

# **Administration d'Oracle® Solaris : Services IP**

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 END USERS:

Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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.

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. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation.

# Table des matières

---

<b>Préface</b> .....	19
<b>Partie I Administration TCP/IP</b> .....	23
<b>1 Planification du développement du réseau</b> .....	25
Planification réseau (liste des tâches) .....	25
Détermination du matériel réseau .....	26
Choix du format d'adressage IP du réseau .....	27
Adresses IPv4 .....	27
Adresses DHCP .....	28
Adresses IPv6 .....	29
Adresses privées et préfixes de documentation .....	29
Obtention du numéro IP du réseau .....	29
Attribution de noms aux entités du réseau .....	30
Administration des noms d'hôtes .....	30
Sélection d'un service de noms et d'un service d'annuaire .....	31
Utilisation de sous-réseaux .....	32
Déploiement de réseaux virtuels .....	32
<b>2 Eléments à prendre en compte lors de l'utilisation d'adresses IPv6</b> .....	33
Planification IPv6 (liste des tâches) .....	33
Scénario de topologie de réseau IPv6 .....	34
Vérification de la prise en charge d'IPv6 .....	36
Préparation d'un plan d'adressage IPv6 .....	37
Obtention d'un préfixe de site .....	37
Création du schéma de numérotation IPv6 .....	37
Configuration des services réseau pour la prise en charge d'IPv6 .....	39

▼ Procédure de préparation de services réseau pour la prise en charge d'IPv6 .....	39
▼ Procédure de préparation de DNS pour la prise en charge d'IPv6 .....	40
Planification de l'utilisation de tunnels dans le réseau .....	41
Considérations de sécurité relatives à l'implémentation d'IPv6 .....	42
<b>3 Configuration d'un réseau IPv4 .....</b>	<b>43</b>
Configuration réseau (liste des tâches) .....	44
Avant de commencer la configuration réseau .....	44
Configuration des composants système sur le réseau .....	45
Topologie du système autonome IPv4 .....	45
▼ Procédure de configuration d'une interface IP .....	47
Modes de configuration système .....	51
Configuration d'un routeur IPv4 .....	56
▼ Procédure de configuration d'un routeur IPv4 .....	57
Tables et types de routage .....	59
Configuration des hôtes multiréseaux .....	62
Configuration du routage de systèmes à interface unique .....	65
Ajout d'un sous-réseau à un réseau .....	68
Contrôle et modification des services de couche transport .....	70
▼ Journalisation des adresses IP de toutes les connexions TCP entrantes .....	71
▼ Ajout de services utilisant le protocole SCTP .....	71
▼ Contrôle d'accès aux services TCP à l'aide des wrappers TCP .....	74
<b>4 Activation d'IPv6 sur le réseau .....</b>	<b>77</b>
Configuration d'une interface IPv6 .....	77
▼ Procédure de configuration d'un système pour IPv6 .....	78
▼ Procédure de désactivation de la configuration automatique des adresses IPv6 .....	80
Configuration d'un routeur IPv6 .....	80
▼ Procédure de configuration d'un routeur compatible IPv6 .....	80
Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs .....	82
Utilisation d'adresses temporaires pour une interface .....	83
Configuration d'un jeton IPv6 .....	86
Administration d'interfaces compatibles IPv6 sur des serveurs .....	88
Configuration de prise en charge de services de noms pour IPv6 .....	89
▼ Procédure d'ajout d'adresses IPv6 à DNS .....	89

▼ Procédure d'affichage des informations relatives au service de noms IPv6 .....	90
▼ Procédure de vérification de la mise à jour correcte des enregistrements PTR DNS IPv6 ..	91
▼ Procédure d'affichage d'informations IPv6 à l'aide de NIS .....	91
<b>5 Administration d'un réseau TCP/IP .....</b>	<b>93</b>
Principales tâches d'administration TCP/IP (liste des tâches) .....	94
Contrôle du statut du réseau à l'aide de la commande <code>netstat</code> .....	95
▼ Affichage des statistiques par protocole .....	95
▼ Affichage du statut des protocoles de transport .....	96
▼ Affichage du statut de l'interface réseau .....	98
▼ Affichage du statut des sockets .....	98
▼ Affichage du statut des transmissions de paquets associés à un type d'adresse spécifique	100
▼ Affichage du statut des routes connues .....	100
Test des hôtes distants à l'aide de la commande <code>ping</code> .....	102
▼ Vérification de l'exécution d'un hôte distant .....	102
▼ Détection de l'abandon de paquets sur un hôte .....	102
Administration et journalisation des affichages de statut du réseau .....	103
▼ Contrôle de la sortie d'affichage des commandes IP .....	103
▼ Journalisation des actions du démon de routage IPv4 .....	104
▼ Suivi des activités du démon de détection des voisins IPv6 .....	105
Affichage des informations de routage à l'aide de la commande <code>traceroute</code> .....	106
▼ Détermination de la route menant à un hôte distant .....	106
▼ Affichage du suivi de toutes les routes .....	106
Contrôle du transfert des paquets à l'aide de la commande <code>snoop</code> .....	107
▼ Vérification des paquets en provenance de toutes les interfaces .....	108
▼ Capture de la sortie de la commande <code>snoop</code> dans un fichier .....	109
▼ Vérification des paquets transmis entre un client et un serveur IPv4 .....	109
▼ Contrôle du trafic réseau IPv6 .....	110
Contrôle des paquets à l'aide de périphériques de couche IP .....	110
Administration de la sélection des adresses par défaut .....	114
▼ Administration de la table des règles de sélection d'adresses IPv6 .....	114
▼ Modification de la table des règles de sélection des adresses IPv6 pour la session en cours uniquement .....	116

<b>6</b>	<b>Configuration de tunnels IP</b>	117
	Présentation des tunnels IP	117
	Administration de tunnels IP dans cette version d'Oracle Solaris	117
	Types de tunnels	118
	Tunnels dans les environnements réseau combinant IPv6 et IPv4	118
	Tunnels 6to4	119
	Déploiement des tunnels	124
	Exigences en matière de création de tunnels	124
	Exigences relatives aux tunnels et aux interfaces IP	125
	Configuration et administration du tunnel avec la commande <code>dladm</code>	126
	Sous-commandes <code>dladm</code>	126
	Configuration des tunnels (liste des tâches)	126
	▼ Création et configuration d'un tunnel IP	127
	▼ Procédure de configuration d'un tunnel 6to4	131
	▼ Procédure de configuration d'un tunnel 6to4 relié à un routeur relais 6to4	133
	▼ Modification d'une configuration de tunnel IP	135
	▼ Affichage d'une configuration de tunnel IP	136
	▼ Affichage des propriétés d'un tunnel IP	137
	▼ Suppression d'un tunnel IP	138
<b>7</b>	<b>Dépannage des problèmes de réseau</b>	139
	Conseils d'ordre général pour le dépannage réseau	139
	Réalisation de diagnostics de base	139
	▼ Vérification logicielle de base sur un réseau	140
	Problèmes courants lors du déploiement d'IPv6	140
	Impossible de mettre à niveau un routeur IPv4 vers IPv6	141
	Problèmes survenant après la mise à niveau de services vers IPv6	141
	Le FAI actuel ne prend pas en charge IPv6	141
	Problèmes de sécurité lors de la création d'un tunnel vers un routeur relais 6to4	142
<b>8</b>	<b>Référence IPv4</b>	143
	Fichiers de configuration réseau	143
	Démon de services Internet <code>inetd</code>	145
	Service SMF <code>name-service/switch</code>	145
	Impact des services de noms sur les bases de données réseau	147

Protocoles de routage dans Oracle Solaris .....	147
RIP (Routing Information Protocol) .....	147
Protocole RDISC (ICMP Router Discovery) .....	148
Tableaux des protocoles de routage dans Oracle Solaris .....	148
<b>9 Référence IPv6 .....</b>	<b>151</b>
Implémentation IPv6 sous Oracle Solaris .....	151
Fichiers de configuration IPv6 .....	151
Commandes associées à IPv6 .....	156
Démons liés à IPv6 .....	160
Protocole ND IPv6 .....	163
Messages ICMP de la détection des voisins .....	164
Processus de configuration automatique .....	164
Sollicitation de voisin et inaccessibilité .....	166
Algorithme de détection d'adresse dupliquée .....	167
Publications de proxy .....	167
Equilibrage de charge entrante .....	167
Modification d'adresse lien-local .....	168
Comparaison du protocole ND et du protocole ARP et autres protocoles IPv4 .....	168
Routage IPv6 .....	170
Publication de routeur .....	170
Extensions IPv6 de services d'assignation de noms Oracle Solaris .....	171
Extensions DNS pour IPv6 .....	172
Modifications apportées aux commandes de services de noms .....	172
Prise en charge IPv6 de NFS et RPC .....	172
Prise en charge d'IPv6 sur ATM .....	172
<b>Partie II DHCP .....</b>	<b>173</b>
<b>10 A propos de DHCP (présentation) .....</b>	<b>175</b>
A propos du protocole DHCP .....	175
Intérêt du protocole DHCP .....	176
Mode de fonctionnement du protocole DHCP .....	177
Serveur DHCP ISC .....	180

Serveur DHCP Sun hérité .....	181
Client DHCP .....	181
<b>11 Administration du service DHCP ISC .....</b>	<b>183</b>
Configuration de l'accès utilisateur aux commandes DHCP .....	183
▼ Procédure d'octroi d'accès aux commandes DHCP .....	183
Tâches du serveur DHCP .....	184
▼ Procédure de désactivation d'un serveur DHCP ISC .....	184
▼ Procédure de modification de la configuration du service DHCP .....	185
<b>12 Configuration et administration du client DHCP .....</b>	<b>187</b>
A propos du client DHCP .....	188
Serveur DHCPv6 .....	188
Différences entre DHCPv4 et DHCPv6 .....	188
Modèle administratif DHCP .....	189
Détails du protocole .....	190
Interfaces logiques .....	190
Négociation d'options .....	191
Syntaxe de configuration .....	191
Démarrage du client DHCP .....	192
Communication DHCPv6 .....	193
Gestion des données de configuration réseau par les protocoles client DHCP .....	193
Arrêt du client DHCP .....	195
Activation et désactivation d'un client DHCP .....	195
▼ Procédure d'activation du client DHCP .....	195
▼ Procédure de désactivation d'un client DHCP .....	196
Administration du client DHCP .....	197
Options de la commande <code>ipadm</code> utilisées par le client DHCP .....	197
Définition des paramètres de configuration du client DHCP .....	198
Systèmes clients DHCP avec plusieurs interfaces réseau .....	199
Noms d'hôtes du client DHCPv4 .....	200
▼ Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique .....	200
Systèmes clients DHCP et services de noms .....	201
Scripts d'événement client DHCP .....	203



<b>13</b>	<b>Commandes et fichiers DHCP (référence)</b>	205
	Commandes DHCP	205
	Fichiers utilisés par le service DHCP	207
	Services SMF utilisés par le service DHCP	208
<b>Partie III</b>	<b>IPsec</b>	209
<b>14</b>	<b>Architecture IPsec (présentation)</b>	211
	Introduction à IPsec	211
	RFC IPsec	213
	Terminologie IPsec	213
	Flux de paquets IPsec	214
	Associations de sécurité IPsec	217
	Gestion des clés dans IPsec	217
	Mécanismes de protection IPsec	218
	En-tête Authentification	218
	ESP (Encapsulating Security Payload, association de sécurité)	219
	Authentification et chiffrement dans IPsec	220
	Stratégies de protection IPsec	221
	Modes Transport et Tunnel dans IPsec	222
	Réseaux privés virtuels et IPsec	224
	Passage de la translation d'adresses et IPsec	225
	IPsec et SCTP	226
	IPsec et les zones Oracle Solaris	226
	IPsec et domaines logiques	226
	Fichiers et utilitaires IPsec	227
<b>15</b>	<b>Configuration d'IPsec (tâches)</b>	229
	Protection du trafic à l'aide d'IPsec	229
	▼ Sécurisation du trafic entre deux systèmes à l'aide d'IPsec	231
	▼ Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.	233
	▼ Affichage des stratégies IPsec	235
	Protection d'un VPN à l'aide d'IPsec	236
	Protection d'un VPN à l'aide d'IPsec en mode Tunnel (exemples)	236

Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN	237
▼ Procédure de protection d'un VPN avec IPsec en mode Tunnel	239
Gestion d'IPsec et d'IKE	242
▼ Création manuelle de clés IPsec	243
▼ Configuration d'un rôle pour la sécurité réseau	245
▼ Procédure de gestion des services IKE et IPsec	246
▼ Vérification de la protection des paquets par IPsec	248
<b>16 Architecture IPsec (référence)</b>	251
Services IPsec	251
Commande ipsecconf	252
Fichier ipsecinit.conf	252
Fichier exemple ipsecinit.conf	253
Considérations de sécurité pour les commandes ipsecinit.conf et ipsecconf	253
Commande ipsecalg	254
Base de données des associations de sécurité IPsec	255
Utilitaires de génération de clés SA dans IPsec	255
Considérations de sécurité pour la commande ipseckey	256
IPsec et commande snoop	257
<b>17 Protocole IKE (présentation)</b>	259
Gestion des clés avec IKE	259
Négociation des clés IKE	260
Terminologie relative aux clés IKE	260
Phase 1 d'IKE	260
Phase 2 d'IKE	261
Choix de configuration IKE	261
IKE avec l'authentification des clés prépartagées	262
IKE avec certificats de clés publiques	262
Utilitaires et fichiers IKE	263
<b>18 Configuration du protocole IKE (tâches)</b>	265
Affichage des informations IKE	265
▼ Procédure d'affichage des groupes et algorithmes disponibles pour les échanges IKE de la phase 1	265

Configuration du protocole IKE (liste des tâches) .....	267
Configuration du protocole IKE avec des clés prépartagées (liste des tâches) .....	268
Configuration du protocole IKE avec des clés prépartagées .....	268
▼ Configuration du protocole IKE avec des clés prépartagées .....	268
▼ Procédure de configuration d'IKE pour un nouveau système homologue .....	271
Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches) .....	273
Configuration du protocole IKE avec des certificats de clés publiques .....	274
▼ Configuration du protocole IKE avec des certificats de clés publiques autosignés .....	274
▼ Configuration du protocole IKE avec des certificats signés par une CA .....	279
▼ Génération et stockage de certificats de clés publiques dans le matériel .....	285
▼ Traitement des listes des certificats révoqués .....	288
Configuration du protocole IKE pour les systèmes portables (liste des tâches) .....	291
Configuration du protocole IKE pour les systèmes portables .....	291
▼ Configuration du protocole IKE pour les systèmes hors site .....	291
Configuration du protocole IKE en vue de l'utilisation du matériel connecté .....	298
▼ Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 6000 .....	298
 <b>19 Protocole IKE (référence) .....</b>	<b>301</b>
Service IKE .....	301
Démon IKE .....	302
Fichier de configuration IKE .....	302
Commande <code>ikeadm</code> .....	303
Fichiers de clés prépartagées IKE .....	304
Commandes et bases de données de clés publiques IKE .....	304
Commande <code>ikecert tokens</code> .....	305
Commande <code>ikecert certlocal</code> .....	305
Commande <code>ikecert certdb</code> .....	306
Commande <code>ikecert certdb</code> .....	306
Répertoire <code>/etc/inet/ike/publickeys</code> .....	307
Répertoire <code>/etc/inet/secret/ike.privatekeys</code> .....	307
Répertoire <code>/etc/inet/ike/crls</code> .....	307
 <b>20 IP Filter dans Oracle Solaris (présentation) .....</b>	<b>309</b>
Introduction à IP Filter .....	309

Sources d'informations pour Open Source IP Filter .....	310
Traitement des paquets avec IP Filter .....	310
Recommandations relatives à l'utilisation d'IP Filter .....	313
Utilisation des fichiers de configuration IP Filter .....	314
Utilisation d'ensembles de règles IP Filter .....	314
Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter .....	314
Utilisation de la fonctionnalité NAT d'IP Filter .....	317
Utilisation de la fonctionnalité de pools d'adresses d'IP Filter .....	319
Crochets de filtre de paquets .....	320
IPv6 pour IP Filter .....	320
Pages de manuel IP Filter .....	321
<b>21 IP Filter (tâches) .....</b>	<b>323</b>
Configuration d'IP Filter .....	323
▼ Activation d'IP Filter .....	324
▼ Réactivation d'IP Filter .....	325
▼ Activation du filtrage de loopback .....	326
Désactivation d'IP Filter .....	327
▼ Désactivation du filtrage de paquets .....	327
▼ Désactivation de NAT .....	328
▼ Désactivation du filtrage de paquets .....	328
Utilisation des ensembles de règles IP Filter .....	329
Gérez les ensembles de règles de filtrage de paquets d'IP Filter .....	330
Gestion des règles NAT d'IP Filter .....	337
Gestion des pools d'adresses d'IP Filter .....	339
Affichage des statistiques et des informations relatives à IP Filter .....	341
▼ Affichage des tables d'état d'IP Filter .....	341
▼ Affichage des statistiques d'état d'IP Filter .....	342
▼ Affichage des statistiques NAT d'IP Filter .....	343
▼ Affichage des statistiques de pool d'adresses d'IP Filter .....	343
Utilisation des fichiers journaux IP Filter .....	344
▼ Configuration d'un fichier journal d'IP Filter .....	344
▼ Affichage des fichiers journaux IP Filter .....	345
▼ Vidage du fichier journal de paquets .....	346
▼ Enregistrement dans un fichier des paquets consignés .....	347

Création et modification des fichiers de configuration IP Filter .....	348
▼ Création d'un fichier de configuration d'IP Filter .....	348
Exemples de fichiers de configuration IP Filter .....	349
<b>Partie IV Performances du réseau .....</b>	<b>355</b>
<b>22 Présentation de l'équilibreur de charge intégré .....</b>	<b>357</b>
Terminologie d'ILB .....	358
Fonctions d'ILB .....	360
Modes de fonctionnement d'ILB .....	360
Algorithmes d'ILB .....	361
Interface de ligne de commande ILB .....	361
Fonction ILB de surveillance des serveurs .....	362
Fonctions ILB supplémentaires .....	363
Processus d'ILB .....	365
Recommandations relatives à l'utilisation d'ILB .....	366
ILB et utilitaire de gestion des services .....	366
Commandes et sous-commandes ILB .....	366
<b>23 Configuration de l'équilibreur de charge intégré (tâches) .....</b>	<b>369</b>
Installation de l'équilibreur de charge intégré .....	369
Activation et désactivation d'ILB .....	370
▼ Procédure d'activation d'ILB .....	370
▼ Procédure de désactivation d'ILB .....	371
Configuration d'ILB .....	371
Topologies DSR, Full-NAT et Half-NAT .....	371
Topologie d'équilibrage de charge Half-NAT .....	373
Topologie d'équilibrage de charge Full-NAT .....	374
Configuration de haute disponibilité ILB (Mode actif/passif uniquement) .....	375
Configuration à haute disponibilité d'ILB à l'aide de la topologie DSR .....	375
Configuration à haute disponibilité ILB avec la topologie Half-NAT .....	377
Configuration de l'autorisation utilisateur pour les sous-commandes de configuration ILB ..	380
Administration des groupes de serveurs ILB .....	381
▼ Procédure de création d'un groupe de serveurs .....	381

▼ Procédure de suppression d'un groupe de serveurs .....	381
Affichage d'un groupe de serveurs .....	382
Administration des serveurs d'arrière-plan dans ILB .....	382
▼ Procédure d'ajout d'un serveur d'arrière-plan à un groupe de serveurs .....	382
▼ Procédure de suppression d'un serveur d'arrière-plan à un groupe de serveurs .....	383
▼ Procédure de réactivation ou désactivation d'un serveur d'arrière-plan .....	384
Administration des contrôles de l'intégrité du serveur dans ILB .....	384
Création d'un contrôle de l'intégrité .....	385
Détails sur le test utilisateur .....	386
Suppression d'un contrôle de l'intégrité .....	386
Liste des contrôles de l'intégrité .....	387
Affichage des résultats du contrôle de l'intégrité .....	387
Administration des règles ILB .....	387
▼ Procédure de création d'une règle .....	387
Suppression d'une règle .....	388
Liste des règles .....	389
Affichage des statistiques ILB .....	389
Obtention de statistiques à l'aide de la sous-commande <code>show-statistics</code> .....	389
Affichage de la table des connexions NAT .....	390
Affichage de la table des correspondances de persistance de session .....	390
Utilisation des sous-commandes Import et Export .....	391
<b>24 Protocole de redondance de routeur virtuel (VRRP) (Présentation) .....</b>	<b>393</b>
Terminologie VRRP .....	394
Présentation de l'architecture VRRP .....	395
Routeur VRRP .....	395
Processus VRRP .....	395
Restrictions de VRRP .....	397
Prise en charge de zone en mode IP exclusif .....	397
Interopérations avec les autres fonctionnalités réseau .....	398
<b>25 Configuration VRRP - Tâches .....</b>	<b>399</b>
Création de VNIC VRRP .....	400
Configuration de <code>vrrpadm</code> .....	400
Sous-commande <code>vrrpadm create-router</code> .....	400

Sous-commande vrrpadm modify-router .....	401
Sous-commande vrrpadm delete-router .....	401
Sous-commande vrrpadm disable-router .....	401
Sous-commande vrrpadm enable-router .....	401
Sous-commande vrrpadm show-router .....	401
Considérations de sécurité .....	403
<b>26 Implémentation du contrôle de congestion .....</b>	<b>405</b>
Congestion du réseau et contrôle de congestion .....	405
▼ Procédure d'implémentation du contrôle de congestion du réseau TCP et SCTP .....	406
<b>Partie V Qualité de service IP (IPQoS) .....</b>	<b>409</b>
<b>27 Présentation d'IPQoS (généralités) .....</b>	<b>411</b>
Principes de base d'IPQoS .....	411
Quels sont les services différenciés ? .....	411
Fonctions IPQoS .....	412
Sources d'informations sur la théorie de la qualité de service et les techniques .....	412
Livraison d'une qualité de service avec IPQoS .....	414
Implémentation des accords de niveau de service .....	414
Garantie d'une qualité de service pour une organisation .....	414
Introduction à la stratégie de qualité de service .....	414
Amélioration de l'efficacité du réseau dans IPQoS .....	415
Impact de la bande passante sur le trafic réseau .....	415
Utilisation des classes de service pour hiérarchiser le trafic .....	416
Modèle de services différenciés .....	417
Présentation du classifieur (ipgpc) .....	417
Présentation des compteurs (tokenmt et tswtclmt) .....	418
Généralités des marqueurs (dscpmk et dlcosmk) .....	419
Généralités sur la comptabilisation des flux (flowacct) .....	419
Transit du trafic par les modules IPQoS .....	420
Trafic sur un réseau compatible IPQoS .....	422
Point de code DS .....	422
PHB (Per-Hop Behaviors) .....	422

<b>28 Planification d'un réseau IPQoS (tâches)</b>	427
Planification générale de la configuration IPQoS (liste des tâches)	427
Planification de la topologie de réseau Diffserv	428
Stratégies matérielles pour le réseau Diffserv	428
Topologies de réseau IPQoS	429
Planification de la stratégie de qualité de service	431
Aides à la planification de la stratégie QoS	431
Planification de la stratégie QoS (liste des tâches)	432
▼ Préparation d'un réseau pour IPQoS	433
▼ Définition des classes pour votre stratégie QoS	434
Définition des filtres	436
▼ Définition de filtres dans la stratégie QoS	437
▼ Planification du contrôle de flux	438
▼ Planification du comportement de transmission	441
▼ Planification de la comptabilisation des flux	444
Présentation d'un exemple de configuration IPQoS	445
Topologie IPQoS	445
 <b>29 Création du fichier de configuration IPQoS (tâches)</b>	 449
Définition d'une stratégie QoS dans le fichier de configuration IPQoS (liste des tâches)	449
Outils de création d'une stratégie QoS	451
Fichier de configuration IPQoS standard	451
Création de fichiers de configuration IPQoS pour les serveurs Web	452
▼ Création du fichier de configuration IPQoS et définition des classes de trafic	454
▼ Définition des filtres dans le fichier de configuration IPQoS	456
▼ Définition de la transmission du trafic dans le fichier de configuration IPQoS	458
▼ Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS	461
▼ Création d'un fichier de configuration IPQoS pour un serveur Web au mieux	462
Création d'un fichier de configuration pour un serveur d'application	465
▼ Configuration d'un fichier de configuration IPQoS pour un serveur d'application	467
▼ Configuration de la transmission du trafic d'une application dans le fichier de Configuration IPQoS	469
▼ Configuration du contrôle de flux dans le fichier de configuration IPQoS	472
Fourniture de services différenciés sur un routeur	475
▼ Configuration d'un routeur dans un réseau compatible IPQoS	475



<b>30</b>	<b>Démarrage et maintenance d'IPQoS (tâches)</b>	477
	Administration d'IPQoS (liste des tâches)	477
	Application d'une configuration IPQoS	478
	▼ Application d'une nouvelle configuration aux modules de noyau IPQoS	478
	▼ Vérification de l'application de la configuration IPQoS après chaque redémarrage	479
	Activation de la journalisation des messages IPQoS syslog	479
	▼ Activation de la journalisation des messages IPQoS au cours de l'amorce	479
	Dépannage à l'aide des messages d'erreur IPQoS	480
<b>31</b>	<b>Utilisation de la comptabilisation des flux et de la collecte statistique (tâches)</b>	485
	Configuration de la comptabilisation des flux (liste des tâches)	485
	Enregistrement des informations sur les flux de trafic	486
	▼ Création d'un fichier contenant les données de comptabilisation des flux	486
	Collecte des informations statistiques	488
<b>32</b>	<b>IPQoS en détails (référence)</b>	491
	Architecture IPQoS et modèle Diffserv	491
	Module de classification	491
	Module de mesure	494
	Module de marquage	497
	Module flowacct	501
	Fichier de configuration IPQoS	504
	Instruction action	505
	Définitions des modules	506
	Clause class	507
	Clause filter	507
	Clause params	508
	Utilitaire de configuration ipqosconf	508
	<b>Glossaire</b>	509
	<b>Index</b>	519



# Préface

---

Bienvenue dans le Administration d'Oracle Solaris : Services IP pour Oracle Solaris. Ce manuel fait partie d'un jeu de quatorze volumes couvrant une partie importante des informations d'administration du système Oracle Solaris. Ce manuel part du principe que vous avez déjà installé Oracle Solaris. Vous devez être prêt à configurer votre réseau ou tout logiciel de gestion de réseau requis.

---

**Remarque** – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Pour connaître les systèmes pris en charge, reportez-vous aux [listes de compatibilité matérielle du SE Oracle Solaris](#). Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

---

## Organisation des guides d'administration système

La liste des différents sujets traités par les guides d'administration système est la suivante.

Titre du manuel	Sujets
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes SPARC</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement de l'initialisation, initialisation à partir de ZFS, gestion de l'archive d'amorçage et dépannage de l'initialisation sur les plates-formes SPARC
<i>Initialisation et arrêt d'Oracle Solaris sur les plates-formes x86</i>	Initialisation et arrêt d'un système, gestion des services d'initialisation, modification du comportement de l'initialisation, initialisation à partir de ZFS, gestion de l'archive d'amorçage et dépannage de l'initialisation sur les plates-formes x86
<i>Administration d'Oracle Solaris : Tâches courantes</i>	Utilisation des commandes Oracle Solaris, initialisation et arrêt d'un système, gestion des comptes et des groupes d'utilisateurs, gestion des services, pannes matérielles, informations système, ressources système, performances système, gestion des logiciels, impression, console et terminaux, dépannage des problèmes système et logiciels
<i>Administration d'Oracle Solaris : Périphériques et systèmes de fichiers</i>	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données

Titre du manuel	Sujets
<i>Administration d'Oracle Solaris : Services IP</i>	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP et IPQoS
<i>Oracle Solaris Administration: Naming and Directory Services .</i>	Services de noms et d'annuaire DNS, NIS et LDAP, transition de NIS à LDAP comprise
<i>Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau</i>	Configuration d'interface IP automatique et manuelle (y compris WiFi, administration de ponts, VLAN, groupements, LLDP et IPMP, NIC virtuels et gestion des ressources).
<i>Administration d'Oracle Solaris : Services réseau</i>	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
<i>Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources</i>	Fonctionnalités de gestion des ressources permettant de contrôler l'utilisation des ressources système disponibles par les applications ; technologie de partitionnement du logiciel Oracle Solaris Zones permettant de virtualiser les services du système d'exploitation pour créer un environnement isolé pour les applications en cours d'exécution ; Oracle Solaris 10 Zones assurant l'hébergement des environnements Oracle Solaris 10 s'exécutant sur le noyau Oracle Solaris 11
<i>Administration d'Oracle Solaris : services de sécurité.</i>	Audit, gestion des périphériques, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique, gestion des clés, privilèges, RBAC, SASL, shell sécurisé et analyse de virus
<i>Oracle Solaris Administration: SMB and Windows Interoperability</i>	Service SMB permettant de configurer un système Oracle Solaris afin que les partages SMB soient disponibles pour les clients SMB ; client SMB permettant d'accéder aux partages SMB ; services de mappage d'identité natifs permettant de mapper des identités d'utilisateurs et de groupes entre des systèmes Oracle Solaris et Windows
<i>Administration d'Oracle Solaris : Systèmes de fichiers ZFS</i>	Création et gestion de pools de stockage et de systèmes de fichiers ZFS, instantanés, clones, sauvegardes à l'aide de listes de contrôle d'accès (ACL) pour protéger les fichiers ZFS, utilisation de Solaris ZFS sur un système Solaris avec des zones installées, volumes émulés et dépannage et récupération de données
<i>Configuration et administration d'Oracle Solaris Trusted Extensions</i>	Installation, configuration et administration système spécifiques à Trusted Extensions
<i>Directives de sécurité d'Oracle Solaris 11</i>	Sécurisation d'un système Oracle Solaris, et scénarios d'utilisation de ses fonctionnalités de sécurité telles que les zones, ZFS et Trusted Extensions

Titre du manuel	Sujets
<i>Transition d'Oracle Solaris 10 vers Oracle Solaris 11</i>	Fournit des informations sur l'administration système et des exemples de transition d'Oracle Solaris 10 vers Oracle Solaris 11 dans les domaines suivants : installation, gestion des périphériques, des disques et des systèmes de fichiers, gestion des logiciels, réseau, sécurité, virtualisation, fonctionnalités du bureau, gestion des comptes utilisateurs et environnements utilisateur

## Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> adapté aux utilisateurs malentendants.

## Conventions typographiques

Le tableau ci-dessous décrit les conventions typographiques utilisées dans ce manuel.

TABLEAU P-1 Conventions typographiques

Type de caractères	Signification	Exemple
AaBbCc123	Noms des commandes, fichiers et répertoires, ainsi que messages système.	Modifiez votre fichier <code>.login</code> .  Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers.  <code>nom_machine%</code> Vous avez reçu du courrier.
<b>AaBbCc123</b>	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	<code>nom_machine% su</code>  Mot de passe :
<i>aabbcc123</i>	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est <code>rm filename</code> .

TABLEAU P-1 Conventions typographiques (Suite)		
Type de caractères	Signification	Exemple
AaBbCc123	Titres de manuel, nouveaux termes et termes importants.	Reportez-vous au chapitre 6 du <i>Guide de l'utilisateur</i> .  Un <i>cache</i> est une copie des éléments stockés localement.  <i>N'enregistrez pas</i> le fichier.  <b>Remarque</b> : en ligne, certains éléments mis en valeur s'affichent en gras.

## Invites de shell dans les exemples de commandes

Le tableau suivant présente l'invite système UNIX par défaut et l'invite superutilisateur pour les shells faisant partie du SE Oracle Solaris. L'invite système par défaut qui s'affiche dans les exemples de commandes dépend de la version Oracle Solaris.

TABLEAU P-2 Invites de shell	
Shell	Invite
Shell Bash, shell Korn et shell Bourne	\$
Shell Bash, shell Korn et shell Bourne pour superutilisateur	#
C shell	nom_machine%
C shell pour superutilisateur	nom_machine#

## PARTIE I

# Administration TCP/IP

Cette partie aborde les tâches et les informations conceptuelles relatives à la configuration, à l'administration et au dépannage de réseaux TCP/IP.





# Planification du développement du réseau

---

Ce chapitre présente brièvement les différents éléments à prendre en considération lors de la configuration du réseau. Ces problématiques vous aideront à déployer votre réseau de manière organisée et économique. Notez que cet ouvrage ne détaille pas la planification du réseau. Seules des indications d'ordre général sont fournies.

Cet ouvrage est destiné à des lecteurs qui connaissent la terminologie et les concepts de base de la mise en réseau. Pour en savoir plus sur ces concepts de base, reportez-vous aux ressources suivantes :

- Pour une présentation de la suite de protocoles TCP/IP et de son implémentation du modèle Open Systems Interconnection (OSI), reportez-vous au [Chapitre 1, “Suite de protocoles réseau TCP/IP Oracle Solaris \(présentation\)” du manuel \*Guide d'administration système : services IP\*](#)
- Pour une brève description de l'implémentation de la suite de protocoles TCP/IP dans la version Oracle Solaris, reportez-vous au [Chapitre 1, “Présentation de la pile réseau” du manuel \*Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau\*](#).

Vous obtiendrez davantage d'informations d'ordre général en consultant les sections appropriées ci-après.

## Planification réseau (liste des tâches)

Le tableau suivant répertorie les différentes tâches de planification de la configuration réseau.

Tâche	Description	Référence
Identification des conditions matérielles requises pour la topologie réseau planifiée	Déterminez les types d'équipement dont vous avez besoin pour votre site réseau.	<p>“Détermination du matériel réseau” à la page 26</p> <p>Pour obtenir des informations sur un type d'équipement spécifique, reportez-vous à la documentation du constructeur de l'équipement.</p>
Identification du type d'adresses IP à utiliser pour obtenir des adresses IP enregistrées	Choisissez entre le déploiement d'un réseau IPv4 et un réseau IPv6, ou un réseau qui utilise ces deux types d'adresses IP. Obtenez des adresses IP uniques pour communiquer sur les réseaux publics du réseau Internet.	<p>“Choix du format d'adressage IP du réseau” à la page 27</p> <p>“Obtention du numéro IP du réseau” à la page 29.</p>
Identification d'un schéma de noms qui identifie les hôtes du réseau et du service de noms à utiliser	Créez une liste de noms à affecter aux systèmes du réseau et décidez des bases de données à utiliser (NIS, LDAP, DNS ou les bases de données réseau du répertoire local /etc).	<p>“Administration des noms d'hôtes” à la page 30</p> <p>“Sélection d'un service de noms et d'un service d'annuaire” à la page 31</p>
(Facultatif) Création de sous-divisions administratives et élaboration d'une stratégie pour les sous-réseaux	Décidez si le site requiert une division du réseau en sous-réseaux pour servir les sous-divisions administratives.	“Utilisation de sous-réseaux” à la page 32
Détermination de l'emplacement auquel positionner les routeurs dans le réseau	Si le réseau est étendu et, par conséquent, requiert des routeurs, créez une topologie réseau prenant en charge ces derniers.	“Planification des routeurs du réseau” du manuel <i>Guide d'administration système : services IP</i>
Création ou non de réseaux virtuels dans le schéma de configuration réseau complet	Vous devrez peut-être créer des réseaux virtuels dans un système afin de réduire l'empreinte matérielle sur le réseau.	Partie III, “Virtualisation du réseau et gestion des ressources” du manuel <i>Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau</i>

## Détermination du matériel réseau

Le nombre de systèmes à prendre en charge modifie la manière de configurer le réseau. Votre organisation peut avoir besoin d'un petit réseau de plusieurs douzaines de systèmes autonomes résidant dans un même bâtiment et au même étage. Vous pouvez aussi configurer un réseau comprenant plus de 1 000 systèmes situés dans différents bâtiments. Cette configuration requiert une division supplémentaire du réseau en sous-divisions appelées *sous-réseaux*.

Dans le cadre de la planification, vous devez prendre les décisions suivantes concernant le matériel :

- Définir la topologie réseau, la disposition et les connexions du matériel réseau
- Définir le type et le nombre de systèmes hôtes que votre réseau peut prendre en charge, y compris les serveurs qui peuvent être requis
- Définir les périphériques réseau à installer sur ces systèmes
- Définir le type de média réseau à utiliser (Ethernet, etc.)
- Définir si des ponts ou routeurs doivent étendre ce média ou connecter le réseau local à des réseaux externes

---

**Remarque** – Pour plus d'informations sur le fonctionnement des routeurs, reportez-vous à la section “[Planification des routeurs du réseau](#)” du manuel *Guide d'administration système : services IP*. Pour avoir une présentation des ponts, reportez-vous à la section “[Présentation du pontage](#)” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*

---

## Choix du format d'adressage IP du réseau

Lors de la planification du schéma d'adressage du réseau, tenez compte des facteurs suivants :

- Le type d'adresse IP à employer : IPv4 ou IPv6
- Le nombre de systèmes potentiels sur le réseau
- Le nombre de systèmes multiréseau ou routeurs, qui requièrent plusieurs cartes d'interface réseau avec leur adresse IP
- Si des adresses privées doivent être utilisées sur le réseau
- Si les pools d'adresses IPv4 doivent être gérés par un serveur DHCP

En résumé, le type d'adresse IP inclut les éléments suivants :

### Adresses IPv4

Ces adresses 32 bits correspondent au format d'adressage IP conçu pour TCP/IP.

Pour une présentation de l'adressage IPv4 basé sur les classes, reportez-vous aux ressources suivantes :

- “[Conception du schéma d'adressage IPv4](#)” du manuel *Guide d'administration système : services IP*
- [Internet Protocol DARPA Internet Program Protocol Specification \(http://tools.ietf.org/html/rfc791\)](http://tools.ietf.org/html/rfc791)

L'IETF a développé des adresses *CIDR* (Classless Inter-Domain Routing, routage inter-domaine sans classe) dans le but de résoudre à court ou moyen terme le problème d'épuisement des adresses IPv4 et de remédier au manque de capacité des tables de routage Internet.

Pour plus d'informations, reportez-vous aux ressources suivantes :

- “Conception du schéma d'adressage IPv4 CIDR” du manuel *Guide d'administration système : services IP*
- Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan (<http://tools.ietf.org/html/rfc4632>)

Le tableau suivant fournit les sous-réseaux au format décimal avec points ainsi que sous la forme d'une notation CIDR.

TABLEAU 1-1 Préfixes CIDR et leurs équivalents décimaux

Préfixe de réseau CIDR	Equivalent en numérotation décimale avec points	Adresses IP disponibles
/19	255.255.224.0	8,192
/20	255.255.240.0	4,096
/21	255.255.248.0	2,048
/22	255.255.252.0	1,024
/23	255.255.254.0	512
/24	255.255.255.0	256
/25	255.255.255.128	128
/26	255.255.255.192	64
/27	255.255.255.224	32

## Adresses DHCP

Le protocole DHCP (Dynamic Host Configuration Protocol, protocole de configuration dynamique d'hôte) permet à un système de recevoir à l'initialisation les informations de configuration d'un serveur DHCP, notamment une adresse IP. Les serveurs DHCP tiennent à jour des pools d'adresses IP à partir desquels attribuer des adresses aux clients DHCP. Cela permet à un site DHCP d'utiliser un pool d'adresses IP plus petit que celui qui serait nécessaire si tous les clients possédaient une adresse IP permanente. Vous pouvez configurer le service DHCP afin de gérer les adresses IP de votre site ou une partie des adresses. Pour plus d'informations, reportez-vous au [Chapitre 10, “A propos de DHCP \(présentation\)”](#).

## Adresses IPv6

Les adresses IPv6 128 bits fournissent un espace d'adressage plus étendu que IPv4. Comme les adresses IPv4 au format CIDR, les adresses IPv6 n'ont pas de classe et utilisent des préfixes pour désigner la partie de l'adresse définissant le réseau du site.

Pour plus d'informations sur les adresses IPv6, reportez-vous aux ressources suivantes :

- “Présentation de l'adressage IPv6” du manuel *Guide d'administration système : services IP*
- *Internet Protocol, Version 6 (IPv6) Specification* (<http://tools.ietf.org/html/rc2460>)

## Adresses privées et préfixes de documentation

L'IANA a réservé un bloc d'adresses IPv4 et un préfixe de site IPv6 à utiliser sur les réseaux privés. Ces adresses privées sont utilisées pour le trafic réseau au sein d'un réseau privé. Ces adresses sont également utilisées dans la documentation

Le tableau suivant répertorie les plages d'adresses IPv4 privées et des masques de réseau respectifs.

Plage d'adresses IPv4	Masque de réseau
10.0.0.0 - 10.255.255.255	10.0.0.0
172.16.0.0 - 172.31.255.255	172.16.0.0
192.168.0.0 - 192.168.255.255	192.168.0.0

Pour les adresses IPv6, le préfixe 2001:db8::/32 est un préfixe IPv6 spécial utilisé spécifiquement dans les exemples de documentation. Les exemples de ce manuel utilisent des adresses IPv4 privées et le préfixe de documentation IPv6 réservé.

## Obtention du numéro IP du réseau

Un réseau IPv4 se définit à l'aide d'un numéro de réseau IPv4 et d'un *masque de réseau*. Un réseau IPv6 est défini par son *préfixe de site* et s'il dispose d'un sous-réseau, par son *préfixe de sous-réseau*.

Pour que le réseau privé communique avec des réseaux externes du réseau Internet, vous devez demander un numéro d'IP enregistré pour votre réseau auprès de l'organisation adéquate. Cette adresse devient le numéro de réseau de votre schéma d'adressage IPv4 ou le préfixe de site de votre schéma d'adressage IPv6.

Les fournisseurs d'accès Internet (FAI) procurent des adresses IP pour les réseaux à un coût dépendant du niveau de service assuré. Comparez les offres de divers FAI afin de déterminer celui qui fournit le service le plus adéquat pour votre réseau. Les FAI offrent généralement des adresses allouées dynamiquement ou des adresses IP statiques aux entreprises. Certains FAI proposent à la fois des adresses IPv4 et IPv6.

Si le site est un FAI, vous pouvez obtenir les blocs d'adresses IP pour vos clients auprès de l'IR (Internet Registry, registre Internet) correspondant à votre environnement linguistique. L'IANA (Internet Assigned Numbers Authority, autorité de numéros assignés sur Internet) est actuellement responsable de la délégation des adresses IP enregistrées aux IR dans le monde entier. Chaque IR possède des modèles et des informations d'enregistrement dédiés à l'environnement linguistique assuré par l'IR. Pour plus d'informations sur l'IANA et les IR, reportez-vous à la [page des services d'adresse IP de l'IANA \(http://www.iana.org/ipaddress/ip-addresses.htm\)](http://www.iana.org/ipaddress/ip-addresses.htm).

## Attribution de noms aux entités du réseau

Les protocoles TCP/IP détectent un système sur le réseau à l'aide de son adresse IP. Cependant, un nom d'hôte permet d'identifier plus facilement les systèmes que les adresses IP. Par conséquent, les protocoles TCP/IP (et Oracle Solaris) nécessitent à la fois l'adresse IP et le nom d'hôte pour identifier de manière unique le système.

Dans le cadre de TCP/IP, un réseau correspond à un ensemble d'entités nommées. Un hôte correspond à une entité possédant un nom. Un routeur correspond à une entité possédant un nom. Le réseau correspond à une entité possédant un nom. Vous pouvez également attribuer un nom à un groupe ou service dans lequel le réseau est installé, ainsi qu'à une division, une région ou une société. Théoriquement, la hiérarchie de noms utilisée pour identifier un réseau est illimitée. Le nom de domaine identifie un *domaine*.

## Administration des noms d'hôtes

Planifiez un schéma de nommage pour les systèmes inclus dans le réseau. Pour les systèmes faisant office de serveurs et possédant plusieurs NIC, au moins un nom d'hôte associé à l'adresse IP de son interface réseau principale doit être fourni.

Vous ne pouvez pas attribuer le même nom d'hôte à deux ordinateurs du réseau. Par conséquent, le nom d'hôte doit être unique à chaque système. Cependant, un hôte ou un système avec son nom unique assigné peut posséder plusieurs adresses IP.

Lors de la planification du réseau, dressez la liste des adresses IP et des noms d'hôtes associés afin d'en faciliter l'accès lors des processus de configuration. Cette liste permet de vérifier que chaque nom d'hôte est unique.

## Sélection d'un service de noms et d'un service d'annuaire

Dans Oracle Solaris, vous pouvez sélectionner parmi trois types de services de noms : fichiers locaux, NIS et DNS. Les services de noms mettent à jour d'importantes informations sur les machines du réseau, par exemple les noms d'hôtes, les adresses IP, les adresses Ethernet, etc. Vous pouvez également utiliser le service d'annuaire LDAP en plus ou à la place d'un service de noms. Pour une introduction aux services de noms sous Oracle Solaris, reportez-vous à la [Partie I, “About Naming and Directory Services” du manuel \*Oracle Solaris Administration: Naming and Directory Services\*](#).

Pendant l'installation du SE, vous devez fournir le nom d'hôte et l'adresse IP de votre serveur, de vos clients ou de votre système autonome. Le programme d'installation ajoute ces informations à la base de données `hosts` utilisée par le service réseau.

La configuration des bases de données réseau est d'une importance capitale. Par conséquent, vous devez choisir le service de noms à utiliser au cours du processus de planification réseau. En outre, l'utilisation des services de noms affecte également l'organisation du réseau en un domaine administratif.

Vous pouvez choisir parmi les noms de services suivants :

- NIS ou DNS : les services de noms NIS et DNS maintiennent des bases de données réseau sur divers serveurs du réseau. [Oracle Solaris Administration: Naming and Directory Services](#) décrit ces services de noms et la configuration des bases de données. En outre, ce manuel explique en détail les concepts d'espace de noms et de domaine administratif.
- Fichiers locaux : si vous n'implémentez pas NIS, LDAP ou DNS, le réseau utilise des *fichiers locaux* pour fournir le service de noms. Le terme "fichiers locaux" fait référence à la série de fichiers du répertoire `/etc` utilisé par les bases de données réseau. Sauf indication contraire, les procédures de ce manuel partent du principe que vous utilisez des fichiers locaux comme service de noms.

---

**Remarque** – Si vous décidez d'utiliser des fichiers locaux en tant que service de noms pour le réseau, vous pouvez configurer plus tard un autre service de noms.

---

## Noms de domaine

De nombreux réseaux organisent leurs hôtes et routeurs selon une hiérarchie de domaines administratifs. Si vous utilisez le service de noms NIS ou DNS, vous devez sélectionner pour l'organisation un nom de domaine unique au monde. Pour vérifier que le nom de domaine est unique, enregistrez-le auprès de l'InterNIC. Si vous souhaitez utiliser DNS, vous devez également enregistrer votre nom de domaine auprès de l'InterNIC.

La structure des noms de domaine est hiérarchique. En général, tout nouveau domaine se place sous un domaine existant associé. Par exemple, le nom de domaine d'une filiale peut se placer sous le nom de domaine de la maison mère. Si le nom de domaine n'a pas d'autre relation, une organisation peut placer son nom de domaine directement sous l'un des domaines supérieurs existants, tels que .com, .org, .edu, .gov etc.

