivos de datos se crean cuando se especifica en la línea de comandos que se copie el archivo de origen en el directorio de cola de impresión. Los nombres de archivos de datos tienen el siguiente formato:  
*D. systmxxxxyyy*: *systm* son los primeros cinco caracteres del nombre del equipo remoto. *xxxx* es un número de secuencia de trabajo de cuatro dígitos asignado por uucp. El número de secuencia de trabajo de cuatro dígitos puede ir seguido de un número posterior. *yyy* se utiliza cuando varios archivos *D.* se crean para un archivo de trabajo (*C.*).
- *X. (archivo ejecutable)*: los archivos ejecutables se crean en el directorio de cola de impresión antes de las ejecuciones remotas de comandos. Los nombres de archivos ejecutables tienen el siguiente formato:

*X. sysnxxxx*

*sys* es el nombre del equipo remoto. *n* es el carácter que representa el nivel (la prioridad) del trabajo. *xxxx* es un número de secuencia de cuatro dígitos asignado por el UUCP. Los archivos ejecutables contienen la siguiente información:

- Nombre de inicio de sesión y nombre de equipo del solicitante.
- Nombres de los archivos que son necesarios para la ejecución.
- Entrada que se utilizará como la entrada estándar para la cadena de comandos.
- Nombre de archivo y equipo para recibir la salida estándar de la ejecución de comandos.
- Cadena de comandos.
- Líneas de opción para solicitudes de estado de retorno.

# Mensajes de error del UUCP

En esta sección, se muestran los mensajes de error que están asociados con el UUCP.

## Mensajes de error ASSERT del UUCP

En la siguiente tabla, se muestran mensajes de error ASSERT.

TABLA 26-7 Mensajes de error ASSERT

Mensaje de error	Descripción o acción
CAN'T OPEN	Falló un comando <code>open()</code> o <code>fopen()</code> .
CAN'T WRITE	Falló un comando <code>write()</code> , <code>fwrite()</code> o <code>fprint()</code> , o un comando similar.
CAN'T READ	Falló un comando <code>read()</code> o <code>fgets()</code> , o un comando similar.
CAN'T CREATE	Falló una llamada <code>creat()</code> .
CAN'T ALLOCATE	Falló una asignación dinámica.
CAN'T LOCK	Falló un intento de realizar un archivo LCK (bloqueo). En algunas situaciones, este error es fatal.
CAN'T STAT	Falló una llamada <code>stat()</code> .
CAN'T CHMOD	Falló una llamada <code>chmod()</code> .
CAN'T LINK	Falló una llamada <code>link()</code> .
CAN'T CHDIR	Falló una llamada <code>chdir()</code> .
CAN'T UNLINK	Falló una llamada <code>unlink()</code> .
WRONG ROLE	Éste es un problema lógico interno.
CAN'T MOVE TO CORRUPTDIR	Falló un intento de mover algunos archivos C. o X. incorrectos al directorio <code>/var/spool/uucp/</code> . Corrupt. Es posible que el directorio no esté o tenga propietarios o modos incorrectos.
CAN'T CLOSE	Falló una llamada <code>close()</code> o <code>fclose()</code> .
FILE EXISTS	Se intenta crear un archivo C. o D., pero el archivo existe. Este error se produce cuando surge un problema con el acceso a archivos de secuencia, lo que, normalmente, indica un error de software.
NO uucp SERVICE NUMBER	Se intenta una llamada TCP/IP, pero no hay ninguna entrada en <code>/etc/services</code> para el UUCP.
BAD UID	El ID de usuario no está en la base de datos de contraseñas. Compruebe la configuración del servicio de nombres.
BAD LOGIN_UID	Igual que la descripción anterior.
BAD LINE	Hay una línea incorrecta en el archivo <code>Devices</code> . No hay suficientes argumentos en una o más líneas.

TABLA 26-7 Mensajes de error ASSERT (Continuación)

Mensaje de error	Descripción o acción
SYSLST OVERFLOW	Desbordó una tabla interna en <code>gename.c</code> . Un solo trabajo intentó comunicarse con más de 30 sistemas.
TOO MANY SAVED C FILES	Igual que la descripción anterior.
RETURN FROM <code>fixline ioctl</code>	Falló un comando <code>ioctl(2)</code> , que nunca debe fallar. Se produjo un problema en el controlador del sistema.
BAD SPEED	Aparece una velocidad de línea incorrecta en el archivo <code>Devices</code> o <code>Systems</code> (campo <code>Class</code> o <code>Speed</code> ).
BAD OPTION	Hay una opción o línea incorrecta en el archivo <code>Permissions</code> . Este error se debe solucionar inmediatamente.
PKCGET READ	El equipo remoto probablemente se colgó. No es necesaria ninguna acción.
PKXSTART	El equipo remoto se interrumpió de una manera no recuperable. Este error, por lo general, se puede ignorar.
TOO MANY LOCKS	Se produjo un problema interno. Póngase en contacto con el proveedor del sistema.
XMV ERROR	Se produjo un problema con algún archivo o directorio. El directorio de cola de impresión es la causa probable, ya que supuestamente se debían comprobar los modos de los destinos antes de intentar realizar este proceso.
CAN'T FORK	Falló un intento de ejecutar un comando <code>fork</code> y <code>exec</code> . El trabajo actual no se debe perder, pero se intentará realizar más tarde ( <code>uuxqt</code> ). No es necesaria ninguna acción.

## Mensajes de error STATUS del UUCP

En la tabla siguiente, se muestra una lista de los mensajes de error STATUS más comunes.

TABLA 26-8 Mensajes STATUS del UUCP

Mensaje de error	Descripción o acción
OK	El estado es aceptable.
NO DEVICES AVAILABLE	Actualmente no hay ningún dispositivo disponible para la llamada. Compruebe si hay un dispositivo válido en el archivo <code>Devices</code> para el sistema concreto. Compruebe el archivo <code>Systems</code> para el dispositivo que se va a utilizar para llamar al sistema.
WRONG TIME TO CALL	Se realizó una llamada al sistema en un horario diferente del especificado en el archivo <code>Systems</code> .
TALKING	Explicativo.
LOGIN FAILED	Falló el inicio de sesión para el equipo en particular. La causa podría ser un inicio de sesión o una contraseña incorrectos, un número equivocado, un equipo lento o un fallo al ejecutar la secuencia de comandos <code>Dialer-Token-Pairs</code> .

TABLA 26–8 Mensajes STATUS del UUCP (Continuación)

Mensaje de error	Descripción o acción
CONVERSATION FAILED	La conversación falló después del inicio con éxito. Normalmente, este error significa que una parte dejó de funcionar, el programa se canceló o la línea (el enlace) se eliminó.
DIAL FAILED	El equipo remoto nunca respondió. La causa puede ser un marcador incorrecto o un número de teléfono incorrecto.
BAD LOGIN/MACHINE COMBINATION	El equipo llamó con un nombre de equipo o inicio de sesión que no concuerda con el archivo <code>Permissions</code> . Este error puede ser un intento de enmascaramiento.
DEVICE LOCKED	El dispositivo que llama que se va a utilizar está actualmente bloqueado y en uso por otro proceso.
ASSERT ERROR	Se produjo un error ASSERT. Consulte el archivo <code>/var/uucp/.Admin/errors</code> para obtener información sobre el mensaje de error y consulte la sección “ <a href="#">Mensajes de error ASSERT del UUCP</a> ” en la página 612.
SYSTEM NOT IN Systems FILE	El sistema no está en el archivo <code>Systems</code> .
CAN'T ACCESS DEVICE	El dispositivo probado no existe o los modos son incorrectos. Compruebe las entradas apropiadas en los archivos <code>Systems</code> y <code>Devices</code> .
DEVICE FAILED	El dispositivo no se puede abrir.
WRONG MACHINE NAME	El equipo que llamó informa un nombre diferente del esperado.
CALLBACK REQUIRED	El equipo que llamó requiere que llame a su equipo.
REMOTE HAS A LCK FILE FOR ME	El equipo remoto tiene un archivo LCK para su equipo. El equipo remoto puede estar intentando llamar a su equipo. Si el equipo remoto tiene una versión más antigua del UUCP, el proceso que se estaba comunicando con su equipo puede haber fallado y puede haber dejado el archivo LCK. Si el equipo remoto tiene la nueva versión del UUCP y no se está comunicando con su equipo, el proceso que tiene un archivo LCK se bloquea.
REMOTE DOES NOT KNOW ME	El equipo remoto no tiene el nombre del nodo de su equipo en el archivo <code>Systems</code> .
REMOTE REJECT AFTER LOGIN	El nombre de inicio de sesión que ha sido utilizado por su equipo para iniciar sesión no concuerda con el que el equipo remoto estaba esperando.
REMOTE REJECT, UNKNOWN MESSAGE	El equipo remoto rechazó la comunicación con su equipo por un motivo desconocido. Es posible que el equipo remoto no esté ejecutando una versión estándar del UUCP.
STARTUP FAILED	El inicio de sesión se completó con éxito, pero el protocolo de enlace inicial falló.
CALLER SCRIPT FAILED	Este error suele ser igual que el error DIAL FAILED. Sin embargo, si este error se produce a menudo, puede deberse a la secuencia de comandos del emisor en el archivo <code>Dialers</code> . Use <code>Uutry</code> para comprobar.

## Mensajes de error numéricos del UUCP

En la siguiente tabla, se muestran los números de código de salida de los mensajes de estado de error producidos por el archivo `/usr/include/sysexits.h`. No todos son utilizados actualmente por uucp.

TABLA 26-9 Mensajes de error por número del UUCP

Número de mensaje	Descripción	Significado
64	Valor de base para mensajes de error	Los mensajes de error comienzan en este valor.
64	Error de uso de línea de comandos	El comando se utilizó de manera incorrecta, por ejemplo, con el número de argumentos incorrecto, un indicador erróneo o una sintaxis incorrecta.
65	Error de formato de datos	Los datos de entrada son incorrectos de alguna forma. Este formato de datos sólo se debe usar para datos del usuario y no para archivos del sistema.
66	No se puede abrir la entrada	Un archivo de entrada, no un archivo del sistema, no existe o no se puede leer. Este problema también puede incluir otros errores, como “Ningún mensaje” para una aplicación de correo.
67	Dirección desconocida	El usuario que se especificó no existe. Este error se puede utilizar para direcciones de correo o inicios de sesión remotos.
68	Nombre de host desconocido	El host no existe. Este error se utiliza en direcciones de correo o solicitudes de red.
69	Servicio no disponible	Un servicio no está disponible. Este error puede ocurrir si un archivo o programa de respaldo no existe. Este mensaje también puede indicar simplemente que algo no funciona y que la causa no se puede identificar actualmente.
70	Error interno de software	Un error interno de software se ha detectado. Este error se debe limitar a errores relacionados con sistemas no operativos, si es posible.
71	Error de sistema	Un error del sistema operativo se ha detectado. Este error se utiliza para ciertas condiciones, como “no es posible bifurcar”, “no es posible crear conducción”. Por ejemplo, este error incluye un retorno <code>getuid</code> de un usuario que no existe en el archivo <code>passwd</code> .
72	Falta archivo crítico del sistema operativo	Un archivo del sistema, como, por ejemplo, <code>/etc/passwd</code> o <code>/var/admin/utmpx</code> , no existe, no se puede abrir o tiene un error, como un error de sintaxis.
73	No es posible crear el archivo de salida	Un archivo de salida especificado por el usuario no se puede crear.
74	Error de entrada o salida	Se produjo un error al realizar la entrada y la salida en algún archivo.
75	Fallo temporal. Se indica al usuario que vuelva a intentar	Fallo temporal que no es realmente un error. En <code>sendmail</code> , esto significa que una aplicación de correo, por ejemplo, no puede establecer una conexión, y la solicitud se debe volver a intentar más tarde.

TABLA 26–9 Mensajes de error por número del UUCP (Continuación)

Número de mensaje	Descripción	Significado
76	Error remoto en protocolo	El sistema remoto devolvió algo que “no era posible” durante un intercambio de protocolo.
77	Permiso denegado	No tiene permiso suficiente para efectuar la operación. Este mensaje no está destinado para problemas del sistema de archivos, que debe usar NOINPUT o CANTCREAT, sino que está destinado para permisos de nivel superior. Por ejemplo, kre utiliza este mensaje para restringir a los estudiantes a los que se puede enviar correos.
78	Error de configuración	El sistema detectó un error en la configuración.
79	No se encuentra la entrada	Entrada no encontrada.
79	Valor máximo mostrado	El valor más alto para mensajes de error.



## P A R T E V I

# Trabajo con sistemas remotos (temas)

En esta sección, se proporcionan instrucciones para administrar un servidor FTP y para acceder a sistemas remotos de un entorno Solaris.



## Trabajo con sistemas remotos (descripción general)

---

En esta sección, se incluye información sobre cómo trabajar con archivos remotos.

- “¿Qué es el servidor FTP?” en la página 619
- “¿Qué es un sistema remoto?” en la página 619
- “Cambios recientes realizados en el servicio de FTP” en la página 620

### ¿Qué es el servidor FTP?

El servidor FTP se basa en wu-ftp. Desarrollado originalmente por la Universidad de Washington en San Luis, wu-ftp se utiliza ampliamente para la distribución de datos masivos por medio de Internet y es el estándar preferido para grandes sitios FTP. Para obtener información sobre las condiciones de licencia, consulte los materiales que se encuentran en `/var/sadm/pkg/SUNWftpu/install/copyright`.

### ¿Qué es un sistema remoto?

Para el objetivo de este capítulo, un *sistema remoto* es una estación de trabajo o un servidor que está conectado al sistema local con cualquier tipo de red física y configurado para la comunicación TCP/IP.

En sistemas que ejecutan una versión de Solaris, la configuración de TCP/IP se establece automáticamente durante el inicio. Para obtener más información, consulte la [Guía de administración del sistema: servicios IP](#).

## Cambios recientes realizados en el servicio de FTP

Las versiones anteriores incluyen varios cambios en el servicio FTP. Por ejemplo, incluye mejoras en el servidor FTP y cambios en los comandos `ftpcount`, `ftpwho` y `ftp`.

Las mejoras realizadas en el servidor FTP mejoran la escalabilidad y el registro de transferencias. Estas opciones se describen en “[Ayuda de configuración para sitios ocupados](#)” en la [página 651](#) y en la página del comando `man ftpaccess(4)`. En específico:

- La función `sendfile()` se usa para las descargas binarias
- El archivo `ftpaccess` admite nuevas funciones
  - `flush-wait` controla el comportamiento al final de una descarga o de un listado de directorios
  - `ipcos` define la clase IP del servicio para el control o la conexión de datos
  - `passive ports` se puede configurar para que el núcleo seleccione el puerto TCP mediante el que se van a recibir las conexiones
  - `quota-info` hace posible la recuperación de la información de cuotas
  - `recvbuf` establece el tamaño de la memoria búfer (de carga) que se debe usar para las transferencias binarias
  - `rhostlookup` habilita o deshabilita la búsqueda del nombre de host remoto
  - `sendbuf` establece el tamaño de la memoria búfer (de descarga) que se debe usar para las transferencias binarias
  - `xferlog` personaliza el formato de la entrada del registro de transferencias
- La opción `-4` hace que el FTP sólo reciba conexiones en un socket IPv4 cuando se ejecuta en modo independiente

Además, `ftpcount` y `ftpwho` ahora son compatibles con la opción `-v`, que muestra información sobre las cuentas de los usuarios y los procesos para las clases de servidor FTP que están definidas en los archivos `ftpaccess` del host virtual. Consulte las páginas del comando `man ftpcount(1)` y `ftpwho(1)` para obtener más información.

El cliente y el servidor FTP ahora son compatibles con Kerberos. Para obtener más información, consulte la página del comando `man ftp(4)` y “[Comandos de usuario de Kerberos](#)” de *Guía de administración del sistema: servicios de seguridad*.

El comando `ftp` se ha cambiado. De manera predeterminada, un cliente FTP de Solaris, conectado a un servidor FTP de Solaris, muestra los dos directorios y los archivos sin formato cuando se emite el comando `ls` al cliente. Si el servidor FTP no se está ejecutando en el sistema operativo Solaris, es posible que los directorios no se muestren. Para que, al conectarse a servidores FTP que no sean Solaris, se obtenga el comportamiento predeterminado de Solaris, será necesario editar el archivo `/etc/default/ftp` en cada cliente Solaris. A fin de realizar el cambio para usuarios individuales, la variable de entorno `FTP_LS_SENDS_NLST` se debe establecer en `yes`. Para obtener más información, consulte la página del comando `man ftp(4)`.

La utilidad de gestión de servicios administra el daemon `ftpd`. 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*.



## Administración del servidor FTP (tareas)

---

En este capítulo, se incluyen las tareas que se describen en la siguiente tabla para configurar y administrar un servidor FTP.

- “Administración del servidor FTP (mapa de tareas)” en la página 624
- “Control del acceso al servidor FTP” en la página 625
- “Configuración de inicios de sesión del servidor FTP” en la página 631
- “Personalización de archivos de mensaje” en la página 634
- “Control del acceso a los archivos en el servidor FTP” en la página 638
- “Control de cargas y descargas en el servidor FTP” en la página 639
- “Hospedaje virtual” en la página 642
- “Inicio del servidor FTP automáticamente” en la página 646
- “Cierre del servidor FTP” en la página 648
- “Depuración del servidor FTP” en la página 649
- “Ayuda de configuración para sitios ocupados” en la página 651

# Administración del servidor FTP (mapa de tareas)

TABLA 28-1 Mapa de tareas: administración del servidor FTP

Tarea	Descripción	Para obtener instrucciones
Configurar el acceso al servidor FTP	Utilice los archivos <code>ftppass</code> , <code>ftpusers</code> y <code>ftphosts</code> en el directorio <code>/etc/ftpd</code> para establecer o restringir el acceso al servidor FTP.	<p>“Cómo establecer límites de inicio de sesión de usuarios” en la página 627</p> <p>“Cómo controlar el número de intentos de inicio de sesión no válidos” en la página 628</p> <p>“Cómo impedir a determinados usuarios el acceso al servidor FTP” en la página 629</p> <p>“Cómo restringir el acceso al servidor FTP predeterminado” en la página 630</p> <p>“Cómo definir clases de servidor FTP” en la página 626</p>
Configurar inicios de sesión del servidor FTP	Establezca cuentas de inicio de sesión para usuarios reales, invitados y anónimos.	<p>“Cómo configurar usuarios reales del FTP” en la página 631</p> <p>“Cómo configurar usuarios invitados del FTP” en la página 632</p> <p>“Cómo configurar usuarios anónimos del FTP” en la página 633</p> <p>“Cómo crear el archivo <code>/etc/shells</code>” en la página 634</p>
Personalizar archivos de mensaje	Edite el archivo <code>/etc/ftpd/ftppass</code> para configurar el servidor FTP para que devuelva al cliente FTP mensajes relacionados con eventos determinados.	<p>“Cómo personalizar archivos de mensaje” en la página 635</p> <p>“Cómo crear mensajes que se van a enviar a los usuarios” en la página 636</p> <p>“Cómo configurar la opción <code>README</code>” en la página 636</p>
Configurar el acceso a los archivos en el servidor FTP	Utilice el archivo <code>/etc/ftpd/ftppass</code> para especificar las clases de usuarios que pueden ejecutar determinados comandos o para descargar y cargar archivos en el servidor FTP.	<p>“Cómo configurar la detección de DA para redes de acceso telefónico” en la página 246</p> <p>“Control de cargas y descargas en el servidor FTP” en la página 639</p>
Habilitar hospedaje virtual completo o limitado	Utilice el archivo <code>/etc/ftpd/ftppass</code> para configurar el servidor FTP para que admita varios dominios en el mismo equipo.	<p>“Cómo permitir el hospedaje virtual limitado” en la página 643</p> <p>“Cómo habilitar el hospedaje virtual completo” en la página 644</p>



TABLA 28-1 Mapa de tareas: administración del servidor FTP (Continuación)

Tarea	Descripción	Para obtener instrucciones
Iniciar el servidor FTP	Cambie las propiedades del servicio para iniciar el servidor FTP en <code>nowait</code> , modo independiente o modo de primer plano.	<p>“Cómo iniciar un servidor FTP mediante SMF” en la página 646</p> <p>“Cómo iniciar un servidor FTP independiente en segundo plano” en la página 647</p> <p>“Cómo iniciar un servidor FTP independiente en primer plano” en la página 647</p>
Cerrar el servidor FTP	Utilice el archivo <code>/etc/ftpd/ftpaccess</code> y ejecute el comando <code>ftpsht</code> para cerrar el servidor FTP.	“Cierre del servidor FTP” en la página 648
Solucionar algunos problemas comunes del servidor FTP	Compruebe <code>syslogd</code> y utilice <code>greeting text</code> y <code>log commands</code> para depurar problemas en el servidor FTP.	<p>“Cómo comprobar <code>syslogd</code> en busca de mensajes del servidor FTP” en la página 649</p> <p>“Cómo utilizar <code>greeting text</code> para verificar <code>ftpaccess</code>” en la página 650</p> <p>“Cómo comprobar los comandos ejecutados por usuarios del FTP” en la página 650</p>

## Control del acceso al servidor FTP

Puede utilizar los siguientes archivos de configuración en el directorio `/etc/ftpd` para controlar el acceso al servidor FTP.

- `ftpusers` se utiliza para enumerar los usuarios que tienen prohibido acceder al servidor FTP.
- `ftphosts` se utiliza para permitir o denegar el inicio de sesión de varios hosts a diversas cuentas en el servidor FTP.
- `ftpaccess` es el archivo de configuración principal del FTP. El servidor FTP sólo lee el archivo `/etc/ftpd/ftpaccess` si se llama con la opción `-a`. Cuando el archivo `ftpaccess` se utiliza, todos los usuarios deben ser miembros de una clase para poder acceder al servidor FTP. Puede especificar muchas directivas `ftpaccess` que se aplican sólo a una clase determinada.

Para obtener más información, consulte `ftpusers(4)`, `ftphosts(4)` y `ftpaccess(4)`.

---

**Nota** – En todos los archivos de configuración del servidor FTP, las líneas que comienzan con signos `#` se tratan como comentarios.

---

## ▼ Cómo definir clases de servidor FTP

Para iniciar sesión en el servidor FTP, los usuarios deben ser miembros de una clase cuando se utiliza el archivo `ftppaccess`. Para agregar la directiva `class` al archivo `ftppaccess`, especifique el nombre de *clase* y la *lista de tipos* de usuarios que tienen permitido el acceso desde un host determinado.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Agregue entradas para usuarios reales, invitados y anónimos al archivo `ftppaccess`.

```
class class typelist addrglob[addrglob...]
```

`class` Palabra clave que se utiliza para definir usuarios de FTP.

`clase` Un nombre definido por la palabra clave `class`. Cada inicio de sesión se compara con una lista de clases definidas. El usuario que inició sesión se considera un miembro de la primera clase coincidente.

`listadetipos` Una lista separada por comas de las palabras clave que coinciden con los tres tipos de usuarios: `anonymous`, `guest` y `real`.

`dircoinc` Un nombre de dominio coincidente o una dirección numérica coincidente. `dircoinc` también puede ser el nombre de un archivo (que comienza con una barra diagonal ['/']), que contiene patrones de direcciones adicionales: `address:netmask` o `address/cidr`.

A continuación, se muestran algunos ejemplos de direcciones coincidentes:

- Dirección numérica IPv4: **10.1.2.3**
- Nombre de dominio coincidente: **\*.provider.com**
- Dirección numérica IPv4 coincidente: **10.1.2.\***
- `address:netmask` numérica IPv4: **10.1.2.0:255.255.255.0**
- Dirección numérica IPv4/CIDR: **10.1.2.0/24**
- Dirección numérica IPv6: **2000::56:789:21ff:fe8f:ba98**
- Dirección numérica IPv6/CIDR: **2000::56:789:21ff:fe8f:ba98/120**

### Ejemplo 28-1 Definición de clases de servidor FTP

```
class local real,guest,anonymous *.provider.com
class remote real,guest,anonymous *
```

El ejemplo anterior define la clase `local` como cualquier usuario del tipo `real`, `guest` o `anonymous` que inicia sesión desde `*.provider.com`. La última línea define a `remote` como cualquier usuario que inicia sesión desde cualquier sitio que no sea `*.provider.com`.

## ▼ Cómo establecer límites de inicio de sesión de usuarios

Puede limitar el número de inicios de sesión simultáneos por los usuarios de una clase específica con las directivas que están definidas en el archivo `ftppaccess`. Cada límite de inicio de sesión contiene el nombre de una clase, una lista de días de semana del estilo del UUCP y un archivo de mensaje para mostrar si el límite se supera.

Para establecer límites de inicio de sesión de usuarios, siga los pasos en el procedimiento siguiente.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Agregue las entradas siguientes al archivo `ftppaccess`:**

<code>limit class n times [message-file]</code>	
<code>limit</code>	Palabra clave que se utiliza para restringir inicios de sesión simultáneos por el número especificado de usuarios de una clase definida a ciertos tiempos de conexión.
<code>clase</code>	Un nombre definido por la palabra clave <code>class</code> . Cada inicio de sesión se compara con una lista de clases definidas. El usuario que inició sesión se considera un miembro de la primera clase coincidente.
<code>n</code>	Número de usuarios.
<code>horas</code>	Día de la semana y hora del día en los que la clase se puede conectar. Use <code>Any</code> para cualquier día.
<code>archivo-mensaje</code>	Archivo de mensaje que se muestra si a un usuario se le niega el acceso.

**Ejemplo 28–2 Configuración de límites de inicio de sesión de usuarios**

```
limit anon 50 Wk0800-1800 /etc/ftpd/ftpmmsg.deny
limit anon 100 Any /etc/ftpd/ftpmmsg.deny
limit guest 100 Any /etc/ftpd/ftpmmsg.deny
```

La primera línea del ejemplo anterior muestra un límite de 50 inicios de sesión simultáneos que están permitidos para los usuarios de la clase `anon` durante las horas laborales de la semana. La segunda línea limita a los usuarios `anon` a 100 inicios de sesión simultáneos fuera de las horas laborales. La última línea muestra un límite de 100 inicios de sesión de `guest` que se permiten en cualquier momento. Para obtener información sobre cómo especificar parámetros de día y hora, consulte [ftppaccess\(4\)](#).

El ejemplo indica, además, que el contenido del archivo `/etc/ftpd/ftpmg.deny` se devuelve cuando se alcanza un límite de inicio de sesión especificado si `ftpmg.deny` existe. Para obtener información sobre cómo utilizar el comando `/usr/sbin/ftpcount` para ver el límite de inicio de sesión y de cantidad de cada clase de usuario que inició sesión en una hora particular, consulte [ftpcount\(1\)](#).

Los usuarios tienen permitido iniciar sesión en el servidor FTP, a menos que se alcance un límite especificado. Los usuarios anónimos inician sesión como el usuario `ftp`. Los usuarios reales inician sesión como ellos mismos y los usuarios invitados inician sesión como usuarios reales con un entorno `chroot` para limitar los privilegios de acceso.

Para obtener información sobre cómo utilizar el comando `/usr/sbin/ftpwho` para comprobar las identidades de los usuarios que iniciaron sesión en el servidor FTP, consulte [ftpwho\(1\)](#).

## ▼ Cómo controlar el número de intentos de inicio de sesión no válidos

Si un inicio de sesión en el servidor FTP falla debido a un problema, como, por ejemplo, si escribe de manera incorrecta la información necesaria, el inicio de sesión, generalmente, se repite. El usuario tiene permitido un número específico de intentos de inicios de sesión consecutivos antes de que un mensaje se registre en el archivo `syslog`. En ese punto, el usuario ya está desconectado. Puede definir un límite de fallos en el número de intentos de inicios de sesión siguiendo los pasos detallados en el procedimiento siguiente.

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue las entradas siguientes al archivo `ftppaccess`.

`loginfails n`

`loginfails` Palabra clave que se utiliza para asignar el número de fallos de inicio de sesión que se permiten antes de que la conexión FTP se termine.

`n` Número de veces que un inicio de sesión puede fallar.

### Ejemplo 28–3 Control del número de intentos de inicio de sesión no válidos

`loginfails 10`

El ejemplo anterior indica que el usuario se desconecta del servidor FTP después de 10 intentos de inicio de sesión fallidos.

## ▼ Cómo impedir a determinados usuarios el acceso al servidor FTP

El archivo `/etc/ftpd/ftpusers` muestra los nombres de usuarios que no tienen permitido iniciar sesión en el servidor FTP. Cuando se intenta un inicio de sesión, el servidor FTP comprueba el archivo `/etc/ftpd/ftpusers` para determinar si al usuario se le debe denegar el acceso. Si el nombre del usuario no se encuentra en ese archivo, el servidor busca en el archivo `/etc/passwd`.

Si el nombre del usuario se encuentra en el archivo `/etc/ftpusers`, se escribe un mensaje `syslogd` que indica que se encontró la coincidencia en un archivo obsoleto. El mensaje también recomienda el uso de `/etc/ftpd/ftpusers` en lugar de `/etc/passwd`.

---

**Nota** – Esta versión ya no admite el archivo `/etc/passwd`. Si el archivo `/etc/passwd` existe cuando el servidor FTP se instala, el archivo se mueve a `/etc/ftpd/ftpusers`.

---

Para obtener más información, consulte [syslogd\(1M\)](#), [in.ftpd\(1M\)](#) y [ftpusers\(4\)](#).

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue entradas al archivo `/etc/ftpd/ftpusers` para los usuarios que no tienen permitido iniciar sesión en el servidor FTP.

#### Ejemplo 28–4 Prohibición del acceso al servidor FTP

```
root
daemon
bin
sys
adm
lp
uccp
nuucp
listen
nobody
noaccess
nobody4
```

El ejemplo anterior muestra las entradas típicas en el archivo `ftpusers`. Los nombres de usuario coinciden con las entradas en `/etc/passwd`. La lista, generalmente, incluye la identidad `root` y otras identidades de aplicación de sistemas y administrativas.

La entrada `root` se incluye en el archivo `ftputers` como una medida de seguridad. La política de seguridad predeterminada es no permitir inicios de sesión remotos para `root`. La política también se sigue para el valor predeterminado que se ha establecido como la entrada `CONSOLE` en el archivo `/etc/default/loginfile`. Consulte [login\(1\)](#).

## ▼ Cómo restringir el acceso al servidor FTP predeterminado

Además de los controles mencionados anteriormente, puede agregar afirmaciones explícitas al archivo `ftpaccess` para restringir el acceso al servidor FTP.

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue las entradas siguientes al archivo `ftpaccess`.

#### a. De manera predeterminada, todos los usuarios tienen permitido el acceso al servidor FTP (no virtual) predeterminado. Para denegar el acceso a usuarios específicos (que no sean `anonymous`), agregue la siguiente entrada:

```
defaultserver deny username [username...]
```

`defaultserver` Palabra clave que se utiliza para identificar el servidor no virtual al cual se puede denegar o permitir el acceso.

`nombre_usuario` Nombre de inicio de sesión de un usuario con acceso restringido a `defaultserver`.

#### b. Para permitir el acceso de usuarios que no se muestran en la línea `deny`, agregue la siguiente línea:

```
defaultserver allow username [username...]
```

#### c. Para impedir el acceso de usuarios anónimos, agregue la entrada:

```
defaultserver private
```

### Ejemplo 28–5 Restricción de acceso al servidor FTP predeterminado

```
defaultserver deny *
defaultserver allow username
```

El ejemplo anterior muestra que el servidor FTP deniega el acceso a todos los usuarios, excepto a los usuarios `anon` y a aquellos usuarios que aparecen en la línea `allow`.

También puede utilizar el archivo `ftphosts` para denegar el acceso a determinadas cuentas de inicio de sesión desde varios hosts. Consulte [ftphosts\(4\)](#) para obtener más información.

## Configuración de inicios de sesión del servidor FTP

Para acceder a un servidor FTP, primero debe iniciar sesión. El servidor FTP admite tres tipos de cuentas de inicio de sesión de usuarios para usuarios *reales*, *invitados* y *anónimos*.

- Los usuarios *reales* tienen cuentas que les permiten establecer sesiones de terminales en los sistemas que ejecutan el servidor FTP. Sujeta a permisos de acceso a archivos y directorios, toda la estructura del disco está visible para los usuarios reales.
- Los usuarios *invitados* también necesitan cuentas para iniciar sesión en el servidor FTP. Cada cuenta de invitado está configurada con un nombre de usuario y una contraseña. Los shells de inicio de sesión que funcionan no se asignan a los invitados para evitar que los usuarios establezcan sesiones de terminales. En el inicio de sesión, el servidor FTP realiza una operación `chroot(2)` para restringir la vista de un invitado de la estructura del disco del servidor.

---

**Nota** – Los shells de inicio de sesión para usuarios reales e invitados deben estar enumerados en el archivo `/etc/shells` para permitir el acceso al servidor FTP.

---

- Los usuarios *anónimos* inician sesión en el servidor FTP usando `ftp` o `anonymous` como nombre de usuario. Por convención, los usuarios anónimos indican una dirección de correo electrónico cuando se les solicita una contraseña.

En el inicio de sesión, el servidor FTP realiza una operación `chroot(2)` que restringe la vista del usuario anónimo de la estructura del disco del servidor. Una única área del archivo es compartida por todos los usuarios anónimos, a diferencia de las áreas separadas que se pueden crear para cada usuario invitado.

Los usuarios reales e invitados inician sesión usando cuentas individuales con contraseñas que sólo una persona conoce. Los usuarios anónimos inician sesión en una cuenta conocida que puede estar disponible para cualquiera. La mayor parte de la distribución de archivos a gran escala se crea usando la cuenta anónima.

### ▼ Cómo configurar usuarios reales del FTP

Para permitir a usuarios reales el acceso al servidor FTP, siga estas instrucciones:

- 1 **Verifique que el usuario tenga una cuenta configurada con un nombre de usuario y una contraseña que se puedan utilizar para establecer una sesión de terminal.**

Para obtener más información, consulte el [Capítulo 4, “Gestión de grupos y cuentas de usuario \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*.

- 2 **Confirme que el usuario real sea un miembro de una clase en el archivo `ftppaccess`.**

Para obtener información sobre las clases de usuario que están definidas en el archivo `ftppaccess`, consulte [“Cómo definir clases de servidor FTP”](#) en la [página 626](#).

- 3 **Verifique que el shell de inicio de sesión del usuario se encuentre en el archivo `/etc/shells`.**

## ▼ **Cómo configurar usuarios invitados del FTP**

La secuencia de comandos `ftpconfig` se utiliza para copiar todos los archivos del sistema necesarios en el directorio principal. Cuando el usuario invitado y el directorio principal del invitado ya existen, la secuencia de comandos `ftpconfig` actualiza el área con los archivos del sistema actuales.

Para obtener más información, consulte [ftpconfig\(1M\)](#).

---

**Nota** – A diferencia del nombre de usuario (`anonymous` o `ftp`) que se define para los usuarios anónimos, los nombres de usuario para invitados del FTP no se fijan. Se puede seleccionar cualquier nombre que funcione como un nombre de usuario real.

---

Para permitir el acceso de un usuario invitado al servidor FTP, realice lo siguiente:

- 1 **Utilice la secuencia de comandos `useradd` para crear una cuenta de usuario invitado con un shell de inicio de sesión de `/bin/true` y un directorio principal de `/dir-root/.dir-principal`.**

Para obtener más información, consulte [useradd\(1M\)](#) y el [Capítulo 4, “Gestión de grupos y cuentas de usuario \(descripción general\)”](#) de *Guía de administración del sistema: administración básica*.

---

**Nota** – En este procedimiento, `/home/guests/.guest1` se utiliza como el nombre del directorio principal para un usuario que se denomina `guest1`.

---

```
# /usr/sbin/useradd -m -c "Guest FTP" -d \  
/home/guests/.guest1 -s /bin/true guest1
```

- 2 **Asigne una contraseña a la cuenta de invitado.**



**3 Agregue una entrada guestuser al archivo ftpaccess.**

```
guestuser guest1
```

---

**Nota** – También puede utilizar la capacidad `guestgroup` en el archivo `ftpaccess` para especificar usuarios invitados. La capacidad `guest - root` en `ftpaccess` elimina la necesidad del `./` en la ruta del directorio principal del usuario invitado.

---

**4 Confirme que el usuario invitado sea miembro de una `class` en el archivo ftpaccess. Consulte [“Cómo definir clases de servidor FTP” en la página 626](#) para obtener más información.****5 Utilice la secuencia de comandos ftpconfig para crear los archivos necesarios en el área chroot.**

```
/usr/sbin/ftpconfig -d /home/guests
```

**6 Confirme que `/bin/true` se encuentre en el archivo `/etc/shells`. Consulte [“Cómo crear el archivo `/etc/shells`” en la página 634](#).****Ejemplo 28–6 Configuración de un servidor FTP invitado**

En este ejemplo, el área del FTP se configura en el directorio `/home/guests`.

```
# /usr/sbin/ftpconfig -d /home/guests
Updating directory /home/guests
```

**▼ Cómo configurar usuarios anónimos del FTP**

La secuencia de comandos `ftpconfig` crea la cuenta de usuario `anonymous` y rellena el directorio principal con los archivos necesarios.

Para obtener más información, consulte [ftpconfig\(1M\)](#).

Para permitir el acceso de un usuario anónimo al servidor FTP, siga estas instrucciones:

**1 Utilice la secuencia de comandos ftpconfig para crear la cuenta de usuario anónimo.**

```
/usr/sbin/ftpconfig anonymous-ftp-directory
```

**2 Confirme que el usuario anónimo esté asignado a una `class` en el archivo ftpaccess.**

Consulte [“Cómo definir clases de servidor FTP” en la página 626](#) para obtener más información.

**Ejemplo 28–7 Configuración de usuarios anónimos del FTP**

En este ejemplo, el área del FTP se configura en el directorio `/home/ftp`.

```
# /usr/sbin/ftpconfig /home/ftp
Creating user ftp
Updating directory /home/ftp
```

## ▼ Cómo crear el archivo `/etc/shells`

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Cree el archivo `/etc/shells`.****3 Edite el archivo `/etc/shells`. Agregue la ruta de acceso completa a cada shell en una sola línea.****Ejemplo 28–8 Creación del archivo `/etc/shells`**

A continuación, se incluye un ejemplo de un archivo `/etc/shells` con un `/bin/true` enumerado para usuarios invitados del FTP:

```
/sbin/sh
/bin/csh
/bin/jsh
/bin/ksh
/bin/remsh
/bin/rksh
/bin/rsh
/bin/sh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/bash
/usr/bin/tcsh
/usr/bin/zsh
/bin/true
```

## Personalización de archivos de mensaje

Puede configurar el servidor FTP para que devuelva al cliente FTP mensajes que están relacionados con eventos específicos. Se puede establecer un mensaje de bienvenida para mostrar cuándo un usuario inicia sesión en el servidor FTP. Otro mensaje puede aparecer cuando el usuario hace un cambio de directorio.

Además de texto sin formato, los archivos de mensaje pueden contener una o más *cookies mágicas*. Una cookie mágica se compone de un % (signo de porcentaje), seguido por un solo carácter. Cuando incrusta una cookie en el texto del mensaje, la información que está asociada con la cookie aparece en la pantalla en el momento en el que el archivo de mensaje se llama.

Por ejemplo, el texto del mensaje puede contener la cookie %L:

```
Welcome to %L!
```

Cuando el mensaje se muestra, la cookie mágica %L se sustituye por el nombre del servidor definido por la instrucción `hostname` en el archivo `ftppass`. Para obtener una lista completa de cookies de mensajes admitidas, consulte [ftppass\(4\)](#).

---

**Nota** – Si el nombre de host no está definido en el archivo `ftppass`, se utiliza el nombre de host predeterminado para el equipo local.

---

## ▼ Cómo personalizar archivos de mensaje

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Edite el archivo de mensaje para incluir cookies mágicas según corresponda.

Consulte [ftppass\(4\)](#) para obtener una lista de las cookies que puede utilizar.

## Ejemplo 28–9 Personalización de archivos de mensaje

A continuación, se muestra un ejemplo de un archivo de mensaje que incluye cookies mágicas:

```
Welcome to %L -- local time is %T.
```

```
You are number %N out of a maximum of %M.  
All transfers are logged.
```

```
If your FTP client crashes or hangs shortly after login  
please try  
using a dash (-) as the first character of your password.  
This will  
turn off the informational messages that may be confusing  
your FTP  
client.
```

```
Please send any comments to %E.
```

## ▼ Cómo crear mensajes que se van a enviar a los usuarios

Una vez que el usuario inicia sesión, los mensajes relacionados con aplicaciones o sistemas se muestran en la pantalla. El archivo `ftppaccess` muestra los eventos que inician instrucciones `message` asociadas.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Agregue las entradas siguientes al archivo `ftppaccess`:

<code>message message-file [when [class ...]]</code>	
<code>message</code>	Palabra clave que se utiliza para especificar el archivo de mensaje que se mostrará cuando un usuario inicie sesión o ejecute el comando para cambiar el directorio de trabajo.
<code>archivo-mensaje</code>	Nombre del archivo de mensaje que se va a mostrar.
<code>cuándo</code>	Parámetro que está establecido como <code>login</code> o <code>cwd=dir</code> . Consulte el ejemplo siguiente.
<code>clase</code>	La especificación <code>class</code> permite que el mensaje se muestre sólo para los miembros de una clase determinada.

### Ejemplo 28–10 Creación de mensajes que se van a enviar a los usuarios

```
message /etc/ftpd/Welcome login anon guest
message .message cwd=*
```

El ejemplo anterior indica que el archivo `/etc/ftpd/Welcome` se muestra al iniciar sesión para los usuarios de la clase `anon` o `guest`. La segunda línea indica que el archivo `.message` en el directorio de trabajo actual se muestra para todos los usuarios.

Los archivos de mensaje se crean en relación con el directorio `chroot` para los usuarios invitados y anónimos.

## ▼ Cómo configurar la opción README

La primera vez que se visita un directorio, los archivos README se pueden enumerar. Para configurar la opción README, agregue las entradas siguientes al archivo `ftppaccess`.

**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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Agregue las entradas siguientes al archivo `ftppaccess`.**

```
readme message-file [when [class...]]
```

**readme** Palabra clave que se utiliza para especificar un archivo de mensaje que se comprobará cuando un usuario inicie sesión o cambie el directorio de trabajo. Si el archivo de mensaje existe, se notifica al usuario y se indica la fecha en la que se modificó el archivo.

**archivo-mensaje** Nombre del archivo de mensaje que se va a comprobar.

**cuándo** Parámetro que está establecido como `login` o `cwd=dir`. Consulte el ejemplo siguiente.

**clase** La especificación `class` permite que el mensaje se muestre sólo para los miembros de una clase determinada.

---

**Nota** – Las palabras clave `greeting` y `banner` también se pueden utilizar para enviar mensajes a los usuarios. Consulte [ftppaccess\(4\)](#).

---

**Ejemplo 28–11 Configuración de la opción README**

```
readme README* login
readme README* cwd=*
```

El ejemplo anterior indica que los archivos que coinciden con `README*` se muestran al inicio de la sesión o cuando un directorio se cambia. A continuación, se muestra un ejemplo de inicio de sesión que se basa en la configuración que se utiliza en ese ejemplo.

```
% ftp earth
Connected to earth.
220 earth FTP server ready.
Name (earth:rimmer): ftp
331 Guest login ok, send your complete e-mail address as password.
Password:
230-
230-Welcome to earth -- local time is Thu Jul 15 16:13:24
1999.
230-
230-You are number 1 out of a maximum of 10.
230-All transfers are logged.
230-
230-If your FTP client crashes or hangs shortly after login
please try
230-using a dash (-) as the first character of your
```

```
password. This will
230-turn off the informational messages that may be
confusing your FTP
230-client.
230-
230-Please send any comments to ftpadmin@earth.
230-
230 Guest login ok, access restrictions apply.
ftp> cd pub
250-Please read the file README
250- it was last modified on Thu Jul 15 16:12:25 1999 - 0
days ago
250 CWD command successful.
ftp> get README /tmp/README
200 PORT command successful.
150 Opening ASCII mode data connection for README (0
bytes).
226 ASCII Transfer complete.
ftp> quit
221 Goodbye.
```

## Control del acceso a los archivos en el servidor FTP

En esta sección, los controles de acceso al servidor FTP complementan los controles estándar de acceso a archivos y directorios disponibles con la versión. Utilice los comandos estándar para restringir quién puede acceder a los archivos o cambiarlos o cargarlos. Consulte [chmod\(1\)](#), [chown\(1\)](#) y [chgrp\(1\)](#).

### ▼ Cómo controlar comandos de acceso a archivos

Para utilizar las capacidades de permiso en `ftppaccess` con el fin de especificar qué tipo de usuario tiene permitido ejecutar qué comandos, realice lo siguiente:

#### 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)” de *Guía de administración del sistema: servicios de seguridad*.

#### 2 Agregue las entradas siguientes al archivo `ftppaccess`:

*command* yes|no *typelist*

*comando* Los comandos `chmod`, `delete`, `overwrite`, `rename` o `umask`.

yes|no Permite o niega a un usuario emitir un comando.

*listadetipos* Una lista separada por comas de cualquiera de las palabras clave `anonymous`, `guest` y `real`.

### Ejemplo 28–12 Control de comandos de acceso a archivos

Los siguientes son ejemplos de permisos que se establecen para funciones de acceso a archivos en el servidor FTP.

```
chmod no anonymous, guest
delete    no anonymous
overwrite no anonymous
rename    no anonymous
umask     no guest, anonymous
```

El ejemplo anterior indica lo siguiente:

- Los usuarios anónimos no tienen permitido eliminar, sobrescribir ni renombrar archivos.
- Los usuarios invitados y anónimos no tienen permitido cambiar modos de acceso ni restablecer el comando umask.

## Control de cargas y descargas en el servidor FTP

Puede controlar las cargas y descargas que se inician hacia el servidor FTP y desde él mediante la definición de permisos en los directorios del servidor. De manera predeterminada, las cargas no se permiten para los usuarios anónimos. Tenga mucho cuidado al permitir cargas anónimas.

### ▼ Cómo controlar las cargas al servidor FTP

Agregue las directivas al archivo `ftppaccess` para especificar permisos de carga y mensajes de error para fallos de cargas.

#### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

#### 2 Agregue las entradas siguientes al archivo `ftppaccess`.

Para permitir a los usuarios cargar archivos, agregue la siguiente entrada:

```
upload [absolute|relative] [class=<classname>]... [-] root-dir \
dirglob yes|no owner group mode [dirs|nodirs] [<d_mode>]
```

```
path-filter typelist mesg allowed-charset {disallowed regexp...}
```

```
upload
```

Palabra clave que se aplica a los usuarios que tienen un directorio principal (el argumento para `chroot()` de `dir-root`. `dir-root` se puede especificar como “\*” para que coincida con cualquier directorio principal.

**absolute|relative**

Parámetro que especifica si las rutas del directorio *dir-root* se interpretan como absolutas o relativas para el directorio *chroot* actual.

**class**

Palabra clave que se utiliza para especificar cualquier número de restricciones *class=<classname>*. Si se especifican restricciones, la cláusula de carga sólo entra en vigor si el usuario actual es un miembro de una de las clases especificadas.

**dir-root**

Directorio root del usuario y el directorio principal para los usuarios anónimos.

**dircoinc**

Un patrón para que coincida con un nombre de directorio. Se puede utilizar un asterisco en cualquier lugar o solo para indicar cualquier directorio.

**yes|no**

Variable que permite o impide cargar al servidor FTP.

**propietario**

Propietario de archivos que se cargan en *dirname*s.

**grupo**

Grupo que está asociado con los archivos que se cargan en *dirname*s.

**modo**

Parámetro que se utiliza para especificar permisos de acceso para los archivos cargados. El modo predeterminado *0440* impide que la cuenta anónima lea los archivos cargados.

**dirs|nodirs**

Palabra clave que permite o impide que los usuarios creen subdirectorios en un directorio que aparece en *dirname*s.

**d\_mode**

Modo opcional que determina los permisos para un directorio recién creado.

**path-filter**

Palabra clave que controla los nombres de los archivos cargados.

**listadetipos**

Una lista separada por comas de cualquiera de las palabras clave *anonymous*, *guest* y *real*.

**mesg**

El archivo de mensaje que se muestra no concuerda con los criterios de *regex*.

**conjuntocar-permitido {regex no permitida...}**

Caracteres alfanuméricos permitidos o no permitidos en nombres de archivo.



**Ejemplo 28–13 Control de cargas al servidor FTP**

```
upload /export/home/ftp /incoming yes ftpadm ftpadmin 0440 nodirs
path-filter anonymous /etc/ftpd/filename.msg ^[-A-Za-z0-9._]*$ ^[.-]
```

El ejemplo anterior indica lo siguiente:

- Las cuentas de usuario del FTP que usan el comando `chroot` para `/export/home/ftp` pueden cargar al directorio `/incoming`. Los archivos cargados son propiedad del usuario `ftpadm` y del grupo `ftpadm`. El modo está establecido en `0440` con la palabra clave `nodirs` para evitar que los usuarios anónimos creen subdirectorios.
- Para los usuarios anónimos, un nombre de archivo es cualquier secuencia de A-Z, a-z, 0-9, . (punto), - (guión) o \_ (subrayado). Los nombres de archivo no pueden iniciar con un . (punto) o - (guión). Si un nombre de archivo no pasa este filtro, el mensaje `/etc/ftpd/filename.msg` se muestra si el administrador del FTP ha creado el archivo de mensaje. Este mensaje es seguido por un mensaje de error del servidor FTP.

La propiedad y los permisos de un directorio en el cual las cargas anónimas están permitidas deben ser estrictamente controlados. El administrador del FTP debe ser el propietario de todos los archivos que se cargan al servidor FTP. Es necesario crear un administrador del FTP cuando los usuarios anónimos tienen permitido cargar archivos. El directorio debe ser propiedad del usuario `ftpadm` y del grupo `ftpadm` con los permisos establecidos en `3773`.

El modo de acceso para los archivos cargados al servidor FTP debe ser `0440`. El modo `0440` evita que la cuenta anónima lea los archivos cargados. Esta restricción evita que el servidor se convierta en un área temporal para la distribución de archivos de terceros.

Para que los archivos cargados estén disponibles para la distribución, el administrador del FTP puede mover los archivos a un directorio público.

## ▼ Cómo controlar descargas al servidor FTP

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Agregue las siguientes entradas al archivo `ftppaccess` para evitar que los usuarios recuperen archivos.

```
noretrieve [absolute|relative] [class=classname]... [-] filename ...
```

`noretrieve` Palabra clave que se utiliza para denegar la recuperación de archivos particulares.

<code>absolute relative</code>	Parámetro que especifica si las rutas del directorio <i>dir-root</i> se interpretan como absolutas o relativas para el directorio <code>chroot</code> actual.
<code>class</code>	Palabra clave que se utiliza para especificar <code>class=&lt;classname&gt;</code> de usuarios a los que se aplican restricciones <code>noretrieve</code> .
<code>nombre_archivo</code>	Nombre del archivo que el usuario no tiene permitido recuperar.

### Ejemplo 28-14 Control de descargas al servidor FTP

```
noretrieve /etc/passwd
```

El ejemplo anterior indica que ningún usuario puede recuperar el archivo `/etc/passwd`.

## Hospedaje virtual

El hospedaje virtual permite al servidor FTP admitir varios dominios en el mismo equipo. Cada host virtual necesita una interfaz lógica y una dirección IP separadas.

El servidor FTP admite dos tipos de hospedaje virtual: *limitado* y *completo*. Con el hospedaje virtual limitado, se utilizan los mismos archivos de configuración para todos los hosts virtuales. Con el hospedaje virtual completo, se pueden utilizar archivos de configuración separados para cada host virtual.

---

**Nota** – De manera predeterminada, los usuarios reales e invitados no tienen permitido iniciar sesión en hosts virtuales. Puede definir las siguientes directivas `ftppass` para sustituir el valor predeterminado.

```
To allow access to specific users:  
virtual address allow username  
To deny access to anonymous users:  
virtual address private username
```

---

Consulte [ftppass\(4\)](#) para obtener más información.

## ▼ Cómo permitir el hospedaje virtual limitado

El hospedaje virtual limitado brinda una compatibilidad parcial para los servidores FTP virtuales. Puede permitir la compatibilidad para hospedajes virtuales limitados especificando el directorio root virtual. Si es necesario, también puede definir los siguientes parámetros para el host virtual en el archivo `ftppaccess`:

- banner
- logfile
- email
- hostname

Todas las directivas en el archivo `ftppaccess` se comparten globalmente en todos los servidores virtuales.

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad.](#)

### 2 Agregue las entradas siguientes al archivo `ftppaccess`.

```
virtual address root|banner|logfile path
virtual address hostname|email string
```

virtual	Palabra clave que se utiliza para habilitar las capacidades del servidor virtual.
dirección	Dirección IP del servidor virtual.
root	El directorio root del servidor virtual.
banner	Archivo de carátula que se muestra cuando se establece una conexión con el servidor virtual.
logfile	Registro de transferencias de archivos que se realizan al servidor virtual y desde él.
ruta	Variable que se usa para especificar la ubicación de directorios y archivos en el servidor virtual.
email	Dirección de correo electrónico que se utiliza en los archivos de mensaje y en el comando HELP.
hostname	Nombre del host que se muestra en el mensaje de saludo o el comando de estado.
cadena	Variable que se utiliza para especificar los parámetros email o hostname.

---

**Nota** – Aunque es posible usar `hostname` como la *dirección* del servidor virtual, se recomienda que utilice la dirección IPv4 en su lugar. El DNS debe estar disponible cuando la conexión del FTP se recibe para que `hostname` se compare. Para un host de IPv6, utilice el nombre de host en lugar de la dirección IPv6.

---

### **Ejemplo 28–15**    Habilitación del hospedaje virtual limitado en el archivo `ftppaccess`

```
virtual 10.1.2.3 root    /var/ftp/virtual/ftp-serv
virtual 10.1.2.3 banner  /var/ftp/virtual/ftp-serv/banner.msg
virtual 10.1.2.3 logfile /var/log/ftp/virtual/ftp-serv/xferlog
```

El ejemplo anterior establece la ubicación del directorio `root`, `banner` y `logfile` en un servidor FTP virtual.

### **Ejemplo 28–16**    Habilitación del hospedaje virtual limitado en la línea de comandos

Se proporciona la secuencia de comandos `ftppaddhost(1M)` con la opción `-l` para configurar hosts virtuales limitados.

En el siguiente ejemplo, `ftppaddhost` se ejecuta con las opciones `-l -b -x` para configurar hospedajes virtuales limitados con una carátula de prueba y el archivo de registro `/var/ftp/virtual/10.1.2.3/xferlog` en un `/var/ftp/virtual/10.1.2.3` root virtual.

```
# ftppaddhost -l -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

## ▼ **Cómo habilitar el hospedaje virtual completo**

El hospedaje virtual completo permite la existencia de archivos de configuración separados para cada dominio virtual. Para habilitar la compatibilidad completa con el hospedaje virtual en el servidor FTP, puede crear o modificar los siguientes archivos de configuración del FTP para dominios concretos:

- `ftppaccess`
- `ftpusers`
- `ftpgroups`
- `ftphosts`
- `ftpconversions`

Para obtener más información, consulte `ftppaccess(4)`, `ftpusers(4)`, `ftpgroups(4)`, `ftphosts(4)` y `ftpconversions(4)`.

---

**Nota** – Si no hay versiones independientes de los archivos de configuración disponibles, se utilizan las versiones maestras de los archivos en el directorio `/etc/ftpd`.

---

**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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

**2 Agregue la entrada siguiente al archivo `/etc/ftpd/ftpservers`.**

*address /config-file-dir*

*dirección* Dirección IP del servidor virtual.

*dir-archivo-config* Directorio que contiene los archivos de configuración que se personalizan para el host virtual.

---

**Nota** – Aunque es posible usar `hostname` como la *dirección* del servidor virtual, se recomienda que utilice la dirección IPv4 en su lugar. El DNS debe estar disponible cuando la conexión del FTP se recibe para que `hostname` se compare. Para un host de IPv6, utilice el nombre de host en lugar de la dirección IPv6.

---

**3 Para crear una versión personalizada de un archivo de configuración del servidor FTP para el host virtual, copie la versión maestra del archivo de `/etc/ftpd` al directorio `/config-file-dir`.**

Para obtener más información, consulte [ftpservers\(4\)](#).

**Ejemplo 28–17** Habilitación del hospedaje virtual completo en el archivo `ftpservers`

```
#
# FTP Server virtual hosting configuration file
#
```

```
10.1.2.3 /net/inet/virtual/somedomain/
10.1.2.4 /net/inet/virtual/anotherdomain/
```

El ejemplo anterior especifica las direcciones IP de dos dominios diferentes en el servidor virtual.

**Ejemplo 28–18** Habilitación del hospedaje virtual completo en la línea de comandos

Se proporciona la secuencia de comandos [ftpaddhost\(1M\)](#) con la opción `-c` para configurar hosts virtuales completos.

En el siguiente ejemplo, `ftppaddhost` se ejecuta con las opciones `-c -b -x` para configurar hospedajes virtuales completos con una carátula de prueba y el archivo de registro `/var/ftp/virtual/10.1.2.3/xferlog` en un `/var/ftp/virtual/10.1.2.3` root virtual.

```
# ftppaddhost -c -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

## Inicio del servidor FTP automáticamente

El servidor FTP se puede iniciar de una de las tres maneras siguientes:

- Como un servidor `nowait` iniciado por `inetd`
- Como un servidor independiente ejecutado en segundo plano
- Como un servidor independiente ejecutado en primer plano desde el archivo `inittab`

Un servidor independiente siempre tiene el tiempo de respuesta más rápido posible y está destinado a grandes servidores que están dedicados a proporcionar servicios de FTP. El servidor independiente proporciona baja latencia de conexión para servidores dedicados porque el sistema autónomo nunca tiene que reiniciarse. El servidor autónomo siempre se está ejecutando, incluso durante las horas no pico, y esperando indefinidamente las conexiones.

### ▼ Cómo iniciar un servidor FTP mediante SMF

De manera predeterminada, el servicio SMF está configurado para iniciar el servidor FTP mediante el modo `nowait`. Si el sitio administra muchas conexiones, el servidor FTP también se puede ejecutar en modo independiente. Consulte la página del comando `man in.ftpd(1M)` para obtener información sobre opciones de líneas de comandos adicionales.

#### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

#### 2 Verifique la propiedad `wait` para el servidor FTP.

La línea que informa `wait=FALSE` indica que el servidor se ha iniciado en el modo `nowait`.

```
# inetadm -l network/ftp
SCOPE      NAME=VALUE
           name="ftp"
           endpoint_type="stream"
           proto="tcp6"
           isrpc=FALSE
           wait=FALSE
           exec="/usr/sbin/in.ftpd -a"
```

```

        user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE

```

### 3 Inicie el servidor FTP.

```
# svcadm enable network/ftp
```

## ▼ Cómo iniciar un servidor FTP independiente en segundo plano

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

### 2 Deshabilite el servidor FTP.

```
# svcadm disable network/ftp
```

### 3 Inicie el servidor FTP independiente.

```
# /usr/sbin/in.ftpd -a -S
```

Agregue la línea a una secuencia de comandos de inicio del servicio FTP. Consulte [“Uso de secuencias de comandos de control de ejecución” de Guía de administración del sistema: administración básica](#) para obtener información sobre la creación de una secuencia de comandos de inicio de sistemas.

## ▼ Cómo iniciar un servidor FTP independiente en primer plano

### 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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Deshabilite el servidor FTP.**

```
# svcadm disable network/ftp
```

**3 Agregue una entrada al archivo `inittab` para iniciar el servicio.**

La nueva entrada en `/etc/inittab` debería parecerse a la siguiente:

```
ftpd:3:respawn:/usr/sbin/in.ftpd -a -s
```

**4 Indique al comando `init` que vuelva a examinar el archivo `/etc/inittab`.**

Este comando debe iniciar el servicio FTP.

```
# init q
```

## Cierre del servidor FTP

El comando `ftpshtut(1M)` cierra el servidor FTP a una hora determinada.

Al ejecutar `ftpshtut`, se genera un archivo a partir de las opciones de la línea de comandos que especifican cuándo se produce el cierre, el punto en el que se rechazan nuevas conexiones y cuándo se eliminan conexiones existentes. Se notifica a los usuarios sobre un cierre del servidor en función de esta información. La ubicación del archivo creado por `ftpshtut` es especificada por la directiva `shutdown` en el archivo `ftpassess`.

### ▼ Cómo cerrar el servidor FTP

Siga los pasos que se indican en este procedimiento para ejecutar `ftpshtut` y para agregar la directiva `shutdown` al archivo `ftpassess`.

**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 \(mapa de tareas\)” de Guía de administración del sistema: servicios de seguridad](#).

**2 Agregue las entradas siguientes al archivo `ftpassess`.**

```
shutdown path
```

`shutdown` Palabra clave que se utiliza para especificar la *ruta* a un archivo que se comprueba regularmente para determinar si el servidor FTP está programado para cerrarse.

*ruta* Ubicación del archivo creado por el comando `ftpshtut`.

**3 Ejecute el comando `ftpshtut`.**

```
ftpshtut [ -V ] [ -l min ] [ -d min ] time [warning-message...]
```



<code>ftpsht</code>	Comando que proporciona un procedimiento para notificar a los usuarios que el servidor FTP se está cerrando.
<code>-V</code>	Opción que se especifica para mostrar información de copyright y versión, y luego terminar.
<code>-l</code>	Indicador que se utiliza para ajustar la hora en la que se deniegan nuevas conexiones al servidor FTP.
<code>-d</code>	Indicador que se utiliza para ajustar la hora en la que se desconectan las conexiones existentes al servidor FTP.
<code>time</code>	Hora de cierre especificada por la palabra <code>now</code> para el cierre inmediato o en uno de los dos formatos (+ <i>número</i> o <i>HHMM</i> ) para un cierre futuro.
<code>[warning-message...]</code>	Cierre de mensaje de notificación.

**4 Utilice el comando `ftprestart` para reiniciar el servidor FTP después de un cierre.**

Para obtener más información, consulte [ftpsht\(1M\)](#), [ftpaccess\(4\)](#) y [ftprestart\(1M\)](#).

## Depuración del servidor FTP

En esta sección, se describen algunas de las formas para depurar problemas con el servidor FTP.

### ▼ Cómo comprobar `syslogd` en busca de mensajes del servidor FTP

El servidor FTP escribe mensajes que son útiles para la depuración en la ubicación especificada para mensajes de daemon en el archivo `/etc/syslog.conf`. Si se produce un problema con el servidor FTP, compruebe primero este archivo en busca de esos mensajes.

Los mensajes del servidor FTP están controlados por el daemon `facility` y la información de nivel. Para enviar mensajes del servidor FTP al archivo `/var/adm/message` y hacer que el archivo `syslogd` relea el archivo de configuración, siga estas instrucciones:

**1 Agregue una entrada como la siguiente al archivo `/etc/syslog.conf`.**

```
daemon.info /var/adm/message
```

**2 Indique a `syslogd` que vuelva a leer la configuración.**

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

Esta acción hace que los mensajes informativos del servidor FTP se escriban en `/var/adm/messages`.