## Utilisation de sous-réseaux

L'utilisation de sous-réseaux est liée au fait que les sous-divisions administratives doivent faire face à des problèmes de taille et de contrôle. A mesure que les nombres d'hôtes et de serveurs augmentent, la gestion du réseau devient de plus en plus complexe. La création de divisions administratives et l'utilisation de sous-réseaux simplifient la gestion d'un réseau complexe. La configuration de sous-divisions administratives pour le réseau dépend des facteurs ci-dessous :

- **Taille du réseau**

Les sous-réseaux sont également utiles dans le cas d'un petit réseau, dont les sous-divisions s'étendent sur une large zone géographique.

- **Besoins courants des groupes d'utilisateurs**

Par exemple, un réseau peut résider entièrement dans un bâtiment et prendre en charge des machines relativement nombreuses. Ces machines sont réparties en plusieurs sous-réseaux. Chaque sous-réseau prend en charge des groupes d'utilisateurs ayant des besoins différents. Dans cet exemple, il serait judicieux de créer une sous-division administrative par sous-réseau.

Pour obtenir une description générale, reportez-vous à la section [“Qu'est-ce que la création de sous-réseaux ?”](#) du manuel *Guide d'administration système : services IP*.

## Déploiement de réseaux virtuels

Cette version Oracle Solaris prend en charge la création de réseaux virtuels dans un seul réseau, en configurant des zones ainsi que des cartes réseau virtuelles (VNIC). Les VNIC sont des interfaces réseau créées sur des NIC physiques. La combinaison de zones et de VNIC est un moyen efficace de consolider un centre de données contenant un grand nombre de systèmes physiques dans des systèmes de plus petite taille. Pour plus d'informations sur les réseaux virtuels, reportez-vous à la [Partie III, “Virtualisation du réseau et gestion des ressources”](#) du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.



## Éléments à prendre en compte lors de l'utilisation d'adresses IPv6

---

Ce chapitre est un complément du [Chapitre 1, “Planification du développement du réseau”](#) et décrit les éléments supplémentaires à prendre en compte en cas d'utilisation d'adresses IPv6 sur votre réseau.

Si vous prévoyez d'utiliser des adresses IPv6 en plus des adresses IPv4, assurez-vous que votre FAI actuel prend en charge les deux types d'adresses. Autrement, vous devrez faire appel à un autre FAI pour prendre en charge les adresses IPv6.

Pour connaître les concepts de base relatifs à IPv6, reportez-vous aux ressources suivantes :

- “Présentation de l'adressage IPv6” du manuel *Guide d'administration système : services IP*
- [Internet Protocol, Version 6 \(IPv6\) Specification \(http://tools.ietf.org/html/rc2460\)](http://tools.ietf.org/html/rc2460)

## Planification IPv6 (liste des tâches)

Le tableau suivant répertorie différents éléments à prendre en compte lorsque vous planifiez l'implémentation d'IPv6 sur votre réseau.

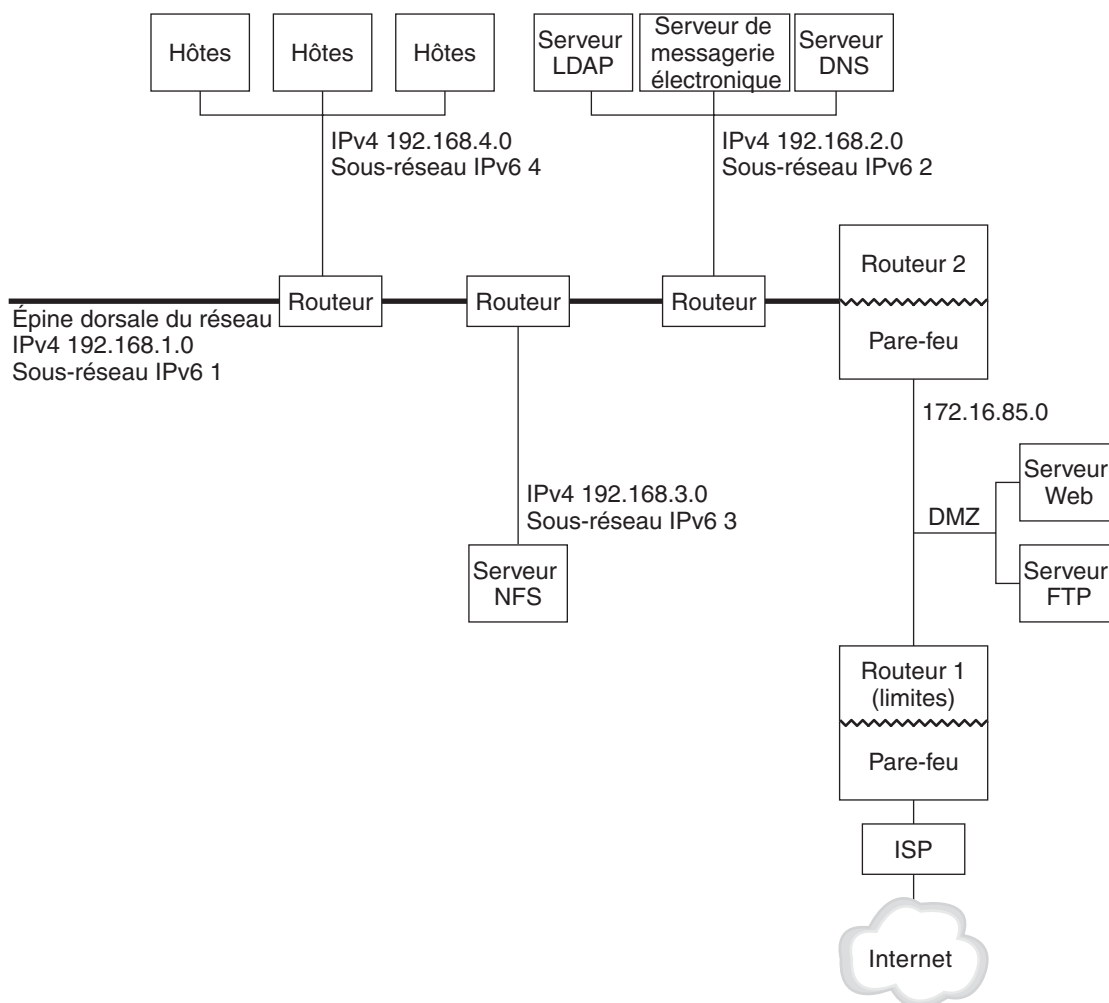
Tâche	Description	Voir
Préparation du matériel pour qu'il prenne en charge IPv6.	Vérifiez qu'il est possible de mettre le matériel à niveau vers IPv6.	<a href="#">“Vérification de la prise en charge d'IPv6” à la page 36</a>
Vérification de la compatibilité des applications avec IPv6.	Assurez-vous que les applications peuvent s'exécuter dans un environnement IPv6.	<a href="#">“Configuration des services réseau pour la prise en charge d'IPv6” à la page 39</a>
Conception d'un plan pour l'utilisation de tunnels.	Déterminez les routeurs qui vont exécuter les tunnels vers d'autres sous-réseaux ou des réseaux externes.	<a href="#">“Planification de l'utilisation de tunnels dans le réseau” à la page 41</a>

Tâche	Description	Voir
Planifiez la sécurisation de vos réseaux et le développement d'une stratégie de sécurité IPv6.	Pour des raisons de sécurité, vous devez disposer d'un plan d'adressage pour la DMZ et ses entités avant de configurer IPv6.  Décidez de la méthode d'implémentation de la sécurité que vous souhaitez utiliser (avec un filtre IP, l'architecture IPsec (IP security), le protocole IKE (Internet Key Exchange) et d'autres fonctionnalités de sécurité de cette version).	<a href="#">“Considérations de sécurité relatives à l'implémentation d'IPv6” à la page 42</a>  <a href="#">Partie III</a>
Création d'un plan d'adressage pour les entités du réseau.	Vous devez disposer au préalable d'un plan pour l'adressage des serveurs, des routeurs et des hôtes avant d'effectuer la configuration d'IPv6. Cette étape inclut l'obtention d'un préfixe de site pour votre réseau ainsi que la planification de sous-réseaux Pv6, le cas échéant.	<a href="#">“Création d'un plan d'adressage IPv6 pour les noeuds” à la page 37</a>

## Scénario de topologie de réseau IPv6

En règle générale, IPv6 est utilisé dans une topologie de réseau mixte qui utilise également IPv4, tel qu'illustré dans la figure suivante. Cette figure est utilisée en guise de référence dans la description des tâches de configuration d'IPv6 dans les sections suivantes.

FIGURE 2-1 Scénario de topologie de réseau IPv6



Le scénario de réseau d'entreprise se compose de cinq sous-réseaux disposant d'adresses IPv4. Les liaisons du réseau correspondent directement aux sous-réseaux administratifs. Les quatre réseaux internes sont affichés avec des adresses IPv4 privées de type RFC 1918, ce qui correspond à une solution courante pour le manque d'adresses IPv4. Le schéma d'adressage de ces réseaux internes est comme suit :

- Le sous-réseau 1 correspond à l'épine dorsale du réseau interne 192.168.1.
- Le sous-réseau 2 correspond au réseau interne 192.168.2, avec LDAP, sendmail et serveurs DNS.

- Le sous-réseau 3 correspond au réseau interne 192 . 168 . 3, avec les serveurs NFS de l'entreprise.
- Le sous-réseau 4 correspond au réseau interne 192 . 168 . 4 qui contient les hôtes des employés de l'entreprise.

Le réseau public externe 172 . 16 . 85 fait office de DMZ pour l'entreprise. Ce réseau contient des serveurs Web, des serveurs FTP anonymes et d'autres ressources que l'entreprise propose au monde extérieur. Le routeur 2 exécute un pare-feu et sépare le réseau public 172 . 16 . 85 de l'épine dorsale interne. Sur l'autre extrémité de la DMZ, le routeur 1 exécute un pare-feu et fait office de serveur de limites de l'entreprise.

Sur la [Figure 2–1](#), la DMZ publique possède l'adresse privée RFC 1918 172 . 16 . 85. Dans le monde réel, la DMZ publique doit disposer d'une adresse IPv4 enregistrée. La plupart des sites IPv4 utilisent une combinaison d'adresses publiques et d'adresses privées RFC 1918. Cependant, lors de l'introduction d'IPv6, le concept d'adresses publiques et privées est modifié. Dans la mesure où IPv6 dispose d'un espace d'adresse beaucoup plus important, les adresses publiques IPv6 s'utilisent à la fois sur les réseaux privés et publics.

Le protocole double pile Oracle Solaris prend en charge à la fois les opérations IPv4 et IPv6. Vous pouvez exécuter des opérations relatives à IPv4 pendant et après le déploiement d'IPv6 sur votre réseau. Lorsque vous déployez IPv6 sur un réseau en cours de fonctionnement qui utilise déjà IPv4, assurez-vous de ne pas perturber les opérations en cours.

Les sections suivantes décrivent les domaines à prendre en compte lors de la préparation de l'implémentation d'IPv6.

## Vérification de la prise en charge d'IPv6

Consultez la documentation du fabricant en matière de compatibilité IPv6 en ce qui concerne les classes de matériel suivantes :

- Routeurs
- Pare-feux
- Serveurs
- Commutateurs

---

**Remarque** – Toutes les procédures décrites dans ce manuel partent du principe qu'il est possible de mettre le matériel à niveau (en particulier les routeurs) vers IPv6.

---

Certains modèles de routeurs ne permettent pas une mise à niveau vers IPv6. Pour obtenir des informations supplémentaire et une solution au problème, reportez-vous à la section [“Impossible de mettre à niveau un routeur IPv4 vers IPv6” à la page 141](#).

Pour chaque NIC des serveurs IPv6, configurez manuellement la partie ID d'interface de l'adresse IPv6 plutôt que d'obtenir automatiquement l'ID à l'aide du protocole Neighbor Discovery. De cette façon, si une NIC est remplacée, le même ID d'interface peut être appliqué à la nouvelle NIC. Un ID différent généré automatiquement par le protocole Neighbor Discovery peut entraîner un comportement inattendu du serveur.

## Préparation d'un plan d'adressage IPv6

Le développement d'un plan d'adressage constitue une des parties les plus importantes de la transition d'IPv4 à IPv6. Cette tâche nécessite les préparatifs suivants :

- “Obtention d'un préfixe de site” à la page 37
- “Création du schéma de numérotation IPv6” à la page 37

### Obtention d'un préfixe de site

Vous devez disposer d'un préfixe de site préalablement à la configuration d'IPv6. Le préfixe de site permet de dériver les adresses IPv6 pour tous les noeuds de votre implémentation IPv6. Pour une introduction aux préfixes de site, reportez-vous à la section “[Préfixes d'IPv6](#)” du *manuel Guide d'administration système : services IP*.

Tout FAI prenant en charge IPv6 devrait être en mesure de fournir un préfixe de site IPv6 de 48 octets. Si votre FAI ne prend en charge que IPv4, vous pouvez faire appel à un autre FAI pour la prise en charge d'IPv6 tout en conservant votre FAI actuel pour la prise en charge d'IPv4. Dans ce cas, il existe plusieurs solutions au problème. Pour plus d'informations, reportez-vous à la section “[Le FAI actuel ne prend pas en charge IPv6](#)” à la page 141.

Si votre entreprise est un FAI, les préfixes de site pour vos clients s'obtiennent auprès du registre Internet adéquat. Pour plus d'informations, reportez-vous au site [Internet Assigned Numbers Authority \(IANA\)](http://www.iana.org) (<http://www.iana.org>).

### Création du schéma de numérotation IPv6

Si votre réseau IPv6 n'est pas entièrement nouveau, basez le schéma de numérotation IPv6 sur la topologie IPv4 existante.

### Création d'un plan d'adressage IPv6 pour les noeuds

Pour la plupart des hôtes, la configuration automatique d'adresses IPv6 sans état pour leurs interfaces constitue une stratégie adéquate et rapide. Lorsque l'hôte reçoit le préfixe de site en provenance du routeur le plus proche, la détection de voisin génère automatiquement des adresses IPv6 pour chaque interface de l'hôte.

Les serveurs doivent disposer d'adresses IPv6 stables. Si vous ne configurez pas manuellement les adresses IPv6 d'un serveur, une nouvelle adresse IPv6 est configurée automatiquement à chaque fois qu'une carte d'interface réseau est remplacée sur le serveur. Tenez compte des conseils suivants lors de la création d'adresses de serveurs :

- Attribuez aux serveurs des ID d'interface significatifs et stables. Vous pouvez par exemple utiliser un schéma de numérotation séquentiel pour les ID d'interface. Par exemple, l'interface interne du serveur LDAP dans la [Figure 2-1](#) pourrait devenir 2001:db8:3c4d:2::2.
- Si vous ne renommez pas régulièrement votre réseau IPv4, vous pouvez également utiliser les adresses IPv4 des routeurs et serveurs en tant qu'ID d'interface. Dans la [Figure 2-1](#), on suppose que l'interface du routeur 1 vers la DMZ a pour adresse IPv4 123.456.789.111. Vous pouvez convertir l'adresse IPv4 vers le format hexadécimale et utiliser le résultat de la conversion en tant qu'ID d'interface. Le nouvel ID d'interface serait ::7bc8:156F.  
  
Cette approche est applicable uniquement si vous êtes propriétaire de l'adresse IPv4 enregistrée, non pas si vous l'avez obtenue auprès d'un FAI. Si vous utilisez une adresse IPv4 qui vous a été fournie par un FAI, vous créez une dépendance qui risque d'entraîner des problèmes en cas de changement de FAI.

En raison du nombre limité d'adresses IPv4, un concepteur de réseau devait auparavant se demander s'il devait utiliser des adresses globales enregistrées ou des adresses privées RFC 1918. Cependant, la notion d'adresses IPv4 privées et publiques ne s'applique pas aux adresses IPv6. Vous pouvez utiliser des adresses globales unicast incluant le préfixe de site, sur toutes les liaisons du réseau, DMZ publique incluse.

### Création d'un schéma de numérotation pour les sous-réseaux

Commencez par mapper les sous-réseaux IPv4 existants vers les sous-réseaux IPv6 équivalents. Par exemple, utilisez les sous-réseaux illustrés sur la [Figure 2-1](#). Les sous-réseaux 1 à 4 utilisent l'identification d'adresse privée IPv4 RFC 1918 pour les 16 premiers octets de leurs adresses, en plus des chiffres 1 à 4 qui identifient le sous-réseau. Par exemple, supposons que le préfixe IPv6 2001:db8:3c4d/48 a été assigné au site.

Le tableau suivant illustre le mappage des préfixes IPv4 privés vers les préfixes IPv6.

Préfixe de sous-réseau IPv4	Préfixe de sous-réseau IPv6 équivalent
192.168.1.0/24	2001:db8:3c4d:1::/64
192.168.2.0/24	2001:db8:3c4d:2::/64
192.168.3.0/24	2001:db8:3c4d:3::/64
192.168.4.0/24	2001:db8:3c4d:4::/64

Pour obtenir une description plus détaillée des sous-réseaux, reportez-vous à la section [“Qu'est-ce que la création de sous-réseaux ?”](#) du manuel *Guide d'administration système : services IP*

## Configuration des services réseau pour la prise en charge d'IPv6

Les services réseau IPv4 suivants de la version active d'Oracle Solaris sont compatibles avec le protocole IPv6 :

- sendmail
- NFS
- HTTP (Apache 2.x ou Orion)
- DNS
- LDAP

Le service de messagerie IMAP est compatible uniquement avec IPv4.

Les noeuds configurés pour IPv6 peuvent exécuter des services IPv4. Lors de l'activation d'IPv6, tous les services n'acceptent pas les connexions IPv6. Les services préparés pour IPv6 acceptent les connexions. Les services qui ne le sont pas continuent de fonctionner avec la partie IPv4 de la pile de protocole.

Certains problèmes peuvent survenir après une mise à niveau des services vers IPv6. Pour plus d'informations, reportez-vous à la section [“Problèmes survenant après la mise à niveau de services vers IPv6”](#) à la page 141.

### ▼ Procédure de préparation de services réseau pour la prise en charge d'IPv6

#### 1 Mettez les services réseau suivants à jour afin qu'ils prennent en charge IPv6 :

- Serveurs de courrier
- Serveurs NIS
- NFS

---

**Remarque** – LDAP prend en charge IPv6 sans aucune configuration supplémentaire nécessaire.

---

#### 2 Assurez-vous que le matériel de votre pare-feu est compatible avec le protocole IPv6.

Reportez-vous à la documentation adéquate pour obtenir des instructions.

**3 Assurez-vous que les autres services de votre réseau ont été préparés pour prendre en charge le protocole IPv6.**

Pour plus d'informations, reportez-vous à la documentation technique et marketing du logiciel.

**4 Si votre site déploie les services suivante, assurez-vous d'avoir pris les mesures adéquates pour ces services :**

- Pare-feux

Pensez à renforcer les stratégies en place pour le protocole IPv4 afin qu'elles prennent en charge le protocole IPv6. Pour prendre connaissance de problèmes de sécurité supplémentaires, reportez-vous à la section [“Considérations de sécurité relatives à l'implémentation d'IPv6”](#) à la page 42.

- Messagerie

Vous pouvez envisager d'ajouter les adresses IPv6 de votre serveur de courrier aux enregistrements MX pour DNS.

- DNS

Pour prendre connaissance des considérations spécifiques à DNS, reportez-vous à la section [“Procédure de préparation de DNS pour la prise en charge d'IPv6”](#) à la page 40.

- IPQoS

Utilisez les mêmes stratégies Diffserv que celles utilisées pour le protocole IPv4 sur l'hôte. Pour plus d'informations, reportez-vous à la section [“Module de classification”](#) à la page 491.

**5 Auditez tout service réseau offert par un noeud avant de convertir ce dernier vers IPv6.**

## ▼ **Procédure de préparation de DNS pour la prise en charge d'IPv6**

La version d'Oracle Solaris actuelle prend en charge la résolution de DNS côté client et côté serveur. Procédez comme suit pour préparer les services DNS à IPv6.

Pour plus d'informations sur la prise en charge de DNS pour IPv6, reportez-vous à la section [Oracle Solaris Administration: Naming and Directory Services](#).

- 1 Assurez-vous que le serveur DNS effectuant la résolution récursive de nom est double pile (IPv4 et IPv6) ou uniquement compatible avec IPv4.**
- 2 Dans le serveur DNS, renseignez la base de données DNS avec les enregistrements AAAA de base de données IPv6 dans la zone de transfert.**



---

**Remarque** – Les serveurs exécutant plusieurs services critiques requièrent une attention particulière. Assurez-vous du bon fonctionnement du réseau. En outre, tous les services critiques doivent avoir été préparés pour IPv6. Ensuite, ajoutez l'adresse IPv6 du serveur à la base de données DNS.

---

- 3 Ajoutez les enregistrements PTR associés aux enregistrements AAAA dans la zone d'inversion.
- 4 Ajoutez des données exclusivement IPv4 ou des données IPv6 et IPv4 à l'enregistrement NS décrivant les zones.

## Planification de l'utilisation de tunnels dans le réseau

L'implémentation d'IPv6 prend en charge un certain nombre de configurations de tunnel faisant office de mécanismes de transition lors de la migration de votre réseau vers un mélange d'IPv4 et d'IPv6. Les tunnels permettent aux réseaux IPv6 isolés de communiquer. Dans la mesure où Internet exécute essentiellement IPv4, les paquets IPv6 de votre site doivent circuler dans Internet via des tunnels ayant pour destination des réseaux IPv6.

Vous trouverez ici les scénarios les plus courants d'utilisation de tunnels dans la topologie de réseau IPv6 :

- Le FAI qui vous fournit des services IPv6 vous permet de créer un tunnel à partir du routeur de bordure du site vers le réseau du FAI. La [Figure 2-1](#) représente un de ces tunnels. Dans ce cas, vous devez exécuter un tunnel manuel IPv6 sur IPv4.
- Vous gérez un réseau distribué de grande taille avec connectivité IPv4. Pour connecter les sites distribués utilisant IPv6, vous pouvez exécuter un tunnel automatique 6to4 à partir du routeur de périphérie de chaque sous-réseau.
- Il est parfois impossible de mettre un routeur à niveau vers IPv6 dans l'infrastructure de l'entreprise. Dans ce cas, vous pouvez créer un tunnel manuel à travers le routeur IPv4, avec deux routeurs IPv6 en guise d'extrémités.

Pour connaître les procédures de configuration des tunnels, reportez-vous à la section [“Configuration des tunnels \(liste des tâches\)”](#) à la page 126. Pour obtenir des informations conceptuelles à propos des tunnels, reportez-vous à la section [“Présentation des tunnels IP”](#) à la page 117.

## Considérations de sécurité relatives à l'implémentation d'IPv6

En cas d'introduction d'IPv6 dans un réseau existant, veillez à ne pas compromettre la sécurité du site. Tenez compte des problèmes de sécurité suivants lors de l'implémentation progressive d'IPv6 :

- La même quantité de filtrage est requise pour les paquets IPv6 et IPv4.
- Les paquets IPv6 sont souvent mis en tunnel via un pare-feu. Par conséquent, implémentez l'un des deux scénarios suivants :
  - Paramétrez le pare-feu de sorte qu'il inspecte le contenu du tunnel.
  - Placez un pare-feu IPv6 avec des règles similaires à l'extrémité opposée du tunnel.
- Certains mécanismes de transition utilisent des tunnels IPv6 sur UDP sur IPv4. Ces mécanismes peuvent s'avérer dangereux et court-circuiter le pare-feu.
- Globalement, il est possible d'atteindre les noeuds IPv6 à partir de l'extérieur du réseau de l'entreprise. Si votre stratégie de sécurité interdit tout accès public, vous devez établir des règles de pare-feu plus strictes. Vous pourriez par exemple configurer un pare-feu avec état.

Ce manuel inclut des fonctionnalités de sécurité qu'il est possible d'utiliser dans une implémentation IPv6.

- La fonction d'architecture IPsec (sécurité IP) permet d'obtenir une protection cryptographique des paquets IPv6. Pour plus d'informations, reportez-vous au [Chapitre 14, "Architecture IPsec \(présentation\)"](#).
- La fonctionnalité IKE (Internet Key Exchange, échange de clé Internet) permet d'utiliser l'authentification de clé publique pour les paquets IPv6. Pour plus d'informations, reportez-vous au [Chapitre 17, "Protocole IKE \(présentation\)"](#).

## Configuration d'un réseau IPv4

---

La configuration réseau s'effectue en deux étapes : l'assemblage du matériel, puis la configuration des démons, fichiers et services d'implémentation du protocole TCP/IP.

Le présent chapitre décrit la configuration d'un réseau implémentant les services et l'adressage IPv4.

De nombreuses tâches abordées dans ce chapitre s'appliquent aussi bien aux réseaux IPv4 uniquement qu'aux réseaux IPv6. Les tâches spécifiques aux réseaux IPv6 figurent dans le [Chapitre 4, “Activation d'IPv6 sur le réseau”](#).

---

**Remarque** – Avant de configurer TCP/IP, passez en revue les différentes tâches de planification répertoriées dans le [Chapitre 1, “Planification du développement du réseau”](#). Si vous prévoyez d'utiliser des adresses IPv6, consultez également le [Chapitre 2, “Éléments à prendre en compte lors de l'utilisation d'adresses IPv6”](#).

---

Le présent chapitre contient les informations suivantes :

- “Configuration réseau (liste des tâches)” à la page 44
- “Avant de commencer la configuration réseau” à la page 44
- “Configuration des composants système sur le réseau” à la page 45
- “Ajout d'un sous-réseau à un réseau” à la page 68
- “Contrôle et modification des services de couche transport” à la page 70

# Configuration réseau (liste des tâches)

Le tableau suivant répertorie les tâches supplémentaires à effectuer une fois que vous êtes passé d'une configuration réseau sans sous-réseaux à un réseau utilisant des sous-réseaux. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Voir
Configuration des interfaces IP du système	Attribue des adresses IP aux interfaces IP du système.	<a href="#">“Procédure de configuration d'une interface IP” à la page 47</a>
Configuration d'un système en mode Fichiers locaux	Modifie des fichiers de configuration spécifiques dans le répertoire /etc du système et configure le service SMF nis/domain.	<a href="#">“Configuration d'un système en mode Fichiers locaux” à la page 53</a>
Configuration d'un serveur de configuration réseau	Active le démon in.tftp et modifie les autres fichiers de configuration dans le répertoire /etc du système.	<a href="#">“Configuration d'un serveur de configuration réseau” à la page 55</a>
Configuration d'un système en mode Client réseau	Modifie les fichiers de configuration dans le répertoire /etc du système.	<a href="#">“Configuration d'un système en mode Client réseau” à la page 54</a>
Spécification de la stratégie de routage du client réseau	Configure les systèmes pour une utilisation du routage statique ou du routage dynamique.	<a href="#">“Activation du routage statique sur un hôte à interface unique” à la page 65</a> et <a href="#">“Activation du routage dynamique sur un système à interface unique” à la page 67</a>

## Avant de commencer la configuration réseau

Dans cette version d'Oracle Solaris, la configuration réseau d'un système est gérée par un *NCP* (*network configuration profile, profil de configuration réseau*) actif. Si le NCP actif du système est `automatic`, la configuration est alors automatiquement gérée par le SE. Si le NCP actif est `DefaultFixed`, la configuration réseau s'effectue manuellement à l'aide des commandes `dladm` et `ipadm`.

**Remarque** – Les commandes `dladm` et `ipadm` ne fonctionnent pas si le NCP actif est `Automatic`.

Pour connaître les procédures permettant de déterminer le profil actif d'un système et pour passer à un NCP fixe, reportez-vous à la section [“Profils et des outils de configuration” du manuel \*Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau\*](#).

Pour plus d'informations sur les NCP, reportez-vous à la [Partie I, “Configuration automatique de réseau” du manuel \*Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau\*](#).

Dans cette documentation, les procédures supposent que le NCP actif sur tous les systèmes du réseau est `DefaultFixed`.

## Configuration des composants système sur le réseau

Lorsque vous configurez des systèmes réseau, les informations de configuration suivantes sont nécessaires :

- Nom d'hôte de chaque système.
- Adresse IP et masque réseau de chaque système. Si le réseau est divisé en sous-réseaux, vous devez disposer des numéros de sous-réseau et du schéma d'adresse IP à appliquer aux systèmes dans chaque sous-réseau, incluant leurs masques réseau respectifs.
- Nom de domaine auquel chaque système appartient.
- Adresse de routeur par défaut.

Vous devez fournir cette information lorsqu'un routeur unique est connecté à chaque réseau de la topologie. Vous devez également la fournir lorsque les routeurs n'utilisent pas de protocoles de routage tels que RDISC (Router Discovery Server Protocol) ou RIP (Router Information Protocol). Pour obtenir des informations supplémentaires sur les routeurs, ainsi que la liste des protocoles de routage pris en charge par Oracle Solaris, reportez-vous à la section [“Transfert et routage de paquets sur des réseaux IPv4” du manuel \*Guide d'administration système : services IP\*](#).

---

**Remarque** – Vous pouvez configurer le réseau tout en installant Oracle Solaris. Pour obtenir des instructions, reportez-vous à la section [Installation des systèmes Oracle Solaris 11](#).

Dans cette documentation, les procédures supposent que vous configurez le réseau après avoir installé le SE.

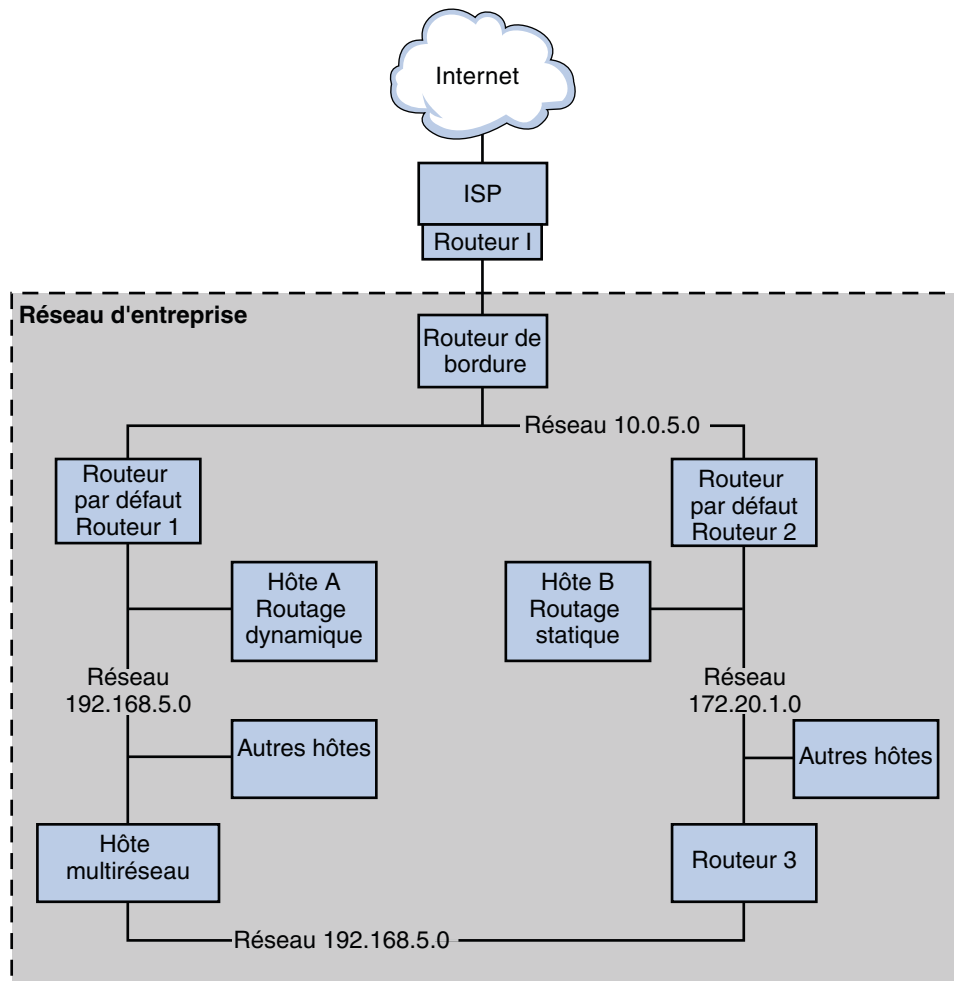
---

Utilisez la [Figure 3–1](#) dans la section suivante en tant que référence pour configurer les systèmes de composant du réseau.

## Topologie du système autonome IPv4

Les sites comportant plusieurs routeurs et réseaux gèrent généralement leur topologie réseau comme un domaine de routage unique, également appelé *système autonome AS (Autonomous System)*.

FIGURE 3-1 Système autonome comportant plusieurs routeurs IPv4



La [Figure 3-1](#) représente un AS divisé en trois réseaux locaux, `10.0.5.0`, `172.20.1.0` et `192.168.5.0`. Le réseau comporte les trois types de systèmes suivants :

- Les routeurs utilisent des protocoles de routage pour gérer comment les paquets de réseau sont dirigés ou acheminés de leur source vers leurs destinations au sein du réseau local ou vers des réseaux externes. Pour obtenir des informations sur les protocoles de routage pris en charge dans Oracle Solaris, reportez-vous à la section [“Tableaux des protocoles de routage dans Oracle Solaris”](#) à la page 148.

Les routeurs sont saisis comme suit :

- Le *routeur de bordure* connecte le réseau local tel que `10.0.5.0` de façon externe à un fournisseur de service.

- Les *routeurs par défaut* gèrent le routage de paquets dans le réseau local, lequel peut inclure plusieurs réseaux locaux. Par exemple, dans la [Figure 3–1](#), le routeur 1 fait office de routeur par défaut pour 192 . 168 . 5. En même temps, Router 1 est également connecté au réseau interne 10 . 0 . 5 . 0. Les interfaces de Router 2 se connectent aux réseaux internes 10 . 0 . 5 . 0 et 172 . 20 . 1 . 0.
- Les *routeurs de transfert de paquet* transfèrent les paquets entre les réseaux internes, mais n'exécutent pas de protocoles de routage. Dans la [Figure 3–1](#), le routeur 3 est un routeur de transfert de paquet avec des connexions aux réseaux 172 . 20 . 1 et 192 . 168 . 5.
- Systèmes clients
  - Systèmes multiréseau ou systèmes dotés de plusieurs NIC. Dans Oracle Solaris, ces systèmes par défaut peuvent transférer des paquets à d'autres systèmes dans le même segment de réseau.
  - Les systèmes à interface unique reposent sur les routeurs locaux pour le transfert de paquets et la réception des informations de configuration.

## ▼ Procédure de configuration d'une interface IP

La procédure suivante fournit un exemple de procédure de configuration basique d'une interface IP.

### Avant de commencer

Déterminez si vous souhaitez renommer les liaisons de données sur le système. En règle générale, vous utilisez les noms génériques affectés par défaut aux liaisons de données. Pour modifier les noms des liens, reportez-vous à la section “[Renommage d'une liaison de données](#)” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 (Facultatif) Affichez les informations sur les attributs physiques des liaisons de données du système.

```
# dladm show-phys
```

Cette commande affiche les cartes réseau physique installées sur le système et certaines de leurs propriétés. Pour plus d'informations sur cette commande, reportez-vous à la section “[Affichage des informations relatives aux attributs physiques des liaisons de données](#)” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

#### 3 Affichez les informations sur les liaisons de données actuelles du système.

```
# dladm show-link
```

Cette commande affiche les liaisons de données et certaines de leurs propriétés, notamment les cartes physiques sur lesquelles les liaisons ont été créées.

#### 4 Créez l'interface IP.

# **ipadm create-interface-class** *interface*

*interface-class* désigne l'une des trois classes d'interfaces que vous créez :

- Interface IP. La classe d'interface, la plus courante, est créée pendant la configuration du réseau. Pour créer cette classe d'interface, utilisez la sous-commande `create-ip`.
- Pilote d'interface réseau virtuelle STREAMS (interface VNI). Pour créer cette classe d'interface, utilisez la sous-commande `create-vni`. Pour plus d'informations sur les périphériques ou interfaces VNI, reportez-vous à la page de manuel [vni\(7d\)](#).
- Interface IPMP. Cette interface sert à configurer les groupes IPMP. Pour créer cette classe d'interface, utilisez la sous-commande `create-ipmp`. Pour plus d'informations sur les groupes IPMP, reportez-vous au [Chapitre 14, "Présentation d'IPMP"](#) du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

*interface* désigne le nom de l'interface. Ce nom est identique à celui de la liaison sur laquelle l'interface est créée.

---

**Remarque** – Vous devez créer l'interface IP avant de pouvoir lui affecter l'adresse IP.

---

#### 5 Configurez l'interface IP avec une adresse IP valide.

La syntaxe suivante affecte une adresse statique à une interface. Pour connaître d'autres options d'affectation d'adresses IP, reportez-vous à la page de manuel [ipadm\(1M\)](#).

# **ipadm create-addr -T** *address-type* **-a** *address/prefixlen addrobj*

**-T** *address-type* Spécifie le type d'adresse IP affecté à l'interface, soit : `static`, `dhcp` ou `addrconf`. `Addrconf` désigne les adresses IPv6 générées automatiquement.

**-a** Spécifie l'adresse IP à configurer sur l'interface. Vous pouvez spécifier une adresse locale seule, ou une adresse locale et une adresse distante dans le cas d'une configuration de tunnel. Généralement, vous affectez simplement une adresse locale. Dans ce cas, vous spécifiez l'adresse directement avec l'option `-a`, comme suit : `-a adress`. L'adresse est automatiquement considérée comme une adresse locale.

Si vous configurez des tunnels, vous devrez peut-être fournir l'adresse locale du système ainsi que l'adresse distante du système de destination. Dans ce cas, vous devez spécifier `local` et `remote` pour distinguer les deux adresses, comme suit : `-a local=local-addr, remote=remote-addr`. Pour obtenir des informations sur la configuration de tunnels, reportez-vous au [Chapitre 6, Configuration de tunnels IP](#).



Si vous utilisez une adresse IP numérique, utilisez le format *adress/ prefixlen* pour les adresses dans la notation CIDR, par exemple, 1.2.3.4/24. Reportez-vous à l'explication pour l'option *prefixlen*.

Si vous le souhaitez, vous pouvez spécifier un nom d'hôte pour *adress* au lieu d'une adresse IP numérique. Vous pouvez utiliser un nom d'hôte si une adresse IP numérique correspondante est définie pour ce nom d'hôte dans le fichier */etc/hosts*. Si aucune adresse IP numérique n'est définie dans le fichier, la valeur numérique ne peut être obtenue qu'en utilisant l'ordre du résolveur spécifié pour *host* dans *name-service/switch*. Si plusieurs entrées existent pour un nom d'hôte donné, une erreur est générée.

---

**Remarque** – Pendant le processus d'initialisation, la création d'adresses IP précède les services de noms mis en ligne. Par conséquent, vous devez vous assurer que tous les noms d'hôte utilisés dans la configuration réseau doivent être définis dans le fichier */etc/hosts*.

---

*/prefixlen*

Spécifie la longueur de l'ID de réseau qui fait partie de l'adresse IPv4 lorsque vous utilisez la notation CIDR. Dans l'adresse 12.34.56.78/24, 24 correspond à *prefixlen*. Si vous n'incluez pas *prefixlen*, le masque de réseau est calculé en fonction de la séquence répertoriée pour *netmask* dans le service *name-service/switch* ou par le biais de classes d'adresse.

*addrobj*

Spécifie un identificateur pour l'adresse IP unique ou l'ensemble d'adresses utilisée dans le système. Les adresses peuvent être de type IPv4 ou IPv6. L'identificateur utilise le format *interface/ chaîne-spécifiée-par-l'utilisateur*.

L'*interface* désigne l'interface IP à laquelle est connectée l'adresse. La variable *interface* doit refléter le nom de la liaison de données sur laquelle l'interface IP est configurée.

*chaîne-spécifiée-par-l'utilisateur* désigne une chaîne de caractères alphanumériques commençant par une lettre et dont la taille ne dépasse pas 32 caractères. Par conséquent, vous pouvez faire référence à *addrobj* au lieu d'utiliser l'adresse IP numérique lorsque vous exécutez une sous-commande *ipadm* qui gère les adresses dans le système, telle que *ipadm show-addr* ou *ipadm delete-addr*.

## 6 (Facultatif) Affichez les informations relatives à l'interface IP qui vient d'être configurée.

Vous pouvez utiliser les commandes suivantes, en fonction des informations à vérifier :

- Affichez le statut général de l'interface.

```
# ipadm show-if [interface]
```

Si vous ne spécifiez pas l'interface, vous obtenez les informations relatives à toutes les interfaces présentes dans le système.

- Affichez les informations d'adresses d'interface.

```
# ipadm show-addr [addrobj]
```

Si vous ne spécifiez pas *addrobj*, vous obtenez les informations relatives à tous les objets d'adresse du système.

Pour en savoir plus sur la sortie de la sous-commande `ipadm show-*`, reportez-vous à la section “Contrôle d’interfaces et d’adresses IP” du manuel *Administration d’Oracle Solaris : interfaces réseau et virtualisation réseau*.

**7 (Facultatif) Ajoutez les entrées relatives aux adresses IP dans le fichier `/etc/hosts`.**

Les entrées de ce fichier sont constituées d'adresses IP et des noms d'hôtes correspondants.

---

**Remarque** – Cette étape est pertinente uniquement si vous configurez des adresses IP statiques qui utilisent des noms d'hôtes. Si vous configurez des adresses DHCP, vous n'avez pas besoin de mettre à jour le fichier `/etc/hosts`.

---

**Exemple 3–1 Configuration d'une interface réseau avec une adresse statique**

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
net3      phys       1500     up         --          --

# ipadm create-ip net3
# ipadm create-addr -T static -a 192.168.84.3/24 net3/v4static

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net3/v4    static    ok         192.168.84.3/24

# vi /etc/hosts
# Internet host table
# 127.0.0.1      localhost
10.0.0.14       myhost
192.168.84.3    campus01
```

Notez que si `campus01` est déjà défini dans le fichier `/etc/hosts`, vous pouvez utiliser le nom d'hôte lorsque vous affectez l'adresse suivante :

```
# ipadm create-addr -T static -a campus01 net3/v4static
```

### Exemple 3–2 Configuration automatique d'une interface réseau avec une adresse IP

Cet exemple utilise le même périphérique réseau que l'exemple précédent, mais il configure l'interface IP de manière à ce qu'elle reçoive son adresse d'un serveur DHCP.

```
# dladm show-phys
LINK      MEDIA      STATE      SPEED      DUPLEX      DEVICE
net3      Ethernet   up         100Mb      full        bge3

# dladm show-link
LINK      CLASS      MTU      STATE      BRIDGE      OVER
net3      phys      1500     up         --          --

# ipadm create-ip net3

# ipadm create-addr -T dhcp net3/dhcp

# ipadm show-if
IFNAME    CLASS      STATE      ACTIVE      OVER
lo0       loopback   ok         yes         --
net3      ip         ok         yes         --

# ipadm show-addr net3/dhcp
ADDROBJ   TYPE      STATE      ADDR
net3/dhcp dhcp      ok         10.8.48.242/24

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/?     static    ok         127.0.0.1/8
net3/dhcp dhcp      ok         10.8.48.242/24
```

## Modes de configuration système

Cette section décrit les procédures de configuration d'un système en vue d'une exécution en *mode Fichiers locaux* ou en *mode Client réseau*. En cas d'exécution en mode fichiers locaux, un système obtient toutes les informations de configuration TCP/IP auprès de fichiers qui se trouvent dans le répertoire local. En mode Client réseau, les informations de configuration sont fournies à tous les systèmes dans le réseau par un serveur de configuration réseau.

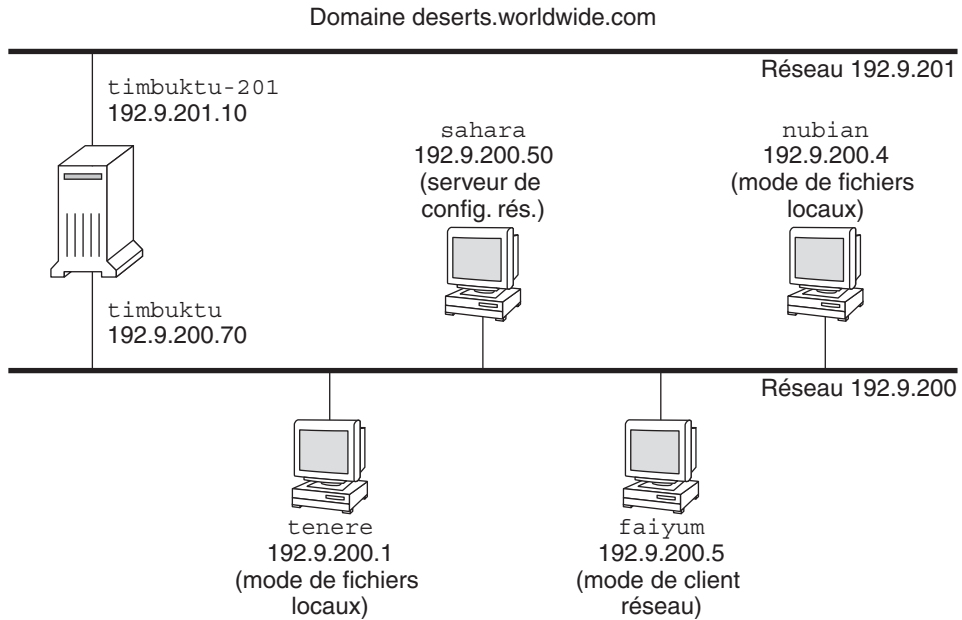
En règle générale, les serveurs dans le réseau s'exécutent en mode fichiers locaux, comme suit :

- Serveurs de configuration réseau
- Serveurs NFS
- Serveurs de noms fournissant les services NIS, LDAP ou DNS

- Serveurs de courrier
- Routeurs

Les clients peuvent s'exécuter dans les deux modes. Par conséquent, dans le réseau, vous pouvez avoir une combinaison de ces deux modes en fonction de la configuration des différents systèmes, comme illustré dans la figure suivante :

FIGURE 3-2 Systèmes dans un scénario de topologie de réseau IPv4



La [Figure 3-2](#) représente les systèmes dans un réseau 192.9.200.

- Tous les systèmes appartiennent au domaine d'organisation `deserts.worldwide.com`.
- `sahara` est un serveur de configuration. En tant que serveur, il s'exécute en mode fichiers locaux, où les informations de configuration TCP/IP sont obtenues auprès du disque local du système.

**Remarque** – Si vous configurez des clients pour qu'ils s'exécutent en mode Client réseau, vous devez alors configurer au moins un serveur de configuration réseau qui fournira les informations de configuration à ces clients.

- `tenere`, `nubian` et `faiyum` sont des clients dans le réseau. `tenere` et `nubian` s'exécutent en mode fichiers locaux. Quel que soit le disque local de `faiyum`, le système est configuré pour fonctionner en mode Client réseau.
- `timbuktu` est configuré en tant que routeur et fonctionne par conséquent en mode fichiers locaux. Le système inclut deux NIC, chacun ayant ses propres interfaces IP configurées. La première interface IP est nommée `timbuktu` et se connecte au réseau 192.9.200. La deuxième interface IP est nommée `timbuktu-201` et se connecte au réseau 192.9.201.

Pour une présentation détaillée des deux modes de configuration, reportez-vous à la section [“Choix des modes de configuration des hôtes”](#) du manuel *Guide d'administration système : services IP*

## ▼ Configuration d'un système en mode Fichiers locaux

Utilisez cette procédure pour configurer tout système afin qu'il s'exécute en mode fichiers locaux tels que ceux qui sont répertoriés dans la section [“Systèmes devant s'exécuter en mode Fichiers locaux”](#) du manuel *Guide d'administration système : services IP*.

### 1 Configurez les interfaces IP du système avec les adresses IP attribuées.

Reportez-vous à la section [“Procédure de configuration d'une interface IP”](#) à la page 47 pour obtenir des informations sur la procédure.

### 2 Vérifiez le nom d'hôte défini dans le fichier `/etc/nodename`.

### 3 Vérifiez que les entrées du fichier `/etc/inet/hosts` sont à jour.

Le programme d'installation Oracle Solaris crée des entrées pour l'interface réseau principale, l'adresse loopback et toute interface supplémentaire configurée lors de l'installation, le cas échéant.

Ce fichier doit inclure le nom du routeur par défaut et l'adresse IP du routeur.

a. (Facultatif) Ajoutez les adresses IP et les noms correspondants des interfaces réseau ajoutées au système après l'installation.

b. (Facultatif) Si le système de fichiers `/usr` est monté sur un système NFS, ajoutez la ou les adresses IP du serveur de fichiers.

### 4 Spécifiez le domaine complet du système en tant que propriété du service SMF `nis/domain`.

Par exemple, vous pourriez spécifier `deserts.worldwide.com` en tant que valeur de la propriété `domainname` du service SMF `nis/domain`.

### 5 Tapez le nom du routeur dans le fichier `/etc/defaultrouter`.

## 6 Ajoutez les informations de masque de réseau, le cas échéant.

---

**Remarque** – Si vous utilisez des services DHCP, passez cette étape.

---

### a. Tapez le numéro et le masque de réseau dans le fichier `/etc/inet/netmasks`.

Pour créer des entrées, utilisez le format *réseau-numéro de masque de réseau*. Par exemple, pour le numéro de réseau de Classe C 192.168.83, vous devez taper :

```
192.168.83.0      255.255.255.0
```

Pour les adresses CIDR, remplacez le préfixe réseau par la représentation décimale avec points équivalente. Les préfixes de réseau et leurs équivalents décimaux à points sont répertoriés dans le [Tableau 1-1](#). Par exemple, pour exprimer le préfixe réseau CIDR 192.168.3.0/22, tapez ce qui suit :

```
192.168.3.0      255.255.252.0
```

### b. Modifiez l'ordre de recherche des masques de réseau dans la propriété SMF du commutateur de sorte que la recherche s'effectue d'abord dans les fichiers locaux, puis actualisez l'instance.