## ▼ Cómo utilizar `greeting text` para verificar `ftppaccess`

Para utilizar la capacidad `greeting text` para comprobar que el archivo `ftppaccess` correcto se esté utilizando, realice lo siguiente:

- 1 **Agregue la siguiente directiva al archivo `ftppaccess`.**

```
greeting text message
```

- 2 **Conéctese al servidor FTP.**

- 3 **Si el mensaje no aparece, realice lo siguiente:**

- a. **Confirme que el archivo `ftppaccess` esté en la ubicación correcta. Utilice el comando `strings(1)` para obtener la ubicación del archivo del binario del servidor FTP.**

```
# strings /usr/sbin/in.ftpd | grep "^/.*ftppaccess"
```

- b. **Compruebe el archivo `ftpservers` para ver si el hospedaje virtual se ha configurado.**

Para obtener más información, consulte `ftppaccess(4)`, `ftpservers(4)`, `strings(1)`, `syslog.conf(4)` y `pgrep(1)`.

## ▼ Cómo comprobar los comandos ejecutados por usuarios del FTP

Para ver qué comandos son ejecutados por usuarios del FTP, utilice la capacidad de registro `log commands` en `ftppaccess`.

- 1 **Agregue la siguiente directiva al archivo `ftppaccess` para registrar comandos individuales por usuarios que están especificados en *listadetipos*.**

```
log commands typelist
```

- 2 **Compruebe los mensajes que se escriben en la ubicación especificada en el archivo `/etc/syslog.conf`.**

## Ayuda de configuración para sitios ocupados

La lista siguiente incluye algunas sugerencias para mejorar el rendimiento en sitios FTP ocupados.

1. Los sitios que normalmente admiten muchas conexiones simultáneas deben ejecutar el servidor FTP en modo independiente. Consulte [“Inicio del servidor FTP automáticamente” en la página 646](#).
2. Utilice `vmstat` y otras utilidades del sistema para supervisar el sistema que hospeda el servidor FTP. Si el sistema se queda con pocos recursos, coloque un límite en el número de conexiones simultáneas. Consulte [“Cómo establecer límites de inicio de sesión de usuarios” en la página 627](#). Para obtener más información sobre la supervisión de sistemas, consulte el [Capítulo 13, “Supervisión del rendimiento del sistema \(tareas\)” de Guía de administración del sistema: Administración avanzada](#).
3. Si impone un límite de conexión, considere el uso de las capacidades `limit-time` y `timeout idle` en el archivo `ftppaccess` para evitar que los usuarios acaparen las conexiones. Si no impone un límite de conexión, especifique la opción `-Q` para `in.ftpd`.
4. Si no necesita registros de inicio y cierre de sesión del FTP en `/var/adm/wtmpx`, especifique la opción `-W` para `in.ftpd`.
5. Para reducir la carga en el sistema que hospeda el servidor FTP, aumente el tamaño de la memoria intermedia de transferencia mediante las capacidades `recvbuf` y `sendbuf` en el archivo `ftppaccess`. Si se seleccionan grandes tamaños de memoria intermedia, es posible que sea necesario aumentar el tiempo de espera de la actividad de los datos mediante la capacidad `timeout data` en el archivo `ftppaccess`.
6. El servidor FTP lee de varias bases de datos, incluidas las bases de datos de hosts, contraseñas, grupos y servicios. Las búsquedas lentas pueden provocar un retraso significativo al iniciar sesión en el servidor FTP. La configuración del origen `files` primero en `nsswitch.conf` minimiza los tiempos de consulta. Para obtener más información, consulte la página del comando `man nsswitch.conf(4)`.
7. De manera predeterminada, el servidor FTP intenta buscar el nombre del host remoto, lo que puede ser lento y provocar un retraso significativo en el inicio de sesión. La capacidad `rhostlookup` en el archivo `ftppaccess` se puede utilizar para detener la consulta. Sin embargo, tenga en cuenta que si el nombre del host remoto no se busca, sólo su dirección IP se compara cuando se utilizan otras capacidades en el archivo `ftppaccess` y cuando se comparan entradas en el archivo `ftphosts`. Además, la dirección IP del host remoto se utilizará en los mensajes y en lugar de la cookie mágica `%R`. Consulte la descripción de la capacidad `rhostlookup` en la página del comando `man ftpaccess(4)` para obtener más información.

8. Recuperar información de cuotas también puede provocar una demora importante al iniciar sesión en el servidor FTP, por lo que sólo debe utilizar la capacidad `quota - info` en el archivo `ftpaccess` si utiliza las cookies mágicas de la cuota. Consulte la página del comando `man ftpaccess(4)` para obtener una lista de las cookies mágicas de cuotas.

## Acceso a sistemas remotos (tareas)

En este capítulo, se describen todas las tareas que son necesarias para iniciar sesión en sistemas remotos y trabajar con sus archivos. Ésta es una lista de instrucciones paso a paso de este capítulo.

- “Acceso a sistemas remotos (mapa de tareas)” en la página 653
- “Inicio de sesión en un sistema remoto (rlogin)” en la página 654
- “Inicio de sesión en un sistema remoto (ftp)” en la página 662
- “Copia remota con rcp” en la página 668

## Acceso a sistemas remotos (mapa de tareas)

En este capítulo, se proporcionan las tareas que se describen en la siguiente tabla para iniciar sesión y copiar archivos de sistemas remotos.

TABLA 29-1 Mapa de tareas: acceso a sistemas remotos

Tarea	Descripción	Para obtener instrucciones
Iniciar sesión en un sistema remoto (rlogin)	<ul style="list-style-type: none"> <li>■ Eliminar archivos .rhosts.</li> <li>■ Utilizar el comando rlogin para acceder a un sistema remoto.</li> </ul>	<p>“Cómo buscar y eliminar archivos .rhosts” en la página 659</p> <p>“Cómo saber si un sistema remoto es operativo” en la página 659</p> <p>“Cómo buscar quién ha iniciado sesión en un sistema remoto” en la página 660</p> <p>“Cómo iniciar sesión en un sistema remoto (rlogin)” en la página 661</p> <p>“Cómo cerrar sesión desde un sistema remoto (exit)” en la página 661</p>

TABLA 29-1 Mapa de tareas: acceso a sistemas remotos (Continuación)

Tarea	Descripción	Para obtener instrucciones
Iniciar sesión en un sistema remoto (ftp)	<ul style="list-style-type: none"><li>■ Abrir y cerrar una conexión ftp.</li><li>■ Copiar archivos en un sistema remoto y desde un sistema remoto.</li></ul>	<p>“Cómo abrir una conexión ftp a un sistema remoto” en la página 663</p> <p>“Cómo cerrar una conexión ftp a un sistema remoto” en la página 664</p> <p>“Cómo copiar archivos de un sistema remoto (ftp)” en la página 664</p> <p>“Cómo copiar archivos a un sistema remoto (ftp)” en la página 666</p>
Copiar archivos remotos con rcp	Utilizar el comando rcp para copiar archivos en un sistema remoto y desde un sistema remoto.	“Cómo copiar archivos entre un sistema local y un sistema remoto (rcp)” en la página 671

## Inicio de sesión en un sistema remoto (rlogin)

El comando `rlogin` le permite iniciar sesión en un sistema remoto. Una vez iniciada la sesión, puede navegar a través del sistema de archivos remoto y manipular su contenido (sujeto a autorización), copiar los archivos o ejecutar comandos remotos.

Si el sistema en el que inicia sesión es un dominio remoto, asegúrese de anexar el nombre de dominio al nombre del sistema. En este ejemplo, SOLAR es el nombre del dominio remoto:

```
rlogin pluto.SOLAR
```

Además, puede interrumpir una operación de inicio de sesión remoto en cualquier momento al escribir Control-d.

## Autenticación para inicios de sesión remotos (rlogin)

La autenticación (establecer la identidad) para operaciones `rlogin` puede ser realizada por el sistema remoto o por el entorno de red.

La diferencia principal entre estas formas de autenticación radica en el tipo de interacción que requieren de usted y la manera en que están establecidas. Si un sistema remoto intenta autenticarlo, se le pedirá una contraseña, a menos que configure el archivo `/etc/hosts.equiv` o `.rhosts`. Si la red intenta autenticarlo, no se le pedirá una contraseña, porque la red ya conoce su identidad.

Cuando el sistema remoto intenta autenticarlo, se basa en información de sus archivos locales, específicamente si se cumple una de las condiciones siguientes:

- El nombre del sistema y el nombre de usuario aparecen en el archivo `/etc/hosts.equiv` del sistema remoto.
- El nombre del sistema y el nombre de usuario aparecen en el archivo `.rhosts` del usuario remoto, bajo el nombre del directorio principal del usuario remoto.

La autenticación de red se basa en uno de estos dos métodos:

- Un “entorno de red de confianza” que se ha configurado con el servicio de información de la red local y el montador automático.
- Uno de los servicios de información de red al que apunta el archivo `/etc/nsswitch.conf` del sistema remoto contiene información acerca de usted.

---

**Nota** – La autenticación de red, por lo general, deja sin efecto la autenticación del sistema.

---

## Archivo `/etc/hosts.equiv`

El archivo `/etc/hosts.equiv` contiene una lista de hosts de confianza para un sistema remoto, uno por línea. Si un usuario intenta iniciar sesión de manera remota (mediante `rlogin`) desde uno de los hosts que se muestran en este archivo y si el sistema remoto puede acceder a la entrada de contraseña del usuario, el sistema remoto permite al usuario iniciar sesión sin una contraseña.

Un archivo `hosts.equiv` típico tiene la siguiente estructura:

```
host1
host2 user_a
+@group1
-@group2
```

Cuando se realiza una simple entrada para un host en `hosts.equiv`, como la entrada anterior para `host1`, significa que el host es de confianza y, por lo tanto, lo es cualquier usuario de ese equipo.

Si el nombre de usuario también se menciona, como en la segunda entrada del ejemplo, entonces el host es de confianza sólo si el usuario especificado intenta acceder.

Un nombre de grupo precedido por un signo más (+) significa que todos los equipos de ese grupo de red son de confianza.

Un nombre de grupo precedido por un signo menos (–) significa que ninguno de los equipos de ese grupo de red es de confianza.

## Riesgos de seguridad al utilizar el archivo `/etc/hosts.equiv`

El archivo `/etc/hosts.equiv` presenta un riesgo de seguridad. Si mantiene un archivo `/etc/hosts.equiv` en el sistema, debe incluir sólo hosts de confianza en la red. El archivo no debe incluir ningún host que pertenezca a una red distinta o ningún equipo de áreas públicas. Por ejemplo, no incluya un host que se encuentre en una sala de terminal.

El uso de hosts que no son de confianza puede ocasionar serios problemas de seguridad. Sustituya el archivo `/etc/hosts.equiv` con uno correctamente configurado o elimine el archivo.

Una sola línea de `+` en el archivo `/etc/hosts.equiv` indica que todos los hosts conocidos son de confianza.

## Archivo `.rhosts`

El archivo `.rhosts` es el equivalente de usuario del archivo `/etc/hosts.equiv`. Este archivo contiene una lista de combinaciones host-usuario en lugar de hosts en general. Si una combinación host-usuario se encuentra en este archivo, se le otorga al usuario especificado permiso para iniciar sesión de manera remota desde el host especificado sin tener que proporcionar una contraseña.

Tenga en cuenta que el archivo `.rhosts` debe residir en el nivel superior del directorio principal del usuario. Los archivos `.rhost` que están ubicados en subdirectorios no se consultan.

Los usuarios pueden crear archivos `.rhosts` en sus directorios principales. Utilizar el archivo `.rhosts` es otra forma de permitir acceso de confianza entre las cuentas propias de los usuarios en sistemas diferentes sin utilizar el archivo `/etc/hosts.equiv`.

## Riesgos de seguridad al utilizar el archivo `.rhosts`

Desafortunadamente, el archivo `.rhosts` presenta un problema de seguridad grave. Si bien el archivo `/etc/hosts.equiv` está bajo el control del administrador del sistema y puede ser gestionado eficazmente, cualquier usuario puede crear un archivo `.rhosts` que conceda acceso a cualquier persona que el usuario elija sin el conocimiento del administrador del sistema.

En una situación en la que todos los directorios principales de los usuarios están en un único servidor y sólo algunos tienen acceso de superusuario en ese servidor, una buena manera de evitar que un usuario use un archivo `.rhosts` es crear un archivo vacío como superusuario en su respectivo directorio principal. A continuación, puede cambiar los permisos en ese archivo a `000`, de manera que sería difícil modificarlo, incluso como superusuario. Este cambio evitaría de manera eficaz que un usuario ponga en riesgo la seguridad del sistema debido al uso irresponsable de un archivo `.rhosts`. Este cambio, sin embargo, no resolvería nada si el usuario puede cambiar la ruta eficaz a su directorio principal.

La única manera segura de gestionar archivos `.rhosts` es deshabilitarlos completamente. Consulte [“Cómo buscar y eliminar archivos `.rhosts`” en la página 659](#) para obtener instrucciones detalladas. Como administrador del sistema, puede comprobar el sistema con



frecuencia para verificar posibles infracciones de la política de seguridad. Una posible excepción a esta política es para la cuenta `root`; es posible que necesite tener un archivo `.rhosts` para realizar copias de seguridad de red y otros servicios remotos.

## Vinculación de inicios de sesión remotos

Si su sistema está configurado correctamente, puede vincular inicios de sesión remotos. Por ejemplo, un usuario en `earth` inicia sesión en `jupiter` y desde allí decide iniciar sesión en `pluto`.

El usuario podría haber cerrado sesión en `jupiter` y, a continuación, haber iniciado sesión directamente en `pluto`, pero este tipo de vinculación puede ser más conveniente.

Para vincular inicios de sesión remotos sin tener que proporcionar una contraseña, debe tener el archivo `/etc/hosts.equiv` o `.rhosts` configurado correctamente.

## Inicios de sesión remotos directos o indirectos

El comando `rlogin` le permite iniciar sesión en un sistema remoto directa o indirectamente.

Un inicio de sesión remoto directo se intenta con el nombre de usuario predeterminado, es decir, el nombre de usuario del individuo que está conectado actualmente en el sistema local. Ésta es la forma más común de inicio de sesión remoto.

Un inicio de sesión remoto indirecto se intenta con un nombre de usuario diferente, el cual se proporciona durante la operación de inicio de sesión remoto. Éste es el tipo de inicio de sesión remoto que es posible que intente desde una estación de trabajo temporal. Por ejemplo, si estuviera en una oficina de un socio y necesitara revisar archivos de su directorio principal, es posible que inicie sesión en su sistema de manera remota, desde el sistema del socio. Sin embargo, realizaría un inicio de sesión remoto indirecto, ya que proporcionaría su propio nombre de usuario.

Las dependencias entre inicios de sesión directos e indirectos, y métodos de autenticación se resumen en la siguiente tabla.

**TABLA 29–2** Dependencias entre método de inicio de sesión y método de autenticación (rlogin)

Tipo de inicio de sesión	Nombre de usuario proporcionado por	Autenticación	Contraseña
Directo	Sistema	Red	Ninguna
		Sistema	Necesaria
Indirecto	Usuario	Red	Ninguna

TABLA 29-2 Dependencias entre método de inicio de sesión y método de autenticación (rlogin)  
(Continuación)

Tipo de inicio de sesión	Nombre de usuario proporcionado por	Autenticación	Contraseña
		Sistema	Necesaria

## Qué sucede después iniciar sesión de manera remota

Cuando inicia sesión en un sistema remoto, el comando `rlogin` intenta encontrar su directorio principal. Si el comando `rlogin` no puede encontrar su directorio principal, lo asigna al directorio (`/`) root del sistema remoto. Por ejemplo:

```
Unable to find home directory, logging in with /
```

Sin embargo, si el comando `rlogin` encuentra su directorio principal, origina los archivos `.cshrc` y `.login`. Por lo tanto, después de un inicio de sesión remoto, su indicador es un indicador de inicio de sesión estándar y el directorio actual es el mismo que usa cuando inicia sesión localmente.

Por ejemplo, si su indicador habitual muestra el nombre del sistema y el directorio de trabajo, y al iniciar sesión, el directorio de trabajo es su directorio principal, el indicador de inicio de sesión es similar al siguiente:

```
earth(/home/smith):
```

Entonces, al iniciar sesión en un sistema remoto, ve un indicador similar y el directorio de trabajo es su directorio principal, independientemente del directorio desde el que introdujo el comando `rlogin`:

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/smith):
```

La única diferencia es que el nombre del sistema remoto sustituiría el sistema local al inicio del indicador. El sistema de archivos remoto es paralelo al directorio principal.

En efecto, si modifica el directorio a `/home` y luego ejecuta `ls`, ve lo siguiente:

```
earth(home/smith): cd ..
earth(/home): ls
smith jones
```

## ▼ Cómo buscar y eliminar archivos . rhosts

### 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 \(mapa de tareas\)](#)” de *Guía de administración del sistema: servicios de seguridad*.

### 2 Busque y elimine archivos . rhosts mediante el comando `find(1)`.

```
# find home-directories -name .rhosts -print -exec rm {} \;
```

*directorios principales*      Identifica la ruta al directorio donde se encuentran los directorios principales de los usuarios. Tenga en cuenta que puede introducir varias rutas para buscar más de un directorio principal a la vez.

`-name .rhosts`      Identifica el nombre del archivo.

`-print`      Imprime el nombre de la ruta actual.

`-exec rm {} \;`      Indica al comando `find` que aplique el comando `rm` a todos los archivos que se identifican mediante el uso del nombre de archivo coincidente.

El comando `find` comienza en el directorio designado y busca cualquier archivo con el nombre `.rhosts`. Si encuentra tal archivo, `find` imprime la ruta en la pantalla y lo elimina.

### Ejemplo 29–1 Búsqueda y eliminación de archivos . rhosts

En el siguiente ejemplo se buscan y eliminan archivos `.rhosts` en todos los directorios principales de usuario ubicados en el directorio `/export/home`.

```
# find /export/home -name .rhosts -print | xargs -i -t rm {} \;
```

## Cómo saber si un sistema remoto es operativo

Sepa si un sistema remoto es operativo mediante el uso del comando `ping`.

```
$ ping system-name | ip-address
```

*nombre\_sistema*      El nombre del sistema remoto

*dirección\_ip*      La dirección IP del sistema remoto

El comando `ping` devuelve uno de tres mensajes:

Mensaje de estado	Explicación
<i>nombre_sistema</i> está activo	Se puede acceder al sistema a través de la red.
ping: unknown host <i>nombre_sistema</i>	El nombre del sistema es desconocido.
ping: no answer from <i>nombre_sistema</i>	El sistema es conocido, pero actualmente no se encuentra operando.

Si el sistema al que "hace ping" se encuentra en un dominio distinto, el mensaje que se devuelve también puede contener información de enrutamiento, que se puede ignorar.

El comando ping tiene un tiempo de espera de 20 segundos. Si no recibe una respuesta en un período de 20 segundos, se devuelve el tercer mensaje. Puede forzar al ping para que espere durante más tiempo (o menos) si introduce un valor de *tiempo de espera*, en segundos:

```
$ ping system-name | ip-address time-out
```

Para obtener más información, consulte [ping\(1M\)](#).

## Cómo buscar quién ha iniciado sesión en un sistema remoto

Busque quién inició sesión en un sistema remoto mediante el comando [rusers\(1\)](#).

```
$ rusers [-l] remote-system-name
```

- rusers** (Sin opciones) Muestra el nombre del sistema seguido del nombre de los usuarios que están conectados actualmente en el sistema, incluyendo root
- l** Muestra información adicional acerca de cada usuario: la ventana de inicio de sesión del usuario, la fecha y hora de inicio de sesión, la cantidad de tiempo conectado y el nombre del sistema remoto desde el que el usuario ha iniciado sesión

### EJEMPLO 29-2 Búsqueda de quién ha iniciado sesión en un sistema remoto

En el siguiente ejemplo se muestra la versión corta de rusers.

```
$ rusers pluto
pluto    smith  jones
```

En el siguiente ejemplo, la versión larga de rusers muestra que dos usuarios iniciaron sesión en el sistema remoto starbug. El primer usuario inició sesión desde la consola del sistema el 10 de septiembre y ha estado conectado por 137 horas y 15 minutos. El segundo usuario inició sesión desde un sistema remoto, mars, el 14 de septiembre.

**EJEMPLO 29-2** Búsqueda de quién ha iniciado sesión en un sistema remoto (Continuación)

```
$rusers -l starbug
root      starbug:console      Sep 10 16:13 137:15
rimmer    starbug:pts/0                Sep 14 14:37      (mars)
```

## Cómo iniciar sesión en un sistema remoto (rlogin)

Inicie sesión en un sistema remoto utilizando el comando `rlogin(1)`.

```
$ rlogin [-l user-name] system-name
```

`rlogin` (Sin opciones) Lo conecta al sistema remoto *directamente*, con su nombre de usuario actual

`-l nombre de usuario` Lo conecta al sistema remoto *indirectamente*, con el nombre de usuario que proporciona

Si la red intenta autenticarlo, no se le solicita una contraseña. Si el sistema remoto intenta autenticarlo, se le pedirá que proporcione una contraseña.

Si la operación se realiza correctamente, el comando `rlogin` muestra información breve sobre el último inicio de sesión remoto en ese sistema, la versión del sistema operativo que se está ejecutando en el sistema remoto y si tiene correo en el directorio principal.

**EJEMPLO 29-3** Inicio de sesión en un sistema remoto (rlogin)

El siguiente ejemplo muestra el resultado de un inicio de sesión remoto en `pluto`. La red ha autenticado al usuario.

```
$ rlogin starbug
Last login: Mon Jul 12 09:28:39 from venus
Sun Microsystems Inc. SunOS 5.8 February 2000
starbug:
```

El siguiente ejemplo muestra el resultado de un inicio de sesión remoto indirecto a `pluto`, con el usuario autenticado por el sistema remoto.

```
$ rlogin -l smith pluto
password: user-password
Last login: Mon Jul 12 11:51:58 from venus
Sun Microsystems Inc. SunOS 5.8 February 2000
starbug:
```

## Cómo cerrar sesión desde un sistema remoto (exit)

Cierre sesión desde un sistema remoto utilizando el comando `exit(1)`.

\$ **exit**

**EJEMPLO 29-4** Cierre de sesión desde un sistema remoto (exit)

En este ejemplo se muestra al usuario smith cerrar sesión desde el sistema pluto.

```
$ exit
pluto% logout
Connection closed.
earth%
```

## Inicio de sesión en un sistema remoto (ftp)

El comando `ftp` abre la interfaz de usuario al protocolo de transferencia de archivos de Internet. Esta interfaz de usuario, denominada intérprete de comandos, le permite iniciar sesión en un sistema remoto y realizar distintas operaciones con su sistema de archivos. Las operaciones principales se resumen en la siguiente tabla.

El beneficio principal de `ftp` en comparación con `rlogin` y `rcp` es que `ftp` no requiere que el sistema remoto ejecute UNIX. El sistema remoto, sin embargo, necesita estar configurado para comunicaciones TCP/IP. Sin embargo, `rlogin` proporciona acceso a un conjunto más grande de comandos de manipulación de archivos del que `ftp` proporciona.

## Autenticación para inicios de sesión remotos (ftp)

La autenticación para operaciones de inicio de sesión remoto `ftp` se puede establecer mediante uno de los siguientes métodos:

- Incluir la entrada de contraseña en el archivo `/etc/passwd` del sistema remoto, o tabla o mapa de servicio de información de red equivalente
- Establecer una cuenta de `ftp` anónima en el sistema remoto

## Comandos ftp esenciales

**TABLA 29-3** Comandos `ftp` esenciales

Comando	Descripción
<code>ftp</code>	Accede al intérprete de comandos <code>ftp</code> .

TABLA 29-3 Comandos ftp esenciales (Continuación)

Comando	Descripción
<code>ftp sistema remoto</code>	Establece una conexión ftp a un sistema remoto. Para obtener instrucciones, consulte <a href="#">“Cómo abrir una conexión ftp a un sistema remoto” en la página 663.</a>
<code>open</code>	Inicia sesión en el sistema remoto desde el intérprete de comandos.
<code>close</code>	Cierra la sesión del sistema remoto y vuelve al intérprete de comandos.
<code>bye</code>	Sale del intérprete de comandos ftp.
<code>help</code>	Muestra todos los comandos ftp o, si se proporciona un nombre de comando, se describe brevemente lo que hace el comando.
<code>reset</code>	Vuelve a sincronizar la secuenciación de respuesta de comando con el servidor ftp remoto.
<code>ls</code>	Muestra los contenidos del directorio de trabajo remoto.
<code>pwd</code>	Muestra el nombre del directorio de trabajo remoto.
<code>cd</code>	Cambia el directorio de trabajo remoto.
<code>lcd</code>	Cambia el directorio de trabajo local.
<code>mkdir</code>	Crea un directorio en el sistema remoto.
<code>rmdir</code>	Elimina un directorio en el sistema remoto.
<code>get, mget</code>	Copia un archivo (o varios archivos) del directorio de trabajo remoto al directorio de trabajo local.
<code>put, mput</code>	Copia un archivo (o varios archivos) del directorio de trabajo local al directorio de trabajo remoto.
<code>delete, mdelete</code>	Elimina un archivo (o varios archivos) del directorio de trabajo remoto.

Para obtener más información, consulte [ftp\(1\)](#).

## ▼ Cómo abrir una conexión ftp a un sistema remoto

### 1 Asegúrese de tener autenticación ftp.

Debe tener autenticación ftp, como se describe en [“Autenticación para inicios de sesión remotos \(ftp\)” en la página 662.](#)

### 2 Abra una conexión a un sistema remoto utilizando el comando ftp.

```
$ ftp remote-system
```

Si la conexión se realiza correctamente, se muestran un mensaje de confirmación y un indicador.

### 3 Escriba el nombre de usuario.

Name (*remote-system:user-name*): *user-name*

### 4 Si se le solicita, especifique la contraseña.

331 Password required for *user-name*:  
Password: *password*

Si el sistema al que accede tiene una cuenta ftp anónima establecida, se le solicita una dirección de correo electrónico para la contraseña. Si la interfaz ftp acepta la contraseña, muestra un mensaje de confirmación y el indicador (ftp>).

Ahora puede utilizar cualquiera de los comandos que proporciona la interfaz ftp, incluida la ayuda. Los comandos principales se resumen en la [Tabla 29-3](#).

## Ejemplo 29-5 Apertura de una conexión ftp a un sistema remoto

Esta sesión ftp la estableció el usuario smith en el sistema remoto pluto:

```
$ ftp pluto
Connected to pluto.
220 pluto FTP server ready.
Name (pluto:smith): smith
331 Password required for smith:
Password: password
230 User smith logged in.
ftp>
```

## Cómo cerrar una conexión ftp a un sistema remoto

Cierre una conexión ftp a un sistema remoto utilizando el comando bye.

```
ftp> bye
221-You have transferred 0 bytes in 0 files.
221-Total traffic for this sessions was 172 bytes in 0 transfers.
221-Thanks you for using the FTP service on spdev.
221 Goodbye.
```

Se muestra un mensaje de despedida, seguido del indicador shell habitual.

## ▼ Cómo copiar archivos de un sistema remoto (ftp)

### 1 Cambie a un directorio en el sistema local donde desea que se copien los archivos del sistema remoto.

```
$ cd target-directory
```



**2 Establezca una conexión ftp.**

Consulte “[Cómo abrir una conexión ftp a un sistema remoto](#)” en la página 663.

**3 Cambie al directorio de origen.**

```
ftp> cd source-directory
```

Si el sistema utiliza el montador automático, el directorio principal del usuario del sistema remoto aparece paralelo al suyo, en /home.

**4 Asegúrese de tener permiso para los archivos de origen.**

```
ftp> ls -l
```

**5 Defina el tipo de transferencia en binary.**

```
ftp> binary
```

**6 Si desea copiar un solo archivo, utilice el comando get.**

```
ftp> get filename
```

**7 Si desea copiar varios archivos a la vez, utilice el comando mget.**

```
ftp> mget filename [filename ...]
```

Puede proporcionar una serie de nombres de archivo individuales y puede utilizar caracteres comodín. El comando mget copia cada archivo de manera individual y solicita confirmación cada vez que copia.

**8 Cierre las conexiones ftp.**

```
ftp> bye
```

**Ejemplo 29-6 Copia de archivos de un sistema remoto (ftp)**

En este ejemplo, el usuario kryten abre una conexión ftp al sistema pluto y utiliza el comando get para copiar un solo archivo del directorio /tmp.

```
$ cd $HOME
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34344)
(0 bytes).
filea
files
```

```

ps_data
226 ASCII Transfer complete.
53 bytes received in 0.022 seconds (2.39 Kbytes/s)
ftp> get filea
200 PORT command successful.
150 ASCII data connection for filea (129.152.221.238,34331)
(0 bytes).
221 Goodbye.

```

En este ejemplo, el mismo usuario kryten utiliza el comando `mget` para copiar un grupo de archivos del directorio `/tmp` al directorio principal. Tenga en cuenta que kryten puede aceptar o rechazar archivos individuales del grupo.

```

$ ftp> cd /tmp
250 CWD command successful.
ftp> ls files
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34345)
(0 bytes).
fileb
filec
filed
remote: files
21 bytes received in 0.015 seconds (1.36 Kbytes/s)
ftp> cd files
250 CWD command successful.
ftp> mget file*
mget fileb? y
200 PORT command successful.
150 ASCII data connection for fileb (129.152.221.238,34347)
(0 bytes).
226 ASCII Transfer complete.
mget filec? y
200 PORT command successful.
150 ASCII data connection for filec (129.152.221.238,34348)
(0 bytes).
226 ASCII Transfer complete.
mget filed? y
200 PORT command successful.
150 ASCII data connection for filed (129.152.221.238,34351)
(0 bytes).
226 ASCII Transfer complete.200 PORT command successful.
ftp> bye
221 Goodbye.

```

## ▼ Cómo copiar archivos a un sistema remoto (ftp)

### 1 Cambie al directorio de origen en el sistema local.

El directorio desde el que escribe el comando `ftp` es el directorio de trabajo local y, por lo tanto, el directorio de origen para esta operación.

### 2 Establezca una conexión ftp.

Consulte “[Cómo abrir una conexión ftp a un sistema remoto](#)” en la página 663.

**3 Cambie al directorio de destino.**

```
ftp> cd target-directory
```

Recuerde que si el sistema utiliza el montador automático, el directorio principal del usuario del sistema remoto aparece paralelo al suyo, en /home.

**4 Asegúrese de tener permisos de escritura para el directorio de destino.**

```
ftp> ls -l target-directory
```

**5 Defina el tipo de transferencia en binary.**

```
ftp> binary
```

**6 Si desea copiar un solo archivo, utilice el comando put.**

```
ftp> put filename
```

**7 Si desea copiar varios archivos a la vez, utilice el comando mput.**

```
ftp> mput filename [filename ...]
```

Puede proporcionar una serie de nombres de archivo individuales y puede utilizar caracteres comodín. El comando mput copia cada archivo de manera individual y solicita confirmación cada vez que copia.

**8 Para cerrar la conexión ftp, escriba bye.**

```
ftp> bye
```

**Ejemplo 29–7 Copia de archivos a un sistema remoto (ftp)**

En este ejemplo, el usuario kryten abre una conexión ftp al sistema pluto y utiliza el comando put para copiar un archivo de su respectivo sistema al directorio /tmp en el sistema pluto.

```
$ cd /tmp
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> put filef
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34357) (0 bytes).
filea
filef
files
```

```
ps_data
226 ASCII Transfer complete.
60 bytes received in 0.058 seconds (1.01 Kbytes/s)
ftp> bye
221 Goodbye.
```

En este ejemplo, el mismo usuario kryten utiliza el comando `mput` para copiar un grupo de archivos de su respectivo directorio principal al directorio de `pluto /tmp`. Tenga en cuenta que kryten puede aceptar o rechazar archivos individuales del grupo.

```
$ cd $HOME/testdir
$ ls
test1  test2  test3
$ ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> mput test*
mput test1? y
200 PORT command successful.
150 ASCII data connection for test1 (129.152.221.238,34365).
226 Transfer complete.
mput test2? y
200 PORT command successful.
150 ASCII data connection for test2 (129.152.221.238,34366).
226 Transfer complete.
mput test3? y
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> bye
221 Goodbye.
```

## Copia remota con rcp

El comando `rcp` copia archivos o directorios entre un sistema local y un sistema remoto, o entre dos sistemas remotos. Puede utilizar este comando desde un sistema remoto (después de iniciar la sesión con el comando `rlogin`) o desde el sistema local (sin tener que iniciar sesión en un sistema remoto).

Con `rcp` puede realizar las siguientes operaciones de copia remota:

- Copiar un archivo o directorio de su sistema a un sistema remoto
- Copiar un archivo o directorio de un sistema remoto a su sistema local
- Copiar un archivo o directorio entre sistemas remotos desde su sistema local

Si se ejecuta el montador automático, puede realizar estas operaciones remotas con el comando `cp`. Sin embargo, el rango de `cp` está restringido al sistema de archivos virtual que el montador

automático crea y a operaciones relativas al directorio principal del usuario. Debido a que rcp realiza las mismas operaciones sin estas restricciones, en esta sección, se describen únicamente las versiones rcp de estas tareas.

## Consideraciones de seguridad para operaciones de copia

Para copiar archivos o directorios entre sistemas, debe tener permiso para iniciar sesión y copiar archivos.



**Precaución** – Los comandos cp y rcp pueden sobrescribir los archivos sin que aparezca ningún mensaje de advertencia. Asegúrese de que los nombres de archivo sean correctos antes de ejecutar el comando.

## Especificación de origen y destino

Con el comando rcp en el shell C, puede especificar el origen (el archivo o directorio que desea copiar) y el destino (la ubicación en la que copiará el archivo o el directorio) ya sea con nombres de ruta absolutos o abreviados.

	Nombres de ruta absolutos	Nombres de ruta abreviados
Desde el sistema local	<code>mars:/home/jones/myfile.txt</code>	<code>~jones/myfile.txt</code>
Después del inicio de sesión remoto	<code>/home/jones/myfile.txt</code>	<code>~jones/myfile.txt</code>

Los nombres de ruta absolutos identifican archivos o directorios que están montados en un sistema específico. En el ejemplo anterior, el primer nombre de ruta absoluto identifica un archivo (`myfile.txt`) en el sistema `mars`. Los nombres de ruta abreviados identifican archivos o directorios relativos a un directorio principal del usuario, dondequiera que resida. En el primer ejemplo anterior, el nombre de ruta abreviado identifica el mismo archivo, `myfile.txt`, pero utiliza el símbolo `"~"` para indicar el directorio principal `jones`:

`~ = mars:/home/jones`

Los ejemplos de la segunda línea muestran el usuario de nombres de ruta absolutos y abreviados después de un inicio de sesión remoto. Ninguna diferencia es evidente para el nombre de ruta abreviado. Sin embargo, debido a que la operación de inicio de sesión remoto montó el directorio principal `jones` en el sistema local (paralelo al directorio principal del usuario local),

el nombre de ruta de acceso absoluto ya no necesita el nombre del sistema `mars`. Para obtener más información acerca de cómo una operación de inicio de sesión remoto monta un directorio principal de otro usuario, consulte [“Qué sucede después iniciar sesión de manera remota” en la página 658](#).

La siguiente tabla proporciona un ejemplo de nombres de ruta absolutos y abreviados que el shell C reconoce. El ejemplo utiliza la siguiente terminología:

- Directorio de trabajo: directorio desde el cual se introduce el comando `rcp`. Puede ser remoto o local.
- Usuario actual: nombre de usuario bajo el cual se introduce el comando `rcp`.

TABLA 29–4    Sintaxis permitidas para nombres de archivo y directorio

Inició sesión en	Sintaxis	Descripción
Sistema local	.	El directorio de trabajo local
	<i>ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> en el directorio de trabajo local
	~	El directorio principal del usuario actual
	~/ <i>ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> debajo del directorio principal del usuario actual
	~ <i>usuario</i>	El directorio principal de <i>usuario</i>
	~ <i>usuario/ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> debajo del directorio principal de <i>usuario</i>
	<i>sistema remoto:ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> en el directorio de trabajo remoto
Sistema remoto	.	El directorio de trabajo remoto
	<i>nombre_archivo</i>	El <i>nombre_archivo</i> en el directorio de trabajo remoto
	<i>ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> en el directorio de trabajo remoto
	~	El directorio principal del usuario actual
	~/ <i>ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> en el directorio principal del usuario actual
	~ <i>usuario</i>	El directorio principal de <i>usuario</i>
	~/ <i>usuario/ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> debajo del directorio principal de <i>usuario</i>
	<i>sistema local:ruta/nombre_archivo</i>	La <i>ruta</i> y el <i>nombre_archivo</i> en el directorio de trabajo local

## ▼ Cómo copiar archivos entre un sistema local y un sistema remoto (rcp)

### 1 Asegúrese de tener permiso para copiar.

Debe tener al menos permiso de lectura en el sistema de origen y permiso de escritura en el sistema de destino.

### 2 Determine la ubicación del origen y el destino.

Si no conoce la ruta de origen o de destino, primero puede iniciar sesión en el sistema remoto con el comando `rlogin`, como se describe en “[Cómo iniciar sesión en un sistema remoto \(rlogin\)](#)” en la [página 661](#). A continuación, navegue por el sistema remoto hasta que encuentre la ubicación. Puede realizar el siguiente paso sin cerrar sesión.

### 3 Copie el archivo o el directorio.

```
$ rcp [-r] source-file|directory target-file|directory
```

`rcp` (Sin opciones) Copia un solo archivo del origen al destino.

`-r` Copia un directorio del origen al de destino.

Esta sintaxis se aplica si inició sesión en el sistema remoto o en el sistema local. Sólo el nombre de ruta del archivo o directorio cambia, como se describe en la [Tabla 29-4](#) y como se puede ver en los siguientes ejemplos.

Puede utilizar los caracteres “~” y “.” para especificar las porciones de ruta de los nombres de archivo o directorio locales. Tenga en cuenta que “~” se aplica al usuario actual, no al sistema remoto, y que “.” se aplica al sistema al que está conectado. Para ver una explicación de estos símbolos, consulte la [Tabla 29-4](#).

### Ejemplo 29-8 Uso de rcp para copiar un archivo remoto a un sistema local

En este ejemplo, `rcp` se utiliza para copiar el archivo `letter.doc` del directorio `/home/jones` del sistema remoto `pluto` al directorio de trabajo (`/home/smith`) en el sistema local, `earth`:

```
earth(/home/smith): rcp pluto:/home/jones/letter.doc .
```

En esta instancia, la operación `rcp` se realiza sin un inicio de sesión remoto. En este caso, el símbolo “.” al final de la línea de comandos hace referencia al sistema local, no al sistema remoto.

El directorio de destino es también el directorio principal del usuario local, por lo tanto, también se puede especificar con el símbolo “~”.

**Ejemplo 29-9** Uso de `rlogin` y `rcp` para copiar un archivo remoto a un sistema local

En este ejemplo, la operación `rcp` se ejecuta después de la ejecución del comando `rlogin` para copiar un archivo de un sistema remoto a un sistema local. Aunque el flujo de la operación es igual al del ejemplo anterior, las rutas cambian para permitir el inicio de sesión remoto:

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp letter.doc ~
```

El uso del símbolo "." al final de la línea de comandos sería inadecuado en esta instancia. Debido al inicio de sesión remoto, el símbolo se referiría simplemente al sistema remoto; básicamente direccionando `rcp` para crear un archivo duplicado. El símbolo "~", sin embargo, hace referencia al directorio principal del usuario actual, incluso cuando el inicio de sesión es para un sistema remoto.

**Ejemplo 29-10** Uso de `rcp` para copiar un archivo local a un sistema remoto

En este ejemplo, `rcp` se utiliza para copiar el archivo `notice.doc` del directorio principal (`/home/smith`) del sistema local `earth` al directorio (`/home/jones`) del sistema remoto, `pluto`:

```
earth(/home/smith): rcp notice.doc pluto:/home/jones
```

Debido a que no se proporciona un nombre de archivo remoto, el archivo `notice.doc` se copia en el directorio `/home/jones` con el mismo nombre.

En esta instancia, se repite la operación `rcp` del ejemplo anterior, pero `rcp` se introduce de un directorio de trabajo diferente en el sistema local (`/tmp`). Tenga en cuenta el uso del símbolo "~" para hacer referencia al directorio principal del usuario actual:

```
earth(/tmp): rcp ~/notice.doc pluto:/home/jones
```

**Ejemplo 29-11** Uso de `rlogin` y `rcp` para copiar un archivo local a un sistema remoto

En este ejemplo, la operación `rcp` se ejecuta después de la ejecución del comando `rlogin` para copiar un archivo local a un directorio remoto. Aunque el flujo de la operación es igual al del ejemplo anterior, las rutas cambian para permitir el inicio de sesión remoto.

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp ~/notice.doc .
```



En esta instancia, el símbolo "~" se puede usar para denotar el directorio principal del usuario actual, aunque esté en el sistema local. El símbolo "." hace referencia al directorio de trabajo en el sistema remoto porque el usuario está conectado al sistema remoto. A continuación, se muestra una sintaxis alternativa que realiza la misma operación:

```
pluto(/home/jones): rcp earth:/home/smith/notice.doc /home/jones
```



## P A R T E V I I

# Supervisión de servicios de red (temas)

Esta sección proporciona instrucciones paso a paso para supervisar los servicios de red.



## Supervisión del rendimiento de la red (tareas)

En este capítulo, se describe cómo supervisar el rendimiento de la red. A continuación, se muestra una lista de las instrucciones paso a paso que se incluyen en este capítulo.

- “Cómo comprobar la respuesta de los hosts en la red” en la página 678
- “Cómo enviar paquetes a los hosts en la red” en la página 678
- “Cómo capturar paquetes de la red” en la página 679
- “Cómo comprobar el estado de la red” en la página 679
- “Cómo mostrar estadísticas de servidor y cliente NFS” en la página 682

## Supervisión del rendimiento de la red

La [Tabla 30–1](#) describe los comandos disponibles para supervisar el rendimiento de la red.

**TABLA 30–1** Comandos para supervisión de la red

Comando	Descripción
ping	Permite consultar la respuesta de los hosts en la red.
spray	Permite probar la fiabilidad del tamaño de los paquetes. Este comando puede indicar si la red retrasa o descarta los paquetes.
snoop	Permite capturar paquetes de la red y rastrear las llamadas de cada cliente a cada servidor.
netstat	Permite mostrar el estado de la red, incluido el estado de las interfaces que se utilizan para el tráfico TCP/IP, la tabla de enrutamiento IP y las estadísticas por protocolo para UDP, TCP, ICMP e IGMP.
nfsstat	Permite mostrar un resumen de las estadísticas de servidor y cliente que se pueden utilizar para identificar problemas relacionados con NFS.

## Cómo comprobar la respuesta de los hosts en la red

Compruebe la respuesta de los hosts en la red con el comando `ping`.

```
$ ping hostname
```

Si sospecha que existe un problema físico, puede usar el comando `ping` para buscar el tiempo de respuesta de varios hosts en la red. Si la respuesta de un host no es la esperada, puede examinar ese host. Las causas de los problemas físicos podrían ser las siguientes:

- Cables o conectores sueltos.
- Conexión a tierra inadecuada.
- Ninguna terminación.
- Reflexión de la señal.

Para obtener más información sobre este comando, consulte [ping\(1M\)](#).

### EJEMPLO 30-1 Comprobación de la respuesta de los hosts en la red

La versión más sencilla de `ping` envía un solo paquete a un host de la red. Si `ping` recibe la respuesta correcta, el comando imprime el mensaje *host is alive*.

```
$ ping elvis
elvis is alive
```

Con la opción `-s`, `ping` envía un datagrama por segundo a un host. Luego, el comando imprime cada respuesta y el tiempo necesario para el recorrido de ida y vuelta. A continuación, se muestra un ejemplo.

```
$ ping -s pluto
64 bytes from pluto (123.456.78.90): icmp_seq=0. time=3.82 ms
64 bytes from pluto (123.456.78.90): icmp_seq=5. time=0.947 ms
64 bytes from pluto (123.456.78.90): icmp_seq=6. time=0.855 ms
^C
----pluto PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max/sttdev = 0.855/1.87/3.82/1.7
```

## Cómo enviar paquetes a los hosts en la red

Pruebe la fiabilidad del tamaño de los paquetes con el comando `spray`.

```
$ spray [ -c count -d interval -l packet-size] hostname
```

`-i recuento`                      Cantidad de paquetes que se enviarán.

`-d intervalo`                    Cantidad de microsegundos de pausa entre el envío de paquetes. Si no utiliza ningún retraso, es posible que los búferes se agoten.

`-l tamaño-paquete`      Tamaño del paquete.  
`nombredehost`            Sistema para enviar paquetes.

Para obtener más información sobre este comando, consulte [spray\(1M\)](#).

#### EJEMPLO 30-2 Envío de paquetes a los hosts en la red

En el siguiente ejemplo, se envían 100 paquetes a un host (`-c 100`), cada uno con un tamaño de 2048 bytes (`-l 2048`). Los paquetes se envían con un tiempo de retraso de 20 microsegundos entre cada ráfaga (`-d 20`).

```
$ spray -c 100 -d 20 -l 2048 pluto
sending 100 packets of length 2048 to pluto ...
no packets dropped by pluto
279 packets/sec, 573043 bytes/sec
```

## Cómo capturar paquetes de la red

Para capturar paquetes de la red y rastrear las llamadas de cada cliente a cada servidor, utilice el comando `snoop`. Este comando proporciona indicaciones de hora precisas que permiten aislar rápidamente algunos problemas relacionados con el rendimiento de la red. Para obtener más información, consulte [snoop\(1M\)](#).

```
# snoop
```

Los paquetes descartados pueden derivar de espacio insuficiente en el búfer o una CPU sobrecargada.

## Cómo comprobar el estado de la red

Para mostrar información del estado de la red, como estadísticas sobre el estado de las interfaces de la red, las tablas de enrutamiento y diferentes protocolos, utilice el comando `netstat`.

```
$ netstat [-i] [-r] [-s]
```

- `-i`      Muestra el estado de las interfaces TCP/IP.
- `-r`      Muestra la tabla de enrutamiento IP.
- `-s`      Muestra estadísticas para los protocolos UDP, TCP, ICMP e IGMP.

Para obtener más información, consulte [netstat\(1M\)](#).

## Ejemplos: Comprobación del estado de la red

El siguiente ejemplo detalla la salida del comando `netstat -i`, que muestra el estado de las interfaces que se utilizan para el tráfico TCP/IP.

```
$ netstat -i
Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis Queue
lo0 8232 software localhost 1280 0 1280 0 0 0
eri0 1500 loopback venus 1628480 0 347070 16 39354 0
```

Esta pantalla muestra la cantidad de paquetes que un equipo transmitió y recibió en cada interfaz. Un equipo con tráfico de red activo debe mostrar tanto `Ipkts` como `Opkts` en constante aumento.

Para calcular la tasa de colisiones de la red, divida la cantidad de colisiones (`Collis`) por la cantidad de paquetes de salida (`Opkts`). En el ejemplo anterior, la tasa de colisiones es del 11%. Una tasa de colisiones en toda la red que es mayor que el 5 al 10% puede indicar un problema.

Para calcular la tasa de errores para los paquetes de entrada, divida la cantidad de errores de entrada por la cantidad total de paquetes de entrada (`Ierrs/Ipkts`). La tasa de errores para los paquetes de salida es la cantidad de errores de salida dividido por la cantidad total de paquetes de salida (`Oerrs/Opkts`). Si la tasa de errores de entrada es alta, superior al 0,25%, es posible que el host descarte paquetes.

El siguiente ejemplo muestra la salida del comando `netstat -s`, que muestra las estadísticas por protocolo para los protocolos UDP, TCP, ICMP e IGMP.

```
UDP
  udpInDatagrams    =196543
  udpOutDatagrams   =187820
  udpInErrors        =      0

TCP
  tcpRtoAlgorithm    =      4
  tcpRtoMax          = 60000
  tcpActiveOpens     = 26952
  tcpAttemptFails    = 1133
  tcpCurrEstab       = 31
  tcpOutDataSegs     =2731494
  tcpRetransSegs     = 36186
  tcpOutAck          =1225849
  tcpOutUrg          = 7
  tcpOutWinProbe     = 0
  tcpOutRsts         = 803
  tcpInSegs          =4587678
  tcpInAckSegs       =2087448
  tcpInDupAck        =109461
  tcpInInorderSegs   =3877639
  tcpInUnorderSegs   = 14756
  tcpInDupSegs       = 34
  tcpInPartDupSegs   = 212
  tcpInPastWinSegs   = 0
  tcpInWinProbe      = 456
  tcpRtoMin          = 200
  tcpMaxConn         = -1
  tcpPassiveOpens    = 420
  tcpEstabResets     = 9
  tcpOutSegs         =3957636
  tcpOutDataBytes    =1865269594
  tcpRetransBytes    =3762520
  tcpOutAckDelayed   =165044
  tcpOutWinUpdate    = 315
  tcpOutControl      = 56588
  tcpOutFastRetrans  = 741
  tcpInAckBytes      =1865292802
  tcpInAckUnsent     = 0
  tcpInInorderBytes  =-598404107
  tcpInUnorderBytes  =17985602
  tcpInDupBytes      = 32759
  tcpInPartDupBytes  =134800
  tcpInPastWinBytes  = 0
  tcpInWinUpdate     = 0
```



```

tcpInClosed          = 99      tcpRttNoUpdate       = 6862
tcpRttUpdate         =435097   tcpTimRetrans        = 15065
tcpTimRetransDrop    = 67      tcpTimKeepalive      = 763
tcpTimKeepaliveProbe= 1        tcpTimKeepaliveDrop  = 0

IP
ipForwarding         = 2        ipDefaultTTL         = 255
ipInReceives         =11757234  ipInHdrErrors        = 0
ipInAddrErrors       = 0        ipInCksumErrs        = 0
ipForwDatagrams      = 0        ipForwProhibits      = 0
ipInUnknownProtos    = 0        ipInDiscards         = 0
ipInDelivers         =4784901   ipOutRequests        =4195180
ipOutDiscards        = 0        ipOutNoRoutes        = 0
ipReasmTimeout       = 60       ipReasmReqds         = 8723
ipReasmOKs           = 7565     ipReasmFails         = 1158
ipReasmDuplicates    = 7        ipReasmPartDups      = 0
ipFragOKs            = 19938     ipFragFails          = 0
ipFragCreates        =116953    ipRoutingDiscards    = 0
tcpInErrs            = 0        udpNoPorts            =6426577
udpInCksumErrs       = 0        udpInOverflows       = 473
rawipInOverflows     = 0

```

```

ICMP
icmpInMsgs           =490338    icmpInErrors          = 0
icmpInCksumErrs      = 0        icmpInUnknowns       = 0
icmpInDestUnreachs   = 618      icmpInTimeExcds      = 314
icmpInParmProbs      = 0        icmpInSrcQuenchs     = 0
icmpInRedirects      = 313      icmpInBadRedirects    = 5
icmpInEchos          = 477      icmpInEchoReps       = 20
icmpInTimestamps     = 0        icmpInTimestampReps  = 0
icmpInAddrMasks      = 0        icmpInAddrMaskReps   = 0
icmpInFragNeeded     = 0        icmpOutMsgs          = 827
icmpOutDrops         = 103      icmpOutErrors         = 0
icmpOutDestUnreachs  = 94       icmpOutTimeExcds     = 256
icmpOutParmProbs     = 0        icmpOutSrcQuenchs    = 0
icmpOutRedirects     = 0        icmpOutEchos         = 0
icmpOutEchoReps      = 477      icmpOutTimestamps    = 0
icmpOutTimestampReps= 0        icmpOutAddrMasks     = 0
icmpOutAddrMaskReps = 0        icmpOutFragNeeded    = 0
icmpInOverflows      = 0

```

```

IGMP:
0 messages received
0 messages received with too few bytes
0 messages received with bad checksum
0 membership queries received
0 membership queries received with invalid field(s)
0 membership reports received
0 membership reports received with invalid field(s)
0 membership reports received for groups to which we belong
0 membership reports sent

```

El siguiente ejemplo muestra la salida del comando `netstat - r`, que muestra la tabla de enrutamiento IP.

```

Routing Table:
Destination      Gateway          Flags  Ref    Use  Interface

```

localhost	localhost	UH	0	2817	lo0
earth-bb	pluto	U	3	14293	eri0
224.0.0.0	pluto	U	3	0	eri0
default	mars-gate	UG	0	14142	

Los campos del informe netstat - r se describen en la siguiente tabla.

TABLA 30-2 Salida del comando netstat - r

Nombre de campo		Descripción
Flags	U	La ruta está activa.
	G	La ruta es a través de una puerta de enlace.
	H	La ruta es a un host.
	D	La ruta se creó de manera dinámica mediante una redirección.
Ref		Muestra la cantidad actual de rutas que comparten la misma capa de enlace.
Use		Indica la cantidad de paquetes que se enviaron.
Interface		Muestra la interfaz de red que se utiliza para la ruta.

## Cómo mostrar estadísticas de servidor y cliente NFS

El servicio de archivos distribuido NFS utiliza una utilidad de llamada a procedimiento remoto (RPC) que traduce los comandos locales en solicitudes para el host remoto. Las llamadas a procedimientos remotos son síncronas. La aplicación cliente se bloquea o se suspende hasta que el servidor completa la llamada y devuelve los resultados. Uno de los principales factores que afecta el rendimiento de NFS es la tasa de retransmisión.

Si el servidor de archivos no puede responder la solicitud de un cliente, el cliente vuelve a transmitir la solicitud una determinada cantidad de veces antes de abandonar el proceso. Cada retransmisión genera una sobrecarga en el sistema y aumenta el tráfico de la red. Las retransmisiones excesivas pueden provocar problemas de rendimiento en la red. Si la tasa de retransmisión es alta, puede comprobar si existen:

- Servidores sobrecargados que completan las solicitudes con demasiada lentitud.
- Una interfaz Ethernet que descarta paquetes.
- Congestión en la red, que ralentiza la transmisión de paquetes.

La siguiente tabla describe las opciones nfsstat para mostrar estadísticas de cliente y servidor.

TABLA 30-3 Comandos para mostrar estadísticas de cliente/servidor

Comando	Visualización
<code>nfsstat -c</code>	Estadísticas de cliente
<code>nfsstat -s</code>	Estadísticas de servidor
<code>netstat -m</code>	Estadísticas de red para cada sistema de archivos

Utilice el comando `nfsstat -c` para mostrar estadísticas de cliente y `nfsstat -s` para mostrar estadísticas de servidor. Utilice `netstat -m` para mostrar estadísticas de red para cada sistema de archivos. Para obtener más información, consulte [nfsstat\(1M\)](#).

### Ejemplos: Visualización de estadísticas de servidor y cliente NFS

El siguiente ejemplo muestra datos sobre RPC y NFS para el cliente `pluto`.

```
$ nfsstat -c

Client rpc:
Connection oriented:
calls      badcalls  badxids  timeouts  newcreds  badverfs  timers
1595799    1511      59       297       0         0         0
cantconn   nomem     interrupts
1198      0         7
Connectionless:
calls      badcalls  retrans  badxids  timeouts  newcreds  badverfs
80785     3135     25029   193      9543     0         0
timers     nomem     cantsend
17399     0        0

Client nfs:
calls      badcalls  clgets   cltoomany
1640097    3112     1640097  0
Version 2: (46366 calls)
null       getattr  setattr  root      lookup    readlink  read
0 0%       6589 14%  2202 4%   0 0%      11506 24%  0 0%      7654 16%
wrcache    write    create   remove    rename    link      symlink
0 0%       13297 28%  1081 2%   0 0%      0 0%      0 0%
mkdir      rmdir    readdir  statfs
24 0%      0 0%    906 1%   3107 6%
Version 3: (1585571 calls)
null       getattr  setattr  lookup    access    readlink  read
0 0%       508406 32%  10209 0%  263441 16%  400845 25%  3065 0%  117959 7%
write      create   mkdir    symlink    mknod     remove    rmdir
69201 4%   7615 0%   42 0%    16 0%     0 0%      7875 0%  51 0%
rename     link     readdir  readdir+   fsstat    fsinfo    pathconf
929 0%    597 0%   3986 0%  185145 11%  942 0%    300 0%  583 0%
commit
4364 0%

Client nfs_acl:
Version 2: (3105 calls)
null       getacl   setacl   getattr  access
```

```
0 0%      0 0%      0 0%      3105 100%  0 0%
Version 3: (5055 calls)
null      getacl    setacl
0 0%      5055 100%  0 0%
```

La salida del comando `nfsstat -c` se describe en la siguiente tabla.

TABLA 30-4 Salida del comando `nfsstat -c`

Campo	Descripción
calls	Cantidad total de llamadas enviadas.
badcalls	Cantidad total de llamadas rechazadas por RPC.
retrans	Cantidad total de retransmisiones. Para este cliente, la cantidad de retransmisiones es menor que el 1% o aproximadamente 10 tiempos de espera agotados en un total de 6888 llamadas. Estas retransmisiones pueden ser causa de fallas temporales. Las tasas superiores pueden indicar un problema.
badxid	Cantidad de veces que se recibió una confirmación duplicada para una única solicitud NFS.
timeout	Cantidad de llamadas con tiempo de espera agotado.
wait	Cantidad de veces que una llamada tuvo que esperar porque no había ningún identificador de clientes disponible.
newcred	Cantidad de veces que se tuvo que actualizar la información de autenticación.
timers	Cantidad de veces que el valor de tiempo de espera fue superior o igual al valor de tiempo de espera especificado para una llamada.
readlink	Cantidad de veces que se realizó una operación <code>read</code> en un enlace simbólico. Si este número es alto, superior al 10%, es posible que haya demasiados enlaces simbólicos.

El siguiente ejemplo muestra la salida del comando `nfsstat -m`.