```
# svccfg -s name-service/switch setprop config/host = astring: "files nis"
# svccfg -s name-service/switch:default refresh
```

## 7 Redémarrez le système.

## ▼ Configuration d'un système en mode Client réseau

Effectuez la procédure suivante sur chaque hôte à configurer en mode Client réseau.

### Avant de commencer

Les clients réseau reçoivent leurs informations de configuration des serveurs de configuration réseau. Par conséquent, avant de configurer un système en tant que client réseau, assurez-vous de configurer au moins un serveur de configuration pour le réseau.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Configurez les interfaces IP du système avec les adresses IP attribuées.

Reportez-vous à la section [“Procédure de configuration d'une interface IP”](#) à la page 47 pour obtenir des informations sur la procédure.

- 3 Assurez-vous que le fichier `/etc/inet/hosts` contient uniquement le nom `localhost` et l'adresse IP de l'interface réseau loopback.  

```
# cat /etc/inet/hosts
# Internet host table
#
127.0.0.1      localhost
```
- 4 Supprimez toute valeur attribuée à la propriété `domainname` du service `SMF nis/domain`.
- 5 Assurez-vous que les chemins de recherche dans le service `name-service/switch` du client reflètent les mêmes exigences service de votre réseau.

## ▼ Configuration d'un serveur de configuration réseau

Vous trouverez des informations sur la configuration de serveurs d'installation et d'initialisation dans le manuel *Installation des systèmes Oracle Solaris 11*.

- 1 Connectez-vous en tant qu'administrateur.  
 Pour plus d'informations, reportez-vous à la section “Procédure d'obtention des droits d'administration” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- 2 Activez le démon `in.tftpd` comme suit :
  - a. Accédez au répertoire root (`/`) du serveur de configuration réseau désigné.
  - b. Créez le répertoire `/tftpboot` :  

```
# mkdir /tftpboot
```

 Cette commande configure le système en tant que serveur RARP, bootparams et TFTP.
  - c. Créez un lien symbolique vers le répertoire.  

```
# ln -s /tftpboot/. /tftpboot/tftpboot
```
- 3 Ajoutez la ligne `tftp` dans le fichier `/etc/inetd.conf`.  
 La ligne devrait être comme suit :  

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

 Cette ligne empêche `in.tftpd` d'extraire un fichier autre que ceux figurant dans `/tftpboot`.
- 4 Dans la base de données `/etc/hosts`, ajoutez les noms d'hôte et les adresses IP de tous les clients sur le réseau.

- 5 Dans la base de données `/etc/ethers`, créez des entrées pour chaque système sur le réseau qui s'exécute en mode client réseau.

Les entrées de cette base de données sont au format suivant :

```
MAC Address      host name      #comment
```

Pour plus d'informations, reportez-vous à la page de manuel [ethers\(4\)](#).

- 6 Dans la base de données `/etc/bootparams`, créez une entrée pour chaque système sur le réseau qui s'exécute en mode client réseau.

Pour obtenir des informations sur la modification de cette base de données, consultez la page de manuel [bootparams\(4\)](#).

- 7 Convertissez l'entrée `/etc/inetd.conf` en un fichier manifeste de service SMF (Service Management Facility) et activez le service obtenu.

```
# /usr/sbin/inetconv
```

- 8 Assurez-vous que `in.tftpd` fonctionne correctement.

```
# svcs network/tftp/udp6
```

La sortie que vous devez recevoir ressemble à ce qui suit :

```
STATE      STIME      FMRI
online      18:22:21   svc:/network/tftp/udp6:default
```

## Informations supplémentaires

### Gestion du démon `in.tftpd`

Le démon `in.tftpd` est géré par SMF (Service Management Facility). La commande `svcadm` permet d'effectuer les opérations de gestion sur `in.tftpd` (par exemple, l'activation, la désactivation ou le redémarrage). L'initiation et la réinitialisation du service s'effectue par l'intermédiaire de la commande `inetd`. Utilisez la commande `inetadm` pour modifier la configuration et afficher les informations de configuration pour `in.tftpd`. La commande `svcs` permet d'interroger l'état du service. Pour une présentation de l'utilitaire de gestion des services, reportez-vous au [Chapitre 6, "Gestion des services \(présentation\)"](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

## Configuration d'un routeur IPv4

Un routeur fournit l'interface entre deux réseaux ou plus. Par conséquent, vous devez attribuer un nom unique et une adresse IP à chacune des interfaces de réseau physique du routeur. Par conséquent, chaque routeur possède un nom d'hôte et une adresse IP associés à son interface réseau principale ainsi qu'un nom et une adresse IP uniques pour chaque interface réseau supplémentaire.



Vous pouvez également effectuer la procédure suivante pour configurer un système doté d'une seule interface physique (un hôte, par défaut) en tant que routeur. Pour être configuré en tant que routeur, un système d'interface unique doit servir d'extrémité de lien PPP, comme décrit à la section [“Planification d'une liaison PPP commutée” du manuel \*Administration d'Oracle Solaris : Services réseau\*](#).

## ▼ Procédure de configuration d'un routeur IPv4

La procédure suivante suppose que vous configurez les interfaces du routeur après l'installation.

### Avant de commencer

Une fois le routeur installé physiquement sur le réseau, configurez le routeur de sorte qu'il fonctionne en mode fichiers locaux, tel que décrit à la section [“Configuration d'un système en mode Fichiers locaux” à la page 53](#). Cette configuration garantit l'initialisation du routeur en cas de panne du serveur de configuration.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

#### 2 Pour chaque NIC installée sur le système, configurez les interfaces IP tel que détaillé dans [“Procédure de configuration d'une interface IP” à la page 47](#).

Assurez-vous que chaque interface IP est configurée avec l'adresse IP du réseau pour lequel le système acheminera les paquets. Par conséquent, si le système sert les réseaux 192.168.5.0 et 10.0.5.0, une NIC doit être configurée pour chaque réseau.



**Attention** – Si vous souhaitez configurer des routeurs IPv4 pour utiliser DHCP, vous devez maîtriser l'administration DHCP.

#### 3 Ajoutez le nom d'hôte et l'adresse IP de chaque interface au fichier `/etc/inet/hosts`.

Par exemple, supposons que les noms assignés aux deux interfaces du routeur 1 sont `krakatoa` et `krakatoa-1`, respectivement. Les entrées dans le fichier `/etc/inet/hosts` seraient comme suit :

```
192.168.5.1      krakatoa      #interface for network 192.168.5.0
10.0.5.1        krakatoa-1    #interface for network 10.0.5.0
```

#### 4 Effectuez le reste des étapes pour configurer ce routeur pour qu'il s'exécute en mode fichiers locaux.

Reportez-vous à la section [“Configuration d'un système en mode Fichiers locaux” à la page 53](#).

- 5 Si le routeur est connecté à un réseau comportant des sous-réseaux, ajoutez le numéro de réseau et le masque de réseau au fichier `/etc/inet/netmasks`.

Par exemple, pour une adresse IPv4 de numérotation classique, telle que 192.168.5.0, vous devez taper :

```
192.168.5.0    255.255.255.0
```

- 6 Activez le transfert de paquets IPv4 sur le routeur.

```
# ipadm set-prop -p forwarding=on ipv4
```

- 7 (Facultatif) Lancez le protocole de routage.

Utilisez l'une des syntaxes de commande suivantes :

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

Le FMRI SMF associé au démon `in.routed` est `svc:/network/routing/route`.

Lorsque vous démarrez un protocole de routage, le démon de routage `/usr/sbin/in.routed` met automatiquement à jour la table de routage ; il s'agit d'un processus appelé *routage dynamique*. Pour plus d'informations sur les types de routage, reportez-vous à la section “[Tables et types de routage](#)” à la page 59. Pour plus d'informations sur la commande `routeadm`, reportez-vous à la page de manuel [routeadm\(1M\)](#).

### Exemple 3–3 Configuration du routeur par défaut d'un réseau

Cet exemple est basé sur la [Figure 3–1](#). Le routeur 2 contient deux connexions réseau câblées, une connexion au réseau 172.20.1.0 et une connexion au réseau 10.0.5.0. L'exemple indique comment configurer le routeur 2 pour qu'il soit le routeur par défaut du réseau 172.20.1.0. L'exemple suppose également que le routeur 2 a été configuré afin de fonctionner en mode Fichiers locaux, tel que décrit dans la section “[Configuration d'un système en mode Fichiers locaux](#)” à la page 53.

Prenez le rôle de superutilisateur ou un rôle équivalent, puis déterminez l'état des interfaces du système.

```
# dladm show-link
LINK    CLASS    MTU    STATE    BRIDGE    OVER
net0     phys     1500    up       --        --
net1     phys     1500    up       --        --
net2     phys     1500    up       --        --
# ipadm show-addr
ADDROBJ  TYPE    STATE    ADDR
lo0/v4   static  ok       127.0.0.1/8
net0/v4   static  ok       172.20.1.10/24
```

Seule `net0` a été configurée avec une adresse IP. Pour que le routeur 2 soit le routeur par défaut, vous devez connecter l'interface `net1` au réseau 10.0.5.0.

```
# ipadm create-ip net1
# ipadm create-addr -T static -a 10.0.5.10/24 net1/v4
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4       static    ok         127.0.0.1/8
net0/v4       static    ok         172.20.1.10/24
net1/v4       static    ok         10.0.5.10/24
```

Ensuite, mettez à jour les bases de données réseau suivantes à l'aide des informations sur l'interface que vous venez de configurer et le réseau auquel elle est connectée.

```
# vi /etc/inet/hosts
127.0.0.1      localhost
172.20.1.10    router2      #interface for network 172.20.1
10.0.5.10      router2-out  #interface for network 10.0.5
# vi /etc/inet/netmasks
172.20.1.0     255.255.255.0
10.0.5.0       255.255.255.0
```

Enfin, activez le transfert de paquets ainsi que le démon de routage `in.routed`.

```
# ipadm set-prop -p forwarding=on ipv4
# svcadm enable route:default
```

La transmission de paquets IPv4 et le routage dynamique via RIP sont maintenant activés sur le Routeur 2. La configuration du routeur par défaut `172.20.1.0` n'est cependant pas terminée. Procédez comme suit :

- Modifiez les hôtes du réseau `172.20.1.0` pour qu'ils reçoivent leurs informations de routage du nouveau routeur par défaut. Pour plus d'informations, reportez-vous à la section [“Activation du routage statique sur un hôte à interface unique”](#) à la page 65.
- Définissez une route statique menant au routeur de bordure dans la table de routage du Routeur 2. Pour plus d'informations, reportez-vous à la section [“Tables et types de routage”](#) à la page 59.

## Tables et types de routage

Les routeurs et les hôtes maintiennent une *table de routage*. La table de routage dresse la liste des adresses IP des réseaux connus du système, notamment le réseau local par défaut. Elle répertorie également la liste des adresses IP d'un système de passerelle pour chaque réseau connu. La *passerelle* est un système qui peut recevoir des paquets sortants et les transférer au saut au-delà du réseau local.

Ce qui suit est une table de routage simple pour un système sur un réseau IPv4 uniquement :

```
Routing Table: IPv4
Destination      Gateway          Flags Ref  Use  Interface
-----
```

default	172.20.1.10	UG	1	532	net0
224.0.0.0	10.0.5.100	U	1	0	net1
10.0.0.0	10.0.5.100	U	1	0	net1
127.0.0.1	127.0.0.1	UH	1	57	lo0

Vous pouvez configurer deux types de routage sur un système Oracle Solaris : statique et dynamique. Vous pouvez configurer l'un ou l'autre, ou les deux sur un même système. Un système qui implémente le *routage dynamique* repose sur les protocoles de routage, notamment RIP pour les réseaux IPv4 et RIPng pour les réseaux IPv6, pour acheminer le trafic réseau et pour mettre à jour les informations de routage dans la table. Avec le *routage statique*, les informations de routage sont conservées manuellement par l'intermédiaire de l'utilisation de la commande `route`. Pour plus d'informations, reportez-vous à la page de manuel [route\(1M\)](#).

Lors de la configuration du routage du réseau local ou d'un système autonome, réfléchissez au type de routage à prendre en charge sur des hôtes et des routeurs particuliers.

Le tableau suivant présente les différents types de routage et les scénarios de mise en réseau auquel chaque type de routage convient le mieux.

Type de routage	Utilisation privilégiée
Statique	Réseaux de petite taille, hôtes qui obtiennent leurs routes d'un routeur par défaut et routeurs par défaut qui n'ont besoin de connaître qu'un ou deux routeurs sur les quelques sauts suivants.
Dynamique	Interréseaux volumineux, routeurs sur des réseaux locaux comportant de nombreux hôtes et hôtes sur des systèmes autonomes d'envergure. Le routage dynamique représente le meilleur choix pour les systèmes résidant sur la plupart des réseaux.
Combinaison statique-dynamique	Routeurs effectuant la connexion entre un réseau au routage statique et un réseau au routage dynamique, et routeurs de bordure reliant un système interne autonome aux réseaux externes. La combinaison routage statique et routage dynamique est pratique courante.

Sur la [Figure 3–1](#), l'AS allie le routage statique au routage dynamique.

---

**Remarque** – Lorsque deux routes présentent la même destination, le système ne procède pas automatiquement à un basculement ou à un équilibrage des charges. Si vous avez besoin de telles fonctionnalités, utilisez IPMP tel que décrit dans le [Chapitre 14, “Présentation d’IPMP” du manuel \*Administration d’Oracle Solaris : interfaces réseau et virtualisation réseau\*](#).

---

## ▼ Ajout d'une route statique à la table de routage

### 1 Affichez l'état actuel de la table de routage.

Pour exécuter la forme suivante de la commande `netstat`, utilisez votre compte utilisateur standard :

```
% netstat -rn
```

La sortie doit ressembler à ceci :

```
Routing Table: IPv4
  Destination      Gateway            Flags  Ref    Use  Interface
-----
192.168.5.125      192.168.5.10      U        1   5879   net0
224.0.0.0          198.168.5.10      U        1     0   net0
default            192.168.5.10      UG       1   91908
127.0.0.1          127.0.0.1         UH       1  811302   lo0
```

### 2 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 3 (Facultatif) Supprimez les entrées existantes de la table de routage.

```
# route flush
```

### 4 Ajoutez une route qui persiste aux réinitialisations du système.

```
# route -p add -net network-address -gateway gateway-address
```

`-p` Crée une route qui doit être conservée après les réinitialisations du système. Si vous souhaitez configurer la route pour la session en cours uniquement, n'utilisez pas l'option `-p`.

`-net network-address` Indique que la route intègre le réseau avec l'adresse *network-address*.

`-gateway gateway-address` Indique que le système de passerelle pour la route spécifiée possède l'adresse IP *gateway-address*.

## Exemple 3–4 Ajout d'une route statique à la table de routage

L'exemple suivant indique comment ajouter une route statique au routeur 2 de la [Figure 3–1](#). La route statique est nécessaire pour le routeur de bordure de l'AS, 10.0.5.150.

Pour afficher la table de routage sur Router 2, effectuez l'opération suivante :

```
# netstat -rn
Routing Table: IPv4
  Destination      Gateway            Flags  Ref    Use  Interface
-----
```

default	172.20.1.10	UG	1	249	ce0
224.0.0.0	172.20.1.10	U	1	0	ce0
10.0.5.0	10.0.5.20	U	1	78	bge0
127.0.0.1	127.0.0.1	UH	1	57	lo0

D'après la table de routage, Router 2 a connaissance de deux routes. La route par défaut utilise l'interface 172.20.1.10 de Router 2 comme passerelle. La deuxième route, 10.0.5.0, a été détectée par le démon `in.routed` exécuté sur le Routeur 2. La passerelle de cette route est Routeur 1, avec l'adresse IP 10.0.5.20.

Pour ajouter une seconde route au réseau 10.0.5.0, dont la passerelle est le routeur de bordure, procédez comme suit :

```
# route -p add -net 10.0.5.0/24 -gateway 10.0.5.150
add net 10.0.5.0: gateway 10.0.5.150
```

La table de routage contient désormais une route destinée au routeur de bordure dont l'adresse IP est 10.0.5.150/24.

```
# netstat -rn
```

Routing Table: IPv4					
Destination	Gateway	Flags	Ref	Use	Interface
-----	-----	-----	-----	-----	-----
default	172.20.1.10	UG	1	249	ce0
224.0.0.0	172.20.1.10	U	1	0	ce0
10.0.5.0	10.0.5.20	U	1	78	bge0
10.0.5.0	10.0.5.150	U	1	375	bge0
127.0.0.1	127.0.0.1	UH	1	57	lo0

## Configuration des hôtes multiréseaux

Dans Oracle Solaris, un système doté de plus d'une interface est considéré comme un *hôte multiréseau*. Les interfaces d'un hôte multiréseau se connectent à différents sous-réseaux, soit sur des réseaux physiques différents, soit sur le même réseau physique.

Sur un système dont les interfaces se connectent à un même sous-réseau, vous devez d'abord configurer les interfaces en tant que groupe IPMP. Dans le cas contraire, le système ne pourra pas être un hôte multiréseau. Pour plus d'informations sur IPMP, reportez-vous au [Chapitre 14, “Présentation d'IPMP”](#) du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

Un hôte multiréseau ne transfère pas les paquets IP, mais il peut être configuré afin d'exécuter des protocoles de routage. Les systèmes habituellement configurés en tant qu'hôtes multiréseaux sont les suivants :

- Les serveurs NFS (en particulier ceux qui fonctionnent en tant que vastes centres de données) peuvent être reliés à plusieurs réseaux et permettre ainsi à un grand nombre d'utilisateurs de partager des fichiers. Ils ne doivent pas forcément gérer des tables de routage.
- Tout comme les serveurs NFS, les serveurs de bases de données peuvent posséder plusieurs interfaces réseau en vue de mettre des ressources à la disposition d'un grand nombre d'utilisateurs.
- Les passerelles pare-feu connectent un réseau d'entreprise avec des réseaux publics, tels qu'Internet. Un pare-feu constitue une mesure de sécurité mise en oeuvre par les administrateurs. Configuré en tant que pare-feu, l'hôte ne transmet pas de paquets entre les réseaux qui sont reliés à ses interfaces. Toutefois, l'hôte peut toujours fournir des services TCP/IP standard, tels que `ssh`, aux utilisateurs autorisés.

---

**Remarque** – Lorsque les pare-feux sur les interfaces d'un hôte multiréseau sont différents, évitez au maximum toute perturbation accidentelle des paquets de l'hôte. Ce problème se produit particulièrement avec les pare-feux avec état. Une des solutions consiste à configurer des pare-feux sans état. Pour plus d'informations sur les pare-feux, reportez-vous à la section [“Systèmes pare-feu” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#) ou à la documentation de votre pare-feu.

---

## ▼ Création d'un hôte multiréseau

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Configurez chaque interface réseau supplémentaire qui n'a pas été configurée lors de l'installation d'Oracle Solaris.

Reportez-vous à la section [“Procédure de configuration d'une interface IP” à la page 47](#).

### 3 Si le transfert de paquets est activé, désactivez ce service.

```
# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY   PERM CURRENT   PERSISTENT   DEFAULT   POSSIBLE
ipv4 forwarding  rw    on           --          off       on,off

ipadm set-prop -p forwarding=off ipv4
```

### 4 (Facultatif) Activez le routage dynamique pour l'hôte multiréseau.

Utilisez l'une des syntaxes de commande suivantes :

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

Le FMRI SMF associé au démon `in.routed` est `svc:/network/routing/route`.

**Exemple 3-5** Configuration d'un hôte multiréseau

L'exemple suivant illustre comment configurer l'hôte multiréseau représenté dans la [Figure 3-1](#). Dans cet exemple, le nom d'hôte du système est `hostc`. Cet hôte présente deux interfaces connectées au réseau `192.168.5.0`.

Commencez par afficher l'état des interfaces du système.

```
# dladm show-link
LINK      CLASS      MTU      STATE    BRIDGE    OVER
net0      phys         1500     up       --        --
net1      phys         1500     up       --        --

# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/v4    static    ok         127.0.0.1/8
net0/v4    static    ok         192.168.5.82/24
```

La commande `dladm show-link` rapporte que `hostc` dispose de deux liaisons de données. Cependant, seule `net0` a été configurée avec une adresse IP. Pour configurer `hostc` en tant qu'hôte multiréseau, configurez `net1` avec une adresse IP dans le même réseau `192.168.5.0`. Assurez-vous que la NIC sous-jacente physique de `net1` est connectée physiquement au réseau.

```
# ipadm create-ip net1
# ipadm create-addr -T static -a 192.168.5.85/24 bge0/v4
# ipadm show-addr
ADDROBJ   TYPE      STATE      ADDR
lo0/v4    static    ok         127.0.0.1/8
net0/v4    static    ok         192.168.5.82/24
net1/v4    static    ok         192.168.5.85/24
```

Ensuite, ajoutez l'interface `net1` à la base de données `/etc/hosts` :

```
# vi /etc/inet/hosts
127.0.0.1      localhost
192.168.5.82   hostc #primary network interface for host3
192.168.5.85   hostc-2 #second interface
```

Désactivez ensuite le transfert de paquets si ce service s'exécute sur `hostc` :

```
# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY  PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw   on        --          off       on,off

# ipadm set-prop -p forwarding=off ipv4

# routeadm
Configuration  Current      Current
Option          Configuration System State
```



```

-----
IPv4 routing    enabled      enabled
IPv6 routing    disabled     disabled

Routing services "route:default ripng:default"

```

La commande `routeadm` rapporte que le routage dynamique via le démon `in.routed` est actuellement activé.

## Configuration du routage de systèmes à interface unique

Les systèmes à interface unique peuvent être configurés avec un routage dynamique ou statique. Avec le routage statique, l'hôte doit utiliser les services d'un routeur par défaut pour les informations de routage. Les sections suivantes décrivent les procédures d'activation des deux types de routage.

### ▼ Activation du routage statique sur un hôte à interface unique

Vous pouvez également suivre la procédure ci-dessous pour configurer le routage statique sur un hôte multiréseau.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Configurez l'interface IP du système avec une adresse IP pour le réseau auquel appartient le système.

Pour obtenir des instructions, reportez-vous à la section [“Procédure de configuration d'une interface IP”](#) à la page 47.

#### 3 Avec un éditeur de texte, créez ou modifiez le fichier `/etc/defaultrouter` en ajoutant l'adresse IP du routeur que le système utilisera.

#### 4 Ajoutez une entrée pour le routeur par défaut dans le fichier local `/etc/inet/hosts`.

#### 5 Assurez-vous que le routage est désactivé.

```

# routeadm
Configuration    Current          Current
                  Option    Configuration    System State
-----
IPv4 routing      enabled      disabled
IPv6 routing      disabled     disabled

Routing services "route:default ripng:default"

```

```
# svcadm disable route:default
```

6 Assurez-vous que le transfert de paquets est désactivé.

```
# # ipadm show-prop -p forwarding ipv4
PROTO PROPERTY    PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw   on       --          off      on,off

# ipadm set-prop -p forwarding=off ipv4
```

Exemple 3–6 Configuration du routage statique sur un système à interface unique

L'exemple suivant explique comment configurer le routage statique pour hostb, un système à interface unique sur le réseau 172.20.1.0 comme illustré dans la [Figure 3–1](#). hostb doit utiliser le routeur 2 en tant que routeur par défaut. L'exemple suppose que vous avez déjà configuré l'interface IP du système.

Tout d'abord, connectez-vous à hostb en tant qu'administrateur. Vérifiez ensuite la présence du fichier /etc/defaultrouter sur le système :

```
# cd /etc
# ls | grep defaultrouter

# vi /etc/defaultrouter
172.20.1.10
```

L'adresse IP 172.20.1.10 appartient au routeur 2.

```
# vi /etc/inet/hosts
127.0.0.1          localhost
172.20.1.18        host2    #primary network interface for host2
172.20.1.10        router2  #default router for host2

# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY    PERM CURRENT  PERSISTENT  DEFAULT  POSSIBLE
ipv4 forwarding  rw   on       --          off      on,off

# ipadm set-prop -p forwarding=off ipv4

# routeadm
Configuration      Current          Current          System State
                  Option          Configuration
-----
                  IPv4 routing    enabled          disabled
                  IPv6 routing    disabled         disabled
Routing services    "route:default  ripng:default"
```

```
# svcadm disable route:default
```

## ▼ Activation du routage dynamique sur un système à interface unique

Le routage dynamique qui utilise un protocole de routage constitue le moyen le plus simple de gérer le routage dans un système.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Configurez l'interface IP du système avec une adresse IP pour le réseau auquel appartient le système.

Pour obtenir des instructions, reportez-vous à la section “[Procédure de configuration d'une interface IP](#)” à la page 47.

### 3 Supprimez toute entrée dans le fichier `/etc/defaultrouter`.

Un fichier `/etc/defaultrouter` vide oblige le système à utiliser le routage dynamique.

### 4 Assurez-vous que le transfert de paquets est désactivé.

```
# ipadm set-prop -p forwarding=off ipv4
```

### 5 Activez les protocoles de routage sur le système.

Exécutez l'une des commandes suivantes :

- `# routeadm -e ipv4-routing -u`
- `# svcadm enable route:default`

## Exemple 3–7 Exécution du routage dynamique sur un système à interface unique

L'exemple suivant montre comment configurer le routage dynamique pour `hosta`, un système à interface unique sur le réseau `192.168.5.0` illustré dans la [Figure 3–1](#). Le système utilise le routeur 1 en tant que routeur par défaut. L'exemple suppose que vous avez déjà configuré l'interface IP du système.

Tout d'abord, connectez-vous à `hosta` en tant qu'administrateur. Vérifiez ensuite la présence du fichier `/etc/defaultrouter` sur le système :

```
# cd /etc
# ls | grep defaultrouter
defaultrouter

# cat defaultrouter
192.168.5.10
```

Le fichier contient l'entrée `192.168.5.10`, qui est l'adresse IP du routeur 1.

```
# routeadm Configuration Current Current
              Option Configuration System State
-----
              IPv4 routing disabled disabled
              IPv6 routing disabled disabled

              Routing services "route:default ripng:default"

# svcadm enable route:default

# ipadm show-prop -p forwarding ipv4
PROTO PROPERTY PERM CURRENT PERSISTENT DEFAULT POSSIBLE
ipv4 forwarding rw on -- off on,off

# ipadm set-prop -p forwarding=off ipv4
```

## Ajout d'un sous-réseau à un réseau

Si vous passez d'un réseau n'utilisant pas de sous-réseau à un réseau qui en utilise un, effectuez les tâches figurant dans la liste suivante. La liste suppose que vous avez déjà préparé un schéma de sous-réseau. Pour obtenir une présentation générale, reportez-vous à la section [“Qu'est-ce que la création de sous-réseaux ?” du manuel \*Guide d'administration système : services IP\*](#).

- Assignez les adresses IP avec le nouveau numéro de sous-réseau aux systèmes qui appartiennent au sous-réseau.  
A titre de référence, reportez-vous à la section [“Procédure de configuration d'une interface IP” à la page 47](#).
- Ajoutez l'adresse IP et le masque de réseau corrects à chaque fichier `/etc/netmasks` de chaque système.
- Réviser chaque fichier `/etc/inet/hosts` de chaque système avec l'adresse IP correcte de sorte qu'elle corresponde aux noms d'hôtes.
- Réinitialisez tous les systèmes dans le sous-réseau.

La procédure est étroitement liée aux sous-réseaux. Si vous implémentez la création de sous-réseaux bien après avoir effectué la configuration initiale du réseau sans cette création de sous-réseaux, effectuez la procédure suivante pour implémenter les modifications.

### ▼ Modification de l'adresse IPv4 et des autres paramètres de configuration réseau

Cette section décrit la procédure de modification de l'adresse IPv4, du nom d'hôte et des autres paramètres réseau d'un système déjà installé. Cette procédure permet de modifier l'adresse IP d'un serveur ou d'un système autonome en réseau. Elle ne s'applique pas aux appareils ou clients réseau. Cette procédure entraîne la création d'une configuration qui sera conservée après les réinitialisations du système.

---

**Remarque** – Les instructions s'appliquent explicitement à la modification de l'adresse IPv4 de l'interface réseau principale. Pour ajouter une autre interface au système, reportez-vous à la section “[Procédure de configuration d'une interface IP](#)” à la page 47.

---

Dans la plupart des cas, les étapes suivantes font appel à la numérotation décimale avec points IPv4 classique afin de spécifier l'adresse IPv4 et le masque de sous-réseau. Vous pouvez aussi indiquer l'adresse IPv4 à l'aide de la numérotation CIDR dans tous les fichiers pertinents. Pour une introduction à la notation CIDR, reportez-vous à la section “[Adresses IPv4 au format CIDR](#)” du manuel *Guide d'administration système : services IP*.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Modifiez l'adresse IP en utilisant la commande `ipadm`.**

La commande `ipadm` ne permet pas de modifier une adresse IP directement. Vous devez d'abord supprimer l'objet d'adressage qui représente l'adresse IP que vous souhaitez modifier. Vous pouvez ensuite affecter une nouvelle adresse à l'aide du même nom d'objet d'adressage.

```
# ipadm delete-addr addrobj
# ipadm create-addr -T static IP-address addrobj
```

**3 Le cas échéant, modifiez le nom d'hôte dans le fichier `/etc/inet/hosts` ou la base de données `hosts` équivalente.**

**4 Le cas échéant, modifiez l'entrée de nom d'hôte dans le service SMF `system/identity:node` :**

```
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: hostname
```

**5 En cas de changement du masque de sous-réseau, modifiez les entrées de sous-réseau dans le fichiers `/etc/netmasks`.**

**6 En cas de changement de l'adresse de sous-réseau, remplacez l'adresse IP du routeur par défaut dans `/etc/default/trouter` par celle du routeur par défaut du nouveau sous-réseau.**

**7 Redémarrez le système.**

```
# reboot -- -r
```

### Exemple 3–8 Modification de l'adresse IP et du nom d'hôte

Cet exemple illustre la modification du nom d'hôte, de l'adresse IP de l'interface réseau principale et du masque de sous-réseau. L'adresse IP de l'interface réseau principale `bge0` passe de `10.0.0.14` à `192.168.34.100`.

```
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4        static    ok          127.0.0.1/8
bge0/v4        static    ok          10.0.0.14/24

# ipadm delete-addr bge0/v4
# ipadm create-addr -T static -a 192.168.34.100/24 bge0/v4
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: mynewhostname

# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4        static    ok          127.0.0.1/8
bge0/v4new     static    ok          192.168.34.100/24

# hostname
mynewhostname
```

**Voir aussi** Pour modifier l'adresse IP d'une interface autre que l'interface réseau principale, reportez-vous au manuel [Administration d'Oracle Solaris : Tâches courantes](#) et à la section “[Procédure de configuration d'une interface IP](#)” à la page 47.

## Contrôle et modification des services de couche transport

Les protocoles de couche de transport TCP, SCTP et UDP font partie du package Oracle Solaris standard. Généralement, ces protocoles fonctionnent correctement sans que l'utilisateur ait à intervenir. Toutefois, dans certaines conditions, vous serez peut-être amené à consigner ou modifier des services exécutés via les protocoles de couche transport. Vous devez ensuite modifier les profils de ces services à l'aide de l'utilitaire de gestion des services (SMF) décrit au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

Le démon `inetd` est chargé de lancer les services Internet standard lors de l'initialisation d'un système. Ces services incluent les applications utilisant les protocoles de couche transport TCP, SCTP ou UDP. Vous pouvez modifier les services Internet existants ou ajouter de nouveaux services à l'aide des commandes SMF. Pour plus d'informations sur `inetd`, reportez-vous à la section “[Démon de services Internet `inetd`](#)” à la page 145.

Opérations impliquant les protocoles de couche transport :

- Journalisation de toutes les connexions TCP entrantes
- Ajout de services faisant appel à un protocole de couche transport, utilisant SCTP comme exemple
- Configuration des wrappers TCP dans le cadre du contrôle d'accès

Pour plus d'informations sur le démon `inetd`, reportez-vous à la page de manuel [inetd\(1M\)](#).

## ▼ Journalisation des adresses IP de toutes les connexions TCP entrantes

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Activez le suivi TCP pour tous les services gérés par inetd.

```
# inetadm -M tcp_trace=TRUE
```

## ▼ Ajout de services utilisant le protocole SCTP

Le protocole de transport SCTP fournit des services aux protocoles de couche d'application de façon similaire à TCP. Toutefois, SCTP permet la communication entre deux systèmes multiréseaux ou deux systèmes dont l'un est multiréseau. La connexion SCTP s'appelle une *association*. Dans une association, une application divise les données à transmettre en *plusieurs flux de messages*. Une connexion SCTP peut atteindre les extrémités à l'aide de plusieurs adresses IP, ce qui s'avère particulièrement important dans le cadre d'applications de téléphonie. Les capacités multiréseau de SCTP améliorent la sécurité des sites ayant recours à IP Filter ou IPsec. La page de manuel [sctp\(7P\)](#) répertorie les points à prendre en considération au niveau de la sécurité.

Par défaut, le protocole SCTP fait partie d'Oracle Solaris et ne nécessite aucune configuration supplémentaire. Toutefois, vous devrez peut-être configurer explicitement certains services de couche d'application pour utiliser SCTP. `echo` et `discard` sont des exemples d'applications. La procédure suivante illustre l'ajout d'un service d'écho qui utilise un socket de type SCTP bi-univoque.

---

**Remarque** – La procédure suivante permet également d'ajouter des services pour les protocoles de couche transport TCP et UDP.

---

La tâche suivante illustre l'ajout dans le référentiel SMF d'un service inet SCTP géré par le démon `inetd`. La tâche décrit ensuite la procédure d'ajout du service à l'aide des commandes SMF (Service Management Facility).

- Pour plus d'informations sur les commandes SMF, reportez-vous à la section “[Utilitaires d'administration en ligne de commande SMF](#)” du manuel *Administration d'Oracle Solaris : Tâches courantes*.
- Pour plus d'informations sur la syntaxe, consultez les pages de manuel sur les commandes SMF citées dans la procédure.

- Pour plus d'informations sur SMF, reportez-vous à la page de manuel [smf\(5\)](#).

**Avant de commencer**

Avant d'effectuer la procédure suivante, créez un fichier manifeste pour le service. En exemple, la procédure fait référence à un fichier manifeste du service echo intitulé `echo.sctp.xml`.

**1 Connectez-vous au système local avec un compte utilisateur disposant de privilèges d'écriture sur les fichiers système.**

**2 Modifiez le fichier `/etc/services` et ajoutez la définition du nouveau service.**

Définissez le service à l'aide de la syntaxe suivante.

```
service-name |port/protocol | aliases
```

**3 Ajoutez le nouveau service.**

Accédez au répertoire de stockage du manifeste de service et tapez ce qui suit :

```
# cd dir-name
# svccfg import service-manifest-name
```

La page de manuel [svccfg\(1M\)](#) contient la syntaxe complète de `svccfg`.

Admettons que vous voulez ajouter un service echo SCTP à l'aide du manifeste `echo.sctp.xml` résidant dans le répertoire `service.dir`. Vous devez taper ce qui suit :

```
# cd service.dir
# svccfg import echo.sctp.xml
```

**4 Assurez-vous que le manifeste de service a été ajouté :**

```
# svcs FMRI
```

Pour l'argument *FMRI*, utilisez le FMRI (Fault Managed Resource Identifier, identificateur de ressources gérées erronées) du manifeste de service. Par exemple, pour le service SCTP echo, vous devez utiliser la commande suivante :

```
# svcs svc:/network/echo:sctp_stream
```

La sortie doit ressembler à ceci :

```
STATE      STIME      FMRI
disabled   16:17:00   svc:/network/echo:sctp_stream
```

Pour plus d'informations sur la commande `svcs`, reportez-vous à la page de manuel [svcs\(1\)](#).

D'après la sortie, le nouveau manifeste de service est désactivé.

**5 Dressez la liste des propriétés du service afin d'identifier les modifications à apporter.**

```
# inetadm -l FMRI
```



Pour plus d'informations sur la commande `inetadm`, reportez-vous à la page de manuel [inetadm\(1M\)](#).

Par exemple, pour le service SCTP echo, vous devez saisir les informations suivantes :

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE
           name="echo"
           endpoint_type="stream"
           proto="sctp"
           isrpc=FALSE
           wait=FALSE
           exec="/usr/lib/inet/in.echod -s"
           .
           .
           default tcp_trace=FALSE
           default tcp_wrappers=FALSE
```

## 6 Activez le nouveau service :

```
# inetadm -e FMRI
```

## 7 Assurez-vous que le service est activé.

Par exemple, pour le nouveau service echo, vous devez taper :

```
# inetadm | grep sctp_stream
.
.
enabled    online          svc:/network/echo:sctp_stream
```

### Exemple 3–9 Ajout d'un service utilisant le protocole de transport SCTP

L'exemple suivant indique les commandes à utiliser et les entrées de fichier requises pour que le service d'écho utilise le protocole de couche transport SCTP.

```
$ cat /etc/services
.
.
echo          7/tcp
echo          7/udp
echo          7/sctp

# cd service.dir

# svccfg import echo.sctp.xml

# svcs network/echo*
STATE      STIME      FMRI
disabled   15:46:44   svc:/network/echo:dgram
disabled   15:46:44   svc:/network/echo:stream
disabled   16:17:00   svc:/network/echo:sctp_stream

# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE
```

```
        name="echo"
        endpoint_type="stream"
        proto="sctp"
        isrpc=FALSE
        wait=FALSE
        exec="/usr/lib/inet/in.echod -s"
        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

# inetadm -e svc:/network/echo:sctp_stream

# inetadm | grep echo
disabled disabled      svc:/network/echo:stream
disabled disabled      svc:/network/echo:dgram
enabled  online         svc:/network/echo:sctp_stream
```

## ▼ Contrôle d'accès aux services TCP à l'aide des wrappers TCP

Le programme `tcpd` met en oeuvre les *wrappers TCP*. Les wrappers TCP représentent une mesure de sécurité supplémentaire pour les démons de services, notamment pour `ftpd`. En effet, ils s'interposent entre le démon et les requêtes de service entrantes. Les wrappers TCP consignent les réussites et les échecs des tentatives de connexion. En outre, ils offrent un contrôle d'accès en autorisant ou en refusant la connexion en fonction de l'origine de la requête. Enfin, ils permettent de protéger les démons, notamment SSH, Telnet et FTP. L'application `sendmail` peut également utiliser des wrappers TCP, comme décrit dans la section [“Prise en charge des wrappers TCP à partir de la version 8.12 de sendmail”](#) du manuel *Administration d'Oracle Solaris : Services réseau*.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Activez les wrappers TCP.

```
# inetadm -M tcp_wrappers=TRUE
```

- 3 Configurez la stratégie de contrôle d'accès des wrappers TCP, telle que décrite à la page de manuel `hosts_access(3)`.**

Cette page de manuel se trouve dans le répertoire `/usr/sfw/man`.



## Activation d'IPv6 sur le réseau

---

Ce chapitre contient les informations d'activation du protocole IPv6 sur un réseau. Il aborde les principaux thèmes suivants :

- “Configuration d'une interface IPv6” à la page 77
- “Procédure de configuration d'un système pour IPv6” à la page 78
- “Configuration d'un routeur IPv6” à la page 80
- “Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs” à la page 82
- “Configuration des tunnels (liste des tâches)” à la page 126
- “Configuration de prise en charge de services de noms pour IPv6” à la page 89

Pour obtenir différents types d'informations sur IPv6, consultez les ressources suivantes :

- Pour une présentation des concepts d'IPv6 : [Chapitre 3, “Présentation d'IPv6” du manuel \*Guide d'administration système : services IP\*](#)
- Pour les tâches de planification d'IPv6 : [Chapitre 2, “Eléments à prendre en compte lors de l'utilisation d'adresses IPv6”](#)
- Pour la préparation à l'utilisation des tunnels IP : [“Planification de l'utilisation de tunnels dans le réseau” à la page 41](#)
- Pour des informations de référence : [Chapitre 9, “Référence IPv6”](#)

## Configuration d'une interface IPv6

L'étape initiale de l'utilisation d'IPv6 sur un réseau consiste à configurer IPv6 sur l'interface IP du système.

Lors de l'installation d'Oracle Solaris, vous pouvez activer le protocole IPv6 sur une ou plusieurs interfaces d'un système. Si vous activez la prise en charge d'IPv6 pendant l'installation, une fois celle-ci terminée, les fichiers et tables IPv6 suivants sont en place :

- Le service SMF `name-service/switch` a été modifié pour prendre en charge les recherches utilisant les adresses IPv6.

- La table des règles de sélection des adresses IPv6 est créée. Cette table définit l'ordre de priorité des formats d'adresse IP à utiliser pour la transmission des données sur une interface IPv6.

Cette section décrit comment activer IPv6 sur les interfaces une fois l'installation d'Oracle Solaris terminée.

## ▼ Procédure de configuration d'un système pour IPv6

La première étape du processus de configuration IPv6 consiste à activer le protocole sur les interfaces des systèmes à définir en tant que noeuds IPv6. En principe, l'adresse IPv6 de l'interface est définie via le processus de configuration automatique décrit à la section [“Configuration automatique d'adresse IPv6” du manuel \*Guide d'administration système : services IP\*](#). Vous pouvez alors personnaliser la configuration du noeud selon sa fonction au sein du réseau IPv6 (hôte, serveur ou routeur).

---

**Remarque** – Si l'interface est définie sur un lien sur lequel un routeur publie un préfixe IPv6, ce préfixe de site figure dans les adresses configurées automatiquement. Pour plus d'informations, reportez-vous à la section [“Procédure de configuration d'un routeur compatible IPv6” à la page 80](#).

---

La procédure suivante explique comment activer le protocole IPv6 sur une interface ajoutée après l'installation d'Oracle Solaris.

### 1 Configurez l'interface IP en utilisant les commandes appropriées.

Reportez-vous à la section [“Procédure de configuration d'une interface IP” à la page 47](#).

---

**Remarque** – Lorsque vous attribuez l'adresse IP, veillez à utiliser l'option correcte pour attribuer une adresse IPv6 :

```
# ipadm create-addr -T addrconf addrobj
```

Pour ajouter davantage d'adresses, utilisez la syntaxe suivante :

```
# ipadm create-addr -T static ipv6-address addrobj
```

---

### 2 Démarrez le démon IPv6 `in.ndpd`.

```
# /usr/lib/inet/in.ndpd
```

### 3 (Facultatif) Créez une route IPv6 statique par défaut.

```
# /usr/sbin/route -p add -inet6 default ipv6-address
```

- 4 (Facultatif) Créez un fichier `/etc/inet/ndpd.conf` définissant les paramètres des variables d'interface du noeud.

Si vous devez créer des adresses temporaires pour l'interface de l'hôte, reportez-vous à la section [“Utilisation d'adresses temporaires pour une interface”](#) à la page 83. Pour plus d'informations sur `/etc/inet/ndpd.conf`, reportez-vous à la page de manuel `ndpd.conf(4)` et à la section [“Fichier de configuration ndpd.conf”](#) à la page 152.

- 5 (Facultatif) Pour afficher le statut des interfaces IP avec leurs configurations IPv6, saisissez la commande suivante :

```
# ipadm show-addr
```

#### Exemple 4–1 Activation d'une interface IPv6 après l'installation

Cet exemple illustre l'activation du protocole IPv6 sur l'interface `net0`. Avant de commencer, vérifiez l'état de toutes les interfaces configurées sur le système.

```
# ipadm show-addr
ADDROBJ  TYPE    STATE  ADDR
lo0/v4   static  ok     127.0.0.1/8
net0/v4   static  ok     172.16.27.74/24
```

L'interface `net0` est la seule interface actuellement configurée sur le système. Pour activer le protocole IPv6 sur cette interface, effectuez la procédure suivante :

```
# ipadm create-addr -T addrconf net0/v6
# ipadm create-addr -T static -a 2001:db8:3c4d:15:203/64 net0/v6add
# /usr/lib/inet/in.ndpd

# ipadm show-addr
ADDROBJ  TYPE        STATE  ADDR
lo0/v4   static      ok     127.0.0.1/8
net0/v4   static      ok     172.16.27.74/24
net0/v6   addrconf    ok     fe80::203:baff:fe13:14e1/10
lo0/v6   static      ok     ::1/128
net0/v6add static      ok     2001:db8:3c4d:15:203/64

# route -p add -inet6 default fe80::203:baff:fe13:14e1
```

#### Étapes suivantes

- Pour configurer le noeud IPv6 en tant que routeur, reportez-vous à la section [“Configuration d'un routeur IPv6”](#) à la page 80.
- Pour désactiver la configuration automatique sur le noeud, reportez-vous à la section [“Procédure de désactivation de la configuration automatique des adresses IPv6”](#) à la page 80.
- Pour personnaliser un noeud et le définir en tant que serveur, reportez-vous aux suggestions de la section [“Administration d'interfaces compatibles IPv6 sur des serveurs”](#) à la page 88.

## ▼ Procédure de désactivation de la configuration automatique des adresses IPv6

En règle générale, la configuration automatique d'adresse permet de générer les adresses IPv6 pour les interfaces des hôtes et des serveurs. Cependant, la désactivation de la configuration automatique peut s'avérer nécessaire, en particulier pour configurer un jeton manuellement, suivant les explications de la section [“Configuration d'un jeton IPv6”](#) à la page 86.