```
pluto$ nfsstat -m
/usr/man from pluto:/export/svr4/man
Flags: vers=2,proto=udp,auth=unix,hard,intr,dynamic,
      rsize=8192, wsize=8192,retrans=5
Lookups: srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
All:      srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
```

Esta salida del comando `nfsstat -m`, que se muestra en milisegundos, se describe en la siguiente tabla.

TABLA 30-5 Salida del comando `nfsstat -m`

Campo	Descripción
srtt	Promedio ajustado de los tiempos de ida y vuelta

TABLA 30-5 Salida del comando `nfsstat -m` (Continuación)

Campo	Descripción
dev	Desviaciones promedio
cur	Tiempo de respuesta “esperado” actual

Si sospecha que los componentes de hardware de la red están creando problemas, debe examinar detenidamente los cables y los conectores.



# Glosario

---

<b>adaptador de terminal (TA) RDSI</b>	Dispositivo de adaptación de señal que proporciona una interfaz similar a un módem para un enlace PPP por marcación telefónica a través de una red RDSI. Se utilizan los mismos archivos de configuración de Solaris PPP 4.0 para configurar un TA RDSI que para configurar un módem estándar.
<b>agente de directorio (DA)</b>	Es un agente SLP opcional que almacena y mantiene una antememoria de avisos de servicios enviados por el agente de servicio (SA). Cuando se implementa, el DA resuelve las solicitudes de servicio del agente de usuario (UA). El DA responde a las solicitudes activas del SA y el UA para los avisos del directorio. Como resultado, el SA y el UA detectan los DA asociados y los <i>alcances</i> . Un DA envía avisos no solicitados periódicos a través de los cuales el UA y el SA detectan el DA dentro de alcances compartidos.
<b>Agente de Servicio (SA)</b>	El agente SLP que mantiene avisos de servicios para los servicios conectados en red. Si no hay ningún DA disponible, el SA responde las solicitudes de servicio de multidifusión de los UA. Si un DA está disponible, el SA registra servicios con DA que admitan sus ámbitos y, opcionalmente, anula su registro.
<b>agente de usuario (UA)</b>	El agente SLP que actúa en nombre de la aplicación del usuario. El agente consulta la identidad de los ámbitos, agentes de directorio y anuncios de servicios correspondientes.
<b>ámbito</b>	Una agrupación de UA y SA que se organizan administrativamente, topológicamente o de alguna otra manera. Puede utilizar ámbitos para modificar cómo suministrar acceso a los servicios en la empresa.
<b>asppp</b>	Una versión de PPP que estaba incluida en el sistema operativo desde la versión Solaris 2.4 hasta la versión Solaris 8. asppp sólo admitía comunicaciones PPP asíncronas.
<b>autenticación</b>	El acto de verificar la identidad suministrada a través de la red por un usuario o una entidad remotos, como un programa. Algunos protocolos de autenticación le permiten crear bases de datos de credenciales de autenticación de usuarios potenciales. Otros protocolos de autenticación utilizan cadenas de certificados de confianza generadas mediante una autoridad de certificación a efectos de autenticación. Estas credenciales pueden autenticar a los usuarios cuando intentan comunicarse con usted o utilizar los servicios de su sitio.
<b>avisos de servicios</b>	Información que distribuye un SA que describe un servicio. Un anuncio de servicio consta de una dirección URL y una recopilación de pares de listas de valores o atributos que describen un servicio. Todos los avisos de servicios tienen una duración. Después de que termina la duración, un anuncio de servicio ya no es válido a menos que se vuelva a registrar.
<b>CHAP</b>	El protocolo de autenticación por reconocimiento de demanda (CHAP) es un protocolo de autenticación que se puede utilizar para verificar la identidad de un emisor de llamada en un enlace PPP. La autenticación CHAP utiliza la noción de <i>demanda y respuesta</i> , por lo que el equipo que recibe una llamada demanda al emisor de la llamada que demuestre su identidad.

Consulte también el [protocolo de autenticación de contraseña \(PAP\)](#).

**contabilidad ampliada**

Una manera flexible de registrar el consumo de recursos por tareas o procesos.

**CSU/DSU**

Un dispositivo de telecomunicaciones síncrono que combina los dispositivos CSU y DSU, y se utiliza en un enlace PPP de línea arrendada. El dispositivo CSU/DSU transfiere las señales de un igual a una línea arrendada. La mayoría de los dispositivos CSU/DSU no necesitan una secuencia de comandos de chat para establecer el enlace. Los dispositivos CSU/DSU a menudo son configurados por el proveedor de la línea arrendada.

Consulte también [unidad de servicio de canal \(CSU\)](#) y [unidad de servicio de datos \(DSU\)](#).

**daemon SLP (slpd)**

El proceso de daemon que actúa como un servidor SA o DA en la implementación de Oracle Solaris de SLP. Los procesos de servicio en el host registran los anuncios de servicio con `slpd` en lugar de mantener los anuncios individualmente. Cada proceso contiene una biblioteca de cliente de SA que se comunica con `slpd` cuando el daemon se configura como servidor de SA. El daemon SLP reenvía todos los registros y las anulaciones de registros a los DA. El daemon agota los anuncios de servicio caducados y mantiene una tabla de los DA disponibles realizando una detección activa y pasiva. Mediante estos mecanismos, la información de DA se proporciona a los clientes UA. Los clientes UA usan `slpd` en un host sólo para la información de DA. Si lo prefiere, puede configurar `slpd` como un DA.

**difusión**

Un procedimiento de capa de enlace de datos que se utiliza para transmitir paquetes a todos los equipos en una subred. Los paquetes de difusión, por lo general, no son enviados más allá de la subred.

**emisores de llamadas de confianza**

En PPP, los iguales remotos a los cuales un servidor de marcación de entrada concede acceso incluyendo las credenciales de seguridad de los iguales en las bases de datos de los secretos de CHAP o PAP del servidor.

**enlace**

En PPP, la conexión de comunicaciones que se ha negociado y establecido entre dos iguales. Solaris PPP 4.0 admite dos tipos de enlaces: por marcación telefónica y línea arrendada.

**enlace PPP de línea arrendada**

Conexión PPP que implica un host y un CSU/DSU conectados a un medio de red síncrona arrendado de un proveedor. OC3 y T1 son ejemplos comunes de medios de línea arrendada. Si bien son más fáciles de administrar, los enlaces de líneas arrendadas son más costosos que los enlaces PPP por marcación telefónica y, por lo tanto, son menos comunes.

**enlace PPP por marcación telefónica**

Una conexión PPP que afecta a un igual y un módem al final de una línea telefónica o un medio de comunicación similar, como un medio proporcionado por RDSI. El término “marcación” hace referencia a la secuencia en la negociación del enlace cuando el módem local llama al igual remoto mediante el número de teléfono del igual. El enlace por marcación telefónica es la configuración PPP más común y menos costosa.

**equipo de marcación de salida**

Es el igual que inicia la llamada para establecer un enlace PPO por marcación telefónica. Una vez configurado, el equipo de marcación de salida puede invocar cualquier número de servidores de marcación de entrada. El equipo de marcación de salida, por lo general, proporciona credenciales de autenticación antes de que pueda establecerse el enlace por marcación telefónica.



<b>expect-send</b>	Un formato de secuencia de comandos que se utiliza en secuencias de comandos de chat PPP y UUCP. La secuencia de comandos de chat comienza con el texto o la instrucción <i>esperar</i> ( <i>expect</i> ) desde el igual remoto. La siguiente línea contiene la respuesta que se <i>enviará</i> ( <i>sent</i> ) desde el host local después de que reciba la cadena expect correcta desde el igual. Las líneas siguientes repiten las instrucciones expect-send entre el host local y el igual hasta que todas las instrucciones necesarias para establecer comunicaciones se negocien correctamente.
<b>igual</b>	En PPP, un equipo individual en un extremo de un enlace de comunicaciones PPP, que consta de dos iguales conectados por un medio de comunicaciones. Puede configurar muchos tipos de equipos informáticos como iguales, como una estación de trabajo, un equipo personal, un enrutador o un mainframe.
<b>Microsoft CHAP (MS-CHAP)</b>	Un protocolo de autenticación para PPP de Microsoft. Solaris PPP 4.0 admite las versiones 1 y 2 de este protocolo en el modo de cliente y de servidor.
<b>multidifusión</b>	Un procedimiento de capa de red que se utiliza para enviar paquetes de datagramas en varios equipos en una red IP. Los paquetes no son manejados por cada equipo, como ocurre con el enrutamiento de datagramas. La multidifusión requiere que los enrutadores se configuren con protocolos de enrutamiento especiales.
<b>PPP a través de Ethernet (PPPoE)</b>	Un protocolo de RedBack Networks que permite a los hosts ejecutar sesiones PPP sobre un enlace Ethernet. PPPoE se suele utilizar con los servicios de línea de suscripción digital (DSL).
<b>PPP asíncrono</b>	Una forma de PPP que se ejecuta en líneas de serie asíncronas, que transfieren datos un carácter a la vez. La forma más común de configuración de PPP, el enlace por marcación telefónica, utiliza comunicaciones PPP asíncronas.
<b>PPP síncrono</b>	Una forma de PPP que se ejecuta en líneas digitales síncronas, que transfieren datos como un flujo continuo de bits básicos. El enlace de línea arrendada PPP utiliza PPP síncrono.
<b>protocolo de autenticación de contraseña (PAP)</b>	Un protocolo de autenticación que se puede utilizar para verificar la identidad de un emisor de llamada en un enlace PPP. PAP utiliza una contraseña no cifrada que se transfiere al enlace, lo que hace posible almacenar la contraseña en uno de los equipos de punto final. Por ejemplo, PAP puede utilizar las entradas de inicio de sesión y contraseña en la base de datos de UNIX passwd del equipo que recibe una llamada para verificar la identidad del emisor de la llamada.  Consulte también <a href="#">CHAP</a> .
<b>protocolo de control de compresión (CCP)</b>	Un subprotocolo de PPP que negocia el uso de compresión de datos en el enlace. A diferencia de la compresión de encabezado, CCP comprime todos los datos en los paquetes que se envían en el enlace.
<b>protocolo de control de devolución de llamadas (CBCP)</b>	Una extensión PPP de Microsoft que se utiliza para negociar una sesión de devolución de llamadas. Solaris PPP 4.0 sólo admite la parte del cliente (emisor de llamada inicial) de este protocolo.

<b>protocolo de control de enlace (LCP)</b>	Un subprotocolo de PPP que se utiliza para negociar el conjunto inicial de parámetros de enlace entre los iguales. Parte de la función de LCP es probar la integridad del enlace, por lo que tantos problemas relacionados con enlaces se manifiestan como fallos de LCP.
<b>protocolo de control de protocolo de internet (IPCP)</b>	Un subprotocolo de PPP que negocia las direcciones IP de los iguales en el enlace. IPCP también negocia la compresión de encabezado para el enlace y permite el uso de los protocolos de capa de red.
<b>protocolo de control versión 6 de protocolo de Internet (IPV6CP)</b>	Consulte <a href="#">protocolo de control de protocolo de internet (IPCP)</a> .
<b>protocolo punto a punto (PPP)</b>	<p>Un protocolo de capa de enlace de datos que proporciona un método estándar para transferir datagramas por medios punto a punto. Una configuración PPP consta de dos equipos de punto final llamados <i>iguales</i> y las líneas telefónicas u otro enlace bidireccional que los iguales utilicen para las comunicaciones. La conexión de software y hardware entre los dos iguales se considera el <i>enlace PPP</i>.</p> <p>PPP se compone de un número de subprotocolos, incluidos PAP, CHAP, LCP y CCP. Hay numerosas implementaciones de PPP disponibles.</p>
<b>secreto de CHAP</b>	Una serie ASCII o cadena binaria que se utiliza para fines de identificación y es conocida por ambos iguales en un enlace PPP. El secreto de CHAP se almacena como texto sin cifrar en un archivo <code>/etc/ppp/chap-secrets</code> del sistema, pero nunca se envía a través del enlace PPP, ni siquiera en formato cifrado. El protocolo CHAP verifica que un hash del secreto de CHAP utilizado por un emisor de llamada coincida con un hash de la entrada del secreto de CHAP del emisor de la llamada en el archivo <code>/etc/ppp/chap-secrets</code> del destinatario.
<b>secuencia de comandos de chat</b>	Instrucciones que le indican a un módem la forma de establecer un enlace de comunicaciones entre en sí mismo y un igual remoto. Tanto los protocolos PPP como los UUCP emplean secuencias de comandos de chat para establecer los enlaces por marcación telefónica y las llamadas de respuesta.
<b>servicios antiguos</b>	Servicio de red que no está habilitado para SLP. Puede crear un registro de proxy para registrar un servicio antiguo con SLP. Los clientes basados en SLP pueden descubrir servicios antiguos (consulte el <a href="#">Capítulo 10, “Incorporación de servicios antiguos”</a> ).
<b>servidor de marcación de entrada</b>	El igual que negocia y establece el destinatario final de un enlace por marcación telefónica después de recibir una llamada de un equipo de marcación de salida. Aunque suele utilizarse el término “servidor de marcación de entrada”, el servidor de marcación de entrada no funciona de acuerdo con el paradigma cliente-servidor. En su lugar, simplemente es el igual que responde a la solicitud para configurar un enlace por marcación telefónica. Después de que se ha configurado, un servidor de marcación de entrada puede recibir llamadas de cualquier cantidad de equipos de marcación de salida.
<b>unidad de servicio de canal (CSU)</b>	Un dispositivo de telecomunicaciones síncrono que proporciona una interfaz local a una línea de telecomunicaciones arrendada y termina la línea. En los Estados Unidos, una CSU termina una línea T1 y proporciona una interfaz DS1 o DSX. Internacionalmente, la CSU suele ser propiedad de la compañía telefónica proveedora.

Consulte también [CSU/DSU](#) y [unidad de servicio de datos \(DSU\)](#).

**unidad de servicio de datos (DSU)** Un dispositivo de telecomunicaciones síncrono que se utiliza en un enlace PPP de línea arrendada. El dispositivo DSU convierte formatos de estructura de datos utilizados en líneas de telecomunicaciones y proporciona una interfaz de datos de comunicaciones estándar.

Consulte también [unidad de servicio de canal \(CSU\)](#) y [CSU/DSU](#).

**URL de servicio** Una dirección URL que se utiliza para anunciar la ubicación de red de los servicios. La dirección URL contiene el tipo de servicio, el nombre de host o la dirección de red del host de servicio. La dirección URL también puede contener un número de puerto y otro tipo de información necesaria para utilizar el servicio.



# Índice

---

## Números y símbolos

- \* (asterisco), en mapas autofs, 225
- / (barra diagonal)
  - /- como punto de montaje de mapa maestro, 206, 209
- directorio root
  - montaje de clientes sin disco, 77
  - nombres de mapa maestro precedidos por, 206
- \ (barra diagonal inversa) en mapas, 207, 209, 210
- (guión)
  - abreviatura de código de marcación, 579
  - en nombres de mapas autofs, 220
  - marcador de posición del campo Line2, 585
  - marcador de posición del campo Speed, 578
- .(punto)
  - sintaxis de comando rcp, 671, 673
- # (signo de almohadilla)
  - comentarios en mapa maestro (auto\_master), 207
  - comentarios en mapas directos, 209
  - comentarios en mapas indirectos, 210
- = (signo igual), abreviatura de código de marcación, 579
- + (signo más)
  - en nombres de mapas autofs, 220, 221
  - sintaxis de archivo /etc/hosts.equiv, 655, 656
- ~ (tilde)
  - nombres de ruta abreviados, 669, 670
  - sintaxis de comando rcp, 671, 673
- & (Y comercial), en mapas autofs, 224

## A

- abreviaturas de código de marcación, 563, 578
- Acelerador y antememoria de red, *Ver* NCA
- ACL NFS
  - descripción, 80, 192–194
- activación
  - comprobación de eco, 591
  - habilitación de devolución de llamada por medio de la secuencia de comandos de chat, 581
- administración NFS, responsabilidades de
  - administrador, 86
- administrador de bloqueo de red, 81
- agente de directorio (SLP)
  - arquitectura del SLP y, 230
  - congestión de red y, 248–249
  - cuándo implementar, 263
  - direcciones de DA, 245
  - dónde colocar, 264–265
  - equilibrio de carga, 264–265
- agente de entrega local, servicios de correo, 344
- agente de servicio (SLP), 245, 249
- agente de usuario (SLP), 245
- agente de usuario de correo /usr/dt/bin/dtmail, 361
- agente de usuario de correo dtmail, 361
- agentes de transferencia de correo, 344
- agentes de usuario de correo, 343–344
- ajuste del rendimiento del SLP, 249
- alias
  - archivo /etc/mail/aliases, 368
  - bucles, 333
  - creación, 350
  - definición, 350

**alias** (*Continuación*)

- mapa aliases NIS, 369
  - tabla mail\_aliases NIS+, 369
  - verificar, 333
- alias .mailrc, 367
- alias postmaster, crear, 322
- ámbitos (SLP)
- ámbito default, 260
  - consideraciones, 259–260
  - cuándo configurar, 259
  - DA y, 247, 262
  - definición, 229
  - hosts múltiples y, 269
  - implementación, 258–261
  - registro del proxy y, 272
- antememoria local y NFS versión 3, 78
- antememoria y NFS versión 3, 78
- anular uso compartido y volver a compartir, NFS
- versión 4, 184
- anuncio de servicio (SLP), 249
- anuncios de proxy (SLP), 271, 273
- anuncios de servicios (SLP), 273
- apertura de conexiones de sistema remoto, 663, 664
- API de filtro de correo MILTER, 341–342
- aplicación de correo
- integrado (sendmail)
  - [TCP] y [IPC], 403
- aplicaciones, colgado, 137
- aplicaciones de CD-ROM, acceso con autofs, 112
- aplicaciones de correo, definición, 344
- archivo /dev/nca, NCA y, 62
- archivo /etc/auto\_direct, 297
- archivo /etc/default/autofs, 141
- configuración de entorno autofs, 108
- archivo /etc/default/nfs, 79
- archivo /etc/default/nfs, palabras clave para, 142
- archivo /etc/default/nfslogd, 142–143
- archivo /etc/default/sendmail, 372
- archivo /etc/dfs/dfstab
- deshabilitación de acceso de montaje para un cliente, 94
  - habilitación de inicio de sesión de servidor NFS, 89
  - habilitación de NFS seguro, 103
  - habilitación de servicio WebNFS, 88

**archivo /etc/dfs/dfstab** (*Continuación*)

- opción de NFS seguro, 103
  - uso compartido de sistema de archivos
    - automático, 87
- archivo /etc/hostname. *interfaz*, NCA y, 63
- archivo /etc/hosts, 63, 292, 293
- archivo /etc/hosts.equiv, 655, 656
- archivo /etc/inet/ntp.client, 70
- archivo /etc/inet/ntp.conf, 69
- archivo /etc/inet/ntp.keys, 70
- archivo /etc/inet/ntp.server, 70
- archivo /etc/inet/services, comprobación del UUCP, 570
- archivo /etc/inet/slp.conf
- anuncios del DA, 246
  - cambio de configuración, 243
  - cambio de interfaces, 267
  - con DA estáticos, 245
  - descripción general, 235
  - elementos, 242
  - enrutamiento de sólo difusión, 253
  - equilibrio de carga, 265
  - implementar DA, 263
  - latido del DA, 248
  - límite de espera aleatoria, 257
  - nuevos ámbitos, 258, 260
  - registro del proxy, 273
  - reregistros de SA, 250
  - tamaño de paquete, 252
  - tiempos de espera, 255
  - time-to-live de multidifusión, 251
- archivo /etc/mail/aliases, 348, 356, 367, 368
- UUCP y, 571
- archivo /etc/mail/aliases.db, 321, 356
- archivo /etc/mail/aliases.dir, 321, 356
- archivo /etc/mail/aliases.pag, 321, 356
- archivo /etc/mail/cf/cf/main.cf, 358
- archivo /etc/mail/cf/cf/main.mc, 358
- archivo /etc/mail/cf/cf/Makefile, 358
- archivo /etc/mail/cf/cf/sendmail.mc, 358
- archivo /etc/mail/cf/cf/submit.cf, 358
- archivo /etc/mail/cf/cf/submit.mc, 358
- archivo /etc/mail/cf/cf/subsidiary.cf, 358
- archivo /etc/mail/cf/cf/subsidiary.mc, 358

- archivo /etc/mail/cf/domain/generic.m4, 359
- archivo
  - /etc/mail/cf/domain/solaris-antispam.m4, 359
- archivo
  - /etc/mail/cf/domain/solaris-generic.m4, 359
- archivo /etc/mail/cf/main-v7sun.mc, 359
- archivo /etc/mail/cf/ostype/solaris2.m4, 359
- archivo /etc/mail/cf/ostype/solaris2.ml.m4, 359
- archivo
  - /etc/mail/cf/ostype/solaris2.pre5.m4, 359
- archivo /etc/mail/cf/ostype/solaris8.m4, 359
- archivo /etc/mail/cf/README, 358
- archivo /etc/mail/cf/subsidiary-v7sun.mc, 359
- archivo /etc/mail/helpfile, 357, 405
- archivo /etc/mail/local-host-names, 357, 405
- archivo /etc/mail/Mail.rc, 356
- archivo /etc/mail/mailx.rc, 356
- archivo /etc/mail/main.cf, 356
- archivo /etc/mail/relay-domains, 357
- archivo /etc/mail/sendmail.cf, 357
- archivo /etc/mail/sendmail.ct, 405
- archivo /etc/mail/sendmail.cw, 405
- archivo /etc/mail/sendmail.hf, 405
- archivo /etc/mail/sendmail.pid, 357
- archivo /etc/mail/statistics, 357
- archivo /etc/mail/submit.cf, 357, 389
- archivo /etc/mail/subsidiary.cf, 292, 357
- archivo /etc/mail/trusted-users, 357, 405
- archivo /etc/mnttab
  - comparación con mapa auto\_master, 212
  - creación, 175
- archivo /etc/nca/nca.if, 63
- archivo /etc/nca/ncakmod.conf, 63
- archivo /etc/nca/ncalogd.conf, 63
- archivo /etc/nca/ncaport.conf, 63
- archivo /etc/netconfig, descripción, 140
- archivo /etc/nfs/nfslog.conf, 143–145
  - habilitación de inicio de sesión de servidor NFS, 89
- archivo /etc/nsswitch.conf, 302, 655
- archivo /etc/passwd
  - ftp y, 662
  - habilitación de inicios de sesión del UUCP, 566
- archivo /etc/ppp/chap-secrets
  - creación
    - para emisores de llamadas de confianza, 479
  - definición, 510
  - direccionamiento
    - estático, 539
    - por número de unidad sPPP, 540
  - ejemplo, para un servidor de acceso PPPoE, 548
  - sintaxis, 536
- archivo /etc/ppp/options
  - creación
    - para un equipo de marcación de salida, 447–448
    - para un servidor de marcación de entrada, 456
  - definición, 510, 514
  - ejemplo PPPoE, 547
  - lista de ejemplos, 515
  - modificación para autenticación PAP, 473
  - plantilla /etc/ppp/options.tmpl, 514
  - privilegios, 512
- archivo /etc/ppp/options.nombre de tty
  - definición, 510, 515
  - direccionamiento dinámico, 538
  - lista de ejemplos, 517
  - para un equipo de marcación de salida, 448, 516
  - para un servidor de marcación de entrada, 456, 516
  - privilegios, 512
- archivo /etc/ppp/pap-secrets
  - creación
    - para un servidor de acceso PPPoE, 488
  - creación para emisores de llamadas de confianza, 471
  - definición, 510
  - direccionamiento
    - estático, 539
    - por número de unidad sPPP, 540
  - ejemplo, para un servidor de acceso PPPoE, 548
  - sintaxis, 533
- archivo /etc/ppp/peers/nombre de igual
  - creación
    - para un punto final en un enlace de línea arrendada, 462
  - definición, 510, 519–520
  - ejemplo, para un cliente PPPoE, 549
  - lista de ejemplos, 521

archivo /etc/ppp/peers/*nombre de igual*  
(Continuación)

modificación

para autenticación PAP, 473

para un cliente PPPoE, 484

opciones útiles, 519

privilegios, 512

archivo /etc/ppp/pppoe

ejemplo, 545, 546

enumeración de servicios, 486

modificación, 487

sintaxis, 544

archivo /etc/ppp/pppoe.*dispositivo*

definición, 546

para un servidor de acceso, 488

sintaxis, 546

archivo /etc/ppp/pppoe.if

creación

en un cliente PPPoE, 483

para un servidor de acceso, 486

definición, 542

ejemplo, 542

archivo /etc/.rootkey

habilitación de NFS seguro, 103

archivo /etc/services, entradas nfsd, 133

archivo /etc/shells, 330

archivo /etc/syslog.conf, 335

archivo /etc/uucp/Config

descripción, 563, 605

formato, 605

archivo /etc/uucp/Devconfig

descripción, 563, 608

formato, 608

archivo /etc/uucp/Devices

campo Class, 585

campo Dialer-Token-Pairs, 586, 588

campo Line, 585

campo Line2, 585

campo Speed del archivo Systems y, 578

campo Type, 583

campo Type del archivo Systems y, 584

definiciones de protocolo, 588, 589

descripción, 563, 583

ejemplo, para una configuración asppp, 553

archivo /etc/uucp/Devices (Continuación)

formato, 583

archivo /etc/uucp/Dialcodes, 563, 594

archivo /etc/uucp/Dialers

descripción, 563, 589

ejemplo, 590

ejemplo, para configuración asppp, 553

archivo /etc/uucp/Grades

campo ID-list, 607, 608

campo Job-size, 607

campo Permit-type, 607

campo System-job-grade, 606, 607

campo User-job-grade, 606

descripción, 563, 605

nivel predeterminado, 606

palabras clave, 606, 607

archivo /etc/uucp/Limits

descripción, 563, 609

formato, 609

archivo /etc/uucp/Permissions

comando uucheck y, 562

configuración de seguridad, 570

consideraciones, 597

daemon uuxqt y, 560

descripción, 563, 596

estructuración de entradas, 596

formato, 596

LOGNAME

combinación con MACHINE, 604

descripción, 597

ID de inicio de sesión para equipos remotos, 597

MACHINE

combinación con LOGNAME, 604

descripción, 597

opción OTHER, 603

permisos o restricciones predeterminados, 597

modificación del nombre de nodo, 598

opción CALLBACK, 600

opción COMMANDS, 600, 602, 604

opción MYNAME, 598

opción NOREAD, 600

opción NOWRITE, 600

opción OTHER, 603

opción READ, 599



- archivo /etc/uucp/Permissions (*Continuación*)
  - opción REQUEST, 597
  - opción SENDFILES, 598
  - opción VALIDATE, 602, 603
  - opción WRITE, 599
  - operación de reenvío, 604
  - permisos de devolución de llamada, 600
  - permisos de ejecución remota, 600, 603
  - permisos de transferencia de archivos, 597, 600
- archivo /etc/uucp/Pol1
  - descripción, 563, 605
  - formato, 605
- archivo /etc/uucp/Sysfiles
  - descripción, 563, 595
  - ejemplos, 595
  - formato, 595
  - impresión de listas de Systems, 596
- archivo /etc/uucp/Sysname, 563, 596
- archivo /etc/uucp/Systems
  - abreviaturas de código de marcación, 563
  - campo Chat Script, 579, 581
  - campo Class del archivo Devices y, 585
  - campo Phone, 578
  - campo Speed, 578
  - campo System-Name, 576
  - campo Time
    - descripción, 577
    - entrada Never, 598
  - campo Type, 578
  - campo Type del archivo Devices y, 584
  - caracteres de escape, 580
  - configuración de paridad, 582
  - configuración del TCP/IP, 569, 570
  - control de flujo de hardware, 582
  - descripción, 563, 575
  - ejemplo, para una configuración asppp, 552
  - formato, 576
  - resolución de problemas, 574
  - varios o diferentes archivos, 563, 575, 595
- archivo /etc/vfstab
  - conmutación por error del lado del cliente, 94
  - montaje de clientes sin disco, 77
  - montaje de sistemas de archivos al momento del inicio, 91
- archivo /etc/vfstab (*Continuación*)
  - opción nolargefiles, 93
  - servidores NFS y, 91
- archivo .forward+detail, 371
- archivo /kernel/fs, comprobación, 140
- archivo .mailrc, 351
- archivo .ppprc
  - creación, 455
  - definición, 510
  - privilegios, 512
- archivo /var/mail, 348
- archivo /var/nca/log, 64
- archivo /var/ntp/ntp.drift, 70
- archivo /var/run/nca\_httpd\_1.door, 64
- archivo /var/run/sendmail.pid, 361
- archivo aliases, 356, 571
- archivo aliases.db, 321, 356
- archivo aliases.dir, 321, 356
- archivo aliases.pag, 321, 356
- archivo auto\_direct, 297
- archivo crontab, para UUCP, 567
- archivo de alias de correo local, configurar, 320
- archivo de claves, NTP, 70
- archivo de configuración /etc/asppp.cf, 551
- archivo de desfase, 70
- archivo de mapa con clave, crear, 321
- archivo de registro, para NCA, 64
- archivo de registro NCA, 64
- archivo de registro pppdebug, 504
- archivo Devconfig
  - descripción, 563, 608
  - formato, 608
- archivo Devices
  - campo Class, 585
  - campo Dialer-Token-Pairs, 586, 588
  - campo Line, 585
  - campo Line2, 585
  - campo Speed del archivo Systems y, 578
  - campo Type, 583
  - campo Type del archivo Systems y, 584
  - definiciones de protocolo, 588, 589
  - descripción, 563, 583
  - formato, 583
  - varios o diferentes archivos, 595

- archivo `dfstab`
  - deshabilitación de acceso de montaje para un cliente, 94
  - habilitación de inicio de sesión de servidor NFS, 89
  - habilitación de NFS seguro, 103
  - habilitación de servicio WebNFS, 88
  - opción de NFS seguro, 103
  - sintaxis para sistemas de archivos NFS, 87
  - uso compartido de sistema de archivos automático, 87
- archivo `Dialcodes`, 563, 594
- archivo `Dialers`
  - descripción, 563, 589
  - ejemplo, 590
- archivo `/etc/ppp/options`, opción para autenticación CHAP name, 477
- archivo `/etc/ppp/pap-secrets`
  - creación
    - para un servidor de marcación de entrada, 468
- archivo `/etc/vfstab`, comando `automount` y, 212
- archivo `ftp`, WebNFS y, 105
- archivo `generic.m4`, 359
- archivo `Grades`
  - campo `ID-list`, 607, 608
  - campo `Job-size`, 607
  - campo `Permit-type`, 607
  - campo `System-job-grade`, 606, 607
  - campo `User-job-grade`, 606
  - descripción, 563, 605
  - nivel predeterminado, 606
  - palabras clave, 606, 607
- archivo `helpfile`, 357
  - comando `sendmail`, 405
- archivo `hostname.interfaz`, NCA y, 63
- archivo `hosts`, 63
- archivo `hosts.equiv`, 655, 656
- archivo `HTML`, WebNFS y, 105
- archivo `Limits`
  - descripción, 563, 609
  - formato, 609
- archivo `local-host-names`, 357, 405
- archivo `Mail.rc`, 356
- archivo `mailx.rc`, 356
- archivo `main.cf`, 356, 358, 366
- archivo `main.mc`, 358, 405
- archivo `main-v7sun.mc`, 359, 405
- archivo `Makefile`, 358
- archivo `mnttab`
  - comparación con mapa `auto_master`, 212
  - creación, 175
- archivo `nca_httpd_1.door`, 64
- archivo `nca.if`, 63
- archivo `nca.if file`, 53
- archivo `ncakmod.conf`, 53, 56, 63
- archivo `ncalogd.conf`, 54, 56, 63
- archivo `ncaport.conf`, 63
- archivo `netconfig`, descripción, 140
- archivo `nfslog.conf`
  - descripción, 143–145
  - habilitación de inicio de sesión de servidor NFS, 89
- archivo `nfslogd`, 142–143
- archivo `nsswitch.conf`, 302, 655
- archivo `ntp.conf`, 68
- archivo `options` en PPP, 447–448
- archivo `options.ttyname(PPP)`, Ver `/etc/ppp/options.nombre de tty`
- archivo `passwd`, habilitación de inicios de sesión del UUCP, 566
- archivo `Permissions`
  - comando `uucheck` y, 562
  - configuración de seguridad, 570
  - consideraciones, 597
  - daemon `uuxqt` y, 560
  - descripción, 563, 596
  - estructuración de entradas, 596
  - formato, 596
- LOGNAME
  - combinación con `MACHINE`, 604
  - descripción, 597
  - ID de inicio de sesión para equipos remotos, 597
- MACHINE
  - combinación con `LOGNAME`, 604
  - descripción, 597
  - opción `OTHER`, 603
  - permisos o restricciones predeterminados, 597
- modificación del nombre de nodo, 598
- opción `CALLBACK`, 600
- opción `COMMANDS`, 600, 602, 604

---

**archivo Permissions (Continuación)**

- opción MYNAME, 598
- opción NOREAD, 600
- opción NOWRITE, 600
- opción OTHER, 603
- opción READ, 599
- opción REQUEST, 597
- opción SENDFILES, 598
- opción VALIDATE, 602, 603
- opción WRITE, 599
- operación de reenvío, 604
- permisos de devolución de llamada, 600
- permisos de ejecución remota, 600, 603
- permisos de transferencia de archivos, 597, 600

**archivo Permissions de LOGNAME**

- combinación con MACHINE, 604
- descripción, 597
- ID de inicio de sesión para equipos remotos, 597
- opción SENDFILES, 598
- opción VALIDATE, 602, 603

**archivo Permissions de MACHINE**

- combinación con LOGNAME, 604
- descripción, 597
- opción COMMANDS, 600, 602
- opción OTHER, 603
- permisos o restricciones predeterminados, 597

**archivo Poll**

- descripción, 563, 605
- formato, 605

**archivo relay-domains, 357****archivo remote.unknown, 609****archivo secrets para PPP, Ver archivo**

/etc/ppp/pap-secrets

**archivo sendmail.cf, 357**

- aplicaciones de correo, descripción, 344
- configuración alternativa para, 312–313
- configuración de proveedor, 342
- descripción, 365–366
- dominios de correo y, 374
- generar el archivo de configuración, 303
- hosts de correo y, 366
- nivel de versión, 342
- niveles de registro, 366
- puertas de enlace del correo y, 353

**archivo sendmail.cf (Continuación)**

- servidores de correo y, 366
- archivo sendmail.ct, 405
- archivo sendmail.cw, 405
- archivo sendmail.hf, 405
- archivo sendmail.mc, 358
- archivo sendmail.pid, 357, 361
- archivo sendmail.st, Ver archivo statistics
- archivo slp.conf, comentarios, 243
- archivo slpd.conf, 245, 259–260
- archivo solaris-antispam.m4, 359
- archivo solaris-generic.m4, 329, 330, 359
- archivo solaris2.m4, 359
- archivo solaris2.ml.m4, 359
- archivo solaris2.pre5.m4, 359
- archivo solaris8.m4, 359
- archivo statistics, 357
- archivo submit.cf, 357, 358, 389
- archivo submit.mc, 358
- archivo subsidiary.cf, 292, 357, 358
- archivo subsidiary.mc, 358, 405
- archivo subsidiary-v7sun.mc, 359, 405

**archivo Sysfiles**

- descripción, 563, 595
- ejemplos, 595
- formato, 595
- impresión de listas de Systems, 596

**archivo syslog.conf, 335****archivo Sysname, 563, 596****archivo Systems**

- abreviaturas de código de marcación, 563, 578
- campo Chat Script, 579, 581
- campo Class del archivo Devices y, 585
- campo Phone, 578
- campo Speed, 578
- campo System-Name, 576
- campo Time
  - descripción, 577
  - entrada Never, 598
- campo Type, 578
- campo Type del archivo Devices y, 584
- caracteres de escape, 580
- configuración de paridad, 582
- configuración del TCP/IP, 569, 570

archivo Systems (*Continuación*)

- control de flujo de hardware, 582
  - descripción, 563, 575
  - formato, 576
  - resolución de problemas, 574
  - varios o diferentes archivos, 563, 575, 595
- archivo trusted-users, 357, 405
- archivo uudemond.crontab, 567
- archivo vfstab
- comando automount y, 212
  - habilitación de conmutación por error del lado del cliente, 94
  - montaje de clientes sin disco, 77
  - montaje de sistemas de archivos al momento del inicio, 91
  - opción nolargefiles, 93
  - servidores NFS y, 91
- archivos .forward
- administrar, 328
  - cambiar ruta de búsqueda, 330
  - deshabilitar, 329
  - para usuarios, 370
- archivos .forward.hostname, 371
- archivos .rhosts
- búsqueda, 659
  - descripción, 656
  - eliminación, 659
  - problemas de seguridad, 656
  - proceso de autenticación de sistema remoto, 655, 656–657
- archivos administrativos (UUCP)
- archivos de bloqueo (LCK), 610
  - archivos de datos temporales (TM), 610
  - archivos de trabajo (C.), 610, 611
  - archivos ejecutables (X.), 560, 611
  - limpieza, 569
- archivos de alias de correo
- administrar, 313
  - alias .mailrc, 367
  - archivo /etc/mail/aliases, 367
  - descripción, 367
- archivos de audio, requisitos de espacio en el buzón y, 352
- archivos de bloqueo (LCK) del UUCP, 610

## archivos de configuración

- comando sendmail, 366
  - UUCP, 605
- archivos de creación de publicaciones, requisitos de espacio en el buzón y, 352
- archivos de datos (D.) del UUCP, limpieza, 569
- archivos de datos D. del UUCP, limpieza, 569
- archivos de datos temporales (TM) del UUCP, 610
- archivos de gran tamaño, descripción general, 199
- archivos de plantilla (PPP)
- /etc/ppp/myisp-chat.tmpl, 524–525
  - /etc/ppp/options.tmpl, 514
  - /etc/ppp/peers/myisp.tmpl, 520
  - lista de plantillas, 445
  - options.ttya.tmpl, 517
- archivos de trabajo (C.) del UUCP
- descripción, 610, 611
  - limpieza, 569
- archivos de trabajo C. del UUCP
- descripción, 610, 611
  - limpieza, 569
- archivos DOS, acceso con autofs, 113
- archivos ejecutables (X.) del UUCP
- descripción, 611
  - ejecución de uuxqt, 560
  - limpieza, 569
- archivos ejecutables X. del UUCP
- ejecución de uuxqt, 560
  - limpieza, 569
- archivos grandes
- compatibilidad con NFS, 81
  - inhabilitación de creación de, 93
- archivos locales, actualización de mapas autofs, 109
- archivos MS-DOS, acceso con autofs, 113
- archivos NTP, 69
- archivos PC-DOS, acceso con autofs, 113
- archivos y sistemas de archivos
- acceso autofs
    - sistemas de archivos NFS utilizando CacheFS, 113, 114
    - sistemas de archivos no NFS, 112, 113
  - archivos NFS ASCII y sus funciones, 140
  - archivos NFS y sus funciones, 139

- archivos y sistemas de archivos (*Continuación*)
  - consolidación de archivos relacionados con el proyecto, 116
  - nombres de ruta abreviados, 669, 670
  - selección autofs de archivos, 219
  - selección de archivos de autofs, 216
  - sistemas de archivos definidos, 75
  - sistemas de archivos locales
    - desmontaje de grupos, 167
  - sistemas de archivos remotos
    - desmontaje de grupos, 167
    - lista de clientes con sistemas de archivos montados remotamente, 174
    - montaje desde tabla de sistema de archivos, 167
  - tratamiento NFS de, 75
  - uso compartido automático, 86
- argumento incorrecto especificado con la opción `index`, 133
- asignación de dirección
  - PPP, 539, 540
- asignación de direcciones, PPP, 538
- asignador de puertos, montaje y, 195–196
- asppp, *Ver* PPP asíncrono (asppp)
- asterisco (\*), en mapas autofs, 225
- atributos de archivo y NFS versión 3, 78
- autenticación
  - Ver también* autenticación (PPP)
  - DH, 204
  - inicios de sesión remotos utilizando el comando `ftp`, 662, 663, 664
  - inicios de sesión remotos utilizando el comando `rlogin`, 654, 656, 661
  - archivo `/etc/hosts.equiv`, 655, 656
  - archivos `.rhosts`, 656
  - autenticación de sistema remoto o de red, 654, 656, 657
  - inicios de sesión directos o indirectos, 657
  - resolución de problemas comunes, 507
  - RPC, 203
  - UNIX, 202, 203
- autenticación (PPP)
  - archivo `secrets`
    - para PAP, 468
    - para PPP, 420
- autenticación (PPP) (*Continuación*)
  - autenticado, 420
  - autenticador, 420
  - compatibilidad para líneas arrendadas, 420
  - configuración de base de datos de credenciales de CHAP, 476
  - configuración de CHAP
    - Ver también* Protocolo de autenticación por desafío mutuo (CHAP)
    - equipo de marcación de salida, 480
    - servidor de marcación de entrada, 475, 477
  - configuración de credenciales de CHAP, 478
  - configuración de PAP
    - Ver también* Protocolo de autenticación de contraseña (PAP)
  - diagrama de proceso
    - para PAP, 534
  - ejemplo de CHAP, 436
  - ejemplo de PAP, 434
  - emisores de llamadas de confianza, 420
  - mapas de tareas para configuración, 465–466, 466–467, 474–475
  - planificación, 433, 436
  - política predeterminada, 420
  - requisitos previos antes de configurar, 433
- autenticación de red para inicios de sesión remotos, 654, 656, 657
- autenticación de sistema para inicios de sesión remotos, 654, 655
- autenticación DH
  - autenticación de usuario, 202
  - descripción general, 204
  - NFS seguro y, 102
  - opción de archivo `dfstab`, 103
  - protección con contraseña, 203
- autenticación KERB, NFS y, 82
- autenticación UNIX, 202, 203
- autenticado (PPP), 420
- autenticador (PPP), 420
- autofs
  - acceso a espacio de nombres compartido, 118
  - acceso de sistema de archivos no NFS, 112, 113
  - administración de mapas, 109
  - capacidad de explorar, 84, 121

**autofs** (*Continuación*)

- caracteres especiales, 225
- configuración de servidor de directorio principal, 115
- consolidación de archivos relacionados con el proyecto, 116
- datos de espacio de nombres, 83
- descripción general, 77
- detención, 98
- directorio /home, 114
- funciones, 83
- identificador de archivos público y, 120
- inicio, 98
- mapas
  - capacidad de explorar y, 84
  - directos, 208, 209
  - indirectos, 210, 211
  - inicio del proceso de navegación, 207, 214
  - maestro, 206
  - master, 206
  - navegación de red, 213
  - opción cachefs, 114
  - opción hsf, 112
  - opción pcfs, 113
  - referencia a otros mapas, 220, 221
  - selección de archivo de sólo lectura, 216, 219
  - sistema de archivos de CD-ROM, 112
  - sistema de archivos de PC-DOS, 113
  - tipos, 109
  - variables, 219, 220
- metacaracteres, 224, 225
- montaje de sistemas de archivos, 92
- proceso de desmontaje, 215
- proceso de montaje, 214, 215
- referencia, 224, 225
- replicación de archivos compartidos entre varios servidores, 119
- resolución de problemas, 129
- sistemas operativos
  - admitir versiones incompatibles, 119
  - URL de NFS y, 121
- automountd daemon, descripción general, 212

**B**

- barra diagonal (/)
  - /- como punto de montaje de mapa maestro, 206, 209
  - directorio root, montaje de clientes sin disco, 77
  - nombres de mapa maestro precedidos por, 206
- barra diagonal inversa (\) en mapas, 207, 209, 210
- base de datos de credenciales de CHAP
  - creación
    - para emisores de llamadas de confianza, 478
    - para un servidor de marcación de entrada, 476
- base de datos de credenciales de PAP
  - creación
    - para emisores de llamadas de confianza, 471–472
    - para un servidor de marcación de entrada, 468
  - creación para un servidor de marcación de entrada, 467–469
- biblioteca /usr/lib/nca\_addr.so, 63
- biblioteca libslp.so, 232
- biblioteca nca\_addr.so, 63
- biblioteca slp.jar, 232
- bit de permanencia para archivos de directorio público, 571
- bloqueo, mejoras de la versión 3 de NFS, 81
- bloqueo NFS, conmutación por error por parte del cliente y, 198
- bucles, alias, 333
- búsqueda
  - archivos .rhosts, 659
  - usuarios que iniciaron sesión en un sistema remoto, 660
- buzón de postmaster
  - crear, 323
  - probar, 333
- buzón postmaster, descripción, 349
- buzones
  - archivos para, 348, 361
  - requisitos de espacio para, 352
  - servidores de correo y, 352

**C**

- cambiar
  - archivo /etc/shells, 330

cambiar (*Continuación*)

- ruta de búsqueda de archivos . forward, 330
- campo Chat Script, archivo /etc/uucp/Systems, 579
- campo Class, archivo Devices, 585
- campo Dialer-Token-Pairs
  - archivo Devices
    - conexión de selector de puerto, 587
    - mismo selector de puerto, 587
    - sintaxis, 586
    - tipos de marcador, 586
- campo expect del campo Chat Script, 579
- campo expect del campo Secuencias de comandos de chat, 579
- campo ID-list del archivo Grades, 607, 608
- campo Job-size del archivo Grades, 607
- campo Line del archivo Devices, 585
- campo Line2 del archivo Devices, 585
- campo Permit-type del archivo Grades, 607
- campo Phone del archivo Systems, 578
- campo Speed
  - archivo Systems, 578
  - campo Class del archivo Devices y, 585
- campo System-job-grade del archivo Grades, 606, 607
- campo System-Name del archivo Systems, 576
- campo Time del archivo Systems, 577, 598
- campo Type
  - archivo Devices, 583
  - archivo Systems, 578
- campo User-job-grade del archivo Grades, 606
- cancelación, inicios de sesión remotos, 654
- capacidad de explorar
  - descripción general, 84
  - deshabilitación, 121
- carácter de escape b, archivo Dialers, 591
- carácter de escape c, archivo Dialers, 591
- carácter de escape D, 588
- carácter de escape d, archivo Dialers, 591
- carácter de escape de barra diagonal inversa
  - cadena de envío del archivo Dialers, 591
  - secuencia de comandos de chat del archivo Systems, 580
- carácter de escape de espacio, 592
- carácter de escape de interrupción, archivo Dialers, 591

- carácter de escape de números octales, 591
- carácter de escape de retorno, 592
- carácter de escape de retraso, 591
- carácter de escape de retroceso, 591
- carácter de escape e, archivo Dialers, 591
- carácter de escape K, archivo Dialers, 591
- carácter de escape N, archivo Dialers, 591
- carácter de escape n, archivo Dialers, 591
- carácter de escape nnn, 591
- carácter de escape nulo, 591
- carácter de escape p, archivo Dialers, 591
- carácter de escape r, archivo Dialers, 592
- carácter de escape s, archivo Dialers, 592
- carácter de escape T
  - archivo Devices, 588
  - archivo Dialers, 588, 592
- caracteres de escape
  - cadena de envío del archivo Dialers, 591
  - secuencia de comandos de chat del archivo Systems, 580
- caracteres de escape de línea nueva, 591
- caracteres de escape de retorno de carro, 591
- caracteres especiales en mapas, 225
- cierre de conexiones de sistema remoto, 664
- cierre de sesión (sistemas remotos), 661, 662
- clave de conversación, 204
- clave secreta
  - base de datos, 204
  - bloqueo de servidor y, 205
  - eliminación de servidor remoto, 205
- cliente NTP, configuración, 68
- cliente PPPoE
  - archivos, 548
  - comandos, 548
  - configuración, 483
  - definición, 422
  - definición de un servidor de acceso, 483
  - equipo, 438
  - mapa de tareas para configuración, 481
  - planificación, 438, 482
  - servidor de acceso y, 549
  - uso de archivo (PPPoE) /etc/ppp/peers/*nombre de igual*, 549



## clientes

*Ver también* clientes de correo, clientes NFS, cliente

NTP y cliente PPPoE

mostrar información sobre, 677, 683, 685

rastrear llamadas a servidores, 677, 679

## clientes de correo

configurar un cliente de correo, 297

definición, 353

sistemas de archivos montados en NFS y, 297

## clientes NFS

admitir sistema operativo incompatible, 119

servicios NFS, 75

## clientes sin disco

requisitos de montaje manual, 77

seguridad durante proceso de inicio, 205

## códigos de estado, SLP, 277–278

## códigos de estado del SLP, 277–278

## cola (UUCP)

archivos administrativos, 610, 611

comando cleanup, 561

daemon uusched

descripción, 561

ejecuciones simultáneas máximas, 563, 609

definiciones de niveles de trabajo, 605, 608

directorio de cola de impresión, 610

programación de daemon, 561

## cola de correo

administrar los directorios de la cola, 324

ejecutar la cola de correo antigua, 328

ejecutar un subconjunto de, 326

forzar procesamiento de cola de correo, 326

mover la cola de correo, 327

## cola de impresión (UUCP)

archivos administrativos, 610, 611

comando cleanup, 561

daemon uusched

descripción, 561

ejecuciones simultáneas máximas, 563, 609

definiciones de niveles de trabajo, 605, 608

directorio, 610

comando, definición /usr/sbin/sppptun, 542

comando (FTP) bye, 664

comando (FTP) get, ejemplo, 665

comando (FTP) mget, ejemplo, 666

comando (FTP) put, ejemplo, 667

comando (FTP)mput, ejemplo, 668

comando /usr/bin/aliasadm, 355

comando /usr/bin/cu

comprobación de módems o ACU, 572

descripción, 562

impresión de listas de Systems, 596

varios o diferentes archivos de configuración, 563, 595

comando /usr/bin/mail, 355

comando /usr/bin/mailq, 355

comando /usr/bin/mailstats, 356

comando /usr/bin/mailx, 356

comando /usr/bin/mconnect, 334–335, 356

comando /usr/bin/ncab2clf, 63

comando /usr/bin/praliases, 356

comando /usr/bin/rmail, 356

comando /usr/bin/uucp

depuración de transmisiones, 573

descripción, 562

directorio principal del ID de inicio de sesión, 561

ejecución de uucico por, 560

permisos para operación de reenvío, 604

comando /usr/bin/uulog, 561, 574

comando /usr/bin/uupick, 562, 572

comando /usr/bin/uustat, 562, 572

comando /usr/bin/uuto

descripción, 562

ejecución de uucico por, 560

eliminación de archivos de directorio público, 572

comando /usr/bin/uux

descripción, 562

ejecución de uucico por, 560

comando /usr/bin/vacation, 356, 365

comando /usr/lib/net/ncacnfd, 63

comando /usr/lib/uucp/uucheck, 562, 574

comando /usr/lib/uucp/uucleanup, 561

comando /usr/lib/uucp/Uutry, 561, 573

comando /usr/sbin/editmap, 361

comando /usr/sbin/makemap, 361

comando /usr/sbin/mount, *Ver* comando mount

comando /usr/sbin/ntpddate, 70

comando /usr/sbin/ntpq, 70

comando /usr/sbin/ntptrace, 70



- comando `/usr/sbin/shareall`
  - Ver también* comando `shareall`
  - habilitación de servicio WebNFS, 88
  - uso compartido de sistema de archivos automático, 87
- comando `/usr/sbin/showmount`, 174
- comando `/usr/sbin/syslogd`, 361
- comando `/usr/sbin/unshareall`, 173
- comando `/usr/sbin/xntpd`, 70
- comando `aliasadm`, 355
- comando `automount`, 158
  - autofs y, 77
  - cuándo ejecutar, 109
  - descripción general, 212
  - mensajes de error, 129
  - modificación de mapa maestro autofs (`auto_master`), 110
  - opción `-v`, 130
- comando `cfsadmin`, acceso a sistemas de archivos NFS, 114
- comando `chkey`, habilitación de NFS seguro, 102
- comando `clear_locks`, 158–159
- comando `cu`
  - comprobación de módems o ACU, 572
  - descripción, 562
  - impresión de listas de Systems, 596
  - varios o diferentes archivos de configuración, 563, 595
- comando `editmap`, 361
- comando `exit`, 661, 662
- comando `find`, búsqueda de archivos `.rhosts`, 659
- comando `ftp`
  - apertura de conexiones de sistema remoto, 663, 664
  - autenticación de inicios de sesión remotos, 662
  - inicios de sesión remotos comparados con `rlogin` y `rcp`, 662
  - interrupción de inicios de sesión, 654
- comando `fuser`, comando `umountall` y opción, 167
- comando `getfacl`, NFS y, 193
- comando `gethostbyname`, 376
- comando `httpd`
  - acceso de cortafuegos y WebNFS, 106
  - NCA y, 64–65
- comando `init`, PPP y, 462
- comando `keylogin`
  - habilitación de NFS seguro, 103
  - problemas de seguridad de inicio de sesión remoto, 205
- comando `keylogout`, NFS seguro y, 205
- comando `login`, NFS seguro y, 205
- comando `ls`, entradas de ACL y, 192
- comando `mail`, 355
- comando `mailq`, 355
- comando `mailstats`, 356
- comando `mailx`, 356
- comando `makemap`, 361
- comando `mconnect`, 334–335, 356
- comando `mount`, 159–165
  - autofs y, 77
  - con URL de NFS, 96
  - conmutación por error con, 163
  - deshabilitación de creación de archivos grandes, 93
  - montaje manual de sistemas de archivos, 92
  - necesidad de clientes sin disco para, 77
  - opciones
    - descripción, 160–163
    - ningún argumento, 165
    - `no largefiles`, 93
    - `public`, 95
    - URL NFS con, 164
    - uso, 163
- comando `mountall`, 166
- comando `ncab2clf`, 63
- comando `ncaconfd`, 63
- comando `netstat`, 237, 679, 682
  - descripción general, 677, 679
  - opción `-i` (interfaces), 679, 680
  - opción `-r` (tabla de enrutamiento IP), 681
  - opción `-s` (por protocolo), 680
- comando `newaliases`, UUCP y, 571
- comando `newkey`, habilitación de NFS seguro, 102
- comando `nfsstat`, 128, 175–177, 683, 685
  - descripción general, 677, 683
  - opción `-c` (clientes), 682, 683
  - opción `-m` (por sistema de archivos), 683, 685
  - opción `-s` (servidores), 683
- comando `nisaddcred`, habilitación de NFS seguro, 102

- comando `nistbladm`
  - modificación de mapa directo autofs, 111
  - modificación de mapa indirecto autofs, 111
  - modificación de mapa maestro autofs (auto\_master), 110
- comando `ntpdate`, 70
- comando `ntpq`, 70
- comando `ntptrace`, 70
- comando `openssl` y `sendmail`, 308
- comando `ping`, 254, 660, 677, 678
- comando `pppd`
  - activación de depuración, 492
  - análisis de opciones, 511
  - definición, 510
  - inicio de una llamada, 457
  - obtención de diagnósticos, 491, 505
  - prueba de una línea DSL, 484
- comando `praliases`, 356
- comando `pstack`, 177
- comando `rcp`, 668, 673
  - copia de directorios, 671
  - copia entre sistemas locales y remotos, 673
  - copia entre un sistema local y un sistema remoto, 671
  - descripción, 668
  - ejemplos, 673
  - especificación de origen y destino, 669, 670
  - nombres de ruta
    - absolutos o abreviados, 669, 670
    - opciones de sintaxis, 670
  - problemas de seguridad, 669
- comando `rdate`, 69
- comando `rlogin`
  - autenticación, 654, 656
    - archivo `/etc/hosts.equiv`, 655, 656
    - archivos `.rhosts`, 656
    - autenticación de sistema remoto o de red, 654, 655
  - descripción, 654
  - inicios de sesión directos o indirectos, 657
  - interrupción de inicios de sesión, 654
  - NFS seguro y, 205
  - proceso después de inicio de sesión, 658
  - uso, 661
- comando `rm`, 656
- comando `rmail`, 356
- comando `rpcinfo`, 177–179
- comando `rusers`, 660
- comando `sendmail`
  - aplicaciones de correo, integradas [TCP] y [IPC], 403
  - archivo `/etc/mail/helpfile`, 405
  - archivo `/etc/mail/local-host-names`, 405
  - archivo `/etc/mail/sendmail.ct`, 405
  - archivo `/etc/mail/sendmail.cw`, 405
  - archivo `/etc/mail/trusted-users`, 405
  - archivo `helpfile`, 405
  - archivo `local-host-names`, 405
  - archivo `main.mc`, 405
  - archivo `main-v7sun.mc`, 405
  - archivo `sendmail.ct`, 405
  - archivo `sendmail.cw`, 405
  - archivo `submit.cf`, 389
  - archivo `subsidiary.mc`, 405
  - archivo `subsidiary-v7sun.mc`, 405
  - archivo `trusted-users`, 405
  - archivos `.forward`, 370
  - cambios de la versión 8.12, 388
  - cambios en el nombre del archivo o la ubicación del archivo de la versión 8.12, 404
  - cambios en la versión 8.13, 379–388
  - comandos alternativos, 342
  - conjuntos de reglas de la versión 8.12, 403
  - declaraciones `FEATURE()`
    - cambios de la versión 8.12, 395
  - declaraciones `FEATURE()` de la versión 8.12
    - compatible, 395
    - no compatible, 398
  - declaraciones `FEATURE()` en la versión 8.13, 387–388
  - declaraciones `MAILER()` de la versión 8.12, 398
  - descripción, 362
  - direcciones IPv6 y versión 8.12, 405
  - ecuaciones para agentes de entrega de la versión 8.12, 400
  - envoltorios TCP y, 388–389
  - `/etc/mail/submit.cf`, 389
  - funciones de, 365

- comando sendmail (*Continuación*)
  - funciones de cola de la versión 8.12, 401
  - indicadores de agente de entrega de la versión 8.12, 399
  - indicadores de compilación, 340
  - interacciones con NIS+ y DNS, 378
  - interacciones con NIS y DNS, 377
  - interacciones de NIS+ y, 377
  - interacciones de NIS y, 376
  - LDAP de la versión 8.12, 401
  - macros
    - macros de configuración m4 de la versión 8.12, 395
    - macros definidas de la versión 8.12, 392
    - macros MAX de la versión 8.12, 394
  - mapa aliases NIS, 369
  - mensajes de error, 336
  - opciones de archivo de configuración en la versión 8.13, 385–387
  - opciones de línea de comandos de la versión 8.12, 389, 391, 392
  - opciones de línea de comandos en la versión 8.13, 385
  - servicios de nombres y, 374
  - tabla mail\_aliases NIS+, 369
- comando setfacl, NFS y, 192
- comando setmnt, 175
- comando share
  - descripción, 167–172
  - opciones, 168
  - problemas de seguridad, 170
- comando shareall, 173
  - deshabilitación de acceso de montaje para un cliente, 95
  - habilitación de inicio de sesión de servidor NFS, 89
  - habilitación de servicio WebNFS, 88
  - uso compartido de sistema de archivos
    - automático, 87
- comando showmount, 174
- comando snoop, 179–180, 677, 679
  - registro de servicios del SLP y, 249
  - supervisión de retransmisión, 256
  - tráfico de SLP y, 264
  - uso con SLP, 236, 237
- comando snoop (*Continuación*)
  - varias solicitudes del SLP y, 267
- comando spray, 677, 678
- comando syslogd, 361
- comando telnet, NFS seguro y, 205
- comando truss, 180
- comando umount
  - autofs y, 77
  - descripción, 165–166
- comando umountall, 167
- comando uname -n, 596
- comando unshare, 172–173
- comando unshareall, 173
- comando uuccheck, 562, 574
- comando uucleanup, 561
- comando uucp
  - depuración de transmisiones, 573
  - descripción, 562
  - directorio principal del ID de inicio de sesión, 561
  - ejecución de uucico por, 560
  - permisos para operación de reenvío, 604
- comando uulog, 561, 574
- comando uuname, 574
- comando uupick
  - descripción, 562
  - eliminación de archivos de directorio público, 572
- comando uustat
  - comprobación de módems o ACU, 572
  - descripción, 562
  - secuencia de comandos de shell uudemondemon.admin para, 569
- comando uuto
  - descripción, 562
  - ejecución de uucico por, 560
  - eliminación de archivos de directorio público, 572
- comando Uutry, 561, 573
- comando uux
  - descripción, 562
  - ejecución de uucico por, 560
- comando vacation, 355, 356, 365
- comando xntpd, 70
- comandos
  - archivos ejecutables (X.) del UUCP, 560, 611
  - cuelgue de programas, 137

comandos (*Continuación*)

- ejecución remota mediante UUCP, 597, 600, 603
- resolución de problemas del UUCP, 574
- comandos administrativos (UUCP), 561, 562
- comandos alternativos, comando `sendmail`, 342
- comandos de correo, interacciones de, 361
- comentarios
  - en mapa maestro (`auto_master`), 207
  - en mapas directos, 209
  - en mapas indirectos, 210
- compartir archivos, mejoras de NFS versión 3, 78
- compatibilidad de uso compartido OPEN, NFS versión 4, 189–190
- comprobación de eco, 591
- comprobación de ID de usuario o grupo sin asignar, 193
- comunicaciones entrantes
  - habilitación por medio de la secuencia de comandos de chat del UUCP, 581
  - seguridad de devolución de llamada, 600
- conexiones de correo con otros sistemas,
  - probar, 334–335
- confianza en entorno de red
  - inicio de sesión remoto
    - proceso de autenticación, 655
- configuración
  - enlaces de `asppp` con bases de datos del UUCP, 564
  - puertas de enlace del correo, 353
  - UUCP
    - adición de inicios de sesión, 566, 567
    - archivos de base de datos, 564
    - redes TCP/IP, 569, 570
    - secuencias de comandos de shell, 567, 569
- configuración de correo
  - correo local y una conexión remota, 292
  - probar, 332
  - sólo local, 291
  - típica, 286
- configuración de proveedor, especificación en el archivo `sendmail.cf`, 342
- configuración de servidor NFS y directorio `/home`, 115
- configuración para autenticación PAP, 468, 471–472, 472, 473

## configurar

- archivo de alias de correo local, 320
- cliente de correo, 297
- host de correo, 298
- host virtual, 305
- mapa NIS `mail.aliases`, 319
- puerta de enlace de correo, 300
- servidor de correo, 328
- configurar SMTP para que utilice TLS, 307–312
- conjunto de reglas `check_eoh`, comando `sendmail`, 404
- conjunto de reglas `check_et rn`, comando `sendmail`, 404
- conjunto de reglas `check_expn`, comando `sendmail`, 404
- conjunto de reglas `check_vrfy`, comando `sendmail`, 404
- conjuntos de reglas
  - probar, 333
  - versión 8.12 de `sendmail`, 403
- conmutación por error
  - compatibilidad con NFS, 81
  - ejemplo de comando `mount`, 163
  - ejemplo de comando `mpunt`, 163
  - mensaje de error, 135
- conmutación por error del lado del cliente,
  - habilitación, 94
- conmutación por error por parte del cliente
  - bloqueo NFS y, 198
  - compatibilidad con NFS, 81
  - descripción general, 196–198
  - NFS versión 4, 198
  - sistemas de archivos replicados, 197–198
  - terminología, 197
- consolidación de archivos relacionados con el proyecto, 116
- contraseñas
  - autenticación para inicios de sesión remotos
    - comando `ftp`, 662, 664
    - comando `rlogin`, 654, 657, 661
  - autofs y contraseñas de superusuarios, 77
  - creación de contraseña RPC segura, 102
  - protección con contraseña DH, 203
  - UUCP con privilegios, 602, 603

- control de flujo de hardware
  - archivo Dialers, 593
  - archivo Systems, 582
- control de flujo de STTY, 582, 593
- copia de archivos (remoto, uso de rcp, 673
- copia de archivos (remoto)
  - uso de ftp, 663
  - uso de rcp, 668
- copia remota
  - uso de ftp, 663
  - uso de rcp, 668, 673
- copias de seguridad, servidores de correo y, 352
- correo electrónico, mantenimiento del UUCP, 571
- cortafuegos
  - acceso a NFS a través, 83
  - acceso WebNFS a través, 106
  - montaje de sistemas de archivos a través, 95
- crear
  - alias postmaster, 322
  - archivo /etc/shells, 330
  - archivo de mapa con clave, 321
  - buzón de postmaster, 323
- credenciales
  - autenticación CHAP, 476
  - autenticación PAP, 467–469
  - autenticación UNIX, 203
  - descripción, 203
- criptografía por clave pública
  - autenticación DH, 204
  - base de datos de claves públicas, 203
  - bases de datos de claves públicas, 204
  - clave común, 204
  - clave de conversación, 204
  - clave secreta
    - base de datos, 204
    - eliminación de servidor remoto, 205
  - sincronización de tiempo, 204
- CSU/DSU
  - configuración, 460
  - resolución de problemas comunes, 507
- cuelgue de programas, 137

## D

- DA (SLP)
  - anuncios, 244, 246, 247, 248
  - deshabilitar detección activa, 245
  - deshabilitar detección pasiva, 245
  - detección, 244, 248, 259
  - detección de redes de acceso telefónico, 246, 248, 638
  - eliminación, 247
  - eliminación de multidifusión, 245
  - implementación, 248–249, 261–262
  - latido, 247, 248, 250
  - multidifusión, 248
  - registro de DA, 262
  - sin multidifusión, 266
  - varios DA, 264–265
- DA\_BUSY\_NOW, 264
- daemon /usr/lib/inet/xntpd, descripción, 70
- daemon /usr/sbin/in.comsat, 361
- daemon /usr/sbin/inetd, in.uucpd invocado por, 561
- daemon automountd, 145
  - autofs y, 77
  - descripción, 84
  - descripción general, 212
  - montaje y, 84
- daemon in.comsat, 361
- daemon in.uucpd, 561
- daemon inetd, in.uucpd invocado por, 561