### 1 Créez un fichier `/etc/inet/ndpd.conf` pour le noeud.

Le fichier `/etc/inet/ndpd.conf` définit les variables d'interface pour le noeud. Pour désactiver la configuration automatique de la totalité des interfaces du serveur, le fichier doit contenir les éléments suivants :

```
if-variable-name StatelessAddrConf false
```

Pour plus d'informations sur `/etc/inet/ndpd.conf`, reportez-vous à la page de manuel [ndpd.conf\(4\)](#), ainsi qu'à la section [“Fichier de configuration ndpd.conf”](#) à la page 152.

### 2 Mettez le démon IPv6 à jour avec vos modifications.

```
# pkill -HUP in.ndpd
```

## Configuration d'un routeur IPv6

Cette section décrit les tâches de configuration d'un routeur IPv6. En fonction des exigences de votre site, il se peut que vous ne deviez effectuer que certaines tâches.

## ▼ Procédure de configuration d'un routeur compatible IPv6

La procédure suivante part du principe que vous avez déjà configuré le système pour IPv6. Pour connaître les procédures, reportez-vous à la section [“Configuration d'une interface IPv6”](#) à la page 77.

### 1 Configurez le transfert de paquets IPv6 sur toutes les interfaces du routeur.

```
# ipadm set-prop -p forwarding=on ipv6
```

### 2 Démarrez le démon de routage.

Le démon `in.ripngd` gère le routage IPv6. Activez le routage IPv6 à l'aide de l'une des méthodes suivantes :

- Utilisez la commande `routeadm` :

```
# routeadm -e ipv6-routing -u
```



- Utilisez la commande SMF adéquate :

```
# svcadm enable ripng:default
```

Pour obtenir des informations sur la syntaxe de la commande `routeadm`, reportez-vous à la page de manuel [routeadm\(1M\)](#).

### 3 Créez le fichier `/etc/inet/ndpd.conf`.

Spécifiez le préfixe de site que doit publier le routeur et les autres informations de configuration dans `/etc/inet/ndpd.conf`. Ce fichier est lu par le démon `in.ndpd`, qui implémente le protocole de détection de voisins IPv6.

Pour obtenir une liste des variables et des valeurs admissibles, reportez-vous à la section “[Fichier de configuration `ndpd.conf`](#)” à la page 152 et à la page de manuel [ndpd.conf\(4\)](#).

### 4 Saisissez le texte suivant dans le fichier `/etc/inet/ndpd.conf` :

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

Ce texte indique au démon `in.ndpd` qu'il doit envoyer les publications de routeur à toutes les interfaces du routeur qui sont configurées pour IPv6.

### 5 Ajoutez du texte supplémentaire au fichier `/etc/inet/ndpd.conf` pour configurer le préfixe de site sur les différentes interfaces du routeur.

Le texte doit posséder le format suivant :

```
prefix global-routing-prefix:subnet ID/64 interface
```

Le fichier d'exemple `/etc/inet/ndpd.conf` suivant configure le routeur de sorte qu'il publie le préfixe de site `2001:0db8:3c4d::/48` sur les interfaces `net0` et `net1`.

```
ifdefault AdvSendAdvertisements true
prefixdefault AdvOnLinkFlag on AdvAutonomousFlag on
```

```
if net0 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:15::0/64 net0
```

```
if net1 AdvSendAdvertisements 1
prefix 2001:0db8:3c4d:16::0/64 net1
```

### 6 Redémarrez le système.

Le routeur IPv6 commence la publication sur la liaison locale de tout préfixe de site dans le fichier `ndpd.conf`.

## Exemple 4–2 Sortie `ipadm show-addr` indiquant les interfaces IPv6

L'exemple suivant illustre la sortie de la commande `ipadm show-addr` telle que vous la recevriez une fois la procédure “[Configuration d'un routeur IPv6](#)” à la page 80 terminée.

ADDROBJ	TYPE	STATE	ADDR
lo0/v4	static	ok	127.0.0.1/8
net0/v4	static	ok	172.16.15.232/24
net1/v4	static	ok	172.16.16.220/24
net0/v6	addrconf	ok	fe80::203:baff:fe11:b115/10
lo0/v6	static	ok	::1/128
net0/v6add	static	ok	2001:db8:3c4d:15:203:baff:fe11:b115/64
net1/v6	addrconf	ok	fe80::203:baff:fe11:b116/10
net1/v6add	static	ok	2001:db8:3c4d:16:203:baff:fe11:b116/64

Dans cet exemple, chaque interface configurée pour IPv6 possède maintenant deux adresses. L'entrée avec le nom d'objet d'adresse comme *interface/v6* indique l'adresse lien-local de l'interface. L'entrée avec le nom d'objet d'adresse comme *interface/v6add* indique une adresse globale IPv6. Cette adresse inclut le préfixe de site que vous avez configuré dans le fichier `/etc/ndpd.conf`, en plus de l'ID d'interface. Notez que la désignation *v6add* est une chaîne définie de façon aléatoire. Vous pouvez définir d'autres chaînes pour constituer la seconde partie du nom d'objet d'adresse, à condition que l'*interface* reflète l'interface sur laquelle vous créez les adresses IPv6, par exemple `net0/myststring`, `net0/ipv6addr` et ainsi de suite.

- Voir aussi**
- Pour configurer des tunnels à partir des routeurs identifiés dans la topologie de réseau IPv6, reportez-vous à la section [“Configuration et administration du tunnel avec la commande `dladm`”](#) à la page 126.
  - Pour obtenir des informations sur la configuration de commutateurs et de hubs sur votre réseau, reportez-vous à la documentation du fabricant.
  - Pour configurer les hôtes IPv6, reportez-vous à la section [“Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs”](#) à la page 82.
  - Pour améliorer la prise en charge d'IPv6 sur les serveurs, reportez-vous à la section [“Administration d'interfaces compatibles IPv6 sur des serveurs”](#) à la page 88.
  - Pour plus d'informations sur les commandes, fichiers et démons IPv6, reportez-vous à la section [“Implémentation IPv6 sous Oracle Solaris”](#) à la page 151.

## Modification de la configuration d'interface IPv6 pour les hôtes et les serveurs

Cette section explique comment modifier la configuration d'interfaces compatibles IPv6 sur les noeuds qui sont des hôtes ou des serveurs. Dans la plupart des cas, il est conseillé d'utiliser la configuration automatique d'adresse pour les interfaces compatibles IPv6, comme expliqué dans la section [“Présentation de la configuration automatique sans état”](#) du manuel *Guide d'administration système : services IP*. Vous pouvez cependant, le cas échéant, modifier l'adresse IPv6 d'une interface comme expliqué dans les tâches décrites dans cette section.

Vous devez effectuer trois tâches générales dans la séquence suivante :

1. Désactivation de la configuration automatique de l'adresse IPv6. Reportez-vous à la section “[Procédure de désactivation de la configuration automatique des adresses IPv6](#)” à la page 80.
2. Créez une adresse temporaire pour un hôte. Reportez-vous à la section “[Procédure de configuration d'une adresse temporaire](#)” à la page 84.
3. Configurez un jeton IPv6 pour l'ID d'interface. Reportez-vous à la section “[Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur](#)” à la page 86.

## Utilisation d'adresses temporaires pour une interface

Une *adresse temporaire* IPv6 contient un numéro de 64 bits généré de manière aléatoire en tant qu'ID d'interface, plutôt que l'adresse MAC d'une interface. Vous pouvez utiliser des adresses temporaires pour toute interface d'un noeud IPv6 dont vous souhaitez préserver l'anonymat. Par exemple, il peut s'avérer utile d'employer des adresses temporaires pour les interfaces d'un hôte devant accéder à des serveurs Web publics. Les adresses temporaires implémentent des améliorations de confidentialité pour IPv6. Ces améliorations sont décrites dans le document RFC 3041, disponible à l'adresse “[Privacy Extensions for Stateless Address Autoconfiguration in IPv6](#)” (<http://www.ietf.org/rfc/rfc3041.txt?number=3041>).

L'activation d'une adresse temporaire s'effectue dans le fichier `/etc/inet/ndpd.conf`, pour une ou plusieurs interfaces, le cas échéant. Cependant, à la différence des adresses IPv6 standard configurées automatiquement, une adresse temporaire se compose d'un préfixe de sous-réseau de 64 bits et d'un numéro de 64 bits généré de façon aléatoire. Ce numéro devient le segment correspondant à l'ID d'interface de l'adresse IPv6. Une adresse lien-local n'est pas générée avec l'adresse temporaire en tant qu'ID d'interface.

Notez que la *durée de vie préférée* par défaut des adresses temporaires est d'un jour. Lors de l'activation de la génération d'adresses temporaires, il est également possible de configurer les variables suivantes dans le fichier `/etc/inet/ndpd.conf` :

<i>Durée de vie valide</i> TmpValidLifetime	Durée d'existence de l'adresse temporaire ; une fois la durée écoulée, l'adresse est supprimée de l'hôte.
<i>Durée de vie préférée</i> TmpPreferredLifetime	Temps écoulé avant que l'adresse temporaire soit désapprouvée. Cette durée doit être inférieure à la durée de vie valide.
<i>Régénération d'adresse</i>	Durée avant l'expiration de la durée de vie préférée, pendant laquelle l'hôte devrait générer une nouvelle adresse temporaire.

La durée des adresses temporaires s'exprime comme suit :

<i>n</i>	<i>n</i> nombre de secondes, valeur par défaut
<i>n h</i>	<i>n</i> nombre d'heures (h)

*n d*                      *n* nombre de jours (d)

## ▼ Procédure de configuration d'une adresse temporaire

### 1 Si nécessaire, activez IPv6 sur les interfaces de l'hôte.

Reportez-vous à la section [“Procédure de configuration d'un système pour IPv6”](#) à la page 78.

### 2 Modifiez le fichier `/etc/inet/ndpd.conf` afin d'activer la génération d'adresses temporaires.

- Pour configurer des adresses temporaires sur les interfaces d'un hôte, ajoutez la ligne suivante au fichier `/etc/inet/ndpd.conf` :

```
ifdefault TmpAddrsEnabled true
```

- Pour configurer une adresse temporaire pour une interface spécifique, ajoutez la ligne suivante au fichier `/etc/inet/ndpd.conf` :

```
if interface TmpAddrsEnabled true
```

### 3 (Facultatif) Spécifiez la durée de vie valide de l'adresse temporaire.

```
ifdefault TmpValidLifetime duration
```

Cette syntaxe spécifie la durée de vie valide de toutes les interfaces d'un hôte. La durée *duration* s'exprime en secondes, en heures ou en jours. La durée de vie valide par défaut est de 7 jours. Vous pouvez également utiliser `TmpValidLifetime` avec des mots-clés d'*interface if* afin de spécifier la durée de vie valide de l'adresse temporaire d'une interface en particulier.

### 4 (Facultatif) Spécifiez une durée de vie préférée pour l'adresse temporaire après laquelle celle-ci est désapprouvée.

```
if interface TmpPreferredLifetime duration
```

Cette syntaxe spécifie la durée de vie préférée de l'adresse temporaire d'une interface donnée. La durée de vie préférée par défaut est d'un jour. Vous pouvez également utiliser `TmpPreferredLifetime` avec le mot-clé `ifdefault` afin de spécifier la durée de vie préférée des adresses temporaires de toutes les interfaces d'un hôte.

---

**Remarque** – La sélection d'adresse par défaut attribue une priorité moindre aux adresses IPv6 désapprouvées. Si une adresse temporaire IPv6 est désapprouvée, la sélection d'adresses par défaut choisit une adresse qui n'a pas été désapprouvées en tant qu'adresse source d'un paquet. Une adresse non désapprouvée peut être l'adresse IPv6 générée automatiquement ou, éventuellement, l'adresse IPv4 de l'interface. Pour plus d'informations sur la sélection d'adresses par défaut, reportez-vous à la section [“Administration de la sélection des adresses par défaut”](#) à la page 114.

---

- 5 (Facultatif) Spécifiez la durée de production en avance de la désapprobation d'adresse, pendant laquelle l'hôte devrait générer une nouvelle adresse temporaire.

```
ifdefault TmpRegenAdvance duration
```

Cette syntaxe spécifie le délai qui doit s'écouler avant la désapprobation d'adresse pour les adresses temporaires de toutes les interfaces d'un hôte. La valeur par défaut est 5 secondes.

- 6 Modifiez la configuration du démon `in.ndpd`.

```
# pkill -HUP in.ndpd
# /usr/lib/inet/in.ndpd
```

- 7 Vérifiez que des adresses temporaires ont bien été créées en exécutant la commande `ipadm show-addr`, comme indiqué dans l'[Exemple 4–4](#).

La sortie de la commande affiche l'indicateur `t` dans le champ `CURRENT` des adresses temporaires.

#### Exemple 4–3 Variables d'adresses temporaires dans le fichier `/etc/inet/ndpd.conf`

L'exemple suivant comporte un segment d'un fichier `/etc/inet/ndpd.conf` avec les adresses temporaires activées pour l'interface du réseau principal.

```
ifdefault TmpAddrsEnabled true
ifdefault TmpValidLifetime 14d
ifdefault TmpPreferredLifetime 7d
ifdefault TmpRegenAdvance 6s
```

#### Exemple 4–4 Sortie de commande `ipadm show-addr` avec adresses temporaires activées

Cet exemple indique la sortie de la commande `ipadm show-addr` une fois les adresses temporaires créées. Notez que seules les informations relatives à IPv6 sont incluses dans l'exemple de sortie.

```
# ipadm show-addr -o all
ADDROBJ  TYPE      STATE  CURRENT  PERSISTENT  ADDR
lo0/v6   static    ok     U----    ---         ::1/128
net0/v6   addrconf  ok     U----    ---         fe80::a00:20ff:feb9:4c54/10
net0/v6a  static    ok     U----    ---         2001:db8:3c4d:15:a00:20ff:feb9:4c54/64
net0/?    addrconf  ok     U--t-    ---         2001:db8:3c4d:15:7c37:e7d1:fc9c:d2cb/64
```

Notez que pour l'objet d'adresse `net0/?`, l'indicateur `t` est défini sous le champ `CURRENT`. L'indicateur informe que l'adresse correspondante est dotée d'un ID d'interface temporaire.

- Voir aussi** ■ Pour définir la prise en charge du service de noms pour les adresses IPv6, reportez-vous à la section “[Configuration de prise en charge de services de noms pour IPv6](#)” à la page 89.

- Pour configurer des adresses IPv6 pour un serveur, reportez-vous à la section “[Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur](#)” à la page 86.
- Pour contrôler les activités sur les noeuds IPv6, reportez-vous au [Chapitre 5](#), “Administration d'un réseau TCP/IP”.

## Configuration d'un jeton IPv6

L'ID d'interface 64 bits d'une adresse IPv6 est également nommé *jeton*, tel que décrit dans la section “[Présentation de l'adressage IPv6](#)” du manuel *Guide d'administration système : services IP*. Lors de la configuration automatique d'adresses, le jeton est associé à l'adresse MAC de l'interface. Dans la plupart des cas, les noeuds qui n'effectuent pas de routage, c'est-à-dire les hôtes et les serveurs IPv6, doivent utiliser leurs jetons configurés automatiquement.

Cependant, l'utilisation de jetons configurés automatiquement peut être problématique pour les serveurs dont les interfaces sont régulièrement dans le cadre de la maintenance système. Lorsque la carte de l'interface est modifiée, l'adresse MAC l'est également. Cela peut entraîner des problèmes pour les serveurs qui dépendent d'adresses IP. Différentes parties de l'infrastructure de réseau, comme le DNS ou le NIS, peuvent disposer d'adresses IPv6 stockées pour les interfaces du serveur.

Pour les problèmes liés aux modifications d'adresses, vous pouvez configurer un jeton manuellement pour l'utiliser en tant qu'ID d'interface dans une adresse IPv6. Pour créer le jeton, spécifiez un numéro hexadécimal de 64 bits maximum afin d'occuper la portion d'ID d'interface de l'adresse IPv6. Par la suite, lors de la configuration automatique d'adresses, le protocole de détection de voisins ne crée pas d'ID d'interface basé sur l'adresse MAC de l'interface. Le jeton créé manuellement devient l'ID d'interface. Ce jeton reste assigné à l'interface, même en cas de remplacement d'une carte.

---

**Remarque** – La différence entre les jetons spécifiés par les utilisateurs et les adresses temporaires réside dans le fait que ces dernières sont générées de façon aléatoire et non pas créées explicitement par un utilisateur.

---

### ▼ Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur

Les instructions suivantes sont particulièrement utiles pour les serveurs dont les interfaces sont régulièrement remplacées. Elles sont également valides pour la configuration de jetons spécifiés par l'utilisateur sur tout noeud IPv6.

- 1 **Vérifiez que l'interface que vous souhaitez configurer avec un jeton existe et qu'aucune adresse IPv6 n'est configurée sur l'interface.**

---

**Remarque** – Assurez-vous que l'interface n'est dotée d'aucune adresse IPv6 configurée.

---

```
# ipadm show-if
IFNAME  CLASS    STATE  ACTIVE  OVER
lo0     loopback  ok     yes     ---
net0    ip        ok     yes     ---

# ipadm show-addr
ADDROBJ  TYPE      STATE  ADDR
lo0/v4   static   ok     127.0.0.1/8
```

Cette sortie indique que l'interface réseau `net0` existe sans adresse IPv6 configurée.

- 2 **Créez un ou plusieurs numéros hexadécimaux de 64 bits à utiliser en tant que jetons pour l'interface du noeud. Pour des exemples de jetons, reportez-vous à la section “Adresse unicast lien-local” du manuel *Guide d'administration système : services IP*.**
- 3 **Configurez chaque interface avec un jeton.**

Utilisez le format suivant de la commande `ipadm` pour chaque interface afin de disposer d'un ID d'interface spécifiée par l'utilisateur (jeton) :

```
# ipadm create-addr -T addrconf -i interface-ID addrobj
```

Par exemple, exécutez la commande suivante afin de configurer l'interface `net0` avec un jeton :

```
# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0/v6add
```

---

**Remarque** – Une fois l'objet d'adresse créé avec le jeton, ce dernier ne peut plus être modifié.

---

- 4 **Mettez le démon IPv6 à jour avec vos modifications.**

```
# kill -HUP in.ndpd
```

#### Exemple 4–5 Configuration d'un jeton spécifié par l'utilisateur sur une interface IPv6

L'exemple suivant représente `net0` en cours de configuration avec une adresse IPv6 et un jeton.

```
# ipadm show-if
IFNAME  CLASS    STATE  ACTIVE  OVER
lo0     loopback  ok     yes     ---
net0    ip        ok     yes     ---

# ipadm show-addr
ADDROBJ  TYPE      STATE  ADDR
lo0/v4   static   ok     127.0.0.1/8

# ipadm create-addr -T addrconf -i ::1a:2b:3c:4d/64 net0/v6
# kill -HUP in.ndpd
```

```
# ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v6        static    ok      ::1/128
net0/v6        addrconf  ok      fe80::1a:2b:3c:4d/10
net0/v6        addrconf  ok      2002:a08:39f0:1:1a:2b:3c:4d/64
```

Une fois le jeton configuré, l'objet d'adresse `net0/v6` dispose à la fois de l'adresse locale du lien ainsi que d'une adresse avec `1a:2b:3c:4d` configurée pour son ID d'interface. Notez qu'après la création de `net0/v6`, ce jeton ne peut plus être modifié pour cette interface.

- Voir aussi**
- Pour la mise à jour des services de noms pour les adresses IPv6 du serveur, reportez-vous à la section [“Configuration de prise en charge de services de noms pour IPv6”](#) à la page 89.
  - Pour contrôler les performances de serveur, reportez-vous au [Chapitre 5, “Administration d'un réseau TCP/IP”](#).

## Administration d'interfaces compatibles IPv6 sur des serveurs

Lors de la planification d'IPv6 sur un serveur, vous devez prendre un certain nombre de décisions relatives à l'activation d'IPv6 sur les interfaces du serveur. Vos décisions affectent la stratégie à utiliser pour la configuration des ID d'interface, également appelés *jetons*, de l'adresse IPv6 d'une interface.

### ▼ Procédure d'activation d'IPv6 sur les interfaces d'un serveur

Cette procédure indique les étapes générales permettant d'activer IPv6 sur les serveurs de votre réseau. Certaines étapes peuvent varier en fonction de la manière dont vous souhaitez implémenter IPv6.

#### 1 Activez IPv6 sur les interfaces IP du serveur.

Pour connaître les procédures, reportez-vous à la section [“Configuration d'une interface IPv6”](#) à la page 77.

#### 2 Assurez-vous qu'un préfixe de sous-réseau IPv6 est configuré sur un routeur situé sur la même liaison que le serveur.

Pour plus d'informations, reportez-vous à la section [“Configuration d'un routeur IPv6”](#) à la page 80.

#### 3 Utilisez la stratégie adéquate pour l'ID des interfaces compatibles IPv6 du serveur.

Par défaut, la configuration automatique d'adresses IPv6 utilise l'adresse MAC d'une interface lors de la création de la partie ID d'interface de l'adresse IPv6. Si l'adresse IPv6 de l'interface est



bien connue, remplacer une interface par une autre peut entraîner des problèmes. L'adresse MAC de la nouvelle interface sera différente. Un nouvel ID d'interface est généré lors de la configuration automatique d'adresses.

- Dans le cas d'une interface compatible IPv6 que vous ne souhaitez pas remplacer, utilisez l'adresse IPv6 configurée automatiquement, comme indiqué dans la section [“Configuration automatique d'adresse IPv6”](#) du manuel *Guide d'administration système : services IP*.
- Dans le cas d'interfaces compatibles IPv6 devant apparaître anonymes hors du réseau local, vous pouvez utiliser un jeton généré de façon aléatoire comme ID d'interface. Pour obtenir des instructions et un exemple, reportez-vous à la section [“Procédure de configuration d'une adresse temporaire”](#) à la page 84.
- Dans le cas d'interfaces compatibles IPv6 que vous pensez échanger régulièrement, créez des jetons pour les ID d'interface. Pour obtenir des instructions et un exemple, reportez-vous à la section [“Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur”](#) à la page 86.

## Configuration de prise en charge de services de noms pour IPv6

Cette section décrit la procédure de configuration des services de noms DNS et NIS pour la prise en charge de services IPv6.

---

**Remarque** – LDAP prend en charge IPv6 sans aucune configuration supplémentaire nécessaire.

---

Pour obtenir des informations détaillées sur l'administration DNS, NIS et LDAP, reportez-vous à la section [Oracle Solaris Administration: Naming and Directory Services](#).

### ▼ Procédure d'ajout d'adresses IPv6 à DNS

- 1 **Modifiez le fichier de zone DNS adéquat en ajoutant les enregistrements AAAA pour chaque noeud compatible IPv6 :**

```
hostname IN AAAA host-address
```

- 2 **Modifiez les fichiers de zone inversée DNS et ajoutez des enregistrements PTR :**

```
hostaddress IN PTR hostname
```

Pour obtenir des informations détaillées sur l'administration de DNS, reportez-vous à la section [Oracle Solaris Administration: Naming and Directory Services](#).

**Exemple 4–6** Fichier de zone inversée DNS

Cet exemple représente une adresse IPv6 dans le fichier de zone inversée.

```
$ORIGIN      ip6.int.  
8.2.5.0.2.1.e.f.f.f.9.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0 \  
      IN      PTR      vallejo.Eng.apex.COM.
```

## ▼ Procédure d'affichage des informations relatives au service de noms IPv6

La commande `nslookup` permet d'afficher des informations relatives au service de noms IPv6.

- 1 **Après vous être connecté à l'aide de votre compte utilisateur, exécutez la commande `nslookup`.**

```
% /usr/sbin/nslookup
```

Le nom et l'adresse par défaut du serveur s'affichent, suivis du crochet d'invite de la commande `nslookup`.

- 2 **Pour obtenir des informations sur un hôte en particulier, saisissez les commandes suivantes à partir du crochet d'invite :**

```
>set q=any  
>hostname
```

- 3 **Saisissez la commande suivante afin d'afficher les enregistrements AAAA :**

```
>set q=AAAA  
hostname
```

- 4 **Quittez la commande `nslookup` en saisissant `exit`.**

**Exemple 4–7** Utilisation de `nslookup` pour l'affichage d'informations IPv6

Cet exemple illustre les résultats de l'exécution de `nslookup` dans un environnement de réseau IPv6.

```
% /usr/sbin/nslookup  
Default Server:  dnsserve.local.com  
Address:  10.10.50.85  
> set q=AAAA  
> host85  
Server:  dnsserve.local.com  
Address:  10.10.50.85  
  
host85.local.com      IPv6 address = 2::9256:a00:fe12:528  
> exit
```

## ▼ Procédure de vérification de la mise à jour correcte des enregistrements PTR DNS IPv6

Dans cette procédure, utilisez la commande `nslookup` afin d'afficher les enregistrements PTR pour le service DNS IPv6.

- 1 Une fois connecté à votre compte utilisateur, exécutez la commande `nslookup`.

```
% /usr/sbin/nslookup
```

Le nom et l'adresse par défaut du serveur s'affichent, suivis du crochet d'invite de la commande `nslookup`.

- 2 Saisissez ce qui suit devant le crochet d'invite afin de visualiser les enregistrements PTR :

```
>set q=PTR
```

- 3 Quittez la commande en saisissant `exit`.

### Exemple 4–8 Utilisation de `nslookup` pour l'affichage d'enregistrements PTR

L'exemple suivant illustre l'affichage d'enregistrements PTR à l'aide de la commande `nslookup`.

```
% /usr/sbin/nslookup
Default Server: space1999.Eng.apex.COM
Address: 192.168.15.78
> set q=PTR
> 8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0.ip6.int

8.2.5.0.2.1.e.f.f.f.0.2.0.0.a.0.6.5.2.9.0.0.0.0.0.0.2.0.0.0.ip6.int name =
vallejo.ipv6.Eng.apex.COM
ip6.int nameserver = space1999.Eng.apex.COM
> exit
```

## ▼ Procédure d'affichage d'informations IPv6 à l'aide de NIS

Dans cette procédure, la commande `ypmatch` permet d'afficher des informations IPv6 par le biais de NIS :

- Une fois connecté à votre compte utilisateur, saisissez ce qui suit afin d'afficher les adresses IPv6 dans NIS :

```
% ypmatch hostname hosts .byname
```

Les informations sur l'hôte *hostname* spécifié s'affichent.



## Administration d'un réseau TCP/IP

---

Ce chapitre présente les tâches permettant d'administrer un réseau TCP/IP. Il aborde les sujets suivants :

- “Principales tâches d'administration TCP/IP (liste des tâches)” à la page 94
- “Contrôle d'interfaces et d'adresses IP” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*
- “Contrôle du statut du réseau à l'aide de la commande `netstat`” à la page 95
- “Test des hôtes distants à l'aide de la commande `ping`” à la page 102
- “Administration et journalisation des affichages de statut du réseau” à la page 103
- “Affichage des informations de routage à l'aide de la commande `tracert`” à la page 106
- “Contrôle du transfert des paquets à l'aide de la commande `snoop`” à la page 107
- “Administration de la sélection des adresses par défaut” à la page 114

---

**Remarque** – Pour en savoir plus sur le contrôle des interfaces réseau, reportez-vous à la section “Contrôle d'interfaces et d'adresses IP” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

---

L'exécution des tâches présentées dans ce chapitre nécessite l'installation d'un réseau TCP/IP opérationnel sur votre site (IPv4 uniquement ou IPv4/IPv6 double pile). Pour plus d'informations sur l'implémentation d'un réseau IPv6, reportez-vous aux chapitres suivants :

- Pour planifier une implémentation IPv6, reportez-vous au [Chapitre 2, “Eléments à prendre en compte lors de l'utilisation d'adresses IPv6”](#).
- Pour configurer un réseau IPv6 et créer un environnement double pile, reportez-vous au [Chapitre 4, “Activation d'IPv6 sur le réseau”](#).

## Principales tâches d'administration TCP/IP (liste des tâches)

Le tableau suivant répertorie les autres tâches permettant de gérer le réseau après la configuration initiale, notamment l'affichage des informations réseau. Le tableau comprend la description des actions de chaque tâche et la section de la documentation actuelle dans laquelle les étapes permettant d'effectuer ces tâches sont décrites en détails.

Tâche	Description	Référence
Affichage des statistiques par protocole.	Contrôlez les performances des protocoles réseau sur un système donné.	<a href="#">“Affichage des statistiques par protocole” à la page 95</a>
Affichage du statut du réseau.	Contrôlez le système en affichant tous les sockets et toutes les entrées de table de routage. La sortie inclut la famille d'adresses inet pour les réseaux IPv4 et la famille d'adresses inet6 pour les réseaux IPv6.	<a href="#">“Affichage du statut des sockets” à la page 98</a>
Affichage du statut des interfaces réseau.	Contrôlez les performances des interfaces réseau, notamment afin de dépanner les transmissions de données.	<a href="#">“Affichage du statut de l'interface réseau” à la page 98</a>
Affichage du statut de transmission des paquets.	Contrôlez le statut des paquets lors de leur transmission sur le réseau câblé.	<a href="#">“Affichage du statut des transmissions de paquets associés à un type d'adresse spécifique” à la page 100</a>
Contrôle de l'affichage des sorties de commandes IPv6.	Contrôle la sortie des commandes ping, netstat et traceroute. Créez un fichier intitulé inet_type. Définissez la variable DEFAULT_IP de ce fichier.	<a href="#">“Contrôle de la sortie d'affichage des commandes IP” à la page 103</a>
Contrôle du trafic réseau.	Affichez tous les paquets IP à l'aide de la commande snoop.	<a href="#">“Contrôle du trafic réseau IPv6” à la page 110</a>
Affichage de toutes les routes connues par les routeurs du réseau.	Affichez toutes les routes à l'aide de la commande traceroute.	<a href="#">“Affichage du suivi de toutes les routes” à la page 106</a>

---

**Remarque** – Pour en savoir plus sur le contrôle des interfaces réseau, reportez-vous à la section [“Contrôle d'interfaces et d'adresses IP”](#) du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*

---

# Contrôle du statut du réseau à l'aide de la commande netstat

La commande `netstat` génère des affichages illustrant le statut du réseau ainsi que les statistiques des protocoles. Vous pouvez afficher le statut des points d'extrémité TCP, SCTP et UDP sous forme de table. Vous pouvez également afficher les informations de table de routage ainsi que les informations d'interface.

La commande `netstat` permet d'afficher différents types d'informations sur le réseau, suivant l'option de ligne de commande sélectionnée. Les affichages obtenus constituent la principale référence pour l'administration du système. L'exemple ci-dessous illustre la syntaxe de base de la commande `netstat` :

```
netstat [-m] [-n] [-s] [-i | -r] [-f famille-adresses]
```

Cette section décrit les options fréquemment utilisées avec la commande `netstat`. Pour obtenir une description détaillée des toutes les options `netstat`, reportez-vous à la page de manuel [netstat\(1M\)](#).

## ▼ Affichage des statistiques par protocole

L'option `-s` de la commande `netstat` permet d'afficher les statistiques des protocoles UDP, TCP, SCTP, ICMP et IP.

---

**Remarque** – Vous pouvez obtenir la sortie de la commande `netstat` à l'aide du compte utilisateur Oracle Solaris.

---

- **Affichez le statut du protocole.**

```
$ netstat -s
```

### Exemple 5–1 Statistiques des protocoles réseau

L'exemple suivant illustre la sortie de la commande `netstat -s`. Certaines parties de la sortie ont été tronquées. La sortie peut signaler les opérations ayant généré des problèmes pour les différents protocoles. Par exemple, les statistiques affichées pour ICMPv4 et ICMPv6 peuvent signaler les opérations ayant généré des erreurs pour le protocole ICMP.

```
RAWIP
    rawipInDatagrams    = 4701    rawipInErrors      = 0
    rawipInCksumErrs    = 0      rawipOutDatagrams  = 4
    rawipOutErrors      = 0

UDP
    udpInDatagrams      = 10091   udpInErrors        = 0
    udpOutDatagrams     = 15772   udpOutErrors       = 0
```

TCP	tcpRtoAlgorithm	=	4	tcpRtoMin	=	400
	tcpRtoMax	=	60000	tcpMaxConn	=	-1
	.					
	tcpListenDrop	=	0	tcpListenDropQ0	=	0
IPv4	tcpHalfOpenDrop	=	0	tcpOutSackRetrans	=	0
	ipForwarding	=	2	ipDefaultTTL	=	255
	ipInReceives	=	300182	ipInHdrErrors	=	0
	ipInAddrErrors	=	0	ipInCksumErrs	=	0
IPv6	.					
	ipsecInFailed	=	0	ipInIPv6	=	0
	ipOutIPv6	=	3	ipOutSwitchIPv6	=	0
	ipv6Forwarding	=	2	ipv6DefaultHopLimit	=	255
ICMPv4	ipv6InReceives	=	13986	ipv6InHdrErrors	=	0
	ipv6InTooBigErrors	=	0	ipv6InNoRoutes	=	0
	.					
	rawipInOverflows	=	0	ipv6InIPv4	=	0
ICMPv6	ipv6OutIPv4	=	0	ipv6OutSwitchIPv4	=	0
	icmpInMsgs	=	43593	icmpInErrors	=	0
	icmpInCksumErrs	=	0	icmpInUnknowns	=	0
	.					
IGMP:	icmpInOverflows	=	0			
	icmp6InMsgs	=	13612	icmp6InErrors	=	0
	icmp6InDestUnreachs	=	0	icmp6InAdminProhibs	=	0
	.					
SCTP	icmp6OutGroupQueries	=	0	icmp6OutGroupResps	=	2
	icmp6OutGroupReds	=	0			
	12287 messages received					
	0 messages received with too few bytes					
SCTP	0 messages received with bad checksum					
	12287 membership queries received					
	sctpRtoAlgorithm	=	vanj			
	sctpRtoMin	=	1000			
SCTP	sctpRtoMax	=	60000			
	sctpRtoInitial	=	3000			
	sctpTimHearBeatProbe	=	2			
	sctpTimHearBeatDrop	=	0			
SCTP	sctpListenDrop	=	0			
	sctpInClosed	=	0			

## ▼ Affichage du statut des protocoles de transport

La commande netstat permet d'afficher le statut des protocoles de transport. Pour plus d'informations, reportez-vous à la page de manuel [netstat\(1M\)](#).



**1 Affichez le statut des protocoles de transport TCP et SCTP sur un système.**

```
$ netstat
```

**2 Affichez le statut d'un protocole de transport donné sur un système.**

```
$ netstat -P transport-protocol
```

La variable *transport-protocol* peut être définie sur les valeurs suivantes : tcp, sctp ou udp.

**Exemple 5-2 Affichage du statut des protocoles de transport TCP et SCTP**

L'exemple ci-dessous illustre la sortie de base de la commande netstat. Les informations contenues dans la sortie se rapportent uniquement à IPv4.

```
$ netstat
```

```
TCP: IPv4
```

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
lhost-1.login	abc.def.local.Sun.COM.980	49640		0	49640	0 ESTABLISHED
lhost-1.login	ghi.jkl.local.Sun.COM.1020	49640		1	49640	0 ESTABLISHED
remhost-1.1014	mno.pqr.remote.Sun.COM.nfsd	49640		0	49640	0 TIME_WAIT

```
SCTP:
```

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	StrsI/O	State
*.echo	0.0.0.0	0	0 102400	0	128/1		LISTEN
*.discard	0.0.0.0	0	0 102400	0	128/1		LISTEN
*.9001	0.0.0.0	0	0 102400	0	128/1		LISTEN

**Exemple 5-3 Affichage du statut d'un protocole de transport donné**

L'exemple ci-dessous illustre le résultat obtenu suite à l'exécution de la commande netstat avec l'option -P.

```
$ netstat -P tcp
```

```
TCP: IPv4
```

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
lhost-1.login	abc.def.local.Sun.COM.980	49640		0	49640	0 ESTABLISHED
lhost.login	ghi.jkl.local.Sun.COM.1020	49640		1	49640	0 ESTABLISHED
remhost.1014	mno.pqr.remote.Sun.COM.nfsd	49640		0	49640	0 TIME_WAIT

```
TCP: IPv6
```

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
localhost.38983	localhost.32777	49152	0	49152	0	ESTABLISHED	
localhost.32777	localhost.38983	49152	0	49152	0	ESTABLISHED	
localhost.38986	localhost.38980	49152	0	49152	0	ESTABLISHED	

## ▼ Affichage du statut de l'interface réseau

L'option `i` de la commande `netstat` illustre le statut des interfaces réseau configurées sur le système local. Cette option permet de déterminer le nombre de paquets transmis et reçus sur un système sur les différents réseaux.

- **Affichez le statut des interfaces sur le réseau.**

\$ `netstat -i`

### Exemple 5-4 Affichage du statut d'interface réseau

L'exemple suivant illustre le statut du flux de paquets IPv4 et IPv6 sur les interfaces de l'hôte.

Par exemple, le nombre de paquets entrants (`Ipkts`) affiché pour un serveur peut augmenter à chaque tentative de démarrage d'un client alors que le nombre de paquets sortants (`Opkts`) reste inchangé. Ce résultat suggère que le serveur détecte les paquets de requête de démarrage envoyés par le client, mais qu'il ne parvient pas à formuler la réponse appropriée. Cette confusion peut être causée par une adresse incorrecte dans la base de données `hosts` ou `ethers`.

En revanche, si le nombre de paquets entrants reste inchangé sur la durée, l'ordinateur ne détecte même pas l'envoi des paquets. Ce résultat suggère un autre type d'erreur, vraisemblablement lié à un problème d'ordre matériel.

Name	Mtu	Net/Dest	Address	Ipkts	Ierrs	Opkts	Oerrs	Collis	Queue
lo0	8232	loopback	localhost	142	0	142	0	0	0
net0	1500	host58	host58	1106302	0	52419	0	0	0

Name	Mtu	Net/Dest	Address	Ipkts	Ierrs	Opkts	Oerrs	Collis
lo0	8252	localhost	localhost	142	0	142	0	0
net0	1500	fe80::a00:20ff:feb9:4c54/10	fe80::a00:20ff:feb9:4c54	1106305	0	52422	0	0

## ▼ Affichage du statut des sockets

L'option `-a` de la commande `netstat` permet d'afficher le statut des sockets sur l'hôte local.

- **Pour afficher le statut des sockets et des entrées de table de routage, saisissez la commande suivante :**

L'exécution de cette option de la commande `netstat` peut s'effectuer à l'aide du compte utilisateur.

% `netstat -a`

### Exemple 5-5 Affichage de l'ensemble des sockets et des entrées de table de routage

La sortie de la commande `netstat -a` contient de nombreuses statistiques. L'exemple ci-dessous illustre certaines parties d'une sortie classique de la commande `netstat -a`.

## UDP: IPv4

Local Address	Remote Address	State
*.bootpc		Idle
host85.bootpc		Idle
*.*		Unbound
*.*		Unbound
*.sunrpc		Idle
*.*		Unbound
*.32771		Idle
*.sunrpc		Idle
*.*		Unbound
*.32775		Idle
*.time		Idle
.		
.		
*.daytime		Idle
*.echo		Idle
*.discard		Idle

## UDP: IPv6

Local Address	Remote Address	State	If
*.*		Unbound	
*.*		Unbound	
*.sunrpc		Idle	
*.*		Unbound	
*.32771		Idle	
*.32778		Idle	
*.syslog		Idle	
.			
.			

## TCP: IPv4

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
*.*	*.*	0	0	49152	0	IDLE
localhost.4999	*.*	0	0	49152	0	LISTEN
*.sunrpc	*.*	0	0	49152	0	LISTEN
*.*	*.*	0	0	49152	0	IDLE
*.sunrpc	*.*	0	0	49152	0	LISTEN
.						
*.printer	*.*	0	0	49152	0	LISTEN
*.time	*.*	0	0	49152	0	LISTEN
*.daytime	*.*	0	0	49152	0	LISTEN
*.echo	*.*	0	0	49152	0	LISTEN
*.discard	*.*	0	0	49152	0	LISTEN
*.chargen	*.*	0	0	49152	0	LISTEN
*.shell	*.*	0	0	49152	0	LISTEN
*.shell	*.*	0	0	49152	0	LISTEN
*.kshell	*.*	0	0	49152	0	LISTEN
*.login						
.						
.						
*.*	0	0	49152	0	LISTEN	

## \*TCP: IPv6

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
*.*	*.*	0	0	49152	0	IDLE	

*.sunrpc	*.*	0	0	49152	0	LISTEN
*.*	*.*	0	0	49152	0	IDLE
*.32774	*.*	0	0	49152		

## ▼ Affichage du statut des transmissions de paquets associés à un type d'adresse spécifique

L'option -f de la commande netstat permet d'afficher les statistiques relatives aux transmissions de paquets associées à une famille d'adresses donnée.

- Affichez les statistiques relatives aux transmissions de paquets IPv4 ou IPv6.

\$ netstat -f inet | inet6

Pour afficher les informations relatives aux transmissions IPv4, définissez l'argument inet pour la commande netstat -f. Pour afficher les informations relatives aux transmissions IPv6, définissez l'argument inet6 pour la commande netstat -f.

### Exemple 5-6 Statut de transmission de paquets IPv4

L'exemple suivant illustre la sortie de la commande netstat -f inet.

TCP: IPv4						
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
host58.734	host19.nfsd	49640	0	49640	0	ESTABLISHED
host58.38063	host19.32782	49640	0	49640	0	CLOSE_WAIT
host58.38146	host41.43601	49640	0	49640	0	ESTABLISHED
host58.996	remote-host.login	49640	0	49206	0	ESTABLISHED

### Exemple 5-7 Statut de transmission de paquets IPv6

L'exemple suivant illustre la sortie de la commande netstat -f inet6.

TCP: IPv6							
Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State	If
localhost.38065	localhost.32792	49152	0	49152	0	ESTABLISHED	
localhost.32792	localhost.38065	49152	0	49152	0	ESTABLISHED	
localhost.38089	localhost.38057	49152	0	49152	0	ESTABLISHED	

## ▼ Affichage du statut des routes connues

L'option -r de la commande netstat permet d'afficher la table de routage de l'hôte local. Cette table représente le statut de toutes les routes connues de l'hôte. L'exécution de cette option de la commande netstat peut s'effectuer à l'aide du compte utilisateur.

● Affichez la table de routage IP.

```
$ netstat -r
```

Exemple 5–8 Sortie de table de routage obtenue à l'aide de la commande netstat

L'exemple suivant illustre la sortie de la commande netstat -r.

Routing Table: IPv4						
Destination	Gateway	Flags	Ref	Use	Interface	
host15	myhost	U	1	31059	net0	
10.0.0.14	myhost	U	1	0	net0	
default	distantrouter	UG	1	2	net0	
localhost	localhost	UH	42019361		lo0	

Routing Table: IPv6							
Destination/Mask	Gateway	Flags	Ref	Use	If		
2002:0a00:3010:2::/64	2002:0a00:3010:2:1b2b:3c4c:5e6e:abcd	U	1	0	net0:1		
fe80::/10	fe80::1a2b:3c4d:5e6f:12a2	U	1	23	net0		
ff00::/8	fe80::1a2b:3c4d:5e6f:12a2	U	1	0	net0		
default	fe80::1a2b:3c4d:5e6f:12a2	UG	1	0	net0		
localhost	localhost	UH	9	21832	lo0		

Le tableau suivant décrit les différents paramètres de la sortie à l'écran de la commande netstat -r.

Paramètre	Description
Destination	Spécifie l'hôte correspondant au point d'extrémité de destination de la route. Dans la table de routage IPv6, le point d'extrémité de destination est représenté par un préfixe de point d'extrémité de tunnel 6to4 (2002:0a00:3010:2::/64).
Destination/Mask	
Gateway	Spécifie la passerelle de transmission des paquets.
Flags	Indique le statut actuel de la route. L'indicateur U signifie que la route fonctionne. L'indicateur G signifie que la route mène à une passerelle.
Use	Affiche le nombre de paquets envoyés.
Interface	Indique l'interface de l'hôte local correspondant au point d'extrémité source de la transmission.

## Test des hôtes distants à l'aide de la commande ping

La commande `ping` permet de déterminer le statut d'un hôte distant. Lors de l'exécution de la commande `ping`, le protocole ICMP envoie un datagramme à l'hôte spécifié et attend la réponse. Le protocole ICMP permet de gérer les erreurs se produisant sur les réseaux TCP/IP. L'exécution de la commande `ping` permet de déterminer l'existence d'une connexion IP pour l'hôte distant spécifié.

L'exemple suivant illustre la syntaxe de base de la commande `ping` :

```
/usr/sbin/ping hôte [délai]
```

Dans cette syntaxe, la variable *hôte* correspond au nom de l'hôte distant. L'argument *délai* indique la durée en secondes pendant laquelle la commande `ping` tente de contacter l'hôte distant. La valeur par défaut est de 20 secondes. Pour plus d'informations sur la syntaxe et les options de la commande, reportez-vous à la page de manuel [ping\(1M\)](#)

### ▼ Vérification de l'exécution d'un hôte distant

- Tapez la commande `ping` suivante :

```
$ ping hostname
```

Si l'hôte *hostname* accepte les transmissions ICMP, le message suivant s'affiche :

```
hostname is alive
```

Ce message indique que *hostname* a répondu à la requête ICMP. En revanche, si *hostname* ne fonctionne pas ou ne reçoit pas les paquets ICMP, la commande `ping` génère la réponse suivante :

```
no answer from hostname
```

### ▼ Détection de l'abandon de paquets sur un hôte

L'option `-s` de la commande `ping` permet de vérifier qu'un hôte distant est en cours d'exécution et de détecter toute perte de paquet sur cet hôte.

- Tapez la commande `ping` suivante :

```
$ ping -s hostname
```

#### Exemple 5-9 Sortie de la commande ping permettant la détection de l'abandon de paquet

La commande `ping -s hostname` envoie des paquets en continu à l'hôte spécifié pendant un laps de temps donné ou jusqu'à l'envoi d'un caractère d'interruption. Les réponses affichées sont comparables à celles de l'écran suivant :

```
& ping -s host1.domain8
PING host1.domain8 : 56 data bytes
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=0. time=1.67 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=1. time=1.02 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=2. time=0.986 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=3. time=0.921 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=4. time=1.16 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.00 ms
64 bytes from host1.domain8.COM (172.16.83.64): icmp_seq=5. time=1.980 ms

^C

----host1.domain8 PING Statistics----
7 packets transmitted, 7 packets received, 0% packet loss
round-trip (ms)  min/avg/max/stddev = 0.921/1.11/1.67/0.26
```

Les statistiques de perte de paquets indiquent si l'hôte a perdu des paquets. En cas d'échec de la commande ping, vérifiez le statut du réseau reporté par les commandes `ipadm` et `netstat`. Reportez-vous aux sections “[Contrôle d'interfaces et d'adresses IP](#)” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau* et “[Contrôle du statut du réseau à l'aide de la commande netstat](#)” à la page 95.

## Administration et journalisation des affichages de statut du réseau

Les tâches suivantes illustrent les procédures de vérification du statut du réseau à l'aide de commandes de réseau standard.

### ▼ Contrôle de la sortie d'affichage des commandes IP

Vous pouvez contrôler la sortie de la commande `netstat` pour afficher uniquement les informations IPv4, ou les informations IPv4 et IPv6.