- daemon keyserve, habilitación de NFS seguro, 102
- daemon lockd, 146–147
- daemon mountd, 147
  - comprobación de respuesta en servidor, 126
  - no registrado con rpcbind, 135
  - verificación de ejecución, 128, 135
- daemon nfs4cbd, 147
- daemon nfsd, 147–148
  - comprobación de respuesta en servidor, 126
  - montaje y, 195–196
  - verificación de ejecución, 127
- daemon nfslogd
  - descripción, 148
  - habilitación de inicio de sesión de servidor NFS, 90

- daemon nfsmapid
  - ACL y, 192–194
  - configuración de dominio predeterminado NFSv4, 153–156
  - descripción, 78, 148–156
  - identificación de dominio NFSv4, 152–153
  - información adicional sobre, 156
  - registros DNS TXT y, 152
  - reglas de precedencia y, 151
- daemon nfsmapid daemon, archivos de configuración y, 150
- daemon pppoe
  - definición, 543
  - inicio, 486
- daemon rpcbind
  - daemon no registrado mountd, 135
  - inactivo o colgado, 135
- daemon slpd, 271, 272, 275
  - ámbitos y, 259
  - anuncios de proxy y, 268
  - cambio de interfaces, 266
  - DA, 256
  - DA estáticos y, 245
  - eliminación de DA, 247
  - equipos de hosts múltiples y, 265
  - latido, 247
  - servidor de SA, 256
- daemon statd, 156–157
- daemon uucico
  - adición de inicios de sesión del UUCP, 566, 567
  - archivo Dialcodes y, 594
  - archivo Systems y, 575
  - comando Uutry y, 561
  - daemon uusched y, 561
  - descripción, 560
  - ejecuciones simultáneas máximas, 563, 609
  - impresión de listas de Systems, 596
  - varios o diferentes archivos de configuración, 563, 575, 595
- daemon uusched
  - descripción, 561
  - ejecuciones simultáneas máximas, 563, 609
  - llamada de secuencia de comandos de shell uudemmon.hour, 568
- daemon uuxqt
  - descripción, 560
  - ejecuciones simultáneas máximas, 563, 609
  - llamada de secuencia de comandos de shell uudemmon.hour, 568
- daemon xntpd, 68, 70
- daemons
  - automountd, 145
  - autofs y, 77
  - descripción general, 212
  - lockd, 146–147
  - mountd, 147
    - comprobación de respuesta en servidor, 126
    - no registrado con rpcbind, 135
    - verificación de ejecución, 128, 135
  - nfs4cbd, 147
  - nfsd
    - comprobación de respuesta en servidor, 126
    - descripción, 147–148
    - verificación de ejecución, 127
  - nfslogd, 148
  - nfsmapid, 148–156
  - requerido para montaje remoto, 123
  - rpcbind
    - mensajes de error de montaje, 135
  - statd, 156–157
- declaración FEATURE() compat\_check, 396
- declaración FEATURE() delay\_checks, 396
- declaración FEATURE() dnsbl, 396, 398
- declaración FEATURE() enhdnsbl, 396, 398
- declaración FEATURE() generics\_entire\_domain, 396
- declaración FEATURE() genericstable, 398
- declaración FEATURE() ldap\_routing, 396
- declaración FEATURE() local\_lmtp, 396
- declaración FEATURE() local\_no\_masquerade, 397
- declaración FEATURE() lookupdotdomain, 397
- declaración FEATURE() no\_default\_msa, 397
- declaración FEATURE() nocalonify, 397
- declaración FEATURE() nouucp, 397
- declaración FEATURE() nullclient, 397
- declaración FEATURE()
  - preserve\_local\_plus\_detail, 397
- declaración FEATURE() preserve\_luser\_host, 397
- declaración FEATURE() queuegroup, 397

- declaración `FEATURE()` `rbl`, 398
- declaración `FEATURE()` `relay_mail_from`, 398
- declaración `FEATURE()` `remote_mode`, 398
- declaración `FEATURE()`
  - `sun_reverse_alias_files`, 398
- declaración `FEATURE()` `sun_reverse_alias_nis`, 398
- declaración `FEATURE()`
  - `sun_reverse_alias_nisplus`, 398
- declaración `FEATURE()` `virtuser_entire_domain`, 398
- declaraciones `FEATURE()` en la versión 8.12
  - compatible, 395
  - no compatible, 398
- declaraciones `FEATURE()` en la versión 8.13 de
  - `sendmail`, 387–388
- declaraciones `MAILER()` de la versión 8.12, 398
- definición `confFORWARD_PATH`, 329, 330
- definiciones de protocolo en el archivo `Devices`, 589
- definiciones de protocolos en el archivo `Devices`, 588
- delegación, NFS versión 4, 190–192
- depuración
  - transmisiones del UUCP, 572, 573
- depuración de PPP
  - activación de depuración, 492
  - depuración de secuencias de comandos de chat, 500
  - diagnóstico de problemas de línea de serie, 503
  - diagnóstico de problemas de PPPoE, 504
  - diagnóstico de problemas de red, 494
  - resolución de problemas de comunicaciones, 496, 498
  - resolución de problemas del módem, 498
- desactivación, comprobación de eco, 591
- deshabilitación
  - acceso de montaje para un cliente, 94–95
  - capacidad de explorar autofs
    - descripción general, 121
    - tareas, 121
  - NCA, 56
  - registro NCA, 56
- deshabilitar, archivos `.forward`, 329
- desmontaje
  - autofs and, 215
  - autofs y, 77
  - ejemplos, 166
  - grupos de sistemas de archivos, 167
  - desmontaje serial, 167
- detección de DA (SLP), 255
- detección de servicios (SLP), 253, 255, 261
- detención
  - desactivación
    - comprobación de eco, 591
  - servicio autofs, 98
  - servicios NFS, 97
- devolución de llamada
  - habilitación de devolución de llamada por medio de la secuencia de comandos de chat, 581
  - opción `CALLBACK` del archivo `Permissions`, 600
  - opción del archivo `Permissions`, 600
- diagnósticos para PPP
  - activado
    - con `pppd`., 491–492
  - archivo de registro para un túnel PPPoE, 504
  - enlace de línea arrendada, 491
  - enlace por marcación telefónica, 491
  - opción `-debug`, 492
- diagrama de proceso, para CHAP, 536
- difusión (SLP), 253, 262, 266
- direccionamiento dinámico, PPP, 538
- direccionamiento estático, PPP, 539
- direcciones de correo
  - % en, 349
  - descripción, 346
  - distinción de mayúsculas y minúsculas, 347
  - dominios y subdominios, 346
  - enrutamiento de correo y, 373
  - locales, 349
- direcciones de correo locales, 349
- direcciones IPv6 y versión 8.12, comando
  - `sendmail`, 405
- direcciones URL del servicio
  - registro del proxy (SLP), 272, 274
- directorio `/etc/mail`, contenido de, 356
- directorio `/etc/mail/cf`, contenido de, 357
- directorio `/etc/mail/cf/domain`, 358
- directorio `/etc/mail/cf/feature`, 359
- directorio `/etc/mail/cf/m4`, 359
- directorio `/etc/mail/cf/mailer`, 359
- directorio `/etc/mail/cf/ostype`, 359
- directorio `/etc/ppp/peers`, 510



- directorio .Status, 574
- directorio /usr, montaje de clientes sin disco, 77
- directorio /usr/bin, contenido de, 355
- directorio /usr/kvm, montaje de clientes sin disco, 77
- directorio /usr/lib, contenido de, 360
- directorio /usr/ntp/ntpstats, 70
- directorio /var/mail, 291, 293
  - configuración de cliente de correo y, 297
  - montaje automático de, 297
- directorio /var/spool/clientmqueue, 361
- directorio /var/spool/mqueue, 361
- directorio /var/uucp/.Admin/errors, 574
- directorio /var/uucp/.Status, 574
- directorio clientmqueue, 361
- directorio de trabajo, definición para comando rcp, 670
- directorio domain, 358
- directorio errors (UUCP), 574
- directorio feature, 359
- directorio m4, 359
- directorio mailer, 359
- directorio mqueue, 361
- directorio ntpstats, 70
- directorio ostype, 359
- directorio root, montaje de clientes sin disco, 77
- directorios (UUCP)
  - administración, 561
  - mantenimiento del directorio público, 571
  - mensajes de error, 574
- dominios
  - definición, 101
  - inicios de sesión remotos y, 654
  - subdominios y, 346
- dominios de correo
  - archivo sendmail.cf y, 374
  - dominios de servicio de nombres y, 375
- dominios de servicio de nombres, dominios de correo y, 375
- DSL, Ver PPPoE
- duración de registro (SLP), 237

## E

- carácter de escape E, archivo Dialers, 591

- ecuaciones para agentes de entrega de la versión 8.12, comando sendmail, 400
- ejecución de SMTP con TLS
  - conjuntos de reglas para, 384
  - consideraciones de seguridad relacionadas con, 385
  - descripción, 380–385
  - macros para, 383–384
  - opciones de archivo de configuración para, 381–383
- ejecución remota (UUCP)
  - archivos de trabajo C., 610, 611
  - comandos, 597, 600, 603
  - daemon, 560
- ejecutar SMTP con TLS, información de tarea, 307–312
- ejemplo, configuraciones de PPP, Ver ejemplos de configuración para PPP
- ejemplos de configuración para PPP
  - autenticación CHAP, 436
  - autenticación PAP, 434
  - enlace de línea arrendada, 431
  - enlace por marcación telefónica, 428
  - túnel PPPoE, 440
- eliminación, archivos .rhosts, 656
- eliminación de bloqueos, 158–159
- emisores de llamadas de confianza, 420
  - configuración para autenticación CHAP, 478
- enlace /usr/sbin/newaliases, 361
- enlace de línea arrendada
  - autenticación para el enlace, 420
  - configuración, 431
  - configuración de interfaz síncrona, 460–461
  - CSU/DSU, 418
  - definición, 417
  - diagnóstico de problemas comunes
    - descripción general, 506–507
    - red, 494
  - ejemplo de configuración, 431
  - hardware, 430
  - mapa de tareas para configuración, 459
  - medios, 419
  - partes del enlace, 418–419
  - planificación, 430, 431, 433, 461
  - proceso de comunicaciones, 419
  - secuencia de comandos demand, 463



- enlace directo, configuración del UUCP, 559
  - enlace newaliases, 361
  - enlace por marcación telefónica
    - autenticación para el enlace, 420
    - creación de secuencias de comandos de chat, 522
    - definición, 413
    - diagnóstico de problemas comunes
      - con pppd, 491
      - líneas de serie, 503
      - red, 494
    - ejemplo, 428
    - inicio de una llamada a un igual, 457–458
    - mapa de tareas, 443
    - partes de un enlace, 414–416
    - planificación, 426, 428
    - plantillas para archivos de configuración, 445
    - proceso de marcación telefónica, 416
    - secuencias de comandos de chat
      - ejemplo, 523–524, 525–526, 530
      - inicio de sesión de estilo UNIX, 526–528
      - plantilla, 524–525
  - enrutamiento de correo, direcciones de correo y, 373
  - enrutamiento de unidifusión (SLP), 265
    - deshabilitado, 267
  - entorno de red de confianza
    - inicio de sesión remoto
      - proceso después de inicio de sesión, 658
  - entorno NFS, sistema NFS seguro, 202
  - entrada Any del campo Time, 576
  - entrada Never del campo Time, 598
  - entrada penril en el archivo Dialers, 592
  - entradas de días del campo Time, 577
  - envoltorios TCP, comando sendmail y, 388–389
  - equipo de marcación de salida
    - configuración
      - autenticación CHAP, 478, 480
      - autenticación PAP, 471–472
      - comunicaciones de línea de serie, 447–448
      - conexión con un igual, 449–451
      - módem, 446–447
      - puerto de serie, 446–447
    - configuración de una línea de serie con
      - /etc/ppp/options.nombre de tty, 516
    - equipo de marcación de salida (*Continuación*)
      - creación de una secuencia de comandos de chat, 448
      - definición, 414
      - direccionamiento
        - dinámico, 538
        - estático, 539
      - información de planificación, 426
      - llamada a igual remoto, 457–458
      - mapa de tareas para configuración, 444–445
    - errores de apertura, NFS y, 78
    - errores de escritura, NFS y, 78
    - espacio de nombre de sistema de archivos, NFS versión 4, 184–186
    - espacio de nombres, acceso compartido, 118
    - espacios de nombres, autofs y, 83
    - Ethernet, probar configuración de correo en, 332
    - evitar los problemas con las ACL en NFS, 193
    - explorar, con una URL de NFS, 105–106
- F**
- falla de asignación de ID, motivos, 192–193
  - fecha, sincronización con otro sistema, 69
  - filtro /usr/bin/mailcompat, 355
  - filtro mailcompat, 355
  - Frame Relay, 419, 459
  - ftp anónimo, cuentas, 662
  - ftphosts, 631
  - funciones de cola de la versión 8.12, comando
    - sendmail, 401
- G**
- GSS-API, y NFS, 82
  - guión (-)
    - abreviatura de código de marcación, 579
    - en nombres de mapas autofs, 220
    - marcador de posición del campo Line2, 585
    - marcador de posición del campo Speed, 578

**H**

## habilitación

- conmutación por error del lado del cliente, 94
- inicio de sesión de servidor NFS, 89–90
- NCA, 53–55
- registro NCA, 56
- servicio WebNFS, 88
- sistema NFS seguro, 102

## hardware

- control de flujo
  - archivo Dialers, 593
  - archivo Systems, 582

## UUCP

- configuraciones, 559
- selector de puerto, 584

## hora

- sincronización con otro sistema, 69

## hosts

- comprobar respuesta de, 678
- desmontaje de todos los sistemas de archivos de, 167
- en archivo `/etc/hosts.equiv`, 655, 656
- enviar paquetes a, 678

## hosts de correo

- configurar un host de correo, 298
- descripción, 351

## hosts múltiples (SLP)

- ámbitos y, 269
- anuncios de proxy, 268
- cambio de interfaces, 266
- configuración, 265
- enrutamiento de sólo difusión, 253
- enrutamiento de unidifusión deshabilitado, 267
- sin multidifusión, 262

## hosts virtuales, configurar, 305

**I**

## ID de usuario o grupo sin asignar, comprobación, 193

## identificador de archivo público, montaje y, 195

## identificador de archivos público

- autofs y, 120
- montaje NFS con, 83
- WebNFS y, 104

## identificadores de archivos volátiles, NFS versión 4, 186–187

## igual

- autenticado, 420
- autenticador, 420
- cliente PPPoE, 422, 438
- definición, 413
- equipo de marcación de salida, 414
- igual de línea arrendada, 418
- servidor de acceso, 422, 439
- servidor de marcación de entrada, 414

## impresión

- lista de archivos compartidos o exportados, 174
- lista de directorios montados remotamente, 174

indicadores de agente de entrega de la versión 8.12, comando `sendmail`, 399indicadores de compilación, comando `sendmail`, 340

## inhabilitación, creación de archivos grandes, 93

## inicio

- activación
  - comprobación de eco, 591
- habilitación de devolución de llamada por medio de la secuencia de comandos de chat, 581
- montaje de sistemas de archivos, 91
- secuencias de comandos de shell del UUCP, 567, 569
- seguridad de cliente sin disco, 205
- servicio autofs, 98
- servicios NFS, 97

## inicio de sesión

## inicios de sesión remotos

- apertura de conexión ftp, 663, 664
- autenticación (`rlogin`), 654, 656
- búsqueda de quién inició sesión, 660
- cierre de conexión ftp, 664
- comando ftp, 663
- directos o indirectos (`rlogin`), 657
- interrupción, 654
- uso de `rlogin`, 654, 661
- vinculación de inicios de sesión, 657

## inicio de sesión de servidor NFS, habilitación, 89–90

## inicios de sesión (UUCP)

- adición, 566, 567
- con privilegios, 602, 603

## inicios de sesión remotos

- apertura de conexión ftp, 663, 664
- autenticación (ftp), 662
- autenticación (rlogin), 654, 656
  - archivo `/etc/hosts.equiv`, 655, 656
  - archivos `.rhosts`, 656
  - autenticación de red o autenticación de sistema remoto, 654, 655
- búsqueda de quién inició sesión, 660
- cierre de conexión ftp, 664
- comandos ftp, 663
- directos o indirectos (rlogin), 657
- dominios, 654
- eliminación de archivos `.rhosts`, 659
- interrupción, 654
- uso del comando `rlogin`, 661
- verificación de operación de sistema remoto, 659
- vinculación de inicios de sesión, 657

## inicios de sesión remotos directos

- inicios de sesión indirectos o
  - comando `rlogin`, 657
  - uso del comando `rlogin`, 661

## inicios de sesión remotos indirectos, 657

## interfaces (PPP)

- conexión de interfaces PPPoE con
  - `/usr/sbin/spptun`, 542
- configuración para un cliente PPPoE, 483
  - Ver también* archivo `/etc/ppp/pppoe.if`
- configuración para un servidor de acceso PPPoE, 486, 542
- interfaz asíncrona para equipo de marcación de salida de PPP, 415
- interfaz asíncrona para marcación de entrada de PPP, 416
- restricción de una interfaz para clientes PPPoE, 487
- secuencia de comandos de configuración HSI/P, 461
- síncrono para líneas arrendadas, 418

## interfaces de red (SLP), consideraciones para no enrutadas, 269–270

- interrupción de inicios de sesión remotos, 654
- interrupción de teclado de montaje, 123

## L

- las réplicas deben tener la misma versión, 138
- latido de DA, frecuencia, 244
- LDAP de la versión 8.12, comando `sendmail y`, 401
- líneas telefónicas, configuración del UUCP, 559
- líneas telefónicas RS-232, configuración del UUCP, 559
- lista
  - clientes con sistemas de archivos montados remotamente, 174
  - sistemas de archivos compartidos, 171
  - sistemas de archivos montados, 165
- lista de control de acceso (ACL) y NFS
  - descripción, 80, 192–194
  - mensaje de error, `Permission denied`, 137
- lista de tareas, NCA, 51
- los mapas (autofs), división líneas largas en, 207
- los montajes replicados deben ser de sólo lectura, 138
- los montajes replicados no pueden ser soft, 138

## M

- macro de configuración `m4 LOCAL_DOMAIN()`, 395
- macro de configuración `m4`
  - `MASQUERADE_EXCEPTION()`, 395
- macro de configuración `m4 SMART_HOST()`, 395
- macro de configuración `m4 VIRTUSER_DOMAIN()`, 395
- macro de configuración `m4`
  - `VIRTUSER_DOMAIN_FILE()`, 395
- macro `MAXBADCOMMANDS`, comando `sendmail`, 394
- macro `MAXETRNCOMMANDS`, comando `sendmail`, 394
- macro `MAXHELOCOMMANDS`, comando `sendmail`, 394
- macro `MAXNOOPCOMMANDS`, comando `sendmail`, 394
- macro `MAXVRFYCOMMANDS`, comando `sendmail`, 394
- macros de la versión 8.12
  - macros de configuración `m4 (sendmail)`, 395
  - macros definidas (`sendmail`), 392
  - macros `MAX (sendmail)`, 394
- mantenimiento del directorio
  - `/var/spool/uucppublic`, 571
- mantenimiento del directorio público (UUCP), 571
- mantenimiento del directorio `uucppublic`, 571
- mantenimiento del UUCP
  - adición de inicios de sesión, 566, 567
  - correo, 571

mantenimiento del UUCP (*Continuación*)

- directorio público, 571
- mantenimiento regular, 571, 572
- secuencias de comandos de shell, 567, 569

## mapa alias NIS, 369

## mapa auto\_home

- configuración de servidor de directorio /home, 115
- directorio /home, 114
- punto de montaje /home, 206, 207

## mapa auto\_master, 103

## mapa de clave pública

- autenticación DH, 204
- habilitación de NFS seguro, 102

## mapa de variable OSREL, 220

## mapa de variable OSVERS, 220

## mapa maestro (auto\_master)

- /- mount point, 206
- /- punto de montaje, 209
- comentarios en, 207
- comparación con archivo /etc/mnttab, 212
- contenido, 206, 208
- cuándo ejecutar el comando automount, 110
- descripción, 109
- descripción general, 206
- habilitación de NFS seguro, 103
- instalado previamente, 114
- modificación, 110
- restricciones de seguridad, 120
- sintaxis, 206
- sustitución de opciones, 114

## mapa NIS mail.alias, configurar, 319

## mapas (autofs)

- caracteres especiales, 225
- comando automount
  - cuándo ejecutar, 109
- comentarios en, 207, 209, 210
- directos, 208, 209
- división líneas largas en, 209, 210
- ejecutable, 222
- evitar conflictos de montaje, 111
- indirectos, 210, 211
- inicio del proceso de navegación, 207, 214
- maestro, 206
- master, 206

mapas (autofs) (*Continuación*)

- métodos de mantenimiento, 109
- modificación
  - mapa maestro, 110
  - mapas directos, 111
  - mapas indirectos, 111
- navegación de red, 213
- referencia a otros mapas, 220, 221
- selección de archivos de sólo lectura para clientes, 219
- selección de archivos de sólo lectura para los clientes, 216
- tareas administrativas, 109
- tipos y sus usos, 109
- variables, 219, 220
- varios montajes, 215

## mapas directos (autofs)

- comentarios en, 209
- cuándo ejecutar el comando automount, 110
- descripción, 109
- descripción general, 209
- ejemplo, 208
- modificación, 111
- sintaxis, 208

## mapas ejecutables, 222

## mapas indirectos (autofs)

- comentarios en, 210
- cuándo ejecutar el comando automount, 110
- descripción, 109
- descripción general, 210, 211
- ejemplo, 211
- modificación, 111
- sintaxis, 210

## marcación enlace

- secuencias de comandos de chat
  - para un adaptador de terminal RDSI, 528–530

## mensaje: ADVERTENCIA: punto de montaje ya

- montado en, 131

## mensaje: archivo demasiado grande, 135

## mensaje: can't mount, 130

## mensaje: clave de mapa incorrecta, 131

## mensaje: clave incorrecta, 130

## mensaje: daemon ya está en ejecución, 134

## mensaje: dir debe empezar con '/', 131

- mensaje: el servidor no responde, 131, 133
  - cuelgue de programas, 137
  - interrupción de teclado para, 123
  - problemas de montaje remoto, 135
- mensaje: el sistema no responde, 131
- mensaje: error de bloqueo, 134
- mensaje: error de comprobación, 135
- mensaje: hierarchical mountpoints, 131
- mensaje: ignorando opción no válida, 136
- mensaje: la opción index no se puede usar sin la opción public, 134
- mensaje: leading space in map entry, 130
- mensaje: nfscast: cannot receive reply, 132
- mensaje: nfscast: cannot send packet, 132
- mensaje: nfscast: select, 132
- mensaje: no encontrado, 130
- mensaje: no es un directorio, 132
- mensaje: no existe tal archivo o directorio, 135
- mensaje: no ha sido posible crear un punto de montaje, 130
- mensaje: no ha sido posible usar una gestión de archivos pública, 134
- mensaje: no hay información, 133
- mensaje: no se puede enviar el paquete, 132
- mensaje: no se puede recibir respuesta, 132
- mensaje: pathconf: el servidor no responde, 133
- mensaje: pathconf: no info, 133
- mensaje: permiso denegado, 135
- mensaje: remount, 131
- mensaje: ya montado, 131
- mensaje NFS can't support nolargefiles, 136
- mensaje NFS V2 can't support largefiles, 136
- mensajes
  - UUCP
    - comprobación de mensajes de error, 574
    - mensajes de error ASSERT, 612, 613
    - mensajes de error STATUS, 613, 614
- mensajes de error
  - el servidor no responde
    - cuelgue de programas, 137
    - interrupción de teclado para, 123
    - problemas de montaje remoto, 135, 137
  - errores de apertura
    - NFS y, 78
- mensajes de error (*Continuación*)
  - errores de escritura
    - NFS y, 78
  - generados por automount -v, 130
  - no existe tal archivo o directorio, 135
  - permiso denegado, 135
  - programa sendmail, 336
  - varios mensajes automount, 131
- mensajes de error ASSERT (UUCP), 574, 612, 613
- mensajes de error STATUS (UUCP), 574, 613, 614
- mensajes MAILER-DAEMON, 336
- mensajes no entregados, resolución de problemas, 333
- MILTER, API de filtro de correo, 341–342
- módem, resolución de problemas del módem, 498
- módem (PPP)
  - configuración
    - equipo de marcación de salida, 446–447
    - servidor de marcación de entrada, 452
  - configuración de la velocidad del módem, 453
  - creación de secuencias de comandos de chat, 522
  - DSL, 424
  - secuencia de comandos de chat
    - ejemplo, 449
  - secuencias de comandos de chat
    - ejemplo, 523–524, 525–526, 530
    - inicio de sesión de estilo UNIX, 526–528
    - para un adaptador de terminal RDSI, 528–530
    - plantilla, 524–525
- módem (UUCP)
  - bases de datos del UUCP
    - campo DTP del archivo Devices, 588
  - bases de datos del UUCP, campo DTP del archivo Devices, 587
  - conexión de selector de puerto, 587, 588
  - conexión directa, 587
  - configuración de características, 582, 593
  - configuración de hardware del UUCP, 559
  - resolución de problemas, 572
- módem DSL, 424
- modificación
  - mapa directo autofs, 111
  - mapa indirecto autofs, 111
  - mapa maestro (auto\_master), 110
- modo de usuario único y seguridad, 205

- modo pasivo, 598
- modo setgid, comando share, 169
- modo setuid
  - comando share, 169
  - RPC seguras y, 205
- módulo ncakmod, 64–65
- montaje
  - asignador de puertos y, 195–196
  - autofs y, 77, 215
  - daemon nfsd y, 195–196
  - directorio /var/mail, 297
  - ejemplos, 163
  - especificación de lectura y escritura, 162
  - especificación de sólo lectura, 162, 163
  - flexible y forzado, 123
  - forzar E/S directas, 161
  - identificador de archivo público y, 195
  - interrupción de teclado durante, 123
  - montaje remoto
    - daemons requeridos, 123
    - resolución de problemas, 124–125, 127
  - reintentos en primer plano, 160
  - reintentos en segundo plano, 160
  - requisitos de cliente sin disco, 77
  - superposición de sistema de archivos ya montado, 163
  - todos los sistemas de archivos en una tabla, 166
- montaje automático
  - directorio /var/mail, 297, 352
- montaje de servidor: error de nombre de ruta, 132
- montaje de sistemas de archivos
  - a través de un cortafuegos, 95
  - autofs y, 92
  - descripción general, 90
  - deshabilitación de acceso para un cliente, 94–95
  - manualmente (en tiempo real), 92
  - mapa de tareas, 90
  - método de tiempo de inicio, 91
  - URL de NFS con, 95–96
- montaje remoto
  - daemons requeridos, 123
  - resolución de problemas, 124, 127
- montaje seguro, opción de archivo dfstab, 103
- montajes jerárquicos (varios montajes), 215

- montajes replicados, opción soft y, 138
- mostrar información de red, 677, 678, 679, 685
- multidifusión (SLP)
  - cambio de interfaces, 266
  - DA, 245, 248
  - equipos de hosts múltiples y, 265
  - propagación, 251
  - propiedad time-to-live, 250
  - si está deshabilitada, 266
  - solicitudes de servicio, 262
  - tráfico, 261
- Multiplexor de acceso a la línea digital de abonado (DSLAM), para PPPoE, 424
- MX (agente de intercambio de correo), registros, 302

## N

- navegación con mapas
  - descripción general, 213
  - inicio del proceso, 207, 214
- NCA
  - arquitectura, 64–65
  - biblioteca del socket, 57
  - cambio de registro, 56
  - descripción de archivos, 62
  - descripción general, 49–50
  - deshabilitación, 56
  - habilitación, 53–55
  - httpd y, 64–65
  - lista de tareas, 51
  - módulo de núcleo, 64–65
  - nuevas funciones, 50
  - requisitos, 52
  - sockets, 52
- negociación
  - seguridad WebNFS, 83
  - tamaño de transferencia de archivo, 194–195
- negociación de versión, NFS, 182–183
- NFS
  - comandos, 157
  - daemons, 145–157
  - negociación de versión, 182–183
  - NFS ACL, mensaje de error, Permission denied, 137
  - NFS versión 4, funciones en, 183–194

- nivel de versión, especificación en el archivo `sendmail.cf`, 342
  - niveles de registro, archivo `sendmail.cf`, 366
  - nombre de nodo
    - alias del UUCP, 563, 598
    - equipo remoto del UUCP, 576, 596
  - nombre de usuario, búsqueda de usuarios que iniciaron sesión en un sistema remoto, 660
  - nombres de buzón, 349
  - nombres de buzón y prefijo `owner-`, 349
  - nombres de buzón y sufijo `-request`, 349
  - nombres de dominio, sistema NFS seguro y, 101
  - nombres de ruta
    - comando `rcp`
      - absolutos o abreviados, 669, 670
      - opciones de sintaxis, 670
    - tilde (`~`) en, 669, 670
  - nombres de usuario
    - búsqueda de usuarios que iniciaron sesión en un sistema remoto, 660
    - inicios de sesión directos o indirectos (`rlogin`), 657
    - usuario actual, 670
  - nombres de usuario, nombres de buzón y, 349
  - nombres/nomenclatura
    - nombre de nodo
      - alias del UUCP, 563, 598
      - equipo remoto del UUCP, 576, 596
  - núcleo, comprobación de respuesta en servidor, 124
  - número de unidad `sppp`, asignación de dirección de PPP, 540
  - números de teléfono en el archivo `Systems`, 578
- O**
- objeto compartido `pppoe.so`, 546, 549
  - opción `-a`
    - comando `umount`, 165
    - comando `showmount`, 174
  - opción `-d`
    - comando `cu`, 572
    - comando `showmount`, 174
  - opción `-e`, comando `showmount`, 174
  - opción `-G`, comando `sendmail`, 391
  - opción `-g`, `daemonlockd`, 146
  - opción `-h`, comando `umountall`, 167
  - opción `-k`, comando `umountall`, 167
  - opción `-L etiqueta`, comando `sendmail`, 391
  - opción `-l`
    - comando `cu`, 572
    - comando `umountall`, 167
  - opción `-O`, comando `mount`, 163
  - opción `-o`
    - comando `share`, 168, 171
  - opción (PPP) `asyncmap`, 516
  - opción (PPP) `auth`, 469
  - opción (PPP) `call`, llamada a un servidor de marcación de entrada, 457
  - opción (PPP) `connect`
    - ejemplo, 450
    - para invocar una secuencia de comandos de chat, 530
  - opción (PPP) `crtstcts`, 448
  - opción (PPP) `local`, 463
  - opción (PPP) `login`
    - en `/etc/ppp/options` para un servidor de marcación de entrada, 469
    - en `/etc/ppp/pap-secrets`, 473, 535
  - opción (PPP) `name`
    - con `noservice`, 548
    - en `/etc/ppp/pap-secrets`, 473
    - para autenticación CHAP, 477
  - opción (PPP) `noauth`, 450, 463
  - opción (PPP) `noccp`, 455
  - opción (PPP) `noipdefault`, 450
  - opción (PPP) `noservice`, 548
  - opción (PPP) `passive`, 463
  - opción (PPP) `persist`, 463
  - opción (PPP) `sync`, 463
  - opción (PPP) `xonxoff`, 456
  - opción `-q`, comando `uustat`, 572
  - opción `-q[!]Isubcadena`, comando `sendmail`, 391
  - opción `-q[!]Rsubcadena`, comando `sendmail`, 391
  - opción `-q[!]Ssubcadena`, comando `sendmail`, 391
  - opción `-r`
    - comando `umountall`, 167
    - comando `uucp`, 573
    - comando `Uutry`, 573
    - comando `mount`, 163



- opción -t, daemonlockd, 146
- opción -U, comando sendmail, 391
- opción -v
  - comando automount, 130
  - comando uucheck, 574
- opción -Ac, comando sendmail, 391
- opción -Am, comando sendmail, 391
- opción anon, comando share, 169
- opción -bP, comando sendmail, 391
- opción bg, comando mount, 160
- opción cachefs, mapas autofs, 114
- opción CALLBACK del archivo Permissions, 600
- opción COMMANDS del archivo Permissions, 600–602, 604
  - opción VALIDATE, 603
- opción de montaje de archivo en primer plano, 160
- opción de montaje de archivo en segundo plano, 160
- opción de montaje de E/S directas, 160
- opción -F, comando unshareall, 173
- opción fg, comando mount, 160
- opción forcedirectio, comando mount, 160
- opción hard, comando mount, 163
- opción hsf, mapas autofs, 112
- opción index
  - en archivo dfstab, 88
  - mensaje de error: sin opción public, 134
  - mensaje de error de argumento incorrecto, 133
  - WebNFS y, 105
- opción -intr, comando mount, 123
- opción largefiles
  - comando mount, 161
  - mensaje de error, 136
- opción log
  - comando share, 169
  - en archivo dfstab, 89
- opción MYNAME del archivo Permissions, 598
- opción nolargefiles
  - comando mount, 93, 161
  - en archivo vfstab, 93
  - mensaje de error, 136
- opción NOREAD del archivo Permissions, 600
- opción nosuid, comando share, 169
- opción NOWRITE del archivo Permissions, 600
- opción nthreads, daemon lockd, 146
- opción -o, comando mount, 163
- opción OTHER del archivo Permissions, 603