#### 1 Créez le fichier `/etc/default/inet_type`.

#### 2 Ajoutez l'une des entrées suivantes au fichier `/etc/default/inet_type` :

- Pour afficher uniquement les informations IPv4 :

```
DEFAULT_IP=IP_VERSION4
```

- Pour afficher les informations IPv4 et IPv6 :

```
DEFAULT_IP=BOTH
```

Ou

```
DEFAULT_IP=IP_VERSION6
```

Pour plus d'informations sur le fichier `inet_type`, reportez-vous à la page de manuel [inet\\_type\(4\)](#).

---

**Remarque** – L'indicateur -f dans la commande `netstat` remplace les valeurs dans le fichier `inet_type`.

---

**Exemple 5–10**    Contrôle de la sortie pour la sélection des informations IPv4 et IPv6

- Si vous spécifiez la variable `DEFAULT_IP=BOTH` ou la variable `DEFAULT_IP=IP_VERSION6` dans le fichier `inet_type`, la sortie suivante s'affiche :

```
% ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v4       static    ok     127.0.0.1/8
net0/v4       static    ok     10.46.86.54/24
lo0/v6       static    ok     ::1/128
net0/v6       addrconf  ok     fe80::a00:fe73:56a8/10
net0/v6add    static    ok     2001:db8:3c4d:5:a00:fe73:56a8/64
```

- Si vous spécifiez la variable `DEFAULT_IP=IP_VERSION4` dans le fichier `inet_type`, la sortie suivante s'affiche :

```
% ipadm show-addr
ADDROBJ      TYPE      STATE  ADDR
lo0/v4       static    ok     127.0.0.1/8
net0/v4       static    ok     10.46.86.54/24
```

## ▼ Journalisation des actions du démon de routage IPv4

Si vous pensez que le démon de routage IPv4 `routed` ne fonctionne pas correctement, vous pouvez créer un journal permettant d'effectuer le suivi de l'activité correspondante. Le journal inclut tous les transferts de paquets à compter du démarrage du démon `routed`.

- **Créez un fichier journal permettant d'effectuer le suivi des opérations du démon :**

```
# /usr/sbin/in.routed /var/log-file-name
```



---

**Attention** – Sur les réseaux à forte activité, la sortie de cette commande peut être générée sur une base quasi continue.

---

**Exemple 5–11**    Journal réseau du démon `in.routed`

L'exemple suivant illustre le début du journal créé à l'aide de la procédure [“Journalisation des actions du démon de routage IPv4”](#) à la page 104.

```
-- 2003/11/18 16:47:00.000000 --
Tracing actions started
RCVBUF=61440
Add interface lo0 #1 127.0.0.1 -->127.0.0.1/32
<UP|LOOPBACK|RUNNING|MULTICAST|IPv4> <PASSIVE>
```



```
Add interface net0 #2 10.10.48.112 -->10.10.48.0/25
    <UP|BROADCAST|RUNNING|MULTICAST|IPv4>
turn on RIP
Add 10.0.0.0 -->10.10.48.112 metric=0 net0 <NET_SYN>
Add 10.10.48.85/25 -->10.10.48.112 metric=0 net0 <IF|NOPROP>
```

## ▼ Suivi des activités du démon de détection des voisins IPv6

Si vous pensez que le démon IPv6 `in.ndpd` ne fonctionne pas correctement, vous pouvez générer le suivi de l'activité correspondante. Le suivi s'affiche sur la sortie standard jusqu'à l'arrêt du processus. Il inclut tous les transferts de paquets à compter du démarrage du démon `in.ndpd`.

- 1 **Générez le suivi du démon `in.ndpd`.**  
# `/usr/lib/inet/in.ndpd -t`
- 2 **Pour arrêter le processus de suivi, appuyez sur les touches Ctrl-C.**

### Exemple 5–12 Suivi de l'activité du démon `in.ndpd`

La sortie suivante illustre le début du suivi du démon `in.ndpd`.

```
# /usr/lib/inet/in.ndpd -t
Nov 18 17:27:28 Sending solicitation to ff02::2 (16 bytes) on net0
Nov 18 17:27:28 Source LLA: len 6 <08:00:20:b9:4c:54>
Nov 18 17:27:28 Received valid advert from fe80::a00:20ff:fee9:2d27 (88 bytes) on net0
Nov 18 17:27:28 Max hop limit: 0
Nov 18 17:27:28 Managed address configuration: Not set
Nov 18 17:27:28 Other configuration flag: Not set
Nov 18 17:27:28 Router lifetime: 1800
Nov 18 17:27:28 Reachable timer: 0
Nov 18 17:27:28 Reachable retrans timer: 0
Nov 18 17:27:28 Source LLA: len 6 <08:00:20:e9:2d:27>
Nov 18 17:27:28 Prefix: 2001:08db:3c4d:1::/64
Nov 18 17:27:28 On link flag:Set
Nov 18 17:27:28 Auto addrconf flag:Set
Nov 18 17:27:28 Valid time: 2592000
Nov 18 17:27:28 Preferred time: 604800
Nov 18 17:27:28 Prefix: 2002:0a00:3010:2::/64
Nov 18 17:27:28 On link flag:Set
Nov 18 17:27:28 Auto addrconf flag:Set
Nov 18 17:27:28 Valid time: 2592000
Nov 18 17:27:28 Preferred time: 604800
```

## Affichage des informations de routage à l'aide de la commande `traceroute`

La commande `traceroute` permet d'obtenir le suivi de la route empruntée par un paquet IP pour accéder à un système distant. Pour plus d'informations sur la commande `traceroute`, reportez-vous à la page de manuel [traceroute\(1M\)](#).

La commande `traceroute` permet de détecter les erreurs de configuration de routage et les échecs de chemin de routage. Si un hôte est inaccessible, la commande `traceroute` permet d'afficher le chemin suivi par les paquets afin de détecter les emplacements susceptibles d'être à l'origine de l'échec.

La commande `traceroute` affiche également le délai d'aller-retour de chaque passerelle sur le chemin d'accès à l'hôte cible. Ces informations permettent notamment de déterminer l'emplacement des ralentissements de trafic entre les deux hôtes.

### ▼ Détermination de la route menant à un hôte distant

- Pour déterminer la route menant à un hôte distant, exécutez la commande suivante :

```
% traceroute destination-hostname
```

L'exécution de cette forme de la commande `traceroute` peut s'effectuer à l'aide du compte utilisateur.

#### Exemple 5–13 Affichage de la route menant à un hôte distant à l'aide de la commande `traceroute`

La sortie suivante de la commande `traceroute` affiche le chemin à sept sauts suivi par les paquets pour circuler du système local `nearhost` vers le système distant `farhost`. La sortie illustre également le temps nécessaire à un paquet pour traverser les différents sauts.

```
istanbul% traceroute farhost.faraway.com
traceroute to farhost.faraway.com (172.16.64.39), 30 hops max, 40 byte packets
 1 frbldg7c-86 (172.16.86.1)  1.516 ms  1.283 ms  1.362 ms
 2 bldg1a-001 (172.16.1.211)  2.277 ms  1.773 ms  2.186 ms
 3 bldg4-bldg1 (172.16.4.42)  1.978 ms  1.986 ms  13.996 ms
 4 bldg6-bldg4 (172.16.4.49)  2.655 ms  3.042 ms  2.344 ms
 5 ferbldg11a-001 (172.16.1.236)  2.636 ms  3.432 ms  3.830 ms
 6 frbldg12b-153 (172.16.153.72)  3.452 ms  3.146 ms  2.962 ms
 7 sanfrancisco (172.16.64.39)  3.430 ms  3.312 ms  3.451 ms
```

### ▼ Affichage du suivi de toutes les routes

Cette procédure permet d'afficher le suivi de toutes les routes à l'aide de l'option `-a` de la commande `traceroute`.

- **Exécutez la commande suivante sur le système local :**

```
% traceroute -ahost-name
```

L'exécution de cette forme de la commande `traceroute` peut s'effectuer à l'aide du compte utilisateur.

### Exemple 5-14 Affichage du suivi de toutes les routes menant à un hôte double pile

L'exemple ci-dessous illustre toutes les routes possibles pour accéder à un hôte double pile.

```
% traceroute -a v6host.remote.com
traceroute: Warning: Multiple interfaces found; using 2::56:a0:a8 @ eri0:2
traceroute to v6host (2001:db8:4a3b::102:a00:fe79:19b0), 30 hops max, 60 byte packets
 1 v6-rout86 (2001:db8:4a3b:56:a00:fe1f:59a1) 35.534 ms 56.998 ms *
 2 2001:db8::255:0:c0a8:717 32.659 ms 39.444 ms *
 3 farhost.faraway.COM (2001:db8:4a3b::103:a00:fe9a:ce7b) 401.518 ms 7.143 ms *
 4 distant.remote.com (2001:db8:4a3b::100:a00:fe7c:cf35) 113.034 ms 7.949 ms *
 5 v6host (2001:db8:4a3b::102:a00:fe79:19b0) 66.111 ms * 36.965 ms

traceroute to v6host.remote.com (192.168.10.75), 30 hops max, 40 byte packets
 1 v6-rout86 (172.16.86.1) 4.360 ms 3.452 ms 3.479 ms
 2 flrmpj17u.here.COM (172.16.17.131) 4.062 ms 3.848 ms 3.505 ms
 3 farhost.farway.com (10.0.0.23) 4.773 ms * 4.294 ms
 4 distant.remote.com (192.168.10.104) 5.128 ms 5.362 ms *
 5 v6host (192.168.15.85) 7.298 ms 5.444 ms *
```

## Contrôle du transfert des paquets à l'aide de la commande snoop

La commande `snoop` permet de contrôler le statut des transferts de données. La commande `snoop` permet de capturer les paquets réseau et d'afficher leur contenu au format spécifié. Les paquets peuvent être affichés dès leur réception ou dès l'enregistrement dans un fichier. L'écriture des données dans un fichier intermédiaire par la commande `snoop` permet de réduire la probabilité de perte de paquet liée à l'activité de suivi. Le fichier est alors également interprété par la commande `snoop`.

Pour capturer des paquets en provenance et à destination de l'interface par défaut en mode promiscuité, vous devez vous connecter en tant qu'administrateur réseau ou superutilisateur. Dans sa forme contractée, la commande `snoop` affiche uniquement les données en rapport avec le protocole principal. Par exemple, un paquet NFS affiche uniquement les informations NFS. Les informations RPC, UDP, IP et Ethernet sont supprimées, mais vous pouvez y accéder en sélectionnant l'une des options détaillées de la commande.

L'exécution répétée à intervalles fréquents de la commande `snoop` permet d'identifier les comportements normaux du système. Pour obtenir de l'aide sur l'analyse des paquets, consultez les livres blancs et documents RFC récents et demandez conseil aux experts dans les domaines

concernés (par exemple, NFS ou NIS). Pour plus d'informations sur l'utilisation de la commande snoop et des options associées, reportez-vous à la page de manuel [snoop\(1M\)](#)

## ▼ Vérification des paquets en provenance de toutes les interfaces

- 1 Imprimez les informations sur les interfaces connectées au système.

```
# ipadm show-if
```

La commande snoop utilise normalement le premier périphérique non-loopback (en principe, l'interface réseau principale).

- 2 Commencez la capture des paquets en exécutant la commande snoop sans argument, comme illustré dans l'[Exemple 5-15](#).
- 3 Pour arrêter le processus, appuyez sur les touches Ctrl-C.

### Exemple 5-15 Sortie de la commande snoop

La commande snoop standard renvoie une sortie comparable à l'écran suivant (pour un hôte double pile).

```
% snoop
Using device /dev/net (promiscuous mode)
router5.local.com -> router5.local.com ARP R 10.0.0.13, router5.local.com is
0:10:7b:31:37:80
router5.local.com -> BROADCAST      TFTP Read "network-config" (octet)
myhost -> DNSserver.local.com      DNS C 192.168.10.10.in-addr.arpa. Internet PTR ?
DNSserver.local.com myhost        DNS R 192.168.10.10.in-addr.arpa. Internet PTR
niserve2.
.
.
.
fe80::a00:20ff:febb:e09 -> ff02::9 RIPng R (5 destinations)
```

Les paquets capturés dans cette sortie comprennent une section de connexion à distance, qui contient des requêtes vers les serveurs NIS et DNS pour la résolution d'adresse. Ils comprennent également des paquets ARP périodiques en provenance du routeur local et des publications de l'adresse IPv6 lien-local sur in.ripngd.

## ▼ Capture de la sortie de la commande snoop dans un fichier

### 1 Capturez une session de commande snoop dans un fichier.

```
# snoop -o filename
```

Exemple :

```
# snoop -o /tmp/cap
Using device /dev/eri (promiscuous mode)
30 snoop: 30 packets captured
```

Dans cet exemple, 30 paquets sont capturés dans le fichier /tmp/cap. Ce fichier peut se trouver dans tout répertoire contenant suffisamment d'espace disque. Le nombre de paquets capturés s'affiche sur la ligne de commande. Vous pouvez dès lors appuyez sur les touches Ctrl-C à tout moment pour arrêter le processus.

La commande snoop génère une charge réseau conséquente, ce qui risque de fausser légèrement les résultats. Pour garantir la précision des résultats, exécutez la commande snoop à partir d'un système tiers.

### 2 Consultez le fichier de capture de sortie de la commande snoop.

```
# snoop -i filename
```

#### Exemple 5-16 Contenu du fichier de capture de sortie de la commande snoop

La sortie suivante illustre diverses captures susceptibles d'être obtenues suite à l'exécution de la commande snoop -i.

```
# snoop -i /tmp/cap
1  0.00000 fe80::a00:20ff:fee9:2d27 -> fe80::a00:20ff:fe8d:4375
    ICMPv6 Neighbor advertisement
...
10 0.91493 10.0.0.40 -> (broadcast) ARP C Who is 10.0.0.40, 10.0.0.40 ?
34 0.43690 nearserver.here.com -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28,
    ID=47453, TO =0x0, TTL=1
35 0.00034 10.0.0.40 -> 224.0.1.1 IP D=224.0.1.1 S=10.0.0.40 LEN=28, ID=57376,
    TOS=0x0, TTL=47
```

## ▼ Vérification des paquets transmis entre un client et un serveur IPv4

### 1 Définissez un système snoop à partir d'un hub connecté soit au serveur soit au client.

Le système tiers (système snoop) vérifie tous les types de trafic entre les deux ordinateurs. Le suivi obtenu grâce à la commande snoop reflète donc le transfert réel de données.

- 2 Exécutez la commande **snoop** associée aux options appropriées, puis enregistrez la sortie dans un fichier.
- 3 Consultez et interprétez la sortie.  
Reportez-vous au document [RFC 1761, Snoop Version 2 Packet Capture File Format](http://www.ietf.org/rfc/rfc1761.txt?number=1761) (<http://www.ietf.org/rfc/rfc1761.txt?number=1761>) pour plus d'informations sur le fichier de capture snoop.

## ▼ Contrôle du trafic réseau IPv6

La commande snoop permet d'afficher les paquets IPv6 uniquement.

- Capturez les paquets IPv6.

```
# snoop ip6
```

Pour plus d'informations sur la commande snoop, reportez-vous à la page de manuel [snoop\(1M\)](#).

### Exemple 5–17 Affichage du trafic réseau IPv6 uniquement

L'exemple suivant illustre la sortie standard susceptible d'être obtenue suite à l'exécution de la commande snoop ip6 sur un noeud.

```
# snoop ip6
fe80::a00:20ff:fe9:2d27 -> ff02::1:ffe9:2d27 ICMPv6 Neighbor solicitation
fe80::a00:20ff:fe9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fe9:2d27 -> fe80::a00:20ff:fe9:2d27 ICMPv6 Neighbor
solicitation
fe80::a00:20ff:fe9:2d27 -> ff02::9 RIPng R (11 destinations)
fe80::a00:20ff:fe9:2d27 -> ff02::1:ffcd:4375 ICMPv6 Neighbor solicitation
```

## Contrôle des paquets à l'aide de périphériques de couche IP

Les périphériques de couche IP ont été introduits dans Oracle Solaris pour améliorer l'observabilité. Ces périphériques donnent accès à tous les paquets avec les adresses associées à l'interface réseau du système. Ces adresses incluent des adresses locales ainsi que des adresses hébergées sur des interfaces sans loopback ou des interfaces logiques. Le trafic observable peut correspondre aux adresses IPv4 et IPv6. Par conséquent, vous pouvez surveiller l'ensemble du trafic destiné au système. Le trafic peut être du trafic d'IP avec loopback, des paquets provenant de machines distantes, des paquets envoyés à partir du système ou la totalité du trafic transféré.

Les périphériques de couche IP permettent à l'administrateur d'une zone globale de surveiller le trafic entre les zones ainsi qu'au sein d'une zone. L'administrateur d'une zone non globale peut également observer le trafic envoyé et reçu par cette zone.

Pour surveiller le trafic sur la couche IP, une nouvelle option, `-I`, est ajoutée à la commande `snoop`. Cette option indique à la commande d'utiliser les nouveaux périphériques de couche IP plutôt que le périphérique sous-jacent de couche liaison pour afficher les données de trafic.

---

**Remarque** – Pour comprendre les distinctions entre les différentes couches, reportez-vous à la section [“Encapsulation de données et pile de protocoles TCP/IP”](#) du manuel *Guide d'administration système : services IP*.

---

## ▼ Vérification des paquets sur la couche IP

- 1 Si nécessaire, imprimez les informations sur les interfaces connectées au système.

```
# ipadm show-if
```

- 2 Capturez le trafic IP sur une interface spécifique.

```
# snoop -I interface [-V | -v]
```

## Exemples de vérification des paquets

Tous les exemples sont basés sur la configuration système suivante :

```
# ipadm show-addr
ADDROBJ    TYPE      STATE   ADDR
lo0/v4      static    ok      127.0.0.1/8
net0/v4      static    ok      192.68.25.5/24
lo0/?       static    ok      127.0.0.1/8
net0/?       static    ok      172.0.0.3/24
net0/?       static    ok      172.0.0.1/24
lo0/?       static    ok      127.0.0.1/8
```

Supposons que deux zones, `sandbox` et `toybox`, utilisent les adresses IP suivantes :

- `sandbox` – 172.0.0.3
- `toybox` – 172.0.0.1

Vous pouvez exécuter la commande `snoop -I` sur les différentes interfaces du système. L'affichage des informations du paquet dépend de si vous êtes administrateur de la zone globale ou de la zone non globale.

**EXEMPLE 5-18** Trafic sur l'interface loopback

```
# snoop -I lo0
Using device ipnet/lo0 (promiscuous mode)
localhost -> localhost    ICMP Echo request (ID: 5550 Sequence number: 0)
```

**EXEMPLE 5-18** Trafic sur l'interface loopback (Suite)

```
localhost -> localhost    ICMP Echo reply (ID: 5550 Sequence number: 0)
```

Pour générer une sortie détaillée, utilisez l'option -v.

```
# snoop -v -I lo0
Using device ipnet/lo0 (promiscuous mode)
IPNET:  ----- IPNET Header -----
IPNET:
IPNET:  Packet 1 arrived at 10:40:33.68506
IPNET:  Packet size = 108 bytes
IPNET:  dli_version = 1
IPNET:  dli_type = 4
IPNET:  dli_srczone = 0
IPNET:  dli_dstzone = 0
IPNET:
IP:  ----- IP Header -----
IP:
IP:  Version = 4
IP:  Header length = 20 bytes
...
```

La prise en charge de l'observation des paquets sur la couche IP introduit un nouvel en-tête ipnet qui précède les paquets observés. Les ID de source et de destination sont tous deux indiqués. L'ID '0' indique que le trafic est généré à partir de la zone globale.

**EXEMPLE 5-19** Flux de paquets du périphérique net0 dans les zones locales

```
# snoop -I net0
Using device ipnet/net0 (promiscuous mode)
toybox -> sandbox TCP D=22 S=62117 Syn Seq=195630514 Len=0 Win=49152 Options=<mss
sandbox -> toybox TCP D=62117 S=22 Syn Ack=195630515 Seq=195794440 Len=0 Win=49152
toybox -> sandbox TCP D=22 S=62117 Ack=195794441 Seq=195630515 Len=0 Win=49152
sandbox -> toybox TCP D=62117 S=22 Push Ack=195630515 Seq=195794441 Len=20 Win=491
```

La sortie présente le trafic des différentes zones au sein du système. Vous pouvez voir tous les paquets associés aux adresses IP net0, y compris les paquets livrés localement aux autres zones. Si vous générez une sortie détaillée, vous pouvez voir les zones impliquées dans le flux de paquets.

```
# snoop -I net0 -v port 22
IPNET:  ----- IPNET Header -----
IPNET:
IPNET:  Packet 5 arrived at 15:16:50.85262
IPNET:  Packet size = 64 bytes
IPNET:  dli_version = 1
IPNET:  dli_type = 0
IPNET:  dli_srczone = 0
IPNET:  dli_dstzone = 1
IPNET:
IP:  ----- IP Header -----
IP:
```



**EXEMPLE 5-19** Flux de paquets du périphérique net0 dans les zones locales (Suite)

```

IP:   Version = 4
IP:   Header length = 20 bytes
IP:   Type of service = 0x00
IP:       xxx. .... = 0 (precedence)
IP:       ...0 .... = normal delay
IP:       .... 0... = normal throughput
IP:       .... .0.. = normal reliability
IP:       .... ..0. = not ECN capable transport
IP:       .... ...0 = no ECN congestion experienced
IP:   Total length = 40 bytes
IP:   Identification = 22629
IP:   Flags = 0x4
IP:       .1.. .... = do not fragment
IP:       ..0. .... = last fragment
IP:   Fragment offset = 0 bytes
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 6 (TCP)
IP:   Header checksum = 0000
IP:   Source address = 172.0.0.1, 172.0.0.1
IP:   Destination address = 172.0.0.3, 172.0.0.3
IP:   No options
IP:
TCP:   ----- TCP Header -----
TCP:
TCP:   Source port = 46919
TCP:   Destination port = 22
TCP:   Sequence number = 3295338550
TCP:   Acknowledgement number = 3295417957
TCP:   Data offset = 20 bytes
TCP:   Flags = 0x10
TCP:       0... .... = No ECN congestion window reduced
TCP:       .0.. .... = No ECN echo
TCP:       ..0. .... = No urgent pointer
TCP:       ...1 .... = Acknowledgement
TCP:       .... 0... = No push
TCP:       .... .0.. = No reset
TCP:       .... ..0. = No Syn
TCP:       .... ...0 = No Fin
TCP:   Window = 49152
TCP:   Checksum = 0x0014
TCP:   Urgent pointer = 0
TCP:   No options
TCP:

```

L'en-tête ipnet indique que le paquet provient de la zone globale (ID 0) et se dirige vers Sandbox (ID 1).

**EXEMPLE 5-20** Observation du trafic par identification de la zone

```

# snoop -I hme0 sandboxsnop -I net0 sandbox
Using device ipnet/hme0 (promiscuous mode)
toybox -> sandbox TCP D=22 S=61658 Syn Seq=374055417 Len=0 Win=49152 Options=<mss
sandbox -> toybox TCP D=61658 S=22 Syn Ack=374055418 Seq=374124525 Len=0 Win=49152
toybox -> sandbox TCP D=22 S=61658 Ack=374124526 Seq=374055418 Len=0 Win=49152
#

```

**EXEMPLE 5-20** Observation du trafic par identification de la zone (Suite)

La capacité d'observer des paquets par identification de la zone est utile dans les systèmes dotés de plusieurs zones. Actuellement, la zone s'identifie uniquement par l'intermédiaire de l'ID de zone. L'utilisation de snoop avec les noms de zone n'est pas prise en charge.

## Administration de la sélection des adresses par défaut

Oracle Solaris permet à une interface unique de disposer de plusieurs adresses IP. Par exemple, certaines fonctionnalités telles que la fonctionnalité IPMP (multipathing sur réseau IP) permettent la connexion de plusieurs cartes d'interface réseau (NIC, network interface card) sur la même couche de liaison IP. Cette liaison peut être associée à une ou plusieurs adresses IP. Les interfaces des systèmes IPv6 possèdent également une adresse IPv6 lien-local, au moins une adresse de routage IPv6 ainsi qu'une adresse IPv4 pour au moins une interface.

Lorsque le système génère une transaction, une application envoie un appel vers le socket `getaddrinfo`. `getaddrinfo` détecte les adresses susceptibles d'être utilisées sur le système de destination. Le noyau établit alors l'ordre de priorité de cette liste afin de déterminer la destination appropriée pour le paquet. Ce processus est appelé *classement des adresses de destination*. Le noyau Oracle Solaris sélectionne le format approprié pour l'adresse source en fonction de l'adresse de destination déterminée pour le paquet. Ce processus est appelé *sélection des adresses*. Pour plus d'informations sur le classement des adresses de destination, reportez-vous à la page de manuel [getaddrinfo\(3SOCKET\)](#).

Le processus de sélection des adresses par défaut doit s'effectuer sur les systèmes IPv4 uniquement ainsi que sur les systèmes double pile IPv4/IPv6. Dans la plupart des cas, il n'est pas nécessaire de modifier les mécanismes de sélection des adresses par défaut. Toutefois, vous devrez peut-être modifier l'ordre de priorité des formats d'adresse de manière à prendre en charge la fonctionnalité IPMP ou à préférer les formats d'adresse 6to4, par exemple.

### ▼ Administration de la table des règles de sélection d'adresses IPv6

La section ci-dessous décrit la procédure de modification de la table des règles de sélection d'adresses. Pour plus d'informations concernant la sélection des adresses IPv6 par défaut, reportez-vous à la section "[Commande `ipaddrsel`](#)" à la page 156.



**Attention** – La table des règles de sélection d'adresses IPv6 doit uniquement être modifiée sur la base des motifs décrits dans la tâche suivante. Les erreurs de définition de la table des règles risquent d'entraîner des problèmes de fonctionnement du réseau. Veillez à enregistrer une copie de sauvegarde de la table des règles, comme indiqué à la procédure suivante.

### 1 Consultez la table de stratégie de sélection d'adresse IPv6 actuelle.

```
# ipaddrsel
# Prefix          Precedence Label
::1/128           50 Loopback
::/0              40 Default
2002::/16         30 6to4
::/96             20 IPv4_Compatible
::ffff:0.0.0.0/96 10 IPv4
```

### 2 Effectuez une copie de la table des règles de sélection d'adresses par défaut.

```
# cp /etc/inet/ipaddrsel.conf /etc/inet/ipaddrsel.conf.orig
```

### 3 Apportez les modifications souhaitées au fichier `/etc/inet/ipaddrsel.conf` dans un éditeur de texte.

Utilisez la syntaxe suivante pour les entrées de fichier `/etc/inet/ipaddrsel` :

*prefix/prefix-length precedence label [# comment]*

Les exemples ci-dessous illustrent les modifications susceptibles d'être apportées le plus souvent à la table des règles :

- Définition des adresses 6to4 sur la priorité la plus élevée :

```
2002::/16          50 6to4
::1/128            45 Loopback
```

Le format d'adresse 6to4 dispose dorénavant de la plus haute priorité (50). Loopback, qui disposait auparavant d'une priorité de 50, dispose dorénavant d'une priorité de 45. Les autres formats d'adresse restent inchangés.

- Définition d'une adresse source spécifique pour les communications avec une adresse de destination donnée :

```
::1/128            50 Loopback
2001:1111:1111::1/128 40 ClientNet
2001:2222:2222::/48  40 ClientNet
::/0               40 Default
```

Ce type de configuration s'utilise notamment pour les hôtes associés à une seule interface physique. Dans cet exemple, l'adresse source `2001:1111:1111::1/128` est définie en tant qu'adresse prioritaire pour les paquets adressés aux destinations du réseau `2001:2222:2222::/48`. L'adresse source `2001:1111:1111::1/128` est associée à la priorité 40, priorité supérieure à celle des autres formats d'adresse configurés pour l'interface.

- Préférence des adresses IPv4 par rapport aux adresses IPv6 :

<code>::ffff:0.0.0.0/96</code>	60 IPv4
<code>::1/128</code>	50 Loopback
<code>.</code>	
<code>.</code>	

La priorité par défaut du format IPv4 `::ffff:0.0.0.0/96` passe de 10 à 60, soit la priorité la plus élevée de la table.

**4 Chargez la table de règles modifiée dans le noyau.**

```
ipaddrsel -f /etc/inet/ipaddrsel.conf
```

**5 Si la table des règles modifiée génère des erreurs, restaurez la table des règles de sélection des adresses IPv6 par défaut.**

```
# ipaddrsel -d
```

## ▼ Modification de la table des règles de sélection des adresses IPv6 pour la session en cours uniquement

Les modifications apportées au fichier `/etc/inet/ipaddrsel.conf` sont conservées lors des sessions suivantes. Si vous souhaitez modifier la table des règles uniquement pour la session en cours, effectuez la procédure suivante.

**1 Copiez le contenu du fichier `/etc/inet/ipaddrsel` dans le fichier *filename*, où *filename* désigne le nom de votre choix.**

```
# cp /etc/inet/ipaddrsel filename
```

**2 Apportez les modifications souhaitées à la table des règles dans le fichier *filename*.**

**3 Chargez la table de règles modifiée dans le noyau.**

```
# ipaddrsel -f filename
```

Le noyau utilise la nouvelle table des règles jusqu'au prochain redémarrage du système.

# Configuration de tunnels IP

---

Ce chapitre contient des descriptions des tunnels IP ainsi que les procédures de configuration et de maintenance des tunnels dans Oracle Solaris.

## Présentation des tunnels IP

Les tunnels IP fournissent un moyen de transporter des paquets de données entre différents domaines lorsque le protocole de ces domaines n'est pas pris en charge par les réseaux intermédiaires. Par exemple, avec l'introduction du protocole IPv6, les réseaux IPv6 nécessitent un moyen de communiquer en dehors de leurs frontières dans un environnement où la plupart des réseaux utilisent le protocole IPv4. La communication devient possible avec l'utilisation des tunnels. Le tunnel IP fournit une liaison virtuelle entre deux noeuds atteignables en utilisant IP. La liaison peut donc être utilisée pour le transport de paquets IPv6 au sein des réseaux IPv4 afin de permettre la communication IPv6 entre les deux sites IPv6.

## Administration de tunnels IP dans cette version d'Oracle Solaris

Dans cette version d'Oracle Solaris, l'administration de tunnel a été révisée afin d'être en cohérence avec le nouveau modèle d'administration de liaison de données de réseau. Les tunnels sont maintenant créés et configurés à l'aide des nouvelles sous-commandes `dladm`. Les tunnels peuvent également utiliser d'autres fonctionnalités de liaison de données du nouveau modèle d'administration. Par exemple, la prise en charge des noms choisis par l'administrateur permet d'attribuer des noms significatifs aux tunnels. Pour plus d'informations sur les sous-commandes `dladm`, reportez-vous à la page de manuel [dladm\(1M\)](#).

## Types de tunnels

La mise sous tunnel implique d'encapsuler un paquet IP dans un autre paquet. Cette encapsulation permet au paquet d'atteindre sa destination par le biais de réseaux intermédiaires qui ne prennent pas en charge le protocole du paquet.

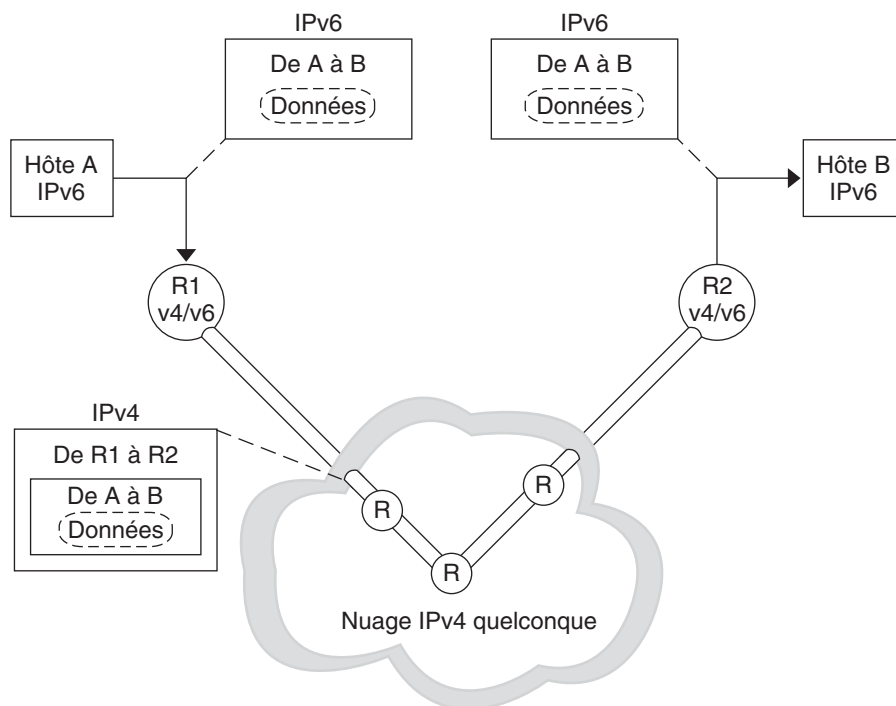
Les tunnels diffèrent en fonction du type d'encapsulation de paquet. Les types de tunnels suivants sont pris en charge dans Oracle Solaris :

- *Tunnels IPv4* :les paquets IPv4 ou IPv6 sont encapsulés dans un en-tête IPv4 et envoyés à une destination IPv4 unicast préconfigurée. Pour indiquer de façon plus spécifique les paquets acheminés dans le tunnel, les tunnels IPv4 sont également appelés *tunnels IPv4 sur IPv4* ou *tunnels IPv6 sur IPv4*.
- *Tunnels IPv6* :les paquets IPv4 ou IPv6 sont encapsulés dans un en-tête IPv6 et envoyés à une destination IPv6 unicast préconfigurée. Pour indiquer de façon plus spécifique les paquets acheminés dans le tunnel, les tunnels IPv6 sont également appelés *tunnels IPv4 sur IPv6* ou *tunnels IPv6 sur IPv6*.
- *Tunnels 6to4* :les paquets IPv6 sont encapsulés dans un en-tête IPv4 et envoyés à une destination IPv4 automatiquement déterminée sur une base par paquet. La détermination est basée sur un algorithme défini dans le protocole 6to4.

## Tunnels dans les environnements réseau combinant IPv6 et IPv4

La plupart des sites dotés de domaines IPv6 communiquent avec les autres domaines IPv6 en traversant des réseaux IPv4, lesquels sont plus répandus que les réseaux exclusivement IPv6. La figure suivante illustre le mécanisme de mise en tunnel entre deux hôtes IPv6 via des routeurs IPv4, signalés dans la figure par la lettre “R.”

FIGURE 6-1 Mécanisme de mise en tunnel IPv6



Dans la figure, le tunnel se compose de deux routeurs configurés afin de disposer d'une liaison virtuelle point à point entre les deux routeurs sur le réseau IPv4.

Un paquet IPv6 est encapsulé dans un paquet IPv4. Le routeur de bordure du réseau IPv6 configure un tunnel point à point sur plusieurs réseaux IPv4 jusqu'au routeur de bordure du réseau IPv6 de destination. Le paquet est transporté dans le tunnel au routeur de bordure de destination, où le paquet est décapsulé. Le routeur transmet ensuite le paquet IPv6 distinct au nœud de destination.

## Tunnels 6to4

Dans Oracle Solaris, les tunnels 6to4 constituent la méthode temporaire recommandée pour effectuer la transition entre les adressages IPv4 et IPv6. Les tunnels 6to4 permettent aux sites IPv6 isolés de communiquer, par le biais d'un tunnel automatique, avec un réseau IPv4 ne prenant pas en charge le protocole IPv6. Pour utiliser des tunnels 6to4, vous devez configurer un routeur de bordure sur le réseau IPv6 en tant que point d'extrémité du tunnel 6to4 automatique. Par la suite, le routeur 6to4 peut participer à un tunnel vers un autre site 6to4 ou vers un site IPv6 natif et non-6to4, le cas échéant.

Cette section fournit des références sur les rubriques concernant les tunnels 6to4 :

- Topologie d'un tunnel 6to4
- Description du flux de paquets dans un tunnel 6to4
- Topologie d'un tunnel reliant un routeur 6to4 et un routeur relais 6to4
- Informations importantes pour la configuration de la prise en charge d'un routeur relais 6to4

Le tableau suivant décrit les autres tâches permettant de configurer des tunnels 6to4 et les ressources permettant obtenir d'autres informations utiles.

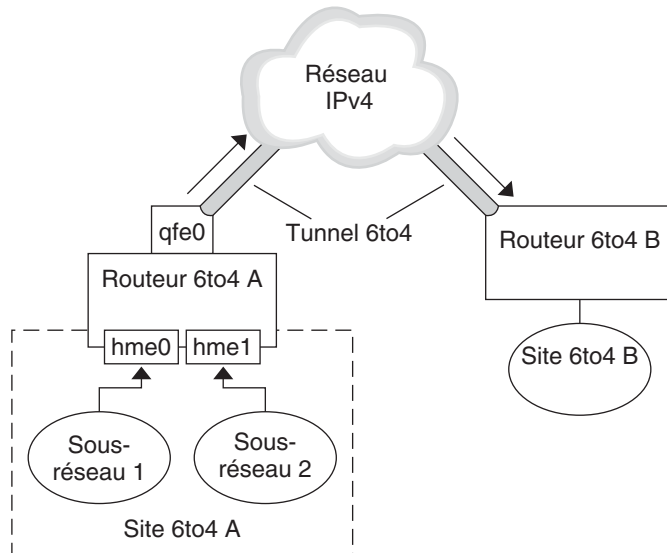
Tâche ou détail	Référence
Configuration d'un tunnel 6to4	<a href="#">“Procédure de configuration d'un tunnel 6to4” à la page 131</a>
RFC lié aux 6to4	<a href="http://www.ietf.org/rfc/rfc3056.txt">RFC 3056, "Connection of IPv6 Domains via IPv4 Clouds"</a> ( <a href="http://www.ietf.org/rfc/rfc3056.txt">http://www.ietf.org/rfc/rfc3056.txt</a> )
Informations détaillées sur la commande 6to4relay (prise en charge des tunnels vers un routeur relais 6to4)	<a href="#">6to4relay(1M)</a>
Problèmes de sécurité avec 6to4	<a href="http://www.ietf.org/rfc/rfc3964.txt">Security Considerations for 6to4</a> ( <a href="http://www.ietf.org/rfc/rfc3964.txt">http://www.ietf.org/rfc/rfc3964.txt</a> )

## Topologie d'un tunnel 6to4

Un tunnel 6to4 offre la connexion IPv6 à tous les sites 6to4, quel que soit leur emplacement. De même, le tunnel offre un lien à l'ensemble des sites IPv6, notamment l'Internet IPv6 natif, à condition d'être configuré pour la transmission vers un routeur relais. La figure suivante illustre un tunnel 6to4 connectant des sites 6to4.



FIGURE 6-2 Tunnel entre deux sites 6to4



La figure représente deux réseaux 6to4 isolés, le site A et le site B. Chaque site a configuré un routeur avec une connexion externe à un réseau IPv4. Un tunnel 6to4 à l'échelle du réseau IPv4 offre une connexion entre sites 6to4.

Pour convertir un site IPv6 en site 6to4, vous devez configurer au moins une interface de routeur prenant en charge 6to4. Cette interface doit assurer la connexion externe au réseau IPv4. L'adresse que vous configurez sur `qfe0` doit être globale et unique. Sur cette figure, l'interface du routeur A (`qfe0`) connecte le site A au réseau IPv4. L'interface `qfe0` doit déjà être configurée avec une adresse IPv4 pour que vous puissiez définir `qfe0` en tant que pseudointerface 6to4.

Dans la figure, le site 6to4 A est composé de deux sous-réseaux qui sont connectés aux interfaces `hme0` et `hme1` du routeur A. Tous les hôtes IPv6 sur l'un des sous-réseaux du site A sont reconfigurés automatiquement avec des adresses dérivées de 6to4 une fois la publication du routeur A reçue.

Le site B est un autre site 6to4 isolé. Pour recevoir correctement le trafic du site A, un routeur de bordure sur le site B doit être configuré pour prendre en charge 6to4. Dans le cas contraire, le routeur ne reconnaît pas les paquets reçus du site A et les abandonne.

## Description du flux de paquets dans un tunnel 6to4

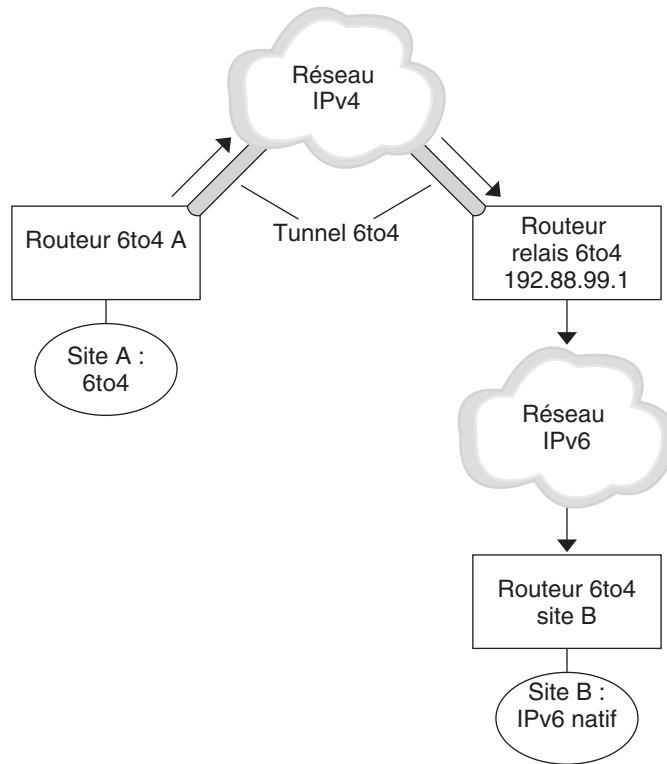
Cette section décrit le flux de paquets allant d'un hôte sur un site 6to4 à un autre hôte sur un site 6to4 distant. Ce scénario utilise la topologie illustrée à la [Figure 6-2](#). Cela suppose également de configurer au préalable les routeurs et les hôtes 6to4.

1. Un hôte du sous-réseau 1 appartenant au site 6to4 A envoie une transmission à un hôte du site 6to4 B. Chaque en-tête de paquet possède des adresses 6to4 dérivées source et cible.
2. Le routeur du site A encapsule chaque paquet 6to4 dans un en-tête IPv4. Dans ce processus, le routeur définit l'adresse cible IPv4 de l'en-tête d'encapsulation sur l'adresse du routeur du site B. L'adresse cible IPv6 de chaque paquet IPv6 transmis via l'interface du tunnel contient également l'adresse cible IPv4. Ainsi, le routeur est en mesure de déterminer l'adresse cible IPv4 définie sur l'en-tête d'encapsulation. Ensuite, il utilise la procédure de routage IPv4 standard pour transmettre le paquet sur le réseau IPv4.
3. Tout routeur IPv4 rencontré par les paquets utilise l'adresse IPv4 cible de ces derniers pour la transmission. Cette adresse constitue l'adresse IPv4 globale et unique de l'interface du routeur B, qui sert également de pseudointerface 6to4.
4. Les paquets du site A arrivent sur le routeur B qui les décapsule en paquets IPv6 à partir de l'en-tête IPv4.
5. Le routeur B se sert alors de l'adresse cible des paquets IPv6 pour transmettre ces derniers à l'hôte destinataire sur le site B.

## **Informations importantes pour la création de tunnels vers un routeur relais 6to4**

Les routeurs relais 6to4 fonctionnent en tant que points d'extrémité des tunnels reliant des routeurs 6to4 à des réseaux IPv6 natifs, non 6to4. Les routeurs relais constituent essentiellement des ponts entre le site 6to4 et les sites IPv6 natifs. Ce type de routeur risque de ne pas garantir la sécurité du réseau ; c'est pourquoi il n'est pas pris en charge par Oracle Solaris. Cependant, si votre site nécessite un tel tunnel, vous pouvez exécuter la commande `6to4relay` pour créer le type de tunnel suivant.

FIGURE 6-3 Tunnel entre un site 6to4 et un routeur relais 6to4



Dans la [Figure 6-3](#), le site 6to4 A doit communiquer avec un noeud du site natif IPv6 B. La figure indique le chemin du trafic en provenance du site A dans un tunnel 6to4 sur un réseau IPv4. Le tunnel dispose d'un routeur A 6to4 et d'un routeur relais 6to4 à chaque extrémité. Au-delà du routeur 6to4 se trouve le réseau IPv6 auquel le site B IPv6 est connecté.

## Flux de paquets entre un site 6to4 et un site IPv6 natif

Cette section décrit le flux de paquets se déplaçant d'un site 6to4 vers un site IPv6 natif. Ce scénario utilise la topologie illustrée à la [Figure 6-3](#).

1. Un hôte sur le site 6to4 A envoie une transmission spécifiant un hôte sur le site natif IPv6 B en tant que destination. Chaque en-tête de paquet dispose d'une adresse dérivée de 6to4 en tant qu'adresse source. L'adresse de destination correspond à une adresse IPv6 standard.
2. Le routeur 6to4 du site A encapsule chaque paquet dans un en-tête IPv4, dont la destination correspond à l'adresse IPv4 du routeur relais 6to4. Ensuite, il utilise la procédure de routage IPv4 standard pour transmettre le paquet sur le réseau IPv4. Tout routeur IPv4 rencontré par les paquets envoie ceux-ci vers le routeur relais 6to4.

3. Le routeur relais 6to4 anycast le plus proche (physiquement) du site A récupère les paquets destinés au groupe anycast 192 . 88 . 99 . 1.

---

**Remarque** – Les routeurs relais 6to4 faisant partie du groupe anycast de routeurs relais 6to4 possèdent l'adresse IP 192 . 88 . 99 . 1. Cette adresse anycast constitue l'adresse par défaut des routeurs relais 6to4. Si vous avez besoin d'un routeur relais 6to4 spécifique, vous pouvez supprimer celui par défaut et spécifier l'adresse IPv4 du routeur en question.

---

4. Ce routeur relais décapsule ensuite l'en-tête IPv4 des paquets 6to4, dévoilant l'adresse de destination sur le réseau IPv6.
5. Le routeur relais envoie ensuite les paquets qui sont à présent IPv6 uniquement sur le réseau IPv6, où ils seront ensuite récupérés par un routeur sur le site B. Le routeur transmet ensuite les paquets au noeud de destination IPv6.

## Déploiement des tunnels

Pour déployer les tunnels IP correctement, vous devez effectuer deux tâches principales. Commencez par créer la liaison de tunnel. Ensuite, configurez une interface IP sur le tunnel. Cette section offre une brève description des exigences en matière de création des tunnels et de leurs interfaces IP correspondantes.

### Exigences en matière de création de tunnels

Pour créer des tunnels correctement, vous devez remplir les exigences suivantes :

- Si vous utilisez des noms d'hôte plutôt que des adresses IP littérales, ces noms doivent être résolus en adresses IP valides compatibles avec le type de tunnel.
- Le tunnel IPv4 ou IPv6 que vous créez ne doit pas partager les mêmes adresses source et de destination de tunnel avec un autre tunnel configuré.
- Le tunnel IPv4 ou IPv6 que vous créez ne doit pas partager la même adresse source avec un tunnel 6to4 existant.
- Si vous créez un tunnel 6to4, celui-ci ne doit pas partager la même adresse source avec un autre tunnel configuré.

Pour obtenir des informations sur la configuration de tunnels sur votre réseau, reportez-vous à la section [“Planification de l'utilisation de tunnels dans le réseau” à la page 41.](#)

## Exigences relatives aux tunnels et aux interfaces IP

Chaque type de tunnel est doté d'exigences spécifiques en matière d'adresses IP sur l'interface IP que vous configurez sur le tunnel. Les exigences sont résumées dans le tableau ci-dessous.

TABLEAU 6-1 Exigences en matière de tunnels et d'interface IP

Type de tunnel	Interface IP autorisée sur le tunnel	Exigence d'interface IP
Tunnel IPv4	Interface IPv4	Les adresses locales et distantes sont spécifiées manuellement.
	Interface IPv6	Les adresses locales et distantes de liaison locale sont définies automatiquement lors de l'exécution de la commande <code>ipadm create-addr -T addrconf</code> . Pour plus d'informations, reportez-vous à la page de manuel <a href="#">ipadm(1M)</a> .
Tunnel IPv6	Interface IPv4	Les adresses locales et distantes sont spécifiées manuellement.
	Interface IPv6	Les adresses locales et distantes de liaison locale sont définies automatiquement lors de l'exécution de la commande <code>ipadm create-addr -T addrconf</code> . Pour plus d'informations, reportez-vous à la page de manuel <a href="#">ipadm(1M)</a> .
Tunnel 6to4	Interface IPv6 uniquement	L'adresse IPv6 par défaut est sélectionnée automatiquement lors de l'exécution de la commande <code>ipadm create-if</code> . Pour plus d'informations, reportez-vous à la page de manuel <a href="#">ipadm(1M)</a> .

Vous pouvez remplacer l'adresse d'interface IPv6 par défaut par des tunnels 6to4 en spécifiant une adresse IPv6 différente à l'aide de la commande `ipadm`.

De même, pour remplacer les adresses de liaison locale définies automatiquement pour les interfaces IPv6 sur les tunnels IPv4 ou IPv6, vous pouvez spécifier différentes adresses source et de destination dans le fichier hôte du tunnel.

# Configuration et administration du tunnel avec la commande `dladm`

Cette section décrit les procédures utilisant la commande `dladm` pour configurer les tunnels.

## Sous-commandes `dladm`

A partir de cette version d'Oracle Solaris, l'administration de tunnel est maintenant séparée de la configuration de l'interface IP. L'aspect données-liaison des tunnels IP est maintenant administré à l'aide de la commande `dladm`. En outre, la configuration d'interface IP, incluant l'interface de tunnel IP, s'effectue à l'aide de la commande `ipadm`.

Les sous-commandes `dladm` suivantes permettent de configurer les tunnels IP :

- `create-iptun`
- `modify-iptun`
- `show-iptun`
- `delete-iptun`
- `set-linkprop`

Pour plus d'informations sur la commande `dladm`, reportez-vous à la page de manuel [dladm\(1M\)](#).

**Remarque** – L'administration de tunnels IP est étroitement liée à la configuration d'IPsec. Par exemple, les VPN IPsec sont l'une des utilisations principales de la mise sous tunnel IP. Pour plus d'informations sur la sécurité dans Oracle Solaris, reportez-vous à la section [Partie III](#). Pour configurer IPsec, reportez-vous au [Chapitre 15](#), “Configuration d'IPsec (tâches)”.

## Configuration des tunnels (liste des tâches)

Tâche	Description	Voir
Création d'un tunnel IP.	Configuration du tunnel à utiliser pour communiquer sur les réseaux.	<a href="#">“Création et configuration d'un tunnel IP” à la page 127</a>
Modification de la configuration d'un tunnel.	Modification des paramètres d'origine du tunnel, comme l'adresse source ou de destination du tunnel.	<a href="#">“Modification d'une configuration de tunnel IP” à la page 135</a>

Tâche	Description	Voir
Affichage d'une configuration de tunnel.	Affichage des informations de configuration pour un tunnel spécifique ou pour tous les tunnels IP du système.	<a href="#">“Affichage d'une configuration de tunnel IP” à la page 136</a>
Suppression d'un tunnel.	Suppression d'une configuration de tunnel.	<a href="#">“Suppression d'un tunnel IP” à la page 138</a>

## ▼ Création et configuration d'un tunnel IP

### 1 Créez le tunnel.

# `dladm create-iptun [-t] -T type -a [local|remote]=addr,... tunnel-link`

Les options ou arguments suivants sont disponibles pour cette commande :

-t	Crée un tunnel temporaire. Par défaut, la commande crée un tunnel persistant.
<hr/>	
<b>Remarque</b> – Si vous souhaitez configurer une interface IP sur le tunnel, vous devez créer un tunnel persistant et ne pas utiliser l'option <code>-t</code> .	
<hr/>	
-T type	Spécifie le type de tunnel à créer. Cet argument est requis pour créer tous les types de tunnel.
-a [local remote]=address,...	Spécifie les adresses IP littérales ou les noms d'hôte correspondant aux adresses locales et à l'adresse de tunnel distant. Les adresses doivent être valides et déjà créées dans le système. Suivant le type de tunnel, spécifiez soit une seule adresse, soit les adresses locales et distantes. Si vous spécifiez les adresses locales et distantes, vous devez les séparer à l'aide d'une virgule. <ul style="list-style-type: none"><li>■ Les tunnels IPv4 nécessitent des adresses IPv4 locales et distantes pour fonctionner.</li><li>■ Les tunnels IPv6 nécessitent des adresses IPv6 locales et distantes pour fonctionner.</li><li>■ Les tunnels 6to4 nécessitent une adresse IPv4 locale pour fonctionner.</li></ul>

---

**Remarque** – Pour les configurations de liaison de données de tunnel IP, si vous utilisez des noms d'hôte en guise d'adresses, ces noms d'hôte sont enregistrés dans le stockage de configuration. Lors d'une initialisation ultérieure du système, si la résolution de noms donne des adresses IP différentes de celles utilisées lors de la création du tunnel, ce dernier acquiert une nouvelle configuration.

---

*tunnel-link*

Spécifie la liaison de tunnel IP. Avec la prise en charge des noms significatifs dans une administration réseau-liaison, les noms de tunnel ne sont plus limités au type de tunnel que vous créez. En revanche, vous pouvez attribuer au tunnel tout nom choisi par l'administrateur. Les noms de tunnel se composent d'une chaîne et du numéro de point de connexion physique, par exemple, *montunnel0*. Pour connaître les règles régissant l'attribution de noms significatifs, reportez-vous à la section “[Règles applicables aux noms de lien valides](#)” du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

Si vous ne spécifiez pas la liaison de tunnel, le nom est fourni automatiquement, conformément aux conventions d'attribution de nom suivantes :

- Pour les tunnels IPv4 : `ip.tun#`
- Pour les tunnels IPv6 : `ip6.tun#`
- Pour les tunnels 6to4 : `ip.6to4tun#`

Le symbole `#` correspond au numéro de point de connexion physique le plus bas disponible pour le type de tunnel que vous êtes en train de créer.

**2 (Facultatif) Définissez les valeurs de la limite de saut ou de la limite d'encapsulation.**

`# dladm set-linkprop -p [hoplimit=value] [encaplimit=value] tunnel-link`

**hoplimit**      Spécifie la limite de saut de l'interface de tunnel pour la mise en tunnel sur IPv6. *hoplimit* est l'équivalent du champ IPv4 de durée de vie pour la mise en tunnel sur IPv4.

**encaplimit**    Spécifie le nombre de niveaux de tunnels imbriqués autorisés pour un paquet. Cette option s'applique uniquement aux tunnels IPv6.

Spécifie le nombre de niveaux de tunnels imbriqués autorisés pour un paquet. Cette option s'applique uniquement aux tunnels IPv6.



---

**Remarque** – Les valeurs définies pour `hoplimit` et `encaplimit` doivent être comprises dans une plage acceptable. `hoplimit` et `encaplimit` sont des propriétés de liaison de tunnel. Par conséquent, ces propriétés sont administrées par les mêmes sous-commandes `dladm` que pour les autres propriétés de liaison. Les sous-commandes sont `dladm set-linkprop`, `dladm reset-linkprop` et `dladm show-linkprop`. Reportez-vous à la page de manuel [dladm\(1M\)](#) pour connaître les différentes sous-commandes utilisées avec la commande `dladm` pour l'administration de liens.

---

### 3 Créez une interface IP sur le tunnel.

```
# ipadm create-ip tunnel-interface
```

où *tunnel-interface* utilise le même nom que la liaison de tunnel.

### 4 Assignez des adresses IP locales et distantes à l'interface de tunnel.

```
# ipadm create-addr [-t] -T static -a local=address,remote=address addrobj
```

<code>-t</code>	Indique une configuration d'IP temporaire plutôt qu'une configuration d'IP persistante sur le tunnel. Si vous n'utilisez pas cette option, la configuration d'interface IP est persistante.
<code>-T static</code>	Indique que les adresses IP statiques sont utilisées plutôt que les procédures d'IP dynamiques.
<code>-a local=address,remote=address</code>	Spécifie l'adresse IP de l'interface de tunnel. Les adresses IP source et de destination sont requises, comme représenté par <code>local</code> et <code>remote</code> . Les adresses locales et distantes peuvent être des adresses IPv4 ou IPv6.
<i>addrobj</i>	Spécifie l'objet d'adressage propriétaire des adresses locales et distantes. <i>addrobj</i> doit utiliser le format suivant : <i>interface / chaîne-spécifiée-par-l'utilisateur</i> . <i>chaîne-spécifiée-par-l'utilisateur</i> fait référence à une chaîne de caractères alphanumériques commençant par une lettre et dont la taille ne dépasse pas 32 caractères.

Pour plus d'informations sur la commande `ipadm` et les différentes options de configuration des interfaces IP, incluant les interfaces de tunnel, reportez-vous à la page de manuel [ipadm\(1M\)](#) et à la section [Partie II, “Configuration de liaisons de données et d’interfaces” du manuel Administration d’Oracle Solaris : interfaces réseau et virtualisation réseau](#).

### 5 Ajoutez les informations de configuration de tunnel au fichier `/etc/hosts`.

### 6 (Facultatif) Vérifiez le statut de la configuration d'interface de l'IP du tunnel.

```
# ipadm show-addr interface
```

**Exemple 6-1** Création d'une interface IPv6 sur un tunnel IPv4

Cet exemple illustre comment créer un IPv6 persistant sur un tunnel IPv4.

```
# dladm create-iptun -T ipv4 -a local=63.1.2.3,remote=192.4.5.6 private0
# dladm set-linkprop -p hoplimit=200 private0
# ipadm create-ip private0
# ipadm create-addr -T addrconf private0/v6
# ipadm show-addr private0/
ADDROBJ      TYPE      STATE      ADDR
private0/v6   static    ok          fe80::a08:392e/10 --> fe80::8191:9a56
```

Pour ajouter d'autres adresses, utilisez la même syntaxe avec une *chaîne-spécifiée-par-l'utilisateur* différente pour *addrobj*. Par exemple, vous pouvez ajouter une adresse globale comme suit :

```
# ipadm create-addr -T static -a local=2001:db8:4728::1, \
remote=2001:db8:4728::2 private0/global
# ipadm show-addr private0/
ADDROBJ      TYPE      STATE      ADDR
private0/v6   addrconf  ok          fe80::a08:392e/10 --> fe80::8191:9a56
private0/global static    ok          2001:db8:4728::1 --> 2001:db8:4728::2
```

Notez que le préfixe `2001:db8` de l'adresse IPv6 est un préfixe IPv6 spécial utilisé spécifiquement pour les exemples de documentation. Pour une description des adresses et du format IPv6, reportez-vous à la section “[Présentation de l'adressage IPv6](#)” du manuel *Guide d'administration système : services IP*.

**Exemple 6-2** Création d'une interface IPv4 sur un tunnel IPv4

Cet exemple illustre comment créer un IPv4 persistant sur un tunnel IPv4.

```
# dladm create-iptun -T ipv4 -a local=63.1.2.3,remote=192.4.5.6 vpn0
# ipadm create-ip vpn0
# ipadm create-addr -T static -a local=10.0.0.1,remote=10.0.0.2 vpn0/v4
# ipadm show-addr
ADDROBJ      TYPE      STATE      ADDR
lo0/v4       static    ok          127.0.0.1
vpn0/v4       static    ok          10.0.0.1-->10.0.0.2
```

Vous pouvez configurer la stratégie IPsec davantage pour fournir des connexions sécurisées aux paquets circulant dans ce tunnel. Pour plus d'informations sur la configuration d'IPsec, reportez-vous au [Chapitre 15, “Configuration d'IPsec \(tâches\)”](#).

**Exemple 6-3** Création d'une interface IPv6 sur un tunnel IPv6

Cet exemple illustre comment créer un IPv6 persistant sur un tunnel IPv6.

```
# dladm create-iptun -T ipv6 -a local=2001:db8:feed::1234,remote=2001:db8:beef::4321 \
tun0
```

```
# ipadm create-ip tun0
# ipadm create-addr -T addrconf tun0/v6
# ipadm show-addr
ADDROBJ    TYPE        STATE    ADDR
lo0/v6     static      ok       ::1/128
tun0/v6    addrconf    ok       2001:db8:feed::1234 --> 2001:db8:beef::4321
```

Pour ajouter des adresses comme une adresse globale ou d'autres adresses locales et distantes, utilisez la commande `ipadm` comme suit :

```
# ipadm create-addr -T static \
-a local=2001:db8::4728:56bc,remote=2001:db8::1428:57ab tun0/alt
# ipadm show-addr tun0/
ADDROBJ    TYPE        STATE    ADDR
tun0/v6    addrconf    ok       2001:db8:feed::1234 --> 2001:db8:beef::4321
tun0/alt   static      ok       2001:db8::4728:56bc --> 2001:db8::1428:57ab
```

## ▼ Procédure de configuration d'un tunnel 6to4

Dans les tunnels 6to4, un routeur 6to4 doit agir en tant que routeur IPv6 pour les noeuds des sites 6to4 du réseau. Par conséquent, lors de la configuration d'un routeur 6to4, ce routeur doit également être configuré en tant que routeur IPv6 sur ses interfaces physiques. Pour plus d'informations sur le routage IPv6, reportez-vous à la section [“Routage IPv6” à la page 170](#).

### 1 Créez un tunnel 6to4.

```
# dladm create-iptun -T 6to4 -a local=address tunnel-link
```

Les options ou arguments suivants sont disponibles pour cette commande :

`-a local=address` Spécifie l'adresse locale de tunnel qui doit déjà exister dans le système pour être valide.

`tunnel-link` Spécifie la liaison de tunnel IP. Avec la prise en charge des noms significatifs dans une administration réseau-liaison, les noms de tunnel ne sont plus limités au type de tunnel que vous créez. En revanche, vous pouvez attribuer au tunnel tout nom choisi par l'administrateur. Les noms de tunnel se composent d'une chaîne et du numéro de point de connexion physique, par exemple, *montunnel0*. Pour connaître les règles régissant l'attribution de noms significatifs, reportez-vous à la section [“Règles applicables aux noms de lien valides” du manuel \*Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau\*](#).

### 2 Créez l'interface IP de tunnel.

```
# ipadm create-ip tunnel-interface
```

où *tunnel-interface* utilise le même nom que la liaison de tunnel.

- 3 (Facultatif) Ajoutez d'autres adresses IPv6 pour une utilisation par le tunnel.
- 4 Modifiez le fichier `/etc/inet/ndpd.conf` pour publier le routage 6to4 en ajoutant les deux lignes suivantes :

```
if subnet-interface AdvSendAdvertisements 1
IPv6-address subnet-interface
```

La première ligne spécifie le sous-réseau qui reçoit cette publication. *subnet-interface* fait référence à la liaison à laquelle est connecté le sous-réseau. Les adresses IPv6 sur la seconde ligne doivent avoir le préfixe 6to4 2000 qui est utilisé pour les adresses IPv6 dans les tunnels 6to4.

Pour obtenir des informations détaillées sur le fichier `ndpd.conf`, reportez-vous à la page de manuel [ndpd.conf\(4\)](#).

- 5 Activez le transfert IPv6.

```
# ipadm set-prop -p forwarding=on ipv6
```

- 6 Réinitialisez le routeur.

Vous pouvez également exécuter la commande `sighup` sur le démon de `/etc/inet/in.ndpd` pour commencer la publication du routeur. Les noeuds IPv6 de chaque sous-réseau devant recevoir le préfixe 6to4 sont alors automatiquement définis sur les nouvelles adresses 6to4 dérivées.

- 7 Ajoutez ces nouvelles adresses au service de noms utilisé par le site 6to4.

Vous trouverez les instructions correspondantes dans la section “[Configuration de prise en charge de services de noms pour IPv6](#)” à la page 89.

#### Exemple 6–4 Création de tunnel 6to4

Dans cet exemple, l'interface de sous-réseau est `bge0`, à laquelle `/etc/inet/ndpd.conf` fait référence dans l'étape adéquate.

Cet exemple indique comment créer un tunnel 6to4. Notez que seules les interfaces IPv6 peuvent être configurées sur les tunnels 6to4.

```
# dladm create-iptun -T 6to4 -a local=192.168.35.10 tun0
# ipadm create-ip tun0
# ipadm show-addr
ADDROBJ      TYPE      STATE   ADDR
lo0/v4       static    ok      127.0.0.1/8
bge0/static   static    ok      192.168.35.10/24
lo0/v6       static    ok      ::1/128
tun0/_a      static    ok      2002:c0a8:57bc::1/64

# ipadm create-addr -T static -a 2002:c0a8:230a::2/16 tun0/a2
# ipadm create-addr -T static -a 2002:c0a8:230a::3/16 tun0/a3
```

```
# ipadm show-addr tun0/
ADDROBJ      TYPE      STATE    ADDR
lo0/v4        static    ok       127.0.0.1/8
bge0/static    static    ok       192.168.35.10/24
lo0/v6        static    ok       ::1/128
tun0/_a       static    ok       2002:c0a8:57bc::1/64
tun0/a2       static    ok       2002:c0a8:230a::2/16
tun0/a3       static    ok       2002:c0a8:230a::3/16

# vi /etc/inet/ndpd.conf
if bge0 AdvSendAdvertisements 1
2002:c0a8:57bc::1/64 bge0

# ipadm set-prop -p forwarding=on ipv6
```

Notez que pour les tunnels 6to4, le préfixe de l'adresse IPv6 est 2002. Pour de plus amples explications, reportez-vous à la section “[Préfixes d'IPv6](#)” du manuel *Guide d'administration système : services IP*.

## ▼ Procédure de configuration d'un tunnel 6to4 relié à un routeur relais 6to4



**Attention** – Pour des raisons de sécurité, la prise en charge des routeurs relais 6to4 est désactivée par défaut dans Oracle Solaris. Voir “[Problèmes de sécurité lors de la création d'un tunnel vers un routeur relais 6to4](#)” à la page 142.

### Avant de commencer

Avant de configurer un tunnel relié à un routeur relais 6to4, vous devez avoir effectué les tâches suivantes :

- Configuration d'un routeur 6to4 sur votre site, comme décrit dans la section “[Création et configuration d'un tunnel IP](#)” à la page 127
- Vérification des problèmes de sécurité susceptibles de se produire avec un tunnel relié à un routeur relais 6to4

### 1 Vous pouvez relier un tunnel à un routeur relais 6to4 de deux façons :

- Liaison a un routeur relais 6to4 de type anycast.

```
# /usr/sbin/6to4relay -e
```

L'option `-e` configure un tunnel entre le routeur 6to4 et un routeur relais 6to4 anycast. Les routeurs relais 6to4 anycast possèdent l'adresse IPv4 courante 192.88.99.1. Le routeur relais anycast le plus proche (physiquement) de votre site devient le point d'extrémité du tunnel 6to4. Ce routeur relais gère ensuite l'envoi des paquets entre votre site 6to4 et un site IPv6 natif.

Pour plus d'informations sur les routeurs relais 6to4 Anycast, reportez-vous à la page [RFC 3068, "An Anycast Prefix for 6to4 Relay Routers"](http://ftp.rfc-editor.org/in-notes/rfc3068.txt) ([ftp://ftp.rfc-editor.org/in-notes/rfc3068.txt](http://ftp.rfc-editor.org/in-notes/rfc3068.txt)).

- Liaison à un routeur relais 6to4 de type spécifique.

```
# /usr/sbin/6to4relay -e -a relay-router-address
```

L'option `-a` est toujours suivie d'une adresse de routeur spécifique. Remplacez *relay-router-address* par l'adresse IPv4 du routeur relais 6to4 spécifique que vous souhaitez relier au tunnel.

Le tunnel relié au routeur relais 6to4 reste actif pendant la suppression de la pseudointerface du tunnel 6to4.

## 2 Supprimez le tunnel relié au routeur relais 6to4 lorsqu'il n'est plus nécessaire :

```
# /usr/sbin/6to4relay -d
```

## 3 (Facultatif) Configurez un tunnel au routeur relais 6to4 qui conserve ses paramètres après chaque redémarrage.

Si votre site requiert, pour quelque raison qu'il soit, que les paramètres du tunnel relié au routeur relais 6to4 soient redéclarés à chaque redémarrage du routeur, effectuez la procédure suivante :

### a. Modifiez le fichier `/etc/default/inetinit`.

La ligne à modifier se trouve à la fin du fichier.

### b. Remplacez la valeur "NO" de la ligne `ACCEPT6T04RELAY=NO` par "YES".

### c. (Facultatif) Créez un tunnel relié à un routeur relais 6to4 spécifique dont les paramètres sont conservés après chaque redémarrage.

Pour le paramètre `RELAY6T04ADDR`, remplacez l'adresse `192.88.99.1` par l'adresse IPv4 du routeur relais 6to4 à utiliser.

## Exemple 6–5 Obtention d'informations sur le statut de la prise en charge des routeurs relais 6to4

La commande `/usr/bin/6to4relay` vous permet de savoir si les routeurs relais 6to4 sont pris en charge ou non par votre site. L'exemple suivant présente la sortie obtenue lorsque les routeurs relais 6to4 ne sont pas pris en charge (sortie par défaut d'Oracle Solaris) :

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is disabled.
```

Lorsque les routeurs relais 6to4 sont pris en charge, la sortie suivante s'affiche :

```
# /usr/sbin/6to4relay
6to4relay: 6to4 Relay Router communication support is enabled.
IPv4 remote address of Relay Router=192.88.99.1
```

## ▼ Modification d'une configuration de tunnel IP

### ● Modifiez la configuration du tunnel.

```
# dladm modify-iptun -a [local|remote]=addr,... tunnel-link
```

Vous ne pouvez pas modifier le type d'un tunnel existant. Par conséquent, l'option `-T type` n'est pas autorisée pour cette commande. Seuls les paramètres de tunnel suivants peuvent être modifiés :

- a [local|remote]=*address*,...      Spécifie les adresses IP littérales ou les noms d'hôte correspondant aux adresses locales et à l'adresse de tunnel distant. Suivant le type de tunnel, spécifiez soit une seule adresse, soit les adresses locales et distantes. Si vous spécifiez les adresses locales et distantes, vous devez les séparer à l'aide d'une virgule.
  - Les tunnels IPv4 nécessitent des adresses IPv4 locales et distantes pour fonctionner.
  - Les tunnels IPv6 nécessitent des adresses IPv6 locales et distantes pour fonctionner.
  - Les tunnels 6to4 nécessitent une adresse IPv4 locale pour fonctionner.

Pour les configurations de liaison de données de tunnel IP, si vous utilisez des noms d'hôte en guise d'adresses, ces noms d'hôte sont enregistrés dans le stockage de configuration. Lors d'une initialisation ultérieure du système, si la résolution de noms donne des adresses IP différentes de celles utilisées lors de la création du tunnel, ce dernier acquiert une nouvelle configuration.

Si vous modifiez les adresses locales et distantes du tunnel, assurez-vous que ces adresses sont cohérentes par rapport au type de tunnel que vous modifiez.

---

**Remarque** – Si vous souhaitez modifier le nom de la liaison de tunnel, n'utilisez pas la sous-commande `modify-iptun`. Utilisez plutôt `dladm rename-link`.

```
# dladm rename-link old-tunnel-link new-tunnel-link
```

De même, n'utilisez pas la commande `modify-iptun` pour modifier les propriétés de tunnel telles que `hoplimit` ou `encaplimit`. Préférez la commande `dladm set-linkprop` pour définir les valeurs de ces propriétés.

---

### Exemple 6–6 Modification de l'adresse et des propriétés d'un tunnel

Cet exemple comporte deux procédures. Tout d'abord, les adresses locales et distantes du tunnel IPv4 `vpn0` sont modifiées temporairement. Une fois le système réinitialisé, le tunnel revient à l'utilisation des adresses d'origine. Une seconde procédure modifie la valeur `hoplimit` de `vpn0` à 60.

```
# dladm modify-iptun -t -a local=10.8.48.149,remote=192.1.2.3 vpn0
# dladm set-linkprop -p hoplimit=60 vpn0
```

## ▼ Affichage d'une configuration de tunnel IP

### ● Affichez la configuration du tunnel IP.

```
# dladm show-iptun [-p] -o fields [tunnel-link]
```

Vous pouvez utiliser les options avec la commande :

- p Affiche les informations dans une format analysable. Cet argument est facultatif.
- o *fields* Affiche les champs sélectionnés qui fournissent des informations spécifiques au tunnel.
- tunnel-link* Spécifie le tunnel dont vous souhaitez afficher les informations de configuration. Cet argument est facultatif. Si vous omettez le nom de tunnel, la commande affiche les informations à propos de tous les tunnels du système.

### Exemple 6–7 Affichage des informations à propos de tous les tunnels

Dans cet exemple, un seul tunnel existe sur le système.

```
# dladm show-iptun
LINK    TYPE    FLAGS    LOCAL          REMOTE
tun0    6to4    --       192.168.35.10  --
```



```
vpn0      ipv4      --      10.8.48.149      192.1.2.3
```

### Exemple 6-8 Affichage de champs sélectionnés dans un format analysable

Dans cet exemple, seuls les champs spécifiques comportant des informations sur les tunnels sont affichés.

```
# dladm show-iptun -p -o link,type,local
tun0:6to4:192.168.35.10
vpn0:ipv4:10.8.48.149
```

## ▼ Affichage des propriétés d'un tunnel IP

### ● Affichez les propriétés de la liaison du tunnel.

```
# dladm show-linkprop [-c] [-o fields] [tunnel-link]
```

Vous pouvez utiliser les options avec la commande :

- c Affiche les informations dans une format analysable. Cet argument est facultatif.
- o *fields* Affiche les champs sélectionnés fournissant des informations spécifiques à propos des propriétés du lien.
- tunnel-link* Spécifie le tunnel dont vous souhaitez afficher les informations sur les propriétés. Cet argument est facultatif. Si vous omettez le nom de tunnel, la commande affiche les informations à propos de tous les tunnels du système.

### Exemple 6-9 Affichage des propriétés d'un tunnel

Cet exemple indique comment afficher toutes les propriétés d'une liaison de tunnel.

```
# dladm show-linkprop tun0
LINK    PROPERTY  PERM    VALUE    DEFAULT    POSSIBLE
tun0    autopush   --      --      --      --
tun0    zone       rw      --      --      --
tun0    state      r-      up      up      up,down
tun0    mtu        r-      65515   --      576-65495
tun0    maxbw      rw      --      --      --
tun0    cpus       rw      --      --      --
tun0    priority   rw      high    high    low,medium,high
tun0    hoplimit   rw      64      64      1-255
```

## ▼ Suppression d'un tunnel IP

- 1 Utilisez la syntaxe adéquate pour démonter l'interface configurée sur le tunnel en fonction du type de l'interface.

```
# ipadm delete-ip tunnel-link
```

---

**Remarque** – Pour supprimer un tunnel correctement, aucune interface IP existante ne peut être montée sur le tunnel.

---

- 2 Supprimez le tunnel IP.

```
# dladm delete-iptun tunnel-link
```

La seule option pour cette commande est `-t`, laquelle entraîne une suppression temporaire du tunnel. Le tunnel est restauré lors de la réinitialisation du système.

### Exemple 6–10 Suppression d'un tunnel IPv6 configuré avec une interface IPv6

Dans cet exemple, un tunnel persistant est supprimé définitivement.

```
# ipadm delete-ip ip6.tun0  
# dladm delete-iptun ip6.tun0
```

# Dépannage des problèmes de réseau

---

Ce chapitre apporte des solutions aux problèmes se produisant couramment sur les réseaux. Il aborde les sujets suivants :

- “Conseils d'ordre général pour le dépannage réseau” à la page 139
- “Problèmes courants lors du déploiement d'IPv6” à la page 140

## Conseils d'ordre général pour le dépannage réseau

L'un des premiers signes de problème sur un réseau est la perte de communication d'un ou plusieurs hôtes. S'il est impossible de communiquer avec un hôte qui vient d'être ajouté au réseau, le problème provient probablement des fichiers de configuration. La carte d'interface réseau peut également être en cause. En effet, si un seul hôte pose problème, la carte d'interface réseau est peut-être défectueuse. Si plusieurs hôtes du réseau peuvent communiquer entre eux, mais pas avec d'autres réseaux, le routeur ou un autre réseau peut être à l'origine du problème.

Vous pouvez utiliser la commande `ipadm` pour obtenir des informations sur les interfaces réseau. Exécutez la commande `netstat` pour afficher les tables de routage et les statistiques de protocoles. Les programmes tiers de diagnostic de réseau fournissent divers outils de dépannage. Pour plus d'informations, reportez-vous à la documentation de ces produits.

D'autres causes moins évidentes peuvent réduire les performances du réseau. Par exemple, l'outil `ping` permet de quantifier des problèmes tels que la perte de paquets par un hôte.

## Réalisation de diagnostics de base

Pour résoudre un problème de réseau, vous pouvez réaliser un certain nombre de vérifications logicielles et dépanner les problèmes élémentaires liés aux logiciels.

## ▼ Vérification logicielle de base sur un réseau

- 1 **Pour obtenir des informations sur le réseau, exécutez la commande `netstat`.**

Pour plus d'informations sur la commande `netstat` et sur sa syntaxe, reportez-vous à la section “[Contrôle du statut du réseau à l'aide de la commande `netstat`](#)” à la page 95 ainsi qu'à la page de manuel [netstat\(1M\)](#).

- 2 **Vérifiez la base de données `hosts` pour vous assurer que les entrées sont correctes et actuelles.**

Pour obtenir des informations sur la base de données `/etc/inet/hosts`, reportez-vous à la section “[Fichiers de configuration réseau](#)” à la page 143 et à la page de manuel [hosts\(4\)](#).

- 3 **Si vous exécutez le protocole RARP (Reverse Address Resolution Protocol), vérifiez les adresses Ethernet de la base de données `ethers` et assurez-vous que les entrées sont correctes et actuelles.**

- 4 **Essayez de vous connecter à l'hôte local au moyen de la commande `telnet`.**

Pour plus d'informations sur la commande `telnet` et sur sa syntaxe, reportez-vous à la page de manuel [telnet\(1\)](#).

- 5 **Assurez-vous que le démon réseau `inetd` est en cours d'exécution.**

```
# ps -ef | grep inetd
```

La sortie suivante permet de vérifier que le démon `inetd` est en cours d'exécution :

```
root 57 1 0 Apr 04 ? 3:19 /usr/sbin/inetd -s
```

- 6 **Si le protocole IPv6 est activé sur le réseau, assurez-vous que le démon IPv6 `in.ndpd` est en cours d'exécution :**

```
# ps -ef | grep in.ndpd
```

La sortie suivante permet de vérifier que le démon `in.ndpd` est en cours d'exécution :

```
root 123 1 0 Oct 27 ? 0:03 /usr/lib/inet/in.ndpd
```

## Problèmes courants lors du déploiement d'IPv6

Cette section décrit les problèmes que vous pouvez rencontrer lors du déploiement d'IPv6 sur votre site. Pour connaître les tâches de planification réelles, reportez-vous au [Chapitre 2](#), “[Éléments à prendre en compte lors de l'utilisation d'adresses IPv6](#)”.

## Impossible de mettre à niveau un routeur IPv4 vers IPv6

Si votre équipement ne peut pas être mis à niveau, vous devrez vous procurer un équipement compatible avec IPv6. Lisez attentivement la documentation du fabricant afin de connaître les procédures de prise en charge spécifiques à l'équipement.

Certains routeurs IPv4 ne peuvent pas être mis à niveau vers IPv6. Si votre topologie se trouve dans cette situation, raccordez un routeur IPv6 au routeur IPv4. Vous pourrez alors créer un tunnel sur le routeur IPv4 partant du routeur IPv6. Pour connaître les tâches de configuration de tunnels, reportez-vous à la section [“Configuration et administration du tunnel avec la commande `d\adm`”](#) à la page 126.

## Problèmes survenant après la mise à niveau de services vers IPv6

Vous pouvez rencontrer les problèmes suivants lors de la préparation des services au protocole IPv6 :

- Certaines applications préparées pour IPv6 ne prennent pas en charge IPv6 par défaut. Vous devez activer IPv6 sur ces applications pour que la prise en charge soit effective.
- Des problèmes peuvent survenir sur un serveur exécutant plusieurs types de services (certains ne prenant en charge qu'IPv4, d'autres prenant en charge IPv4 et IPv6). En effet, certains clients nécessitent l'utilisation de ces deux types de services, ce qui peut semer la confusion au niveau du serveur.

## Le FAI actuel ne prend pas en charge IPv6

Si vous envisagez de déployer IPv6 sur votre réseau alors que votre FAI actuel ne prend pas en charge l'adressage IPv6, vous pouvez remplacer votre FAI actuel ou opter pour l'un des choix suivants :

- Louer un FAI fournissant au site une seconde ligne dédiée aux communications IPv6. Cette solution est onéreuse.
- Acquérir un *FAI virtuel*. Les FAI virtuels fournissent un accès IPv6 sans connexion physique. La connexion s'effectue de fait par le biais d'un tunnel reliant le FAI virtuel et le site à travers le FAI IPv4.
- Créer un tunnel 6to4 vers d'autres sites IPv6 à travers le FAI actuel. Configurez l'adresse IPv4 enregistrée du routeur 6to4 en tant qu'entité topologique publique de l'adresse IPv6.

## Problèmes de sécurité lors de la création d'un tunnel vers un routeur relais 6to4

De par sa nature, un tunnel reliant un routeur 6to4 à un routeur relais 6to4 ne constitue pas une connexion sécurisée. Les problèmes de sécurité suivants sont inhérents à ce type de tunnel :

- Les routeurs relais 6to4 encapsulent et décapsulent des paquets, mais ne vérifient pas leur contenu.
- La mystification d'adresses est l'un des problèmes majeurs des tunnels sur routeurs relais 6to4. En effet, lorsque le routeur 6to4 reçoit des données du trafic entrant, il est incapable de faire correspondre l'adresse IPv4 du routeur relais et l'adresse IPv6 de la source. L'adresse de l'hôte IPv6 peut alors être facilement mystifiée. Il en va de même pour l'adresse du routeur relais 6to4.
- Par défaut, il n'existe aucun mécanisme de validation entre le routeur 6to4 et le routeur relais 6to4. Un routeur 6to4 ne peut donc pas déterminer si le routeur relais 6to4 est digne de confiance ou s'il est légitime. Une relation de confiance doit exister entre la source 6to4 et la destination IPv6 pour que ces deux sites ne s'exposent pas à d'éventuelles attaques.

Tous les problèmes de sécurité inhérents aux routeurs relais 6to4, y compris ceux cités précédemment, sont expliqués dans le brouillon Internet intitulé *Security Considerations for 6to4*. D'une manière générale, n'activez la prise en charge des routeurs relais 6to4 que dans l'un des cas suivants :

- Votre site 6to4 tente de communiquer avec un réseau IPv6 de confiance privé. Par exemple, activez la prise en charge du routeur relais 6to4 sur un réseau universitaire constitué de sites 6to4 isolés et de sites IPv6 natifs.
- Il est essentiel que votre site 6to4 communique avec certains hôtes IPv6 natifs.
- Vous avez implémenté les modèles de vérification et de validation suggérés dans le brouillon Internet intitulé *Security Considerations for 6to4*.

## Référence IPv4

---

Ce chapitre fournit des informations de référence sur les fichiers de configuration réseau pour les réseaux TCP/IP, notamment les types de réseau, leur objectif et le format d'entrée des fichiers.

Ce chapitre contient les informations suivantes :

- “Fichiers de configuration réseau” à la page 143
- “Démon de services Internet `inetd`” à la page 145
- “Service SMF `name-service/switch`” à la page 145
- “Protocoles de routage dans Oracle Solaris” à la page 147

## Fichiers de configuration réseau

Dans un réseau, les informations de configuration sont stockées dans différents fichiers et bases de données qui régulent le fonctionnement du réseau. Cette section fournit une brève description de ces fichiers. Certains fichiers nécessitent une mise à jour et de la maintenance lors de l'implémentation de modifications sur le réseau. D'autres fichiers ne nécessitent que peu, voire pas d'administration.

<code>/etc/defaultrouter</code>	Ce fichier contient les noms d'interface IP des routeurs directement connectés au réseau. L'existence de ce fichier dans le système est facultative. Si le fichier existe, le système est alors configuré pour prendre en charge le routage statique.
<code>/etc/inet/hosts</code>	Ce fichier contient les adresses IPv4 dans le réseau ainsi que les noms d'interface correspondantes sur lesquelles les adresses sont configurées. Si vous utilisez un service de noms NIS ou DNS, ou le service de répertoire LDAP, les informations de l'hôte sont alors stockées dans une base de données différente, comme <code>hosts.byname</code> , qui existe dans les serveurs. Pour plus

	d'informations, reportez-vous au manuel <i>Oracle Solaris Administration: Naming and Directory Services</i> .
<code>/etc/inet/netmasks</code>	Ce fichier contient le numéro de réseau, par exemple 192 . 168 . 0 . 0, ainsi que les informations de masque de réseau pour ce numéro de réseau, par exemple 255 . 255 . 0 . 0. Dans un réseau utilisant NIS ou LDAP, ces informations sont stockées dans une base de données de masque de réseau, dans les serveurs. Reportez-vous à la page de manuel <a href="#">netmasks(4)</a> pour plus d'informations.
<code>/etc/bootparams</code>	Ce fichier contient des paramètres qui déterminent les processus d'initialisation pour les systèmes configurés pour s'initialiser en mode client réseau. Pour plus d'informations reportez-vous à la section “ <a href="#">Modes de configuration système</a> ” à la page 51. Ce fichier est la base pour la création de la base de données <code>bootparams</code> utilisée par le service de noms si vous n'utilisez pas le mode de fichiers locaux. Pour obtenir des informations spécifiques sur le contenu et le format de ce fichier, reportez-vous à la page de manuel <a href="#">bootparams(4)</a> .
<code>/etc/ethers</code>	Le fichier associe les noms d'hôtes à leurs adresses MAC. Le fichier est la base de la création d'une base de données <code>ethers</code> en vue d'une utilisation dans le réseau où les systèmes sont configurés en tant que clients réseau. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">ethers(4)</a> .
<code>/etc/inet/networks</code>	Ce fichier associe les noms de réseau et les numéros de réseau. Il est possible d'ajouter des commentaires pour clarifier davantage chaque entrée dans la base de données. Ce fichier permet aux applications d'utiliser et d'afficher les noms plutôt que les numéros de réseau. Par exemple, le programme <code>netstat</code> utilise les informations de cette base de données pour générer les tables d'état. Tous les sous-réseaux qui se connectent au réseau local par l'intermédiaire de routeurs doivent être inclus dans ce fichier. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">networks(4)</a> .
<code>/etc/inet/protocols</code>	Ce fichier répertorie les protocoles TCP/IP installés sur votre système ainsi que leurs numéros de protocole. Ce fichier requiert rarement des tâches d'administration. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">protocols(4)</a> .
<code>/etc/inet/services</code>	Ce fichier répertorie les noms des services TCP et UDP ainsi que leurs numéros de ports connus. Cette liste est employée par les programmes faisant appel aux services réseau. En général, ce fichier ne requiert aucune tâche d'administration. Pour plus



d'informations, reportez-vous à la page de manuel [services\(4\)](#).

## Démon de services Internet inetd

Le démon `inetd` lance les services Internet standard à l'initialisation du système et peut redémarrer un service lorsque le système est en cours d'exécution. Le SMF (Service Management Facility, utilitaire de gestion de service) permet de modifier les services Internet standard et d'indiquer au démon `inetd` de démarrer d'autres services, le cas échéant.

Exécutez les commandes SMF suivantes pour gérer les services démarrés par `inetd` :

<code>svcadm</code>	Permet d'effectuer des tâches administratives sur un service, telle que l'activation, la désactivation et le redémarrage. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">svcadm(1M)</a> .
<code>svcs</code>	Permet d'effectuer des requêtes relatives au statut d'un service. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">svcs(1)</a> .
<code>inetadm</code>	Permet d'afficher et modifier les propriétés d'un service. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">inetadm(1M)</a> .

La valeur du champ `proto` dans le profil `inetadm` d'un service particulier indique le protocole de couche de transport sur lequel le service s'exécute. Si le service gère exclusivement des requêtes IPv4, le champ `proto` doit être défini sur `tcp`, `udp` ou `sctp`.

- Pour plus d'informations sur l'utilisation des commandes SMF, reportez-vous à la section “[Utilitaires d'administration en ligne de commande SMF](#)” du manuel *Administration d'Oracle Solaris : Tâches courantes*.
- Pour une tâche utilisant les commandes SMF afin d'ajouter un service s'exécutant sur SCTP, reportez-vous à la section “[Ajout de services utilisant le protocole SCTP](#)” à la page 71.
- Pour obtenir des informations sur l'ajout de services gérant à la fois des requêtes IPv4 et des requêtes IPv6, reportez-vous à la section “[Démon de services Internet inetd](#)” à la page 145

## Service SMF name-service/switch

Le service SMF `name-service/switch` définit l'ordre de recherche des bases de données réseau pour les informations de configuration. Certaines informations de configuration réseau qui étaient auparavant stockées dans des fichiers de configuration, comme le domaine par défaut, ont été converties pour devenir des propriétés de ce service SMF. Les propriétés de ce service SMF déterminent l'implémentation des services de noms sur le système. Les propriétés sont les suivantes :

```
% svccfg -s name-service/switch listprop config
config                                application
config/value_authorization           solaris.smf.value.name-service.switch
config/default                       files
config/password                     "files nis"
config/group                         "files nis"
config/host                          "files dns nis"
config/network                      "nis [NOTFOUND=return] files"
config/protocol                     "nis [NOTFOUND=return] files"
config/rpc                          "nis [NOTFOUND=return] files"
config/ether                        "nis [NOTFOUND=return] files"
config/netmask                      "files nis"
config/bootparam                    "nis [NOTFOUND=return] files"
config/publickey                    "nis [NOTFOUND=return] files"
config/netgroup                     nis
config/automount                    "files nis"
config/alias                        "files nis"
config/service                      "files nis"
config/printer                      "user nis"
config/auth_attr                    "files nis"
config/prof_attr                    "files nis"
config/project                      "files nis"
```

Les valeurs définies pour chacune des propriétés déterminent dans quel service de noms rechercher les informations qui auraient une incidence sur les utilisateurs réseau, par exemple les mots de passe, les alias ou encore les masques réseau. Dans cet exemple, les propriétés de montage automatique et de mot de passe sont définies sur `files` et `nis`. Par conséquent, les informations de montage automatique et de mot de passe s'obtiennent à partir des fichiers et du service NIS.

Si vous souhaitez passer d'un service de noms à un autre, vous devez définir les propriétés adéquates du service SMF `name-service/switch` pour activer le service de noms sélectionné.

Par exemple, supposons que vous souhaitez utiliser le service de noms LDAP sur votre réseau. Les propriétés suivantes du service SMF doivent être configurées.

- `config/default` doit être défini afin d'utiliser les fichiers et LDAP.
- `config/host` doit être défini afin d'utiliser les fichiers et DNS.
- `config/netgroup` doit être défini afin d'utiliser LDAP.
- `config/printer` doit être défini afin d'utiliser l'utilisateur, les fichiers et LDAP.

Par conséquent, vous devez saisir les commandes suivantes pour définir ces propriétés correctement.