- opción pcfs, mapas autofs, 113
- opción PidFile, comando sendmail, 392
- opción ProcessTitlePrefix, comando sendmail, 392
- opción public
  - comando mount, 95, 162
  - en archivo dfstab, 88
  - mensaje de error de uso compartido, 138
  - WebNFS y, 105
- opción -qf, comando sendmail, 391
- opción -qGnombre, comando sendmail, 391
- opción -qptiempo, comando sendmail, 391
- opción READ del archivo Permissions, 599
- opción REQUEST del archivo Permissions, 597
- opción ro
  - comando mount, 162
  - comando mount con indicador -o, 163
  - comando share, 168, 171
- opción root, comando share, 169
- opción rw
  - comando mount, 162
  - comando share, 168
- opción rw=client, comando umountall, 168
- opción sec=dh
  - archivo dfstab, 103
  - mapa auto\_master, 103
- opción SENDFILES del archivo Permissions, 598
- opción soft, comando mount, 163
- opción VALIDATE del archivo Permissions, 602, 603
  - opción COMMANDS, 600, 602
- opción WRITE del archivo Permissions, 599
- opciones (PPP)
  - análisis por el daemon pppd, 511
  - asynmap, 516
  - auth, 469
  - call, 457, 519
  - connect, 450, 530
  - crtscs, 448
  - debug, 492
  - directrices de uso, 509–517
  - init, 462, 516
  - local, 463
  - login, 469, 535



## opciones (PPP) (*Continuación*)

- name, 473
- noauth, 450, 463
- noccp, 455
- noipdefault, 450
- noservice, 548
- passive, 463
- persist, 463
- privilegios de opciones, 512
- sync, 463
- xonxoff, 456
- opciones de línea de comandos de la versión 8.12
  - comando sendmail, 389, 391, 392
- opciones de uso compartido de archivos, 168
- opciones en el comando sendmail
  - opción PidFile, 392
  - opción ProcessTitlePrefix, 392
- opciones de archivo de configuración en la versión 8.13, 385–387
- opciones de línea de comandos de la versión 8.12, 389, 391, 392
- opciones de línea de comandos en la versión 8.13, 385
- opciones para PPP -debug, 492
- opciónrw, comando share, 171
- operación de reenvío (UUCP), 604
- owner-owner y nombres de buzón, 349

## P

- palabra clave ACU del campo Type, 584
- palabra clave Any
  - archivo Grades (UUCP), 606, 608
  - campo Speed (UUCP), 578
- palabra clave del campo User-job-grade, 606
- palabra clave direct del campo DTP, 586
- palabra clave Direct del campo Type, 583
- palabra clave Group del campo Permit-type, 608
- palabra clave NFS\_CLIENT\_VERSMAX, 142
- palabra clave NFS\_CLIENT\_VERSMIN, 142
- palabra clave NFS\_SERVER\_DELEGATION, 142
- palabra clave NFS\_SERVER\_VERSMAX, 142
- palabra clave NFS\_SERVER\_VERSMIN, 142
- palabra clave NFSMAPID\_DOMAIN, 142, 193

- palabra clave Non-group del campo Permit-type, 608
- palabra clave Non-user del campo Permit-type, 607
- palabra clave User del campo Permit-type, 607
- palabra clave uudirect del campo DTP, 586
- palabras clave
  - archivo Grades, 606, 607, 608
  - campo Type del archivo Devices, 583
  - negociación de versión en NFS, 182–183
- paquetes descartados, 679
- parámetro GRACE\_PERIOD, daemon lockd, 146
- parámetro LOCKD\_GRACE\_PERIOD, daemon lockd, 146
- parámetro LOCKD\_RETRANSMIT\_TIMEOUT, daemon lockd, 146
- parámetro LOCKD\_SERVERS, daemon lockd, 146
- parámetro nfsmapid\_domain, 150
- paridad
  - archivo Dialers, 593
  - archivo Systems, 582
- Perl 5, introducción, 46–47
- permisos
  - copia de requisitos, 671
  - mejora de NFS versión 3, 78
- permisos de archivo
  - mejora de NFS versión 3, 78
  - WebNFS y, 105
- plantilla /etc/ppp/myisp-chat.tmpl, 524–525
- plantilla /etc/ppp/options.ttya.tmpl, 517
- plantilla /etc/ppp/peers/myisp.tmpl, 520
- plantilla /etc/ppp/options.tmpl, 514
- ponderación de servidores en mapas, 219
- PPP
  - autenticación, 419, 421
  - compatibilidad, 410
  - compatibilidad de DSL, 422
  - compatibilidad de RSDI, 416
  - conversión de PPP asíncrono, 555
  - descripción general, 409
  - diferencia de asppp, 411
  - ejemplos de secuencias de comandos de chat, 449
  - enlace de línea arrendada, 417
  - enlace por marcación telefónica, 413
  - mapa de tareas para planificación de PPP, 425
  - opciones para archivos de configuración
    - Ver opciones (PPP)

**PPP (Continuación)**

- partes de un enlace, 413–419, 422–424
- pppd
  - Ver también* comandoppd
- PPPoE, 422
- privilegios de archivos, 512
- problemas comunes, 490
- recursos, externo, 411
- resolución de problemas
  - Ver también* resolución de problemas de PPP
- resumen de archivos de configuración, 510
- RFC relacionados, 412
- PPP asíncrono (asppp)
  - archivos en una configuración, 551
  - configuración de bases de datos del UUCP, 564
  - conversión a Solaris PPP 4.0, 555
  - diferencia de Solaris PPP 4.0, 411
  - documentación, 410
- PPP de Universidad Nacional de Australia (ANU, Australian National University), compatibilidad con Solaris PPP 4.0, 410
- PPP síncrono
  - Ver* enlace de línea arrendada
  - configuración de dispositivos síncronos, 460
- PPPoE
  - configuración de un servidor de acceso, 487, 488
  - configuración un servidor de acceso, 485
  - descripción general, 422
  - DSLAM, 424
  - lista de comandos y archivos, 541
  - mapas de tareas para configuración, 481
  - obtención de rastreos snoop, 505
  - planificación del túnel, 438, 440, 441
  - proporcionar servicios desde un servidor de acceso, 544–546, 546
  - resolución de problemas comunes, 504, 505
- prefijo owner-, alias de correo con, 350
- probar
  - alias de correo, 333
  - conexiones de correo con otros sistemas, 334–335
  - configuración de correo, 332
  - conjuntos de reglas, 333
- problema de configuración de transporte, mensaje de error, 133
- problemas con ACL en NFS, evitar, 193
- programa chat en PPP, *Ver* secuencia de comandos de chat
- programación de daemon para UUCP, 561
- programas, cuelgue, 137
- propiedad net.slp.DAActiveDiscoveryInterval, 245
  - definición, 244
- propiedad net.slp.DAAddresses, 248, 260, 265
  - definición, 245
- propiedad net.slp.DAAttributes, 249
- propiedad net.slp.DAHeartBeat, 248, 250
  - definición, 244
- propiedad net.slp.interfaces
  - cambio de interfaces, 268
  - configuración, 266
  - DA y, 264
  - hosts múltiples y, 269
  - interfaces no enrutadas y, 269
- propiedad net.slp.isBroadcastOnly, 253, 266
- propiedad net.slp.isDA, 244
- propiedad net.slp.MTU, 252
- propiedad net.slp.multicastTTL, 250
- propiedad net.slp.passiveDADetection, 245
  - definición, 244
- propiedad net.slp.randomWaitBound, 256
- propiedad net.slp.serializedRegURL, 273
- propiedad net.slp.useScopes, 259–260, 260, 275
  - definición, 258
- Protocolo de autenticación de contraseña (PAP)
  - archivo /etc/ppp/pap-secrets, 532
  - configuración
    - emisores de llamadas de confianza, 471–472, 472, 473
    - en un servidor de marcación de entrada, 469–470
  - creación de una base de datos de credenciales de PAP, 467–469
  - definición, 532
  - ejemplo de configuración, 434
  - mapas de tareas, 466–467
  - planificación, 466
  - proceso de autenticación, 534
  - sugerencias para contraseñas, 533
  - uso de la opción login, 535

- Protocolo de autenticación por desafío mutuo (CHAP)
    - definición, 535
    - ejemplo de configuración, 436
    - mapas de tareas para configuración, 474–475
    - proceso de autenticación, 538
    - sintaxis de `/etc/ppp/chap-secrets`, 536
  - protocolo de transporte, negociación NFS, 194
  - protocolo `e` en el archivo `Devices`, 589
  - protocolo `f` en el archivo `Devices`, 589
  - protocolo `g` en el archivo `Devices`, 588
  - protocolo ICMP, 680
  - protocolo IGMP, 680
  - Protocolo punto a punto, *Ver* PPP
  - protocolo `t` en el archivo `Devices`, 588
  - protocolo TCP, 680
  - protocolo UDP, 680
  - protocolos de transmisión de dispositivos, 588, 589
  - proyectos, consolidación de archivos, 116
  - prueba, fiabilidad de paquetes, 677
  - puertas de enlace de correo
    - configurar una puerta de enlace de correo, 300
    - probar, 332
  - puertas de enlace del correo
    - archivo `sendmail.cf` y, 353
    - configuración, 353
    - definición, 353
  - puerto de serie
    - configuración
      - equipo de marcación de salida, 446–447
      - para un servidor de marcación de entrada, 452
    - configuración en un servidor de marcación de entrada, 516
  - puertos
    - entrada del archivo `Devices`, 585
    - UUCP, 570
  - punto (`.`)
    - en direcciones de dominio, 347
    - en nombres de buzón, 349
    - sintaxis de comando `rcp`, 671, 673
  - punto de montaje `/home`, 206, 207
  - punto de montaje `/net`, 207
  - puntos de montaje
    - `/-` como punto de montaje de mapa maestro, 206, 209
  - puntos de montaje (*Continuación*)
    - evitar conflictos, 111
    - `/home`, 206, 207
    - `/net`, 207
- R**
- rastreo snoop, para PPPoE, 505
  - recuperación de cliente, NFS versión 4, 187–189
  - red de área extensa (WAN)
    - Usenet, 559, 575
  - red de área local (LAN), configuración del UUCP, 560
  - redes
    - comandos para supervisar rendimiento, 677
    - mostrar información de rendimiento, 677, 678, 679, 685
    - estadísticas de cliente, 683, 685
    - estadísticas de interfaz, 679, 682
    - estadísticas de servidor, 683, 685
    - respuesta de host, 678
    - tabla de enrutamiento IP, 681
    - tasa de colisiones, 680
  - paquetes
    - cantidad transmitida, 680
    - capturar de red, 677, 679
    - descartados, 679
    - enviar a hosts, 678
    - prueba de fiabilidad, 677, 678
    - tasas de errores, 680
  - rastrear llamadas de clientes a servidores, 677, 679
  - resolución de problemas
    - componentes de hardware, 685
    - tasa de retransmisión alta, 682
  - redes TCP/IP
    - UUCP mediante, 569, 570
  - registro
    - limpieza de archivo de registro del UUCP, 569
    - visualización de archivos de registro del UUCP, 561
  - registro de proxy (SLP), hosts múltiples, 268
  - registro del proxy (SLP), 272, 274
  - registro del servidor NFS, descripción general, 83
  - registros del agente de intercambio de correo (MX), 302

- replicación de archivos compartidos entre varios servidores, 119
- resolución de problemas
  - alias de correo, 333
  - autofs, 129
    - diversos mensajes de error, 131
    - evitar conflictos de punto de montaje, 111
    - mensajes de error generados por automount -v, 130
  - conexiones de correo con otros sistemas, 334–335
  - conjuntos de reglas, 333
  - correo no entregado, 333
  - mensajes MAILER-DAEMON y, 336
- NFS
  - cuelgue de programas, 137
  - determinación de si se produjo una falla en el servicio NFS, 128
  - estrategias, 123
  - problemas de montaje remoto, 124, 135
  - problemas de servidor, 124
- redes, 682, 685
- servicios de correo, 331
- UUCP, 572, 614
  - comandos para solucionar problemas, 574
  - comprobación de información básica, 574
  - comprobación de mensajes de error, 574
  - comprobación del archivo Systems, 574
  - depuración de transmisiones, 572, 573
  - mensajes de error, 614
  - mensajes de error ASSERT, 574, 612, 613
  - mensajes de error STATUS, 574, 613, 614
  - módem o ACU con errores, 572
- resolución de problemas de PPP
  - mapa de tareas, 489
  - obtención de diagnósticos, 491–492, 492
  - problemas comunes, 490
    - autenticación, 507
    - comunicaciones generales, 497
    - con la configuración de PPP, 498
    - enlaces de líneas arrendadas, 506
    - líneas de serie, 503
    - para redes, 495
    - secuencia de comandos de chat, 501
    - secuencias de comandos de chat, 500, 502

- resolución de problemas NFS
  - cuelgue de programas, 137
  - determinación de si se produjo una falla en el servicio NFS, 128
  - estrategias, 123
  - problemas de montaje remoto, 135
  - problemas de servidor, 124
- RPC, 682, 683
  - autenticación, 203
  - segura
    - descripción general, 203
  - seguras
    - problemas de autorización DH, 205
- RPC segura, descripción general, 203
- RPC seguras
  - problemas de autorización DH, 205
- RPCSEC\_GSS, 82
- RSDI en un enlace de PPP, 416

## S

- s, comando umountall, 167
- SA (SLP), 259, 267, 272
- secuencia de comandos /etc/init.d/ncakmod, 63
- secuencia de comandos /etc/init.d/slpd, 273
- secuencia de comandos
  - /etc/mail/cf/sh/check-hostname, 361
- secuencia de comandos
  - /etc/mail/cf/sh/check-permissions, 360
- secuencia de comandos /usr/sbin/etrn, 361
- secuencia de comandos check-hostname, 299, 301, 361
- secuencia de comandos check-permissions, 360
- secuencia de comandos de chat
  - creación de un programa de chat ejecutable, 531
  - diseño de secuencia de comandos de chat, 522
- ejemplos (PPP)
  - para un adaptador de terminal RDSI, 528–530
  - secuencia de comandos de chat de inicio de sesión de estilo UNIX, 449, 526–528
  - secuencia de comandos de chat de módem básica, 523–524
  - secuencia de comandos de chat para llamar a un ISP, 525–526
- invocar, en PPP, 530–531

- secuencia de comandos de chat para un adaptador de terminal (TA), 528–530
- secuencia de comandos de conversión asppp2pppd
  - configuración asppp estándar, 551
  - conversión a Solaris PPP 4.0, 555
  - visualización de archivos convertidos a Solaris PPP 4.0, 555
- secuencia de comandos de inicialización para PPP demand, 463
- secuencia de comandos de shell uudemon.admin, 569
- secuencia de comandos de shell uudemon.cleanup, 569
- secuencia de comandos de shell uudemon.hour
  - descripción, 568
  - ejecución de daemon uusched por, 561
  - ejecución del daemon uuxqt por, 560
- secuencia de comandos de shell uudemon.poll, 605
- secuencia de comandos/etc/init.d/nalogd, 63
- secuencia de comandos etrn, 361
- secuencia de comandos gen-etc-shells, 330
- secuencia de comandos nalogd, 63
- secuencias de comandos
  - secuencias de comandos de chat (UUCP), 581
    - campo expect, 579
    - caracteres de escape, 580
    - formato, 579
    - habilitación de devolución de llamada, 581
    - secuencia de comandos básica, 579
  - secuencias de comandos de shell (UUCP), 567, 569
- secuencias de comandos de shell (UUCP), 567, 569
  - ejecución automática, 567
  - ejecución manual, 567
  - uudemon.admin, 569
  - uudemon.cleanup, 569
  - uudemon.hour
    - descripción, 568
  - uudemon.hour
    - ejecución de daemon uusched por, 561
    - ejecución del daemon uuxqt por, 560
  - uudemon.poll, 568, 605
- secuencias de comandos de shell uudemon.poll, 568
- seguridad
  - aplicación de restricciones autofs, 120
  - autenticación DH
    - autenticación de usuario, 202
  - seguridad, autenticación DH (*Continuación*)
    - descripción general, 204
    - descripción general, 204
    - opción de archivo dfstab, 103
    - protección con contraseña, 203
  - autenticación UNIX, 202, 203
  - NFS versión 3 y, 78
  - problemas de archivo /etc/hosts.equiv, 656
  - problemas de archivo .rhosts, 656, 659
  - problemas de operación de copia, 669
  - problemas en el uso compartido de archivos, 168, 170
  - RPC segura
    - descripción general, 203
  - RPC seguras
    - problemas de autorización DH, 205
  - sistema NFS seguro
    - administración, 101
    - descripción general, 202
  - UUCP
    - bit de permanencia para archivos de directorio público, 571
    - configuración, 570
    - opción COMMANDS del archivo
      - Permissions, 600, 602
    - opción VALIDATE del archivo
      - Permissions, 602, 603
- seguridad de capa de transporte (TLS) y SMTP
  - consideraciones de seguridad relacionadas con, 385
  - opciones de archivo de configuración para, 381–383
- seguridad de la capa de transporte (TLS) y SMTP
  - conjuntos de reglas para, 384
  - descripción, 380–385
- Seguridad de la capa de transporte (TLS) y SMTP,
  - información de tarea, 307–312
- seguridad de la capa de transporte (TLS) y SMTP
  - macros para, 383–384
- seguridad y NFS
  - descripción, 80, 192–194
  - mensaje de error, Permission denied, 137
- selección de modo de seguridad y comando mount, 162
- servicio de nombres DNS, programa sendmail y, 302
- servicio de nombres NIS, actualización de mapas autofs, 109

- servicio de nombres NIS+, actualización de mapas autofs, 109
- servicio WebNFS
  - cortafuegos y, 106
  - descripción, 200–201
  - descripción general, 82
  - explorar, 105–106
  - habilitación, 88
  - mapa de tareas, 103
  - planificación para, 104–105
  - tipos de servicio URL y, 106
- servicios antiguos (SLP)
  - anuncios, 271, 275
  - definición, 271
- servicios de bases de datos, puerto del UUCP, 570
- servicios de bases de datos de redes, puerto del UUCP, 570
- servicios de correo
  - cambios a sendmail de la versión 8.12, 388
  - cambios a sendmail en la versión 8.13, 379–388
  - componentes de hardware
    - cliente de correo, 353
    - elementos necesarios, 351
    - host de correo, 351
    - puerta de enlace del correo, 353
    - servidor de correo, 352
  - componentes de software, 343
    - agente de entrega local, 344
    - agente de transferencia de correo, 344
    - agente de usuario de correo, 343–344
    - alias de correo, 350
    - aplicaciones de correo, 344
    - archivos de buzón, 348
    - direcciones de correo, 346
  - mapas de tareas
    - administrar archivos .forward, 328
    - administrar archivos de alias de correo, 313
    - administrar los directorios de la cola, 324
    - configurar servicios de correo, 294
    - mapa de tareas integral, 289
    - procedimientos y consejos para la resolución de problemas, 331
  - planificación del sistema de correo, 291

- servicios de envío de correo
  - aplicaciones de correo de Solaris, 344
  - servicios de envío de correo de Solaris, 344
  - servicios de envío de correo del comando UNIX-to-UNIX Copy (UUCP), 345
  - servicios de envío de correo del protocolo simple de transferencia de correo (SMTP), 345
- servicios de nombres, métodos de mantenimiento de mapas autofs, 109
- servicios NFS
  - detención, 97
  - inicio, 97
  - mapa de tareas, 96
  - reinicio, 128
  - selección de diferentes versiones en cliente mediante modificación del archivo /etc/default/nfs, 100
  - uso del comando mount, 101
  - selección de diferentes versiones en servidor, 98–99
- servidor de acceso (PPP)
  - archivo /etc/ppp/chap-secrets, 548
  - archivo /etc/ppp/options, 547
  - archivo /etc/ppp/pap-secrets, 548
  - comandos y archivos para configuración, 543, 544–546
  - configuración, para PPPoE, 485, 487, 546–548
  - definición, 422
  - mapa de tareas para configuración, 481–482
  - planificación de mapa de tareas, 439
  - restricción de una interfaz para clientes PPPoE, 487
- servidor de marcación de entrada
  - configuración
    - autenticación CHAP, 475, 477
    - autenticación PAP, 467–469, 469–470
    - comunicaciones de línea de serie, 456–457, 516
    - módem, 452
    - puerto de serie, 452
  - creación de cuentas para usuarios de PPP, 454
  - definición, 414
  - información de planificación, 427, 453
  - mapa de tareas para configuración, 451–452
  - recepción de llamadas, 457–458
  - UUCP, 581
- servidor de SA (SLP), 256

- servidor FTP, nowait, 646
- servidor NTP, configuración, 68
- servidores
  - Ver también* servidores NFS
  - bloqueos y claves secretas, 205
  - configuración de servidor de directorio principal, 115
  - mostrar información sobre, 677, 683, 685
  - rastrear llamadas de clientes a, 677, 679
  - selección de archivos de autofs, 216
  - servicios NFS, 75
  - servidores NFS y archivo `vfstab`, 91
- servidores de correo, 352
  - buzones en, 349, 352
  - configurar un servidor de correo, 328
  - copias de seguridad y, 352
  - descripción, 352
  - requisitos de espacio para, 352
- servidores NFS
  - daemons requeridos para montaje remoto, 123
  - identificación actual, 128
  - mantenimiento, 86
  - ponderación en mapas, 219
  - replicación de archivos compartidos, 119
  - resolución de problemas
    - problemas de montaje remoto, 124, 135
    - resolución de problemas, 124
  - selección autofs de archivos, 219
- servidores y clientes, servicio NFS, 75
- sesiones ftp
  - apertura de conexiones de sistema remoto, 664
  - cierre de conexiones de sistema remoto, 664
  - copia de archivos
    - a sistema remoto, 666
    - del sistema remoto, 665
  - cuentas de ftp anónimas, 662
- signo de almohadilla (#)
  - comentarios en mapa maestro (auto\_master), 207
  - comentarios en mapas directos, 209
  - comentarios en mapas indirectos, 210
- signo de número (#)
  - comentarios en mapa maestro (auto\_master), 207
  - comentarios en mapas directos, 209
  - comentarios en mapas indirectos, 210
- signo de porcentaje (%) en nombres de buzón, 349
- signo igual (=) en abreviatura de código de marcación, 579
- signo más (+)
  - en nombres de mapas autofs, 220, 221
  - sintaxis de archivo `/etc/hosts.equiv`, 655, 656
- signo menos (-), sintaxis de archivo `/etc/hosts.equiv`, 655
- sincronización de hora, con otro sistema, 69
- sincronización de tiempo, 204
- sistema de archivos replicado, 197–198
- sistema NFS seguro
  - administración, 101
  - autenticación DH y, 102
  - configuración, 102
  - descripción general, 202
  - nombre de dominio, 101
- sistemas de archivos
  - estadísticas de red para, 683, 685
- sistemas de archivos locales, desmontaje de grupos, 167
- sistemas de archivos montados en NFS
  - clientes de correo y, 294, 297
  - servidores de correo y, 295
- sistemas de archivos remotos
  - desmontaje de grupos, 167
  - lista de clientes con sistemas de archivos montados remotamente, 174
- sistemas de archivos y NFS, 75
- sistemas operativos
  - admitir versiones incompatibles, 119
  - variables de mapa, 220
- sistemas remotos
  - cierre de sesión (salida), 661, 662
  - copia de archivo remota
    - uso de comando `ftp`, 663
  - copia remota
    - uso de `rcp`, 668, 673
  - definición, 619
  - inicio de sesión, 654, 664
  - verificación de operación, 659
- SLP
  - agentes y procesos, 230–232
  - ajuste de rendimiento, 249



**SLP** (*Continuación*)

- análisis de un rastreo de snoop slp, 237
- anuncios, 262
- archivo de configuración, 241, 242–243
- arquitectura, 229
- configuración, 235–236
- daemon, 232
- enrutamiento de difusión, 253
- implementación, 232
- planificación de implementación, 235–236
- propiedades de configuración, 242
- registro, 229
- solicitudes de detección, 254
- tamaño de paquete, 252

SLPv2, interoperabilidad con SLPv1, 262

SMTP (protocolo simple de transferencia de correo)

- archivo sendmail.cf, 390
- servicios de envío de correo, 345

SMTP y TLS

- conjuntos de reglas para, 384
- consideraciones de seguridad relacionadas con, 385
- descripción, 380–385
- información de tarea, 307–312
- macros para, 383–384
- opciones de archivo de configuración para, 381–383

sockets, NCA y, 52

Solaris, versión de UUCP, 575

Solaris PPP 4.0, *Ver* PPP

Solicitudes de comentarios (RFC), PPP, 412

solicitudes de detección (SLP), 254

solicitudes de servicio (SLP), 262

sondeo de equipos remotos (UUCP), 563, 605

STREAMS, configuración de dispositivos, 608

subcampo retry del campo Time, 577

subcomandos ftp, descripción, 663

subrayado ( \_ ) en nombres de buzón, 349

superposición de sistema de archivos ya montado, 163

superusuarios, autofs y contraseñas, 77

**T**

- tabla de enrutamiento IP, 681
- tabla mail\_aliases NIS+, 369

- tabla NIS+ mail\_aliases
  - agregar alias en, 316
  - agregar entradas mediante edición, 317
  - editar entradas en, 318
  - eliminar entradas de, 319
  - iniciar tablas, 315
  - mostrar coincidencias parciales, 316
  - mostrar todo el contenido de, 315
  - mostrar una entrada individual en, 316
- tamaño de archivo de transferencia, negociación, 194–195
- tamaño de paquete, configuración para SLP, 252
- tareas de configuración para PPP
  - autenticación, 465–466
  - diagnóstico de problemas de configuración, 498
  - enlace por marcación telefónica, 443
  - líneas arrendadas, 459
  - túnel PPPoE, 481
- tasa de colisiones (red), 680
- TCP, NFS versión 3 y, 80
- tiempo de sincronización, 204
- tiempos de espera (SLP), 254, 262
- tilde (~)
  - nombres de ruta abreviados, 669, 670
  - sintaxis de comando rcp, 671, 673
- tipo de dispositivo para enlace de comunicación del UUCP, 578
- tipo de lectura y escritura
  - montaje de sistemas de archivos como, 162
  - uso compartido de sistemas de archivos, 168, 171
- tipo de sistema de archivos de antememoria
  - acceso autofs utilizando, 113, 114
- tipo de sólo lectura
  - montaje de sistemas de archivos como, 162, 163
  - selección de archivo por autofs, 219
  - selección de archivos por autofs, 216
  - uso compartido de sistemas de archivos, 168, 171
- tipos de enlace en PPP
  - comparación de líneas arrendadas y por marcación telefónica, 417
  - línea arrendada, 417
  - marcación telefónica, 413
  - medios de enlace físico, 413
  - partes de un enlace, 413



tipos de mensaje, SLP, 278–279  
tipos de mensaje del SLP, 278–279  
tipos de seguridad, 82  
tipos de servicio URL, WebNFS y, 106  
TLS y SMTP  
conjuntos de reglas para, 384  
consideraciones de seguridad relacionadas con, 385  
descripción, 380–385  
información de tarea, 307–312  
macros para, 383–384  
opciones de archivo de configuración para, 381–383  
tokens (pares de marcador y token), 586, 588  
tráfico TCP/IP, 677, 679, 680  
transferencias de archivos (UUCP)  
archivos de trabajo C., 610, 611  
daemon, 560  
permisos, 597, 600  
resolución de problemas, 572, 573  
túnel  
definición (PPP), 422  
ejemplo de configuración, 440, 441  
mapas de tareas para configuración, 481

## U

UA, solicitudes, 249  
UA (SLP), 236, 262  
tiempo de espera de solicitudes, 264  
UDP, NFS y, 80–81  
unidad de llamada automática (ACU)  
campo Type del archivo Devices, 584  
configuración de hardware del UUCP, 559  
resolución de problemas, 572  
unidad de servicio de canal/unidad de servicio de datos  
(CSU/DSU), definición, 418  
unidifusión UDP/TCP (SLP), 265  
URL de NFS  
autofs y, 121  
montaje con, 83  
montaje de sistemas de archivos con, 95–96  
sintaxis, 105–106  
WebNFS y, 104  
URL NFS, ejemplo de comando mount, 164  
Usenet, 559, 575

uso compartido, otorgamiento de acceso root, 169  
uso compartido de archivos  
acceso de lectura y escritura, 168, 171  
acceso de sólo lectura, 168, 171  
descripción general, 167  
ejemplos, 171  
mejoras de la versión 3 de NFS, 81  
problemas de seguridad, 168, 170, 202  
replicación de archivos compartidos entre varios  
servidores, 119  
sistemas de archivos múltiples, 173  
sólo para los clientes mostrados, 168  
uso no compartido, 173  
usuarios no autenticados y, 169  
uso compartido de sistema de archivos, automático, 86  
uso compartido de sistema de archivos automático, 86  
uso compartidos de archivos, acceso de sólo  
lectura, 168  
uso no compartido de sistemas de archivos  
comando unshare, 172  
comando unshareall, 173  
usuario actual, 670  
usuario anónimo de ftp, configuración, 633  
usuario invitado de ftp, configuración, 632  
usuario real de ftp, configuración, 631  
utilidad pppoec  
definición, 549  
obtención de diagnósticos, 505  
UUCP  
"shell de inicio de sesión", 560  
acumulación de correo, 571  
archivos administrativos, 610, 611  
archivos de base de datos, 563, 609  
archivos de configuración básica, 564  
configuración de asppp, 564  
descripción, 563, 564  
varios o diferentes archivos, 563, 575, 595  
archivos de registro  
limpieza, 569  
visualización, 561  
cola de impresión  
comando cleanup, 561  
definiciones de niveles de trabajo, 605, 608  
programación de daemon, 561

**UUCP (Continuación)**

- comandos administrativos, 561, 562
- comandos de usuario, 562
- configuración
  - adición de inicios de sesión del UUCP, 566, 567
  - ejecución de UUCP mediante TCP/IP, 570
  - ejecución del UUCP mediante TCP/IP, 569
- configuración de STREAMS, 608
- configuraciones de hardware, 559
- daemons
  - descripción general, 560, 561
- descripción, 559, 575
- directorios
  - administración, 561
  - mantenimiento del directorio público, 571
  - mensajes de error, 574
- ejecución remota
  - archivos de trabajo C., 610, 611
  - comandos, 597, 600, 603
  - daemon, 560
- inicios de sesión
  - adición, 566, 567
  - privilegios, 602, 603
- inicios de sesión y contraseñas con privilegios, 602, 603
- mantenimiento, 571, 572
- mantenimiento del directorio público, 571
- modo pasivo, 598
- nombre de nodo
  - alias, 563, 598
  - equipo remoto, 576, 596
- opción CALLBACK, 600
- operación de reenvío, 604
- resolución de problemas, 572, 614
  - ACU con errores, 572
  - comandos para solucionar problemas, 574
  - comprobación de información básica, 574
  - comprobación de mensajes de error, 574, 614
  - comprobación del archivo Systems, 574
  - depuración de transmisiones, 572, 573
  - mensajes de error ASSERT, 574, 612, 613
  - mensajes de error STATUS, 574, 613, 614
  - módem con errores, 572
- secuencias de comandos de shell, 567, 569

**UUCP (Continuación)**

- seguridad
  - bit de permanencia para archivos de directorio público, 571
- configuración, 570
- opción COMMANDS del archivo
  - Permissions, 600, 602
- opción VALIDATE del archivo
  - Permissions, 602, 603
- sobrescritura manual de parámetros, 605
- sondeo de equipos remotos, 563, 605
- transferencias de archivos
  - archivos de trabajo C., 610, 611
  - daemon, 560
  - permisos, 597, 600
  - resolución de problemas, 572, 573
- velocidad de transferencia, 578, 585
- versión de Solaris, 559, 575
- visualización de archivos de registro, 561
- UUCP (comando de copia de UNIX a UNIX), probar la conexión, 332
- UUCP (comando UNIX-to-UNIX Copy), servicios de envío de correo, 345

**V**

- opción -V, comando umount, 165
- valor ALL en la opción COMMANDS, 602
- variable de mapa ARCH, 219
- variable de mapa CPU, 220
- variable de mapa de tipo de procesador, 220
- variable de mapa HOST, 220
- variable de mapa OSNAME, 220
- variable Port Selector en el archivo Devices, 584
- variable Sys-Name del campo Type, 584
- variables en entradas de mapa, 219
- variables en entradas de mapas, 220
- varios archivos (ftp), 665
- velocidad de transferencia para el enlace de comunicación del UUCP, 578, 585
- verificación, operación de sistema remoto, 659
- verificadores, sistema de autenticación RPC, 203
- vinculación de inicios de sesión remotos, 657

**W**

WebNFS servicio, seguridad negociaciones y, 83

**Y**

Y comercial (&), en mapas autofs, 224