```
# svccfg -s name-service/switch setprop config/default = astring: "files ldap"
# svccfg -s name-service/switch setprop config/host = astring: "files dns"
# svccfg -s name-service/switch setprop config/netgroup = astring: "ldap"
# svccfg -s name-service/switch setprop config/printer = astring: "user files ldap"
# svccfg -s name-service/switch:default refresh
```

Pour obtenir des informations détaillées sur le commutateur de service de noms, reportez-vous au manuel *Oracle Solaris Administration: Naming and Directory Services*.

## Impact des services de noms sur les bases de données réseau

Le format de la base de données réseau dépend du type de service de noms sélectionné pour votre réseau. Par exemple, la base de données `hosts` contient au moins le nom d'hôte et l'adresse IPv4 du système local, ainsi que toute interface réseau directement connectée au système local. Cependant, la base de données `hosts` peut contenir d'autres adresses IPv4 et noms d'hôtes, selon le type de service de noms utilisé sur le réseau.

Les bases de données réseau sont utilisées comme suit :

- Les réseaux qui utilisent les fichiers locaux pour leurs services de noms se basent sur les fichiers dans les répertoires `/etc/inet` et `/etc`.
- NIS utilise des bases de données appelées cartes NIS.
- DNS utilise des enregistrements dotés d'informations d'hôte.

---

**Remarque** – Les fichiers d'initialisation et de données DNS ne correspondent pas directement aux bases de données réseau.

---

Reportez-vous au document *Oracle Solaris Administration: Naming and Directory Services* pour obtenir des informations sur les correspondances de bases de données réseau dans NIS, DNS et LDAP.

## Protocoles de routage dans Oracle Solaris

Cette section décrit les protocoles de routage pris en charge par Oracle Solaris: RIP (Routing Information Protocol, protocole d'informations de routage) et RDISC (ICMP Router Discovery, détection de routeur ICMP). RIP et RDISC constituent des protocoles TCP/IP standard. Pour obtenir des listes complètes des protocoles de routage disponibles dans Oracle Solaris, reportez-vous au [Tableau 8-1](#) et au [Tableau 8-2](#).

### RIP (Routing Information Protocol)

Le protocole RIP est implémenté par le démon de routage `in.routed` qui démarre à l'initialisation du système. Exécuté sur un routeur avec l'option `s`, le démon `in.routed`

renseigne la table de routage du noyau en indiquant une route pour chaque réseau accessible et publie l'accessibilité via toutes les interfaces réseau.

Exécuté sur un hôte avec l'option `q`, le démon `in.routed` extrait les informations de routage mais ne publie pas l'accessibilité. Sur les hôtes, vous pouvez extraire les informations de routage de deux façons :

- Ne spécifiez *pas* l'indicateur `S` (`S` majuscule : mode d'économie d'espace). `in.routed` construit une table de routage complète exactement de la même manière que sur un routeur.
- Spécifiez l'indicateur `S`. `in.routed` crée une table de routage minimale pour le noyau, contenant une seule route par défaut pour chaque routeur disponible.

## Protocole RDISC (ICMP Router Discovery)

Les hôtes utilisent RDISC pour obtenir les informations de routage des autres routeurs. Par conséquent, lorsque les hôtes exécutent RDISC, les routeurs doivent également exécuter un autre protocole, par exemple RIP, afin d'échanger les informations de routeur.

RDISC est implémenté par le démon `in.routed`, qui doit s'exécuter à la fois sur les routeurs et sur les hôtes. Sur les hôtes, `in.routed` utilise RDISC pour détecter les routes par défaut des routeurs qui se publient eux-mêmes via RDISC. Sur les routeurs, `in.routed` utilise RDISC pour publier les routes par défaut des hôtes sur les réseaux directement connectés. Reportez-vous aux pages de manuel [in.routed\(1M\)](#) et [gateways\(4\)](#).

## Tableaux des protocoles de routage dans Oracle Solaris

Le tableau suivant répertorie tous les protocoles de routage pris en charge dans Oracle Solaris.

TABLEAU 8-1 Protocoles de routage d'Oracle Solaris

Protocole	Démon associé	Description	Voir
RIP (Routing Information Protocol)	<code>in.routed</code>	IGP acheminant les paquets IPv4 et gérant une table de routage	<a href="#">“Procédure de configuration d'un routeur IPv4” à la page 57</a>
Détection de routeur ICMP (Internet Control Message Protocol)	<code>in.routed</code>	Permet aux hôtes de détecter la présence d'un routeur sur le réseau	<a href="#">“Activation du routage statique sur un hôte à interface unique” à la page 65</a> et <a href="#">“Activation du routage dynamique sur un système à interface unique” à la page 67</a>

**TABLEAU 8-1** Protocoles de routage d'Oracle Solaris (Suite)

Protocole	Démon associé	Description	Voir
Protocole RIPng (Routing Information Protocol, next generation, protocole d'informations de routage, nouvelle génération)	in.ripngd	IGP acheminant les paquets IPv6 et gérant une table de routage	<a href="#">“Procédure de configuration d'un routeur compatible IPv6” à la page 80</a>
Protocole ND (Neighbor Discovery)	in.ndpd	Signale la présence d'un routeur IPv6 et détecte les hôtes IPv6 sur un réseau	<a href="#">“Configuration d'une interface IPv6” à la page 77</a>

Le tableau suivant répertorie tous les protocoles Quagga également pris en charge dans Oracle Solaris.

**TABLEAU 8-2** Protocoles Quagga OpenSolaris

Protocole	Démon	Description
Protocole RIP	ripd	Protocole IGP à vecteur de distance IPv4 qui achemine les paquets IPv4 et signale sa table de routage aux routeurs adjacents.
RIPng	ripngd	Protocole IGP à vecteur de distance IPv6 qui achemine les paquets IPv6 et gère une table de routage.
Protocole OSPF (Open Shortest Path First)	ospfd	Protocole IGP d'état des liens IPv4 pour le routage des paquets et la mise en réseau à haute disponibilité.
BGP (Border Gateway Protocol)	bgpd	Protocole EGP IPv4 et IPv6 pour le routage d'un domaine administratif à l'autre.



## Référence IPv6

---

Ce chapitre contient des informations de référence concernant l'implémentation du protocole IPv6 sous Oracle Solaris.

- [“Implémentation IPv6 sous Oracle Solaris” à la page 151](#)
- [“Protocole ND IPv6” à la page 163](#)
- [“Routage IPv6” à la page 170](#)
- [“Extensions IPv6 de services d'assignation de noms Oracle Solaris” à la page 171](#)
- [“Prise en charge IPv6 de NFS et RPC” à la page 172](#)
- [“Prise en charge d'IPv6 sur ATM” à la page 172](#)

Pour une présentation d'IPv6, reportez-vous au [Chapitre 3, “Présentation d'IPv6” du manuel \*Guide d'administration système : services IP\*](#) Les tâches de configuration d'un réseau compatible IPv6 sont décrites au [Chapitre 4, “Activation d'IPv6 sur le réseau”](#). Pour obtenir des informations sur les tunnels IP, reportez-vous au [Chapitre 6, “Configuration de tunnels IP”](#).

## Implémentation IPv6 sous Oracle Solaris

Cette section décrit les fichiers, commandes et démons nécessaires au protocole IPv6 sous Oracle Solaris. Pour une présentation détaillée des adresses IPv6 et du format d'en-tête IPv6, reportez-vous à la section [“Notions approfondies sur les formats d'adressage IPv6” du manuel \*Guide d'administration système : services IP\*](#).

### Fichiers de configuration IPv6

Cette section décrit les fichiers de configuration faisant partie de l'implémentation IPv6 :

- [“Fichier de configuration `ndpd.conf`” à la page 152](#)
- [“Fichier de configuration `/etc/inet/ipaddrsel.conf`” à la page 155](#)

## Fichier de configuration ndpd.conf

Le fichier de configuration `/etc/inet/ndpd.conf` sert à configurer les options utilisées par le démon Neighbor Discovery `in.ndpd`. Pour un routeur, `ndpd.conf` sert principalement à configurer le préfixe du site à publier vers le lien. Pour un hôte, `ndpd.conf` sert à désactiver la configuration automatique des adresses ou à configurer des adresses temporaires.

Le tableau suivant présente les mots-clés utilisés dans le fichier `ndpd.conf`.

TABLEAU 9-1 Mots-clés de `/etc/inet/ndpd.conf`

Variable	Description
<code>ifdefault</code>	Spécifie le comportement du routeur pour toutes les interfaces. Utilisez la syntaxe suivante pour définir les paramètres du routeur et les valeurs correspondantes :  <code>ifdefault [valeur variable]</code>
<code>prefixdefault</code>	Spécifie le comportement par défaut pour la publication du préfixe. Utilisez la syntaxe suivante pour définir les paramètres du routeur et les valeurs correspondantes :  <code>prefixdefault [valeur variable]</code>
<code>if</code>	Définit les paramètres de l'interface. Utilisez la syntaxe suivante :  <code>if interface [valeur variable]</code>
<code>prefix</code>	Publie les informations du préfixe par interface. Utilisez la syntaxe suivante :  <code>prefix préfixe/longueur interface [valeur variable]</code>

Dans le fichier `ndpd.conf`, vous utilisez des mots-clés du tableau avec jeu de variables de configuration du routeur. Ces variables sont définies en détail dans le document [RFC 2461, Neighbor Discovery for IP Version 6 \(IPv6\)](http://www.ietf.org/rfc/rfc2461.txt?number=2461) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>).

Le tableau suivant répertorie les variables de configuration d'une interface et fournit une brève définition de chacune.

TABLEAU 9-2 Variables de configuration d'interface du fichier `/etc/inet/ndpd.conf`

Variable	Par défaut	Définition
<code>AdvRetransTimer</code>	0	Spécifie la valeur du champ Retrans Timer pour la publication de messages envoyés par le routeur.
<code>AdvCurHopLimit</code>	Diamètre actuel du réseau Internet	Spécifie la valeur à entrer dans le champ Hop Limit pour la publication de messages envoyés par le routeur.
<code>AdvDefaultLifetime</code>	3 + <code>MaxRtrAdvInterval</code>	Spécifie la durée de vie par défaut des publications du routeur.



TABLEAU 9-2 Variables de configuration d'interface du fichier `/etc/inet/ndpd.conf` (Suite)

Variable	Par défaut	Définition
AdvLinkMTU	0	Spécifie une valeur d'unité de transmission maximale (MTU) que le routeur doit envoyer. Une valeur nulle indique que le routeur ne spécifie pas d'options MTU.
AdvManaged Flag	False	Spécifie la valeur à entrer dans l'indicateur de configuration de la gestion des adresses pour la publication du routeur.
AdvOtherConfigFlag	False	Spécifie la valeur à entrer dans l'indicateur de configuration des autres paquets avec état pour la publication du routeur.
AdvReachableTime	0	Spécifie la valeur du champ Reachable Time pour la publication de messages envoyés par le routeur.
AdvSendAdvertisements	False	Indique si le noeud doit envoyer des publications et répondre aux requêtes du routeur. Vous devez définir explicitement la variable sur TRUE dans le fichier <code>ndpd.conf</code> afin d'activer les fonctions de publication du routeur. Pour plus d'informations, reportez-vous à la section <a href="#">“Procédure de configuration d'un routeur compatible IPv6”</a> à la page 80.
DupAddrDetect Transmits	1	Définit le nombre de messages de requête voisine consécutifs que le protocole Neighbor Discovery doit envoyer lors de la détection d'adresses du noeud local dupliquées.
MaxRtrAdvInterval	600 secondes	Spécifie le temps d'attente maximal lors de l'envoi de publications de multidiffusion non requises.
MinRtrAdvInterval	200 secondes	Spécifie le temps d'attente minimal lors de l'envoi de publications de multidiffusion non requises.
StatelessAddrConf	True	Détermine si le noeud configure son adresse IPv6 par le biais de la configuration automatique des adresses sans état. Si la valeur False est déclarée dans le fichier <code>ndpd.conf</code> , l'adresse doit être configurée manuellement. Pour plus d'informations, reportez-vous à la section <a href="#">“Procédure de configuration d'un jeton IPv6 spécifié par l'utilisateur”</a> à la page 86.
TmpAddrsEnabled	False	Indique si une adresse temporaire doit être créée pour toutes les interfaces ou pour une interface particulière d'un noeud. Pour plus d'informations, reportez-vous à la section <a href="#">“Procédure de configuration d'une adresse temporaire”</a> à la page 84.
TmpMaxDesyncFactor	600 secondes	Spécifie une valeur aléatoire à soustraire de la variable de durée de vie préférée <code>TmpPreferredLifetime</code> au démarrage de la commande <code>in.ndpd</code> . L'objectif de la variable <code>TmpMaxDesyncFactor</code> est d'éviter que tous les systèmes de votre réseau ne régénèrent leurs adresses temporaires en même temps. <code>TmpMaxDesyncFactor</code> permet de remplacer la limite supérieure par cette valeur.

TABLEAU 9-2 Variables de configuration d'interface du fichier /etc/inet/ndpd.conf (Suite)

Variable	Par défaut	Définition
TmpPreferredLifetime	False	Définit la durée de vie préférée d'une adresse temporaire. Pour plus d'informations, reportez-vous à la section “Procédure de configuration d'une adresse temporaire” à la page 84.
TmpRegenAdvance	False	Spécifie à l'avance la durée d'obtention d'une désapprobation pour une adresse temporaire. Pour plus d'informations, reportez-vous à la section “Procédure de configuration d'une adresse temporaire” à la page 84.
TmpValidLifetime	False	Définit la durée de vie correcte d'une adresse temporaire. Pour plus d'informations, reportez-vous à la section “Procédure de configuration d'une adresse temporaire” à la page 84.

Le tableau suivant répertorie les variables utilisées pour configurer les préfixes IPv6.

TABLEAU 9-3 Variables de configuration de préfixe du fichier /etc/inet/ndpd.conf

Variable	Par défaut	Définition
AdvAutonomousFlag	True	Spécifie la valeur à entrer dans le champ Autonomous Flag figurant dans les informations sur le préfixe.
AdvOnLinkFlag	True	Spécifie la valeur à entrer dans l'indicateur on-link "L-bit" figurant dans les informations sur le préfixe.
AdvPreferredExpiration	Non définie	Spécifie la date d'expiration préférée du préfixe.
AdvPreferredLifetime	604 800 secondes	Spécifie la valeur à entrer pour la durée de vie préférée dans les informations sur le préfixe.
AdvValidExpiration	Non définie	Spécifie la date d'expiration correcte du préfixe.
AdvValidLifetime	2 592 000 secondes	Spécifie la durée de vie correcte du préfixe qui est configurée.

EXEMPLE 9-1 Fichier /etc/inet/ndpd.conf

L'exemple suivant répertorie les mots-clés et les variables de configuration utilisés dans le fichier ndpd.conf. Supprimez le commentaire (#) pour activer la variable.

```
# ifdefault      [variable-value ]*
# prefixdefault [variable-value ]*
# if ifname      [variable-value ]*
# prefix prefix/length ifname
#
# Per interface configuration variables
#
#DupAddrDetectTransmits
#AdvSendAdvertisements
#MaxRtrAdvInterval
#MinRtrAdvInterval
```

**EXEMPLE 9-1** Fichier /etc/inet/ndpd.conf (Suite)

```

#AdvManagedFlag
#AdvOtherConfigFlag
#AdvLinkMTU
#AdvReachableTime
#AdvRetransTimer
#AdvCurHopLimit
#AdvDefaultLifetime
#
# Per Prefix: AdvPrefixList configuration variables
#
#
#AdvValidLifetime
#AdvOnLinkFlag
#AdvPreferredLifetime
#AdvAutonomousFlag
#AdvValidExpiration
#AdvPreferredExpiration

ifdefault AdvReachableTime 30000 AdvRetransTimer 2000
prefixdefault AdvValidLifetime 240m AdvPreferredLifetime 120m

if qe0 AdvSendAdvertisements 1
prefix 2:0:0:56::/64 qe0
prefix fec0:0:0:56::/64 qe0

if qe1 AdvSendAdvertisements 1
prefix 2:0:0:55::/64 qe1
prefix fec0:0:0:56::/64 qe1

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:1::/64 qfe0

if hme1 AdvSendAdvertisements 1
prefix 2002:8192:56bb:2::/64 hme1

```

**Fichier de configuration /etc/inet/ipaddrsel.conf**

Le fichier /etc/inet/ipaddrsel.conf contient la table des règles de sélection d'adresse IPv6 par défaut. Si vous avez activé le protocole IPv6 lors de l'installation d'Oracle Solaris, ce fichier contient les éléments présentés dans le [Tableau 9-4](#).

Vous pouvez modifier le contenu de /etc/inet/ipaddrsel.conf. Toutefois, cette opération n'est pas recommandée. Si cela s'avère nécessaire, reportez-vous à la procédure décrite à la section “[Administration de la table des règles de sélection d'adresses IPv6](#)” à la page 114. Pour plus d'informations sur le fichier ipaddrsel.conf, reportez-vous à la section “[Raisons pour lesquelles le tableau des règles de sélection d'adresses IPv6 doit être modifié](#)” à la page 156 ainsi qu'à la page de manuel [ipaddrsel.conf\(4\)](#).

# Commandes associées à IPv6

Cette section décrit les commandes ajoutées lors de l'implémentation du protocole IPv6 sous Oracle Solaris. Les commandes existantes qui ont été modifiées pour prendre en charge IPv6 y sont également détaillées.

## Commande ipaddrsel

La commande `ipaddrsel` permet de modifier le tableau des règles de sélection des adresses IPv6 par défaut.

Le noyau Oracle Solaris utilise la table des règles de sélection des adresses IPv6 par défaut pour le classement des adresses de destination et la sélection des adresses sources pour les en-têtes de paquet IPv6. Le fichier `/etc/inet/ipaddrsel.conf` contient ce tableau de règles.

Le tableau suivant répertorie les formats d'adresse par défaut ainsi que les priorités de chacune telles qu'elles doivent figurer dans le tableau de règles. Vous pouvez rechercher des informations techniques sur la sélection d'adresses IPv6 dans la page de manuel [inet6\(7P\)](#).

TABLEAU 9–4 Tableau des règles de sélection des adresses IPv6 par défaut

Préfixe	Priorité	Définition
::1/128	50	Loopback
::/0	40	Par défaut
2002::/16	30	6to4
::/96	20	IPv4 Compatible
::ffff:0:0/96	10	IPv4

Dans ce tableau, les préfixes IPv6 (: : 1/128 et : : /0) ont la priorité sur les adresses 6to4 (2002 : : /16) et les adresses IPv4 (: : /96 et : : ffff:0:0/96). Par conséquent, le noyau choisit par défaut l'adresse IPv6 globale de l'interface pour les paquets envoyés vers une autre destination IPv6. L'adresse IPv4 de l'interface est moins prioritaire, notamment pour les paquets envoyés vers une destination IPv6. Etant donné l'adresse IPv6 source sélectionnée, le noyau utilise également le format IPv6 pour l'adresse de destination.

## Raisons pour lesquelles le tableau des règles de sélection d'adresses IPv6 doit être modifié

En règle générale, le tableau des règles de sélection d'adresses IPv6 par défaut n'a pas besoin d'être modifié. En cas de modification nécessaire, exécutez la commande `ipaddrsel`.

Les situations suivantes nécessitent une modification du tableau :

- Si le système possède une interface qui est utilisée pour un tunnel 6to4, vous pouvez définir une priorité plus élevée pour les adresses 6to4.
- Si vous souhaitez qu'une adresse source particulière communique avec une adresse de destination particulière, vous pouvez ajouter ces adresses au tableau de règles. Ensuite, vous pouvez les marquer comme vos adresses préférées à l'aide de la commande `ipadm`. Pour plus d'informations sur la commande `ipadm`, reportez-vous à la page de manuel [ipadm\(1M\)](#).
- Si vous voulez que les adresses IPv4 aient la priorité sur les adresses IPv6, vous pouvez remplacer la priorité de `::ffff:0:0/96` par un chiffre plus élevé.
- Si vous devez assigner une priorité plus élevée à des adresses désapprouvées, vous pouvez ajouter ces adresses au tableau de règles. Prenons l'exemple des adresses de site locales, actuellement désapprouvées sur le réseau IPv6. Ces adresses possèdent le préfixe `fec0::/10`. Vous pouvez modifier le tableau de règles afin de définir une priorité plus élevée pour ces adresses.

Pour plus d'informations sur la commande `ipaddrsel`, reportez-vous à la page de manuel [ipaddrsel\(1M\)](#).

## Commande 6to4relay

La *création de tunnel 6to4* permet à des sites 6to4 isolés de communiquer. Cependant, pour transférer des paquets vers un site IPv6 natif et non-6to4, le routeur 6to4 doit être relié au routeur relais 6to4 par un tunnel. Le *routeur relais 6to4* transfère ensuite les paquets 6to4 au réseau IPv6 et, finalement, au site IPv6 natif. Si un site 6to4 doit échanger des données avec un site IPv6, vous pouvez créer le tunnel approprié à l'aide de la commande `6to4relay`.

Sous Oracle Solaris, la liaison de tunnels à des routeurs relais est désactivée car l'utilisation des routeurs relais n'est pas sécurisée. Avant de relier un tunnel à un routeur relais 6to4, vous devez être conscient des problèmes qui peuvent survenir avec ce type de scénario. Pour plus d'informations sur les routeurs relais 6to4, reportez-vous à la section “[Informations importantes pour la création de tunnels vers un routeur relais 6to4](#)” à la page 122. Pour activer la prise en charge d'un routeur relais 6to4, vous pouvez suivre la procédure indiquée à la section “[Création et configuration d'un tunnel IP](#)” à la page 127.

## Syntaxe de la commande 6to4relay

La commande `6to4relay` possède la syntaxe suivante :

```
6to4relay -e [-a IPv4-address] -d -h
```

-e Assure la prise en charge de tunnels entre le routeur 6to4 et un routeur relais 6to4 anycast. Ainsi, l'adresse du point d'extrémité du tunnel est définie sur 192.88.99.1, soit l'adresse du groupe anycast de routeurs relais 6to4.

- a *IPv4-address* Assure la prise en charge de tunnels entre le routeur 6to4 et un routeur relais 6to4 possédant l'*IPv4-address* spécifiée.
- d Désactive la prise en charge de tunnels vers un routeur relais 6to4 (paramètre par défaut d'Oracle Solaris).
- h Affiche l'aide concernant la commande 6to4relay.

Pour plus d'informations, reportez-vous à la page de manuel 6to4relay(1M).

**EXEMPLE 9-2** Affichage par défaut du statut de la prise en charge de routeurs relais 6to4

La commande 6to4relay, sans argument, affiche le statut actuel de la prise en charge des routeurs relais 6to4. Cet exemple indique la sortie par défaut de l'implémentation du protocole IPv6 sous Oracle Solaris.

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is disabled
```

**EXEMPLE 9-3** Affichage du statut avec prise en charge des routeurs relais 6to4 activée

Lorsque la prise en charge des routeurs relais est activée, la commande 6to4relay affiche la sortie suivante :

```
# /usr/sbin/6to4relay
6to4relay:6to4 Relay Router communication support is enabled
IPv4 destination address of Relay Router=192.88.99.1
```

**EXEMPLE 9-4** Affichage du statut avec un routeur relais 6to4 spécifié

Si vous spécifiez l'option -a et une adresse IPv4 dans la commande 6to4relay, l'adresse IPv4 fournie avec l'option -a remplace l'adresse 192.88.99.1.

La commande 6to4relay ne signale pas l'exécution des options -d, -e et -a *IPv4 address*. Cependant, 6to4relay n'affiche aucun message d'erreur lié à l'exécution de ces options.

## Modification de la commande netstat en vue de la prise en charge IPv6

La commande netstat affiche le statut des réseaux IPv4 et IPv6. Vous pouvez choisir les informations de protocole à afficher en définissant la valeur de DEFAULT\_IP dans le fichier /etc/default/inet\_type ou en utilisant l'option -f dans la ligne de commande. Avec une valeur de DEFAULT\_IP permanente, vous vous assurez que la commande netstat affiche uniquement les informations IPv4. Vous pouvez ignorer ce paramètre et utiliser l'option -f. Pour plus d'informations sur le fichier inet\_type, reportez-vous à la page de manuel [inet\\_type\(4\)](#).

L'option -p de la commande netstat affiche la table des connexions réseau-média, c'est-à-dire la table des protocoles de résolution d'adresse pour l'IPv4 et le cache voisin pour l'IPv6. Pour

plus d'informations, reportez-vous à la page de manuel [netstat\(1M\)](#) La section “Affichage du statut des sockets” à la page 98 décrit les procédures impliquant l'exécution de cette commande.

## Modification de la commande snoop en vue de la prise en charge IPv6

La commande snoop permet de capturer des paquets IPv4 et IPv6. Cette commande peut s'afficher avec des en-têtes IPv6, des en-têtes d'extension IPv6, des en-têtes ICMPv6 et des données de protocole Neighbor Discovery. Par défaut, la commande snoop affiche les deux types de paquet (IPv4 et IPv6). Pour afficher soit l'un, soit l'autre, spécifiez le mot-clé de protocole ip ou ip6 avec la commande snoop. L'option de filtrage IPv6 vous permet de filtrer tous les paquets IPv4 et IPv6 et d'afficher uniquement les paquets IPv6. Pour plus d'informations, reportez-vous à la page de manuel [snoop\(1M\)](#) La section “Contrôle du trafic réseau IPv6” à la page 110 décrit les procédures impliquant l'exécution de la commande snoop.

## Modification de la commande route en vue de la prise en charge IPv6

La commande route fonctionne sur les routes IPv4 (par défaut) et IPv6. Pour réaliser des opérations sur les routes IPv6, tapez l'option -inet6 immédiatement à la suite de la commande route dans la ligne de commande. Pour plus d'informations, reportez-vous à la page de manuel [route\(1M\)](#).

## Modification de la commande ping en vue de la prise en charge IPv6

La commande ping se sert des protocoles IPv4 et IPv6 pour sonder les hôtes cibles. Le choix du protocole dépend des adresses renvoyées par le serveur de noms pour l'hôte cible spécifique. Par défaut, si ce serveur renvoie une adresse IPv6 pour l'hôte cible, la commande ping utilise le protocole IPv6. S'il renvoie une adresse IPv4, la commande ping utilise le protocole IPv4. Pour ignorer cette action, vous pouvez taper l'option -A dans la ligne de commande et spécifier le protocole à utiliser.

Pour plus d'informations, reportez-vous à la page de manuel [ping\(1M\)](#) La section “Test des hôtes distants à l'aide de la commande ping” à la page 102 décrit les procédures impliquant l'exécution de la commande ping .

## Modification de la commande traceroute en vue de la prise en charge IPv6

Vous pouvez exécuter la commande traceroute pour tracer les routes IPv4 et IPv6 vers un hôte spécifique. Du point de vue du protocole, traceroute utilise le même algorithme que la commande ping. Pour ignorer ce choix, tapez l'option -A dans la ligne de commande. Vous pouvez tracer chaque route vers chaque adresse d'un hôte multiréseau en tapant l'option -a dans la ligne de commande.

Pour plus d'informations, reportez-vous à la page de manuel [traceroute\(1M\)](#) La section “Affichage des informations de routage à l'aide de la commande `traceroute`” à la page 106 décrit les procédures qui impliquent l'exécution de la commande `traceroute`.

## Démons liés à IPv6

Cette section présente les démons liés à IPv6.

### Démon `in.ndpd` pour Neighbor Discovery

Le démon `in.ndpd` implémente le protocole IPv6 Neighbor Discovery ainsi que celui de découverte de routeur. Il implémente également la configuration automatique d'adresse IPv6. Les options suivantes sont prises en charge par `in.ndpd`.

- d Active le débogage.
- D Active le débogage dans le cadre d'événements spécifiques.
- f Spécifie un fichier de données de configuration spécifique au lieu du fichier `/etc/inet/ndpd.conf`.
- I Imprime les informations associées à chaque interface.
- n Ne met pas en boucle les publications du routeur.
- r Ignore la réception de paquets.
- v Spécifie le mode détaillé en faisant état de plusieurs types de message de diagnostic.
- t Active le suivi des paquets.

Le démon `in.ndpd` est contrôlé par les paramètres définis dans le fichier de configuration `/etc/inet/ndpd.conf` et par ceux du fichier de démarrage `/var/inet/ndpd_state.interface` qui s'appliquent.

Lorsque le fichier `/etc/inet/ndpd.conf` existe, il est analysé et utilisé pour configurer un noeud en tant que routeur. Le [Tableau 9–1](#) répertorie les mots-clés corrects susceptibles de figurer dans ce fichier. Lors de l'initialisation d'un hôte, les routeurs risquent de ne pas être disponibles immédiatement. Les paquets publiés par le routeur risquent d'être abandonnés. En outre, les paquets risquent de ne pas atteindre l'hôte.

Le fichier `/var/inet/ndpd_state.interface` est un fichier d'état. Ce fichier est régulièrement mis à jour par chaque noeud. En cas de défaillance et de redémarrage du noeud, ce dernier peut configurer ses interfaces en l'absence de routeurs. Ce fichier contient l'adresse de l'interface, l'heure de la dernière mise à jour du fichier et la durée de validité du fichier. Il contient également d'autres paramètres “hérités” de précédentes publications de routeur.



---

**Remarque** – Il est inutile de modifier le contenu des fichiers d'état. Le démon `in.ndpd` assure la maintenance automatique des fichiers d'état.

---

Consultez les pages de manuel `in.ndpd(1M)` et `ndpd.conf(4)` pour obtenir des listes des variables de configuration et des valeurs acceptables.

## Démon `in.ripngd`, pour routage IPv6

Le démon `in.ripngd` implémente les informations de RIPng (Routing Information Protocol next-generation, protocole d'informations de routage nouvelle génération) pour les routeurs IPv6. Le RIPng définit l'équivalent IPv6 de RIP (Routing Information Protocol, protocole d'informations de routage). Lorsque vous configurez un routeur IPv6 avec la commande `routeadm` et activez le routage IPv6, le démon `in.ripngd` implémente RIPng sur le routeur.

Vous trouverez ci-dessous les options RIPng prises en charge.

- p *n*      *n* spécifie le numéro de port alternatif utilisé pour l'envoi ou la réception de paquets RIPng.
- q          Supprime les informations de routage.
- s          Force le routage d'informations même si le démon fait office de routeur.
- P          Supprime l'utilisation du poison reverse.
- S          Si `in.ripngd` n'agit pas en tant que routeur, le démon saisit uniquement une route par défaut pour chaque routeur.

## Démon `inetd` et services IPv6

Une application de serveur compatible IPv6 peut gérer les requêtes IPv4 et IPv6, ou les requêtes IPv6 uniquement. Le serveur gère toujours les requêtes par le biais d'un socket IPv6. En outre, le serveur utilise le même protocole qu'utilise le client correspondant.

Pour ajouter ou modifier un service pour IPv6, utilisez les commandes disponibles à partir du service SMF (Service Management Facility, utilitaire de gestion des services).

- Pour plus d'informations sur les commandes SMF, reportez-vous à la section “[Utilitaires d'administration en ligne de commande SMF](#)” du manuel *Administration d'Oracle Solaris : Tâches courantes*.
- Pour obtenir une tâche d'exemple utilisant le service SMF pour configurer un manifeste de service IPv4 s'exécutant sur SCTP, reportez-vous à la section “[Ajout de services utilisant le protocole SCTP](#)” à la page 71.

Pour configurer un service IPv6, vous devez vous assurer que la valeur du champ `proto` dans le profil `inetadm` pour ce service répertorie la valeur adéquate :

- Pour un service assurant la gestion de requêtes IPv4 et IPv6, sélectionnez `tcp6`, `udp6` ou `sctp`. Une valeur `proto` de `tcp6`, `udp6` ou `sctp6` a pour conséquence de faire passer `inetd` sur un socket IPv6 vers le serveur. Le serveur contient une adresse mappée IPv4 au cas où un client IPv4 recevrait une requête.
- Pour un service qui gère uniquement les requêtes IPv6, sélectionnez `tcp6only` ou `udp6only`. Si `proto` a l'une de ces valeurs, `inetd` passe le serveur à un socket IPv6.

Si vous remplacez une command'Oracle Solaris par une autre implémentation, vous devez vous assurer que l'implémentation de ce service prend en charge le protocole IPv6. Si l'implémentation ne prend pas IPv6 en charge, vous devez spécifier la valeur `proto` en tant que `tcp`, `udp` ou `sctp`.

Voici un profil qui résulte de l'exécution de `inetadm` pour un manifeste de service `echo` prenant IPv4 et IPv6 en charge, et s'exécute sur SCTP :

```
# inetadm -l svc:/network/echo:sctp_stream
SCOPE      NAME=VALUE      name="echo"
            endpoint_type="stream"
            proto="sctp6"
            isrpc=FALSE
            wait=FALSE
            exec="/usr/lib/inet/in.echod -s"
            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
```

La syntaxe suivante permet de modifier la valeur du champ `proto` :

```
# inetadm -m FMRI proto="transport-protocols"
```

Tous les serveurs fournis avec le logiciel Oracle Solaris ne nécessitent qu'une entrée de profil spécifiant `proto` en tant que `tcp6`, `udp6` ou `sctp6`. Cependant, le serveur shell distant (`shell`) et le serveur d'exécution distant (`exec`) sont à présent composés d'une instance de service unique, nécessitant une valeur `proto` contenant les valeurs `tcp` et `tcp6only`. Par exemple, pour définir la valeur `proto` pour `shell`, émettez la commande suivante :

```
# inetadm -m network/shell:default proto="tcp,tcp6only"
```

Consultez les extensions IPv6 de l'API Socket dans la section *Programming Interfaces Guide* pour obtenir des informations supplémentaires sur l'écriture de serveurs compatibles IPv6 qui utilisent des sockets.

## Informations importantes relatives à la configuration d'un service pour IPv6

Gardez les éléments suivants à l'esprit lorsque vous ajoutez ou modifiez un service pour IPv6 :

- Vous devez spécifier la valeur `proto` en tant que `tcp6`, `sctp6` ou `udp6` afin d'activer les connexions IPv4 ou IPv6. Si vous spécifiez la valeur pour `proto` en tant que `tcp`, `sctp` ou `udp`, le service n'utilise qu'IPv4.
- Bien qu'il soit possible d'ajouter une instance de service utilisant des sockets SCTP de style un à plusieurs à `inetd`, il est déconseillé de le faire. `inetd` ne fonctionne pas avec les sockets SCTP de style un à plusieurs.
- Si un service nécessite deux entrées en raison de propriétés `wait-status` ou `exec` différentes, vous devez créer deux instances/services à partir du service d'origine.

## Protocole ND IPv6

IPv6 présente le protocole Neighbor Discovery, comme décrit dans le document [RFC 2461, Neighbor Discovery for IP Version 6 \(IPv6\)](http://www.ietf.org/rfc/rfc2461.txt?number=2461) (<http://www.ietf.org/rfc/rfc2461.txt?number=2461>). Pour une présentation des principales fonctionnalités de Neighbor Discovery, reportez-vous à la section “Présentation du protocole de détection de voisins IPv6” du manuel *Guide d'administration système : services IP*.

Cette section décrit les fonctionnalités suivantes du protocole ND :

- “Messages ICMP de la détection des voisins” à la page 164
- “Processus de configuration automatique” à la page 164
- “Sollicitation de voisin et inaccessibilité” à la page 166
- “Algorithme de détection d'adresse dupliquée” à la page 167
- “Comparaison du protocole ND et du protocole ARP et autres protocoles IPv4” à la page 168

## Messages ICMP de la détection des voisins

La détection de voisins définit cinq nouveaux messages ICMP (Internet Control Message Protocol, protocole de messages de contrôle Internet). Les messages remplissent les fonctions suivantes :

- **Sollicitation de routeur** : lorsqu'une interface est activée, les hôtes peuvent demander des messages de sollicitation de routeur. Les sollicitations demandent aux routeurs de générer immédiatement des publications de routeurs, plutôt qu'à la prochaine heure prévue.
- **Publication de routeur** : les routeurs publient leur présence, divers liens de paramètres et divers liens de paramètres Internet. Les routeurs effectuent des publications régulières ou en réponse à un message de sollicitation de routeur. Les publications de routeur contiennent des préfixes utilisés pour la détermination sur lien ou la configuration d'adresse, une valeur de limite de saut recommandée, et ainsi de suite.
- **Sollicitation de voisin** : les noeuds envoient des messages de sollicitation de voisins afin de déterminer l'adresse de couche liaison du voisin. Les messages de sollicitation de voisin sont également envoyés afin de vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache. Les sollicitations s'utilisent également pour la détection d'adresses dupliquées.
- **Publication de voisins** : un noeud envoie des messages de publication de voisinage en réponse à un message de sollicitation de voisinage. Le noeud peut également envoyer des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.
- **Redirection** : les routeurs utilisent les messages de redirection afin d'informer les hôtes de l'existence d'un meilleur saut pour une destination ou que la destination se trouve sur la même liaison.

## Processus de configuration automatique

Cette section comprend une présentation des étapes typiques effectuées par une interface lors d'une configuration automatique. La configuration automatique s'effectue uniquement sur des liaisons compatibles multicast.

1. Une interface compatible multicast est activée, par exemple, lors du démarrage système d'un noeud.
2. Le noeud démarre le processus de configuration automatique en générant une adresse lien-local pour l'interface.  
L'adresse lien-local est formée à partir de l'adresse MAC (Media Access Control) de l'interface.
3. Le noeud envoie un message de sollicitation de voisin contenant l'adresse lien-local provisoire en guise de cible.

Le message a pour objectif de vérifier que l'adresse possible n'est pas déjà utilisée par un autre nœud sur la liaison. Une fois la vérification effectuée, l'adresse lien-local peut être assignée à l'interface.

- a. Si un autre nœud utilise déjà l'adresse proposée, celui-ci renvoie une publication de voisin indiquant que l'adresse est déjà en cours d'utilisation.
- b. Si un autre nœud tente également d'utiliser la même adresse, le nœud envoie également une sollicitation de voisinage pour la cible.

Le nombre de transmissions ou de retransmissions de sollicitation de voisins, ainsi que le temps d'attente entre sollicitations, sont spécifiques aux liaisons. Au besoin, vous pouvez définir ces paramètres.

4. Si un nœud détermine que son adresse lien-local possible n'est pas unique, la configuration automatique est interrompue. Dans ce cas, vous devrez configurer manuellement l'adresse lien-local de l'interface.

Pour simplifier la récupération, vous pouvez fournir un autre ID d'interface qui remplace l'identifiant par défaut. Ensuite, le mécanisme de configuration automatique peut reprendre, en utilisant le nouvel ID d'interface, qui est a priori unique.

5. Lorsqu'un nœud détermine l'unicité de sa future adresse lien-local, il assigne celle-ci à l'interface.

Le nœud dispose alors d'une connectivité de niveau IP avec les nœuds voisins. Les étapes restantes de la configuration automatique sont effectuées exclusivement par les hôtes.

## Obtention d'une publication de routeur

La phase suivante de la configuration automatique consiste à obtenir une publication de routeur ou à déterminer une absence totale de routeurs. Si les routeurs sont présents, ils envoient des publications de routeur qui spécifient le type de configuration automatique que doit effectuer un hôte.

Les routeurs envoient des publications de routeur à intervalles réguliers. Cependant, le temps d'attente entre publications successives est en règle générale plus long que le temps d'attente possible d'un hôte effectuant la configuration automatique. Afin d'obtenir une publication dans les plus brefs délais, un hôte envoie une ou plusieurs sollicitations de routeur au groupe multicast tous routeurs.

## Variables de préfixes de configuration

La publication de routeur contient également des variables de préfixe avec des informations utilisées par la configuration automatique d'adresse sans état pour la génération de préfixes. Le champ de configuration automatique d'adresse sans état dans les publications de routeur sont traitées indépendamment. Un champ d'option contenant les informations de préfixe, l'indicateur de configuration automatique d'adresse, indique si l'option s'applique également à la configuration automatique sans état. Si le champ d'option s'y applique, des champs d'option

supplémentaires contiennent un préfixe de sous-réseau avec des valeurs de durée de vie. Ces valeurs indiquent la durée de validité et de préférence des adresses créées à partir du préfixe.

Dans la mesure où les routeurs génèrent régulièrement des publications de routeur, les hôtes reçoivent de nouvelles publications en continu. Les hôtes compatibles IPv6 traitent les informations contenues dans chaque publication. Les hôtes ajoutent des informations. Ils actualisent également les informations reçues dans les publications précédentes.

## Unicité des adresses

Pour des raisons de sécurité, l'unicité de toutes les adresses doit être vérifiée, préalablement à leur assignation à une interface. La situation est différente pour les adresses créées par configuration automatique sans état. L'unicité d'une adresse est déterminée principalement par la partie de l'adresse formée à partir d'un ID d'interface. Par conséquent, si un noeud a déjà vérifié l'unicité d'une adresse lien-local, il est inutile de tester les adresses supplémentaires individuellement. Les adresses doivent être créées à partir du même ID d'interface. Toutes les adresses obtenues manuellement doivent par contre être testées individuellement pour leur unicité. Les administrateurs système de certains sites pensent que les bénéfices de la détection d'adresses dupliquées ne vaut pas le temps système qu'elle utilise. Pour ces sites, l'utilisation de la détection des adresses dupliquées peut être désactivée en définissant un indicateur de configuration par interface.

Pour accélérer le processus de configuration automatique, un hôte peut générer son adresse lien-local et vérifier son unicité, pendant que l'hôte attend une publication de routeur. Un routeur peut retarder une réponse à une sollicitation de routeur de quelques secondes. Par conséquent, le temps total nécessaire à la configuration automatique peut être bien plus long si les deux étapes sont effectuées en série.

## Sollicitation de voisin et inaccessibilité

La détection de voisins utilise les messages de *sollicitation de voisin* pour déterminer si plusieurs noeuds sont assignés à la même adresse unicast. *La détection d'inaccessibilité de voisin* détecte la défaillance d'un voisin ou du chemin de transfert du voisin. Cette détection nécessite une confirmation de la réception des paquets par le voisin. La détection d'inaccessibilité de voisins détermine également que les paquets sont traités correctement par la couche IP du noeud.

La détection d'inaccessibilité de voisin utilise les confirmations en provenance de deux sources : les protocoles de couche supérieure et les messages de sollicitation de voisin. Lorsque c'est possible, les protocoles de couche supérieure fournissent une confirmation positive de la *progression* d'une connexion. Par exemple, à la réception d'accusés de réception TCP, il est confirmé que les données précédemment envoyées ont été livrées correctement.

Lorsqu'un noeud n'obtient pas de confirmation en provenance des protocoles de couche supérieure, le noeud envoie des messages de sollicitation de voisins. Ces messages sollicitent des

publications de voisinage en tant que confirmation d'accessibilité à partir du prochain saut. Pour réduire le trafic réseau inutile, les messages de sonde sont envoyés uniquement au noeud envoyant des paquets activement.

## Algorithme de détection d'adresse dupliquée

Pour garantir que toutes les adresses configurées sont susceptibles d'être uniques sur un lien donné, les noeuds exécutent un algorithme de *détection d'adresse dupliquée* sur les adresses. Les noeuds doivent exécuter l'algorithme avant d'assigner les adresses à une interface. L'algorithme de détection d'adresses dupliquées est exécuté sur toutes les adresses.

Le processus de configuration automatique décrit dans cette section s'applique uniquement aux hôtes et non aux routeurs. Dans la mesure où la configuration automatique utilise des informations publiées par les routeurs, ces derniers doivent être configurés différemment. Cependant, les routeurs génèrent des adresses lien-local à l'aide du mécanisme décrit dans ce chapitre. En outre, les routeurs doivent réussir l'algorithme de détection d'adresses dupliquées sur toutes les adresses préalablement à l'assignation d'une adresse à une interface.

## Publications de proxy

Un routeur qui accepte les paquets à la place d'une adresse cible peut émettre des publications de voisin impossibles à ignorer. Le routeur peut accepter des paquets pour une adresse cible incapable de répondre aux sollicitations de voisins. L'utilisation de proxy n'est actuellement pas spécifiée. Cependant, la publication de proxy pourrait être utilisée pour la gestion de cas comme ceux de noeuds mobiles qui ont été déplacés hors liaison. Notez que l'utilisation de proxy n'est pas destinée à l'être en tant que mécanisme général de gestion des noeuds qui n'implémentent pas ce protocole.

## Equilibrage de charge entrante

Les noeuds avec interfaces répliquées peuvent avoir besoin d'équilibrer la charge de la réception de paquets entrants sur plusieurs interfaces réseau situées sur la même liaison. Ces noeuds possèdent plusieurs adresses lien-local assignées à la même interface. Par exemple, un pilote de réseau unique peut représenter plusieurs cartes d'interface réseau en tant qu'interface logique unique possédant plusieurs adresses lien-local.

La gestion de l'équilibrage de charge s'effectue en autorisant les routeurs à omettre l'adresse lien-local source des paquets de publication de routeur. Par conséquent, les voisins doivent utiliser les messages de sollicitation de voisin afin de connaître les adresses lien-local des routeurs. Les messages renvoyés de publication des voisins peuvent contenir des adresses lien-local différentes, selon l'adresse qui a envoyé la demande.

## Modification d'adresse lien-local

Un noeud qui sait que son adresse lien-local a été modifiée peut envoyer des paquets de publication de voisins multicast non sollicités. Le noeud peut envoyer des paquets multicast à tous les noeuds pour une mise à jour des adresses lien-local mises en cache qui ne sont plus valides. L'envoi de publications non sollicitées constitue uniquement une amélioration des performances. L'algorithme de détection d'inaccessibilité des voisins assure la fiabilité de la détection de la nouvelle adresse par le noeud, bien que le temps d'attente risque d'être légèrement plus long.

## Comparaison du protocole ND et du protocole ARP et autres protocoles IPv4

La fonctionnalité du protocole ND (Neighbor Discovery, détection des voisins) IPv6 correspond à une combinaison des protocoles IPv4 : ARP (Address Resolution Protocol, protocole de résolution d'adresse), détection de routeur ICMP (Internet Control Message Protocol, protocole de messages de contrôle Internet) et redirection ICMP. IPv4 ne possède pas de protocole ou de mécanisme accepté par tous pour la détection d'inaccessibilité. Cependant, les exigences de l'hôte spécifient les algorithmes possibles pour la détection de passerelles bloquées. La détection de passerelles bloquées est un sous-ensemble des problèmes résolus par la détection d'inaccessibilité de voisins.

La liste suivante compare le protocole de détection de voisins à la suite de protocoles IPv4 associés.

- La détection de routeur fait partie du jeu de protocoles IPv6 de base. Les hôtes IPv6 n'ont pas besoin d'émettre la commande snoop aux protocoles de routage pour rechercher un routeur. IPv4 utilise le protocole ARP, la détection de routeur ICMP et la redirection ICMP pour la détection de routeur.
- Les publications de routeur IPv6 gèrent les adresses lien-local. Aucun échange de paquet supplémentaire n'est nécessaire pour la résolution de l'adresse lien-local du routeur.
- Les publications de routeur gèrent les préfixes de site pour une liaison. Aucun mécanisme séparé n'est nécessaire pour la configuration du masque de réseau, contrairement à IPv4.
- Les publications de routeur sont compatibles avec la configuration automatique d'adresse. La configuration automatique n'est pas implémentée dans IPv4.
- La détection de voisins permet aux routeurs IPv6 de publier la MTU utilisable pour les hôtes sur la liaison. Par conséquent, tous les noeuds utilisent la même valeur de MTU sur des liaisons ne disposant pas d'une MTU correctement définie. Les hôtes IPv4 sur un même réseau peuvent avoir des MTU différentes.



- Contrairement aux adresses de diffusion IPv4, la multidiffusion de résolution d'adresse IPv6 est répartie sur 4 milliards ( $2^{32}$ ) d'adresses multicast, ce qui réduit de façon significative les interruptions relatives à la résolution d'adresses sur des noeuds autres que la cible. En outre, les ordinateurs non IPv6 ne doivent pas être éteints.
- Les redirections IPv6 contiennent l'adresse lien-local du premier nouveau saut. La résolution d'adresse séparée n'est pas nécessaire lors de la réception d'une redirection.
- Il est possible d'associer plusieurs préfixes de site au même réseau IPv6. Par défaut, les hôtes sont informés de tous les préfixes de site locaux par les publications de routeur. Cependant, les routeurs peuvent être configurés afin d'omettre certains ou tous les préfixes des publications de routeur. Dans de tels cas, les hôtes partent du principe que les destinations se trouvent sur des réseaux distants. Par conséquent, les hôtes envoient le trafic aux routeurs. Un routeur peut alors émettre des redirections le cas échéant.
- Contrairement à IPv4, le destinataire d'un message IPv6 redirigé part du principe que le nouveau saut suivant se trouve sur le réseau local. Dans IPv4, un hôte ignore les messages de redirection qui spécifient un saut suivant qui ne se trouve pas sur le réseau local, selon le masque de réseau. Le mécanisme de redirection IPv6 est similaire à l'utilitaire XRedirect d'IPv4. Le mécanisme de redirection est utile sur des liens de non diffusion ou de médias partagés. Sur ces réseaux, les noeuds ne doivent pas effectuer de vérification sur tous les préfixes pour les destinations de liaison locale.
- La détection d'inaccessibilité de voisin IPv6 améliore la livraison de paquets en la présence de routeurs défaillants. Cette capacité améliore la livraison de paquets sur des liaisons partiellement défaillantes ou partitionnées. Cette capacité améliore également la livraison de paquet sur des noeuds qui modifient leurs adresses lien-local. Par exemple, les noeuds mobiles peuvent se déplacer hors du réseau local sans aucune perte de connectivité en raison d'anciens caches ARP. IPv4 ne possède pas de méthode correspondante de détection d'inaccessibilité de voisins.
- Contrairement au protocole ARP, la détection de voisins détecte les défaillances de demi liaison à l'aide de la détection d'inaccessibilité de voisins. La détection de voisins évite d'envoyer du trafic aux voisins en l'absence de connectivité bidirectionnelle.
- En utilisant les adresses lien-local pour identifier les routeurs de façon unique, les hôtes IPv6 peuvent conserver les associations de routeur. La capacité d'identification de routeurs est requise pour les publications de routeur et pour les messages de redirection. Les hôtes doivent conserver les associations de routeur si le site utilise de nouveaux préfixes globaux. IPv4 ne possède pas de méthode comparable d'identification des routeurs.
- Dans la mesure où les messages de détection de voisins ont une limite de saut de 255 après réception, le protocole n'est pas affecté par les attaques de mystification en provenance de noeuds hors liaison. Les noeuds IPv4 hors liaison sont eux capables d'envoyer des messages de redirection ICMP. Les noeuds IPv4 hors liaison peuvent également envoyer des messages de publication de routeur.

- En plaçant la résolution d'adresse à la couche ICMP, la détection de voisins est moins dépendante de médias que le protocole ARP. Par conséquent, les mécanismes standard d'authentification IP et de sécurité peuvent être utilisés.

## Routage IPv6

Le routage IPv6 est quasiment identique au routage IPv4 sous CIDR (Classless Inter-Domain Routing, routage inter-domaine sans classe). La seule différence est la taille des adresses qui sont de 128 bits dans IPv6 au lieu de 32 bits dans IPv4. Avec des extensions simples, il est possible d'utiliser la totalité des algorithmes de routage d'IPv4 comme OSPF, RIP, IDRP et IS-IS.

IPv6 comprend également des extensions de routage simples qui prennent en charge de nouvelles capacités de routage puissantes. La liste suivante décrit les nouvelles capacités de routage :

- Sélection de fournisseur en fonction de la stratégie, des performances, des coûts, etc.
- Hébergement de mobilité, routage vers emplacement actuel
- Réadressage automatique, routage vers nouvelle adresse

Les nouvelles capacités de routage s'obtiennent par la création de séquences d'adresses IPv6 utilisant l'option de routage IPv6. Une source IPv6 utilise l'option de routage afin de répertorier un ou plusieurs noeuds intermédiaires, ou groupes topologiques, à visiter en cours d'acheminement vers la destination du paquet. Cette fonction possède énormément de similitudes avec l'option IPv4 de source lâche et de route d'enregistrement.

Pour que les séquences d'adresses soient une fonction générale, les hôtes IPv6 doivent, dans la plupart des cas, inverser les routes d'un paquet reçu par un hôte. Le paquet doit être authentifié à l'aide de l'utilisation de l'en-tête d'authentification IPv6. Le paquet doit contenir des séquences d'adresse afin d'être renvoyé à son point d'origine. Cette technique force les implémentations d'hôtes IPv6 pour la prise en charge de la gestion et de l'inversion des routes source. La gestion et l'inversion des routes source est la clé permettant aux fournisseurs de travailler avec les hôtes qui implémentent les nouvelles capacités IPv6 comme la sélection de fournisseur et les adresses étendues.

## Publication de routeur

Sur des liens compatibles multicast et des liens point à point, chaque routeur envoie régulièrement un paquet de publication de routeur au groupe multicast pour lui annoncer sa disponibilité. Un hôte reçoit des publications de routeur de la totalité des routeurs, constituant une liste des routeurs par défaut. Les routeurs génèrent des publications de routeur de façon suffisamment fréquente pour permettre aux hôtes d'être avertis de leur présence en quelques minutes. Cependant, les routeurs n'effectuent pas de publications à une fréquence suffisante

pour se fier à une absence de publication permettant de détecter une défaillance de routeur. Un algorithme de détection séparé qui détermine l'inaccessibilité de voisin fournit la détection de défaillance.

## Préfixes de publication de routeurs

Les publications de routeur contiennent une liste de préfixes de sous-réseau utilisés pour déterminer si un hôte se trouve sur le même lien que le routeur. La liste de préfixes est également utilisée pour la configuration d'adresses autonomes. Les indicateurs associés aux préfixes spécifient les utilisations spécifiques d'un préfixe particulier. Les hôtes utilisent les préfixes sur liaison publiés afin de constituer et de maintenir une liste utilisée pour décider lorsque la destination d'un paquet se trouve sur la liaison ou au-delà d'un routeur. Une destination peut se trouver sur une liaison même si celle-ci n'est couverte par aucun préfixe sur liaison publié. Dans de tels cas, un routeur peut envoyer une redirection. La redirection informe l'expéditeur que la destination est un voisin.

Les publications de routeur et les indicateurs par préfixe permettent aux routeurs d'informer des hôtes de la méthode qu'ils doivent utiliser pour effectuer une configuration automatique d'adresse sans état.

## Messages de publication de routeurs

Les messages de publication de routeur contiennent également des paramètres Internet, comme la limite de saut, que les hôtes devraient utiliser dans des paquets entrants. Les messages de publication de routeur peuvent également (facultativement) contenir des paramètres de liens, comme le lien MTU. Cette fonctionnalité permet l'administration centralisée des paramètres critiques. Les paramètres peuvent être définis sur des routeurs et propagés automatiquement à tous les hôtes qui y sont connectés.

Les noeuds effectuent la résolution d'adresses par l'envoi de sollicitation de voisin à un groupe multicast, demandant au noeud cible de retourner son adresse de couche liaison. Les messages de sollicitation de voisin multicast sont envoyés à l'adresse de noeud multicast demandée de l'adresse cible. La cible retourne son adresse de couche liaison dans un message de publication d'un voisin unicast. Une paire de paquets de requête-réponse unique est suffisante pour permettre à l'initiateur et à la cible de résoudre les adresses de couche liaison de l'un et de l'autre. L'initiateur inclut son adresse de couche liaison dans la sollicitation de voisin.

# Extensions IPv6 de services d'assignation de noms Oracle Solaris

Cette section décrit les modifications en matière d'attribution de noms introduites par l'implémentation d'IPv6. Vous pouvez stocker les adresses IPv6 dans les fichiers de services de

noms, NIS, LDAP, DNS ou tout autre fichier Oracle Solaris de votre choix. Vous pouvez également utiliser le protocole NIS à travers les transports RPC IPv6 pour la récupération de données NIS.

## Extensions DNS pour IPv6

Un enregistrement de ressources spécifique IPv6, l'enregistrement de ressource AAAA, a été spécifié dans le document RFC 1886 *DNS Extensions to Support IP Version 6*. Cet enregistrement AAAA mappe un nom d'hôte en une adresse IPv6 de 128 bits. L'enregistrement PTR est toujours utilisé avec IPv6 pour mapper les adresses IP en noms d'hôtes. Les 32 quartets de d'adresse 128 bits sont inversés pour une adresse IPv6. Chaque quartet est converti dans sa valeur hexadécimale ASCII correspondante. Ensuite, `ip6.int` est joint.

## Modifications apportées aux commandes de services de noms

Pour la prise en charge d'IPv6, vous pouvez rechercher les adresses IPv6 avec les commandes de service de noms existantes. Par exemple, la commande `ypmatch` fonctionne avec les nouvelles cartes NIS. La commande `nslookup` peut rechercher les nouveaux enregistrements AAAA dans DNS.

## Prise en charge IPv6 de NFS et RPC

Les logiciels NFS et RPC (Remote Procedure Call, appel de procédure distant) prennent IPv6 en charge de façon totalement fluide. Les commandes existantes relatives aux services NFS restent inchangées. Il est également possible d'exécuter la plupart des applications RPC sur IPv6 sans aucune modification. Certaines applications RPC avancées de reconnaissance d'acheminement peuvent nécessiter une mise à jour.

## Prise en charge d'IPv6 sur ATM

Oracle Solaris prend en charge le protocole IPv6 sur des ATM, des PVC (Permanent Virtual Circuits, circuits virtuels permanents) et des SVC (Switched Virtual Circuits, circuits virtuels à commutation) statiques.

## PARTIE II

# DHCP

Cette partie traite des concepts propres au protocole DHCP (Dynamic Host Configuration Protocol) et décrit les tâches nécessaires à la planification, à la configuration, à l'administration et au dépannage du service DHCP.



## A propos de DHCP (présentation)

---

Ce chapitre vous propose de découvrir le protocole DHCP (Dynamic Host Configuration Protocol) et les concepts à la base de ce protocole. Il décrit également les avantages que présente le protocole DHCP pour votre réseau.

Le présent chapitre contient les informations suivantes :

- “A propos du protocole DHCP” à la page 175
- “Intérêt du protocole DHCP” à la page 176
- “Mode de fonctionnement du protocole DHCP” à la page 177
- “Serveur DHCP ISC” à la page 180
- “Client DHCP” à la page 181

## A propos du protocole DHCP

Le protocole DHCP permet de procéder automatiquement à la configuration des systèmes hôtes d'un réseau TCP/IP au moment de leur initialisation. Le protocole DHCP utilise un mécanisme client/serveur. Les serveurs stockent et gèrent les informations de configuration des clients et les fournissent à leur demande. Ces informations comprennent l'adresse IP du client ainsi que des données sur les services réseau accessibles au client.

DHCP est l'évolution d'un protocole précédent, BOOTP, conçu pour l'initialisation des systèmes sur un réseau TCP/IP. Il utilise le même format que le protocole BOOTP pour les messages échangés entre le client et le serveur. A la différence des messages BOOTP, les messages DHCP peuvent contenir des données de configuration du réseau pour le client.

L'un des avantages majeurs du protocole DHCP est sa capacité à gérer les affectations d'adresses IP au moyen de *baux*. L'intérêt des *baux* est de pouvoir récupérer les adresses IP lorsqu'elles ne sont plus utilisées afin de les attribuer à d'autres clients. Cela permet à un site DHCP d'utiliser un pool d'adresses IP plus petit que celui qui serait nécessaire si tous les clients possédaient une adresse IP permanente.

## Intérêt du protocole DHCP

Le service DHCP vous fait gagner un temps précieux en prenant à sa charge un certain nombre de tâches liées à la configuration d'un réseau TCP/IP et à l'administration quotidienne de ce réseau. Notez que dans l'implémentation Oracle Solaris, DHCP fonctionne uniquement avec IPv4.

DHCP offre les avantages suivants :

- **Gestion des adresses IP** : l'un des principaux atouts de DHCP est effectivement de faciliter l'administration des adresses IP. Dans un réseau sans protocole DHCP, vous devez allouer manuellement les adresses IP. Il faut attribuer des adresses IP uniques à chaque client et configurer chacun d'eux individuellement. Si un client est transféré sur un autre réseau, il faut alors effectuer manuellement les modifications se rapportant à ce client. Par contre, si vous activez le protocole DHCP, le serveur DHCP gère et assigne lui-même les adresses IP sans que l'administrateur ait à intervenir. Les clients peuvent être placés sur d'autres sous-réseaux sans nécessiter de reconfiguration manuelle, car ils sont capables d'obtenir d'un serveur DHCP les informations client correspondant au nouveau réseau.
- **Configuration centralisée des clients du réseau** : vous pouvez créer une configuration sur mesure pour certains clients ou pour certains types de client. Les données de configuration sont stockées au même endroit : à l'intérieur du magasin de données DHCP. Vous n'avez pas besoin de vous connecter à un client pour changer sa configuration. Il est possible de modifier plusieurs clients à la fois en changeant simplement les informations dans le magasin de données.
- **Prise en charge des clients BOOTP** : les serveurs BOOTP et les serveurs DHCP se chargent d'écouter et de répondre aux messages diffusés par les clients. Le serveur DHCP peut répondre aussi bien aux requêtes des clients BOOTP qu'à celles des clients DHCP. Les clients BOOTP reçoivent une adresse IP et les informations nécessaires au démarrage à partir d'un serveur.
- **Prise en charge des clients locaux et distants** : le protocole BOOTP permet de relayer les messages d'un réseau à un autre. Le protocole DHCP utilise cette fonctionnalité BOOTP de différentes manières. La plupart des routeurs de réseau peuvent être configurés comme des agents de relais BOOTP dans le but de transmettre des requêtes BOOTP à des serveurs ne figurant pas sur le réseau du client. Les requêtes DHCP peuvent être relayées de la même manière, dans la mesure où le routeur ne fait aucune distinction entre les requêtes DHCP et les requêtes BOOTP. Il est également possible de configurer le serveur DHCP de sorte qu'il se comporte comme un agent de relais BOOTP, lorsqu'un routeur compatible avec la fonctionnalité de relais BOOTP n'est pas disponible.
- **Initialisation à partir du réseau** : les clients peuvent utiliser le protocole DHCP pour obtenir les informations nécessaires à un démarrage à partir d'un serveur du réseau, au lieu de faire appel au protocole RARP (Reverse Address Resolution Protocol) et au fichier `bootparams`. Le serveur DHCP peut donner au client tous les renseignements dont il a besoin pour fonctionner : adresse IP, serveur d'initialisation et données de configuration du réseau. Comme les requêtes DHCP peuvent être relayées d'un sous-réseau à un autre, vous



pouvez vous contenter de déployer un nombre moins important de serveurs d'initialisation sur votre réseau lorsque vous avez recours au service d'initialisation de réseau DHCP. L'initialisation RARP exige un serveur d'initialisation par sous-réseau.

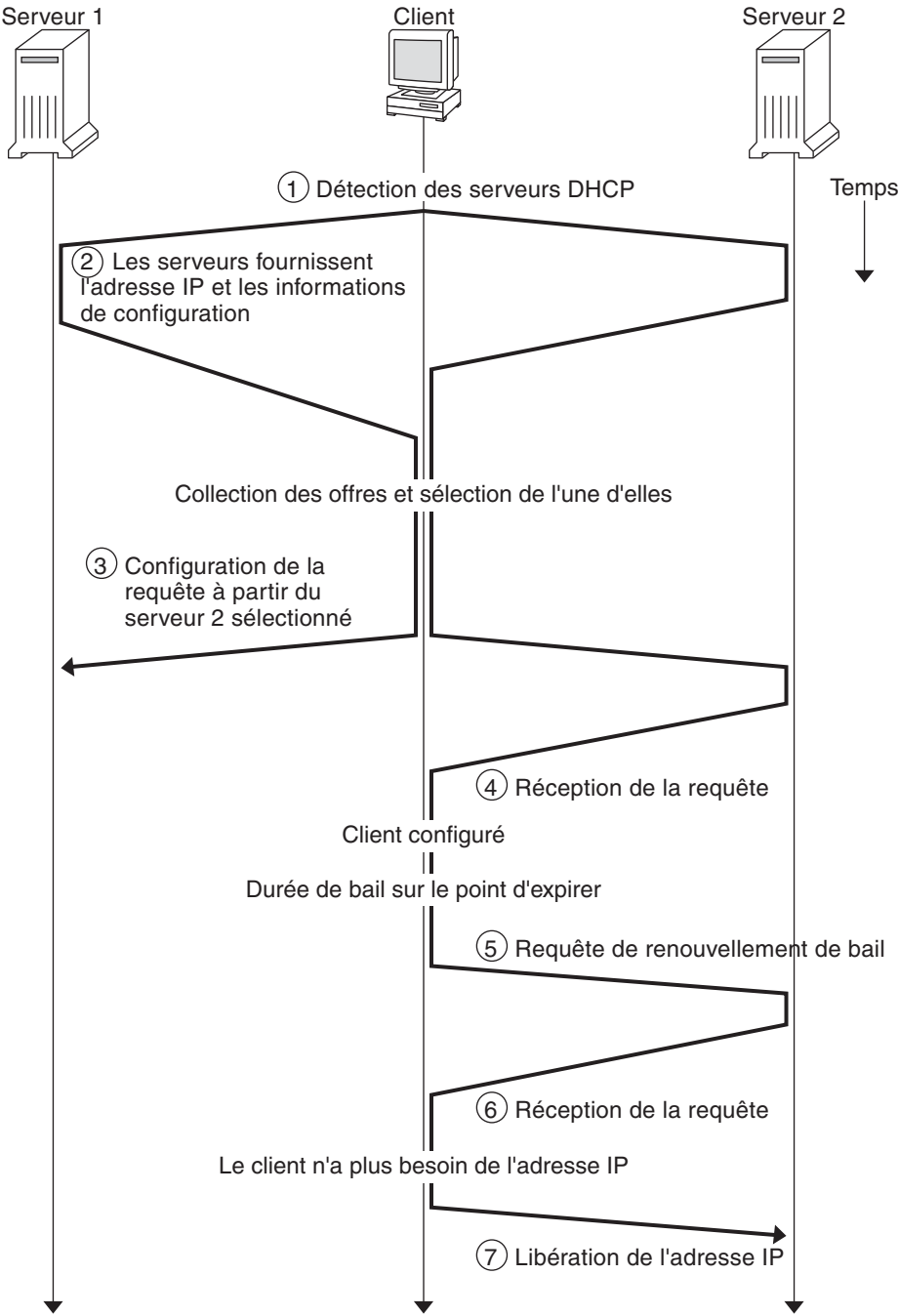
- **Gestion de réseaux de grande taille** : DHCP peut être exploité par des réseaux comptant des millions de clients DHCP. Le serveur DHCP utilise la technique de multithreading pour traiter plusieurs requêtes client à la fois. Il gère également les magasins de données, c'est-à-dire des espaces de stockage optimisés pour traiter de grandes quantités de données. L'accès aux magasins de données est contrôlé par des modules de traitement indépendants. Grâce aux magasins de données, vous êtes libre de travailler avec toutes les bases de données qui vous intéressent.

## Mode de fonctionnement du protocole DHCP

Vous devez commencer par installer et configurer le serveur DHCP. Lors de la phase de configuration, il est nécessaire de fournir un certain nombre d'informations au sujet du réseau avec lequel les clients vont communiquer. Une fois ces précisions apportées, les clients auront la possibilité de demander et de recevoir des informations spécifiques au réseau.

Le schéma ci-après montre comment s'enchaînent les différents événements liés au service DHCP. Les nombres figurant dans les cercles correspondent aux étapes numérotées de la description suivant le schéma.

FIGURE 10-1 Séquence des événements pour le service DHCP



Le schéma précédent présente les étapes suivantes :

1. Le client identifie un serveur DHCP en diffusant un *message de détection* à l'adresse de diffusion limitée (255 . 255 . 255 . 255) sur le sous-réseau local. Si un routeur est présent et configuré pour agir comme un agent de relais BOOTP, la requête est transmise à d'autres serveurs DHCP sur d'autres sous-réseaux. Le *message de diffusion* du client comprend son identifiant unique (ID) lequel, dans le cadre de l'implémentation DHCP dans Oracle Solaris, est dérivé de l'adresse MAC (Media Access Control) du client. Sur un réseau Ethernet, l'adresse MAC est identique à l'adresse Ethernet.

Les serveurs DHCP qui reçoivent le message de détection sont capables d'identifier le réseau du client en effectuant l'analyse suivante :

- Sur quelle interface réseau la requête est-elle parvenue ? Le serveur peut en déduire que le client appartient au réseau auquel l'interface est connectée ou que le client utilise un agent de relais BOOTP relié à ce réseau.
  - La requête contient-elle l'adresse IP d'un agent de relais BOOTP ? Lorsqu'une requête transite par un agent de relais, celui-ci insère son adresse dans l'en-tête de la requête. Lorsque le serveur détecte une *adresse d'un agent de relais*, il sait que la portion réseau de l'adresse désigne l'adresse réseau du client dans la mesure où l'agent de relais doit obligatoirement être connecté au réseau du client.
  - Le réseau du client comporte-t-il des sous-réseaux ? Le serveur consulte la table *netmasks* pour identifier le masque de sous-réseau utilisé sur le réseau désigné par l'adresse de l'agent de relais ou par l'adresse de l'interface réseau ayant reçu la requête. Dès que le serveur connaît cette information, il peut déterminer la portion de l'adresse réseau correspondant à la portion de l'hôte, puis sélectionner une adresse IP qui convient pour le client. Pour plus d'informations sur les *netmasks*, reportez-vous à la page de manuel [netmasks\(4\)](#).
2. Une fois que les serveurs DHCP ont réussi à identifier le réseau du client, ils sélectionnent une adresse IP appropriée et s'assurent qu'elle est libre. Ils répondent ensuite au client en diffusant un *message d'offre*. Ce message contient l'adresse IP sélectionnée et des informations au sujet des services pouvant être configurés pour le client. Chaque serveur réserve provisoirement l'adresse IP proposée jusqu'à ce que le client choisisse ou non d'accepter l'adresse IP en question.
  3. Le client sélectionne la meilleure offre en fonction du nombre et du type de services proposés. Il diffuse alors une requête indiquant l'adresse IP du serveur ayant fait la meilleure offre. Tous les serveurs DHCP ayant répondu savent ainsi que le client a fait son choix. Les serveurs non sélectionnés peuvent dès lors annuler la réservation des adresses IP proposées.
  4. Le serveur sélectionné alloue l'adresse IP au client et stocke cette information dans le magasin de données DHCP. Il adresse également un accusé de réception (message ACK) au client. L'*accusé de réception* contient les paramètres de configuration du réseau pour le client. Le client se sert de l'utilitaire *ping* pour tester l'adresse IP et s'assurer qu'elle n'est utilisée par aucun autre système. Il continue ensuite la procédure d'initialisation afin de se connecter au réseau.

5. Le client contrôle la durée du bail. Au bout d'un certain temps, il envoie un nouveau message au serveur sélectionné pour lui demander d'augmenter la durée du bail.
6. Le serveur DHCP recevant la requête prolonge le bail à condition que le bail soit conforme à la stratégie de location définie par l'administrateur. Si le serveur ne répond pas dans les 20 secondes, le client diffuse une requête de sorte que l'un des autres serveurs DHCP prolonge son bail.
7. Lorsque le client n'a plus besoin de l'adresse IP, il prévient le serveur que l'adresse IP a été libérée. Cette notification peut survenir lors d'un arrêt méthodique ou être effectuée de façon manuelle.

## Serveur DHCP ISC

Une implémentation du serveur DHCP Internet Systems Consortium (ISC) a été ajoutée à Oracle Solaris. Ce logiciel n'étant pas installé automatiquement, vous pouvez ajouter ce serveur au système en tapant la commande suivante :

```
# pkg install pkg:/service/network/dhcp/isc-dhcp
```

Le serveur DHCP ISC, `dhcpcd`, implémente les protocoles DHCP (Dynamic Host Configuration Protocol) et BOOTP (Internet Bootstrap Protocol). DHCP prend en charge les demandes et les affectations d'adresses IP pour les hôtes d'un réseau TCP/IP et permet à ces hôtes d'obtenir des informations sur le réseau auquel ils sont attachés. BOOTP fournit une fonctionnalité similaire.

La liste suivante répertorie certains des ajouts importants à la version de DHCP :

- Plusieurs services ont été ajoutés afin de prendre en charge ISC DHCP et le service DHCP Sun hérité. Reportez-vous à la section [“Services SMF utilisés par le service DHCP” à la page 208](#) pour connaître la liste de tous les services utilisés par DHCP.
- Trois commandes ont été ajoutées : `dhcpcd`, `dhcprelay` et `omshell`. Reportez-vous à la section [“Fichiers utilisés par le service DHCP” à la page 207](#) pour connaître la liste de toutes les commandes associées à DHCP.
- Les fichiers de configuration du serveur DHCP ISC sont `/etc/inet/dhcdp4.conf` pour DHCPv4 et `/etc/inet/dhcdp6.conf` pour DHCPv6.
- Un utilisateur nommé `dhcpserv` a été ajouté au service DHCP ISC.
- Trois nouvelles commandes peuvent être gérées par les autorisations `solaris.smf.manage.dhcp` et `solaris.smf.value.dhcp`.

Pour plus d'informations sur DHCP ISC, reportez-vous à la page Web de [documentation sur DHCP ISC](#).

## Serveur DHCP Sun hérité

Le logiciel du serveur DHCP Sun hérité est toujours inclus dans la version Oracle Solaris 11, mais il a été marqué comme obsolète et sera supprimé dans une version future. Pour plus d'informations sur ce service DHCP hérité, reportez-vous au [Chapter 11, Administration du service DHCP ISC](#).

## Client DHCP

Le terme "client" est parfois employé pour faire référence à une machine physique jouant le rôle de client sur le réseau. Or, le client DHCP décrit dans ce document est une entité logicielle. Le client DHCP est un démon (dhcagent) s'exécutant dans Oracle Solaris, sur un système configuré pour recevoir sa configuration réseau d'un serveur DHCP. Le client DHCP peut interagir à la fois avec le serveur DHCP Sun hérité et le serveur DHCP ISC.

Pour plus d'informations sur le client DHCP, reportez-vous au [Chapitre 12, "Configuration et administration du client DHCP"](#).



# Administration du service DHCP ISC

---

Ce chapitre décrit les différentes tâches que vous aurez besoin d'effectuer pour gérer le service DHCP ISC. Il aborde les sujets suivants :

- “Configuration de l'accès utilisateur aux commandes DHCP” à la page 183
- “Tâches du serveur DHCP” à la page 184

## Configuration de l'accès utilisateur aux commandes DHCP

Par défaut, seul l'utilisateur root peut exécuter `svcadm` et les autres commandes requises pour configurer le service DHCP. Pour que les utilisateurs non root puissent également les utiliser, il est possible de configurer le contrôle d'accès basé sur les rôles (RBAC) pour ces commandes.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuration initiale RBAC (liste des tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

Les pages de manuel suivantes sont également des sources de référence intéressantes : [rbac\(5\)](#), [exec\\_attr\(4\)](#) et [user\\_attr\(4\)](#).

La procédure suivante explique comment attribuer le profil de gestion DHCP qui permet à l'utilisateur d'exécuter les commandes DHCP.

### ▼ Procédure d'octroi d'accès aux commandes DHCP

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil DHCP Management.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuration initiale RBAC (liste des tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Ajoutez un utilisateur ou un rôle au fichier `/etc/user_attr`.**

Editez le fichier `/etc/user_attr` afin d'y ajouter une entrée sous la forme suivante. Prévoyez une entrée pour chaque utilisateur ou rôle censé gérer le service DHCP.

```
username:::type=normal;profiles=DHCP Management
```

Voici, par exemple, l'entrée qu'il convient d'ajouter pour un utilisateur appelé `ram` :

```
ram:::type=normal;profiles=DHCP Management
```

# Tâches du serveur DHCP

## ▼ Procédure de désactivation d'un serveur DHCP ISC

Vous pouvez utiliser ces étapes pour la configuration initiale d'un serveur DHCP ISC.

**1 Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil DHCP Management.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

**2 Editez le fichier de configuration DHCP.**

Créez le fichier `/etc/dhcp/dhcpd4.conf` ou le fichier `/etc/dhcp/dhcpd6.conf`. Pour plus d'informations, reportez-vous à la page de manuel `dhcpd.conf(5)`.

**3 Activez le service requis.**

```
# svcadm enable service
```

*service* peut correspondre à l'une des valeurs suivantes :

<code>svc:/network/dhcp/server:ipv4</code>	Fournit des demandes DHCP et BOOTP issues des clients IPv4
<code>svc:/network/dhcp/server:ipv6</code>	Fournit des demandes DHCP et BOOTP issues des clients IPv6
<code>svc:/network/dhcp/relay:ipv4</code>	Relaie les demandes DHCP et BOOTP issues des clients IPv4 vers un réseau avec un serveur DHCP
<code>svc:/network/dhcp/relay:ipv6</code>	Relaie les demandes DHCP et BOOTP issues des clients IPv6 vers un réseau avec un serveur DHCP



## ▼ Procédure de modification de la configuration du service DHCP

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil DHCP Management.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Editez le fichier de configuration DHCP.**

Editez le fichier `/etc/dhcp/dhcpd4.conf` ou le fichier `/etc/dhcp/dhcpd6.conf`. Pour plus d'informations, reportez-vous à la page de manuel `dhcpd.conf(5)`.

- 3 **Actualisez les données SMF.**

```
# svcadm refresh service
```



# Configuration et administration du client DHCP

---

Ce chapitre traite du client DHCP (Dynamic Host Configuration Protocol) faisant partie d'Oracle Solaris. Il décrit le mode de fonctionnement des protocoles DHCPv4 et DHCPv6 du client et explique comment vous pouvez modifier le comportement du client.

L'un de ces protocoles, à savoir le protocole DHCPv4, fait depuis longtemps partie d'Oracle Solaris. Il permet aux serveurs DHCP de transmettre des paramètres de configuration tels que les adresses réseau IPv4 aux noeuds IPv4.

L'autre protocole, DHCPv6, joue le même rôle auprès des serveurs DHCP en leur donnant la possibilité de communiquer des paramètres de configuration (adresses réseau IPv6, par exemple) aux noeuds IPv6. DHCPv6 est la contrepartie sans état à la spécification " Autoconfiguration d'adresse sans état IPv6 " (RFC 2462). Ce protocole peut être utilisé indépendamment du mode sans état ou lui être associé afin d'obtenir des données de configuration.

Le présent chapitre contient les informations suivantes :

- [“A propos du client DHCP” à la page 188](#)
- [“Activation et désactivation d'un client DHCP” à la page 195](#)
- [“Administration du client DHCP” à la page 197](#)
- [“Systèmes clients DHCP avec plusieurs interfaces réseau” à la page 199](#)
- [“Noms d'hôtes du client DHCPv4” à la page 200](#)
- [“Systèmes clients DHCP et services de noms” à la page 201](#)
- [“Scripts d'événement client DHCP” à la page 203](#)

## A propos du client DHCP

Le client DHCP est le démon `dhcpgent`. Si vous installez Oracle Solaris avec l'interface graphique d'installation du LiveCD, les protocoles DHCPv4 et DHCPv6 sont activés sur le système installé. Si vous installez Oracle Solaris en utilisant le programme d'installation en mode texte, vous êtes invité à sélectionner la manière dont le réseau doit être configuré sur le système installé. Si vous spécifiez la configuration automatique du réseau, les protocoles DHCPv4 et DHCPv6 sont activés sur le système installé.

Vous ne devez effectuer aucune autre action sur le client Oracle Solaris pour utiliser le protocole DHCP. La configuration du serveur DHCP détermine les informations communiquées aux systèmes clients DHCP faisant appel au service DHCP.

Si un système client exécute déjà Oracle Solaris sans le service DHCP, vous devez le reconfigurer pour pouvoir utiliser le service DHCP. Vous pouvez également reconfigurer un système client DHCP de façon à ce qu'il cesse d'utiliser le protocole DHCP et qu'il exploite les informations de réseau statiques que vous fournissez. Pour plus d'informations, reportez-vous à la section [“Activation et désactivation d'un client DHCP” à la page 195](#).

## Serveur DHCPv6

Aucun serveur DHCPv6 n'est disponible par le biais de Sun Microsystems pour Oracle Solaris. Les serveurs proposés par des tiers sont compatibles avec DHCPv6 de Sun. Si le réseau comporte un serveur DHCPv6, le client DHCPv6 de Sun l'utilise.

## Différences entre DHCPv4 et DHCPv6

Les deux principales différences entre DHCPv4 et DHCPv6 sont les suivantes :

- **Modèle administratif**
  - DHCPv4 – L'administrateur active DHCP pour chaque interface. L'administration se fait sur la base d'une interface logique.
  - DHCPv6 – Aucune configuration explicite n'est utile. Ce protocole est activé sur une interface physique donnée.
- **Détails du protocole**
  - DHCPv4 – Le serveur DHCP fournit le masque de sous-réseau pour chaque adresse. Une option de nom d'hôte définit le nom du noeud à l'échelle du système.
  - DHCPv6 – Le masque de sous-réseau est fourni par les publications du routeur, et non par le serveur DHCPv6. Il n'existe pas d'option de nom d'hôte DHCPv6.

## Modèle administratif DHCP

**DHCPv4** exige une configuration explicite du client. Vous devez configurer le système DHCPv4 pour effectuer une procédure d'adressage chaque fois que cela est nécessaire, soit lors de l'installation initiale du système, soit de façon dynamique par le biais de la commande `ipadm`. Reportez-vous à la page de manuel `ipadm(1M)`.

**DHCPv6** ne nécessite pas de configuration explicite du client. DHCP est une caractéristique inhérente du réseau. Le signal permettant d'utiliser ce protocole est acheminé dans les messages des publications du routeur à partir des routeurs locaux. Le client DHCP crée et détruit automatiquement les interfaces logiques chaque fois que cela est nécessaire.

Le mécanisme DHCPv6 est très similaire, d'un point de vue administratif, à la configuration d'adresse sans état (automatique) IPv6 existante. Dans le cas d'une configuration d'adresse sans état, il est nécessaire d'appliquer un indicateur au routeur local afin d'indiquer que, pour un nombre donné de préfixes, chaque client est tenu de configurer automatiquement une adresse par lui-même en utilisant le préfixe publié plus un jeton d'interface local ou un nombre aléatoire. En ce qui concerne DHCPv6, les mêmes préfixes sont exigés mais les adresses sont acquises et gérées via un serveur DHCPv6 au lieu d'être assignées de façon aléatoire.

### Adresse MAC et ID de client

**DHCPv4** utilise l'adresse MAC et un ID de client facultatif pour identifier le client dans le but d'assigner une adresse. Chaque fois que le même client se connecte au réseau, il obtient la même adresse dans la mesure du possible.

**DHCPv6** procède essentiellement de la même manière, mais rend l'ID de client obligatoire et impose une structure. L'ID de client dans DHCPv6 se compose de deux parties : un identificateur unique DHCP (DUID) et un identificateur d'association d'identité (IAID). Le DUID identifie le **système** client (et non pas seulement une interface, comme dans DHCPv4), et l'IAID identifie l'interface sur ce système.

Comme indiqué dans le document RFC 3315, une association d'identité est le moyen utilisé par un serveur et un client pour identifier, regrouper et gérer un ensemble d'adresses IPv6 liées. Le client doit lier au moins une association d'identité (IA) distincte à chacune de ses interfaces réseau. Il utilise ensuite les IA assignées pour obtenir des informations de configuration d'un serveur pour cette interface. Pour plus d'informations sur les IA, reportez-vous à la section suivante (Détails du protocole).

Il est possible également d'associer DUID+IAID avec DHCPv4. Vous pouvez concaténer ces identificateurs sans ambiguïté pour vous en servir comme ID de client. Pour des raisons de compatibilité, cela ne s'applique pas aux interfaces IPv4 standard. En revanche, pour les interfaces logiques (`bge0:1`), DUID+IAID est utilisé si aucun ID de client n'est configuré.

A la différence d'IPv4 DHCP, DHCPv6 n'offre pas d'option "nom de client". Il n'y a donc aucun moyen de nommer vos systèmes en les basant uniquement sur DHCPv6. Si vous avez besoin de connaître le nom DNS associé à une adresse fournie par DHCPv6, utilisez la résolution inverse

DNS (requête adresse vers nom à l'aide de la fonction `getaddrinfo(3SOCKET)`) pour obtenir le nom correspondant. Si vous utilisez uniquement DHCPv6 et souhaitez attribuer un nom spécifique à un noeud, vous devez alors spécifier le nom du noeud à l'aide de la commande `svccfg` comme suit :

```
# svccfg -s svc:/system/identity:node setprop config/nodename = astring: hostname
```

## Détails du protocole

Avec DHCPv4, le serveur DHCP fournit le masque du sous-réseau à associer à l'adresse assignée. Avec DHCPv6, le masque du sous-réseau (appelé aussi "longueur du préfixe") est attribué par les publications du routeur et n'est pas géré par le serveur DHCP.

DHCPv4 dispose d'une option Hostname prévue pour définir le nom du noeud à l'échelle du système. DHCPv6 ne propose pas ce type d'option.

Pour configurer un ID de client pour DHCPv6, vous devez spécifier un DUID au lieu de permettre au système d'en choisir un automatiquement. Vous pouvez le faire de façon globale pour le démon ou procéder interface par interface. Pour définir le DUID global, respectez le format suivant (notez la présence du point initial) :

```
.v6.CLIENT_ID=DUID
```

Pour configurer une interface de façon à utiliser un DUID précis (et donner l'impression que le système est constitué de multiples clients indépendants pour le serveur DHCPv6), tapez la commande suivante :

```
bge0.v6 CLIENT ID=DUID
```

A chaque association d'identité (IA) correspond un type d'adresse. Une association d'identité pour des adresses temporaires (IA\_TA) contient, par exemple, des adresses provisoires, alors qu'une association d'identité pour des adresses non temporaires (IA\_NA) dispose d'adresses allouées de façon permanente. La version de DHCPv6 décrite dans ce manuel offre uniquement des associations IA\_NA.

Oracle Solaris assigne sur demande une IAID à chaque interface. Cette dernière est stockée dans un fichier à l'intérieur du système de fichiers racine de façon à rester la même pendant tout le cycle de vie de la machine.

## Interfaces logiques

Au niveau du client DHCPv4, chaque interface logique est considérée comme indépendante et comme une unité d'administration. Outre l'interface logique numéro zéro (laquelle adopte par défaut l'adresse MAC de l'interface comme identificateur), l'utilisateur a la possibilité de configurer des interfaces logiques spécifiques afin d'exécuter DHCP en spécifiant un CLIENT\_ID dans le fichier de configuration `dhcpage` . Exemple :

```
hme0:1.CLIENT_ID=orangutan
```

DHCPv6 ne procède pas de la même manière. L'interface logique numéro zéro sur une interface IPv6, à la différence d'IPv4, est toujours une adresse lien-local. une adresse lien-local sert à assigner automatiquement une adresse IP à un périphérique sur un réseau IP lorsque aucune autre méthode d'affectation n'est disponible, comme par exemple un serveur DHCP. L'interface logique numéro zéro ne peut pas être placée sous le contrôle de DHCP. Aussi, même si DHCPv6 est exécuté sur l'interface logique numéro zéro (appelée également interface "physique"), il alloue les adresses uniquement aux interfaces logiques n'ayant pas le numéro zéro.

En réponse à une demande du client DHCPv6, le serveur DHCPv6 renvoie une liste d'adresses à configurer par le client.

## Négociation d'options

Dans DHCPv6, vous disposez d'une fonction de demande d'option qui donne une indication au serveur sur les préférences d'affichage du client. Si toutes les options possibles ont été transmises du serveur au client, il est possible qu'une partie des informations ait été abandonnée en chemin. Le serveur peut utiliser l'indication pour sélectionner les options à inclure dans la réponse. Il peut également l'ignorer et choisir d'inclure d'autres éléments. Sur Oracle Solaris par exemple, les options préférentielles peuvent contenir le domaine d'adresse DNS ou NIS d'Oracle Solaris, mais ne contiendront probablement pas le serveur NetBIOS.

Le même type d'indication est fourni pour DHCPv4, mais sans la fonction de demande d'option spéciale. Au lieu de cela, DHCPv4 utilise la liste `PARAM_REQUEST_LIST` dans `/etc/default/dhcpagent`.

## Syntaxe de configuration

Configurez le client DHCPv6 de la même manière que le client DHCPv4 existant, à l'aide de `/etc/default/dhcpagent`.

La syntaxe inclut en plus le marqueur ".v6", inséré entre le nom de l'interface (le cas échéant) et le paramètre à configurer. Par exemple, la liste des demandes d'option IPv4 globale est configurée comme suit :

```
PARAM_REQUEST_LIST=1,3,6,12,15,28,43
```

Il est possible de configurer une interface individuelle afin d'omettre l'option de nom d'hôte comme suit :

```
bge0.PARAM_REQUEST_LIST=1,3,6,15,28,43
```

Pour définir une liste de demandes globale pour DHCPv6, n'oubliez pas le point initial :

```
.v6.PARAM_REQUEST_LIST=23,24
```

Suivez cet exemple pour configurer une interface individuelle :

```
bge0.v6.PARAM_REQUEST_LIST=21,22,23,24
```

A titre de référence, voici à quoi ressemble un fichier `/etc/default/dhcpagent` pour la configuration DHCPv6 :

```
# The default DHCPv6 parameter request list has preference (7), unicast (12),  
# DNS addresses (23), DNS search list (24), NIS addresses (27), and  
# NIS domain (29). This may be changed by altering the following parameter-  
# value pair. The numbers correspond to the values defined in RFC 3315 and  
# the IANA dhcpv6-parameters registry.  
.v6.PARAM_REQUEST_LIST=7,12,23,24,27,29
```

## Démarrage du client DHCP

Dans la plupart des cas, vous n'avez pas à intervenir pour lancer le client DHCPv6. Le démon `in.ndpd` démarre automatiquement DHCPv6 lorsque cela est nécessaire.

Cependant, pour le protocole DHCPv4, vous devez demander le démarrage du client, si cela n'a pas été fait lors de l'installation d'Oracle Solaris. Reportez-vous à la section [“Procédure d'activation du client DHCP” à la page 195](#).

Le démon `dhcpagent` obtient les informations de configuration nécessaires aux autres processus impliqués dans l'initialisation du système. C'est pour cette raison que les scripts de démarrage du système lancent `dhcpagent` au tout début du processus d'initialisation et attendent l'arrivée des informations de configuration du réseau provenant du serveur DHCP.

Bien que la procédure par défaut consiste à exécuter DHCPv6, vous pouvez en décider autrement. Vous pouvez arrêter DHCPv6 à l'aide de la commande `ipadm delete-addr`. Rien ne vous empêche également de désactiver DHCPv6 pour éviter son lancement au redémarrage. Il suffit pour cela de modifier le fichier `/etc/inet/ndpd.conf`.

L'exemple suivant illustre la procédure d'arrêt immédiat de DHCPv6 :

```
ex# echo ifdefault StatefulAddrConf false >> /etc/inet/ndpd.conf  
ex# kill -HUP -x in.ndpd  
ex# ipadm delete-addr -r dhcp-addrobj
```

Au démarrage, s'il existe des configurations DHCP sur le système, `dhcpagent` démarre dans le cadre des processus de script de démarrage. `dhcpagent` configure alors les interfaces réseau comme décrit dans la section [“Mode de fonctionnement du protocole DHCP” à la page 177](#).



## Communication DHCPv6

A la différence de DHCPv4, lequel est appelé par configuration manuelle, DHCPv6 est exécuté par les publications du routeur (RAs). Selon le mode de configuration du routeur, le système appelle automatiquement DHCPv6 au niveau de l'interface sur laquelle le message Router Advertisement a été reçu et utilise DHCP pour obtenir une adresse et d'autres paramètres, ou demande uniquement les données autres que l'adresse (serveurs DNS, par exemple) avec DHCPv6.

Le démon `in.ndpd` réceptionne le message des publications du routeur. Il effectue cette opération de façon automatique sur toutes les interfaces montées pour IPv6 sur le système. Lorsque `in.ndpd` découvre un RA exigeant l'exécution de DHCPv6, il fait appel à DHCPv6.

Pour éviter que `in.ndpd` ne démarre DHCPv6, il suffit de modifier le contenu du fichier `/etc/inet/ndpd.conf`.

Vous pouvez également arrêter DHCPv6 en utilisant l'une des versions suivantes de la commande `ipadm` :

```
ipadm delete-addr dhcp-addrobj
```

ou

```
ipadm delete-addr -r dhcp-addrobj
```

## Gestion des données de configuration réseau par les protocoles client DHCP

Les protocoles client DHCPv4 et DHCPv6 procèdent de différentes manières pour gérer les données de configuration réseau. Avec DHCPv4, la négociation porte sur le bail d'une seule adresse et de quelques options supplémentaires. Avec DHCPv6, la négociation concerne un lot d'adresses et un ensemble d'options.

Pour plus d'informations sur l'interaction entre le client DHCPv4 et le serveur, reportez-vous au [Chapitre 10, “A propos de DHCP \(présentation\)”](#).

### Traitement des données de configuration réseau par le client DHCPv4

Après avoir obtenu un paquet de données du serveur DHCP, `dhcpageant` se charge de configurer l'interface réseau et d'afficher l'interface. Le démon contrôle l'interface pendant toute la durée du bail de l'adresse IP et gère les données de configuration dans une table interne. Les scripts de démarrage du système utilisent la commande `dhcpcinfo` pour extraire les valeurs des options de configuration à partir de la table interne. Les valeurs servent à configurer le système et lui permettent de communiquer sur le réseau.

Le démon `dhcpcagent` attend de façon passive pendant un laps de temps qui équivaut généralement à la moitié de la durée du bail. Il envoie ensuite une demande de prolongement du bail à un serveur DHCP. Si le système signale à `dhcpcagent` que l'interface est arrêtée ou que l'adresse IP a changé, le démon ne prend pas le contrôle de l'interface tant qu'il n'a pas reçu instruction de le faire par le biais de la commande `ipadm`. Si `dhcpcagent` constate que l'interface fonctionne et que l'adresse n'a pas changé, le démon demande un renouvellement de bail au serveur. Si le renouvellement n'est pas possible, `dhcpcagent` arrête l'interface à la fin du bail.

Chaque fois que `dhcpcagent` effectue une action ayant trait au bail, le démon recherche un fichier exécutable appelé `/etc/dhcp/eventhook`. S'il trouve un fichier exécutable ayant ce nom, `dhcpcagent` lance ce fichier. Pour plus d'informations sur l'utilisation d'un fichier exécutable d'événement, reportez-vous à la section [“Scripts d'événement client DHCP” à la page 203](#).

## Traitement des données de configuration réseau par le client DHCPv6

La communication DHCPv6 entre le client et le serveur commence par l'envoi d'un message de sollicitation par le client qui lui permet de localiser les serveurs. En guise de réponse, tous les serveurs disponibles pour le service DHCP envoient un message de publication. Le message du serveur contient plusieurs enregistrements `IA_NA` ainsi que d'autres options (telles que les adresses serveur DNS) susceptibles d'être fournies par le serveur.

Un client peut demander des adresses particulières (et même un grand nombre) en définissant ses propres enregistrements `IA_NA/IAADDR` dans son message de requête. Cela est généralement le cas lorsqu'il possède d'anciennes adresses enregistrées et qu'il souhaite obtenir les mêmes du serveur, dans la mesure du possible. Quel que soit le comportement du client (même s'il ne demande aucune adresse), le serveur peut fournir un nombre quelconque d'adresses au client lors d'une même transaction DHCPv6.

Voici comme se déroule le dialogue entre les clients et les serveurs.

- Un client envoie un message de sollicitation pour localiser les serveurs.
- Les serveurs envoient un message de publication pour signaler qu'ils se mettent à la disposition du service DHCP.
- Un client envoie un message de requête pour demander des paramètres de configuration, ainsi que des adresses IP, aux serveurs possédant les valeurs de préférence les plus élevées. Les valeurs de préférence sont définies par l'administrateur et vont de 0 à 255.
- Le serveur envoie un message de réponse dans lequel figurent les baux des adresses et les données de configuration.

Si la valeur de préférence dans le message de publication équivaut à 255, le client DHCPv6 sélectionne immédiatement ce serveur. Si le serveur privilégié ne répond pas ou ne parvient pas à adresser un message en réponse au message de requête, le client continue de rechercher des serveurs (en fonction de l'ordre de préférence) jusqu'à ce qu'il ne reste plus de messages de publication. Arrivé à ce stade, le client recommence la procédure en envoyant à nouveau des messages de sollicitation.

Le serveur choisi envoie un message de réponse contenant les adresses assignées et les paramètres de configuration en réponse à un message de sollicitation ou de requête.

## Arrêt du client DHCP

Lors de la mise à l'arrêt, le client envoie un message de libération au serveur ayant alloué des adresses au client pour lui indiquer qu'il n'utilisera plus une ou plusieurs adresses assignées. Lors de l'arrêt normal du système client DHCPv4, `dhcpcd` écrit les informations de configuration actuelles dans un fichier, si ce fichier existe. Le nom de fichier pour DHCPv4 est `/etc/dhcp/interface.dhc` et `/etc/dhcp/interface.dh6` pour DHCPv6. Par défaut, le bail est enregistré au lieu d'être libéré. Le serveur DHCP ne peut donc pas détecter si l'adresse IP est en cours d'utilisation, ce qui permet au client de récupérer facilement l'adresse lors de la prochaine initialisation. L'action par défaut est la même que celle initiée par la commande `ipadm delete-addr dhcp-addrobj`.

Si le bail dans ce fichier est encore valide au redémarrage du système, `dhcpcd` envoie une requête abrégée afin d'utiliser la même adresse IP et les mêmes données de configuration. Dans le cas de DHCPv4, il s'agit du message de requête. Dans le cas de DHCPv6, il s'agit du message de confirmation.

Si le serveur DHCP autorise cette requête, `dhcpcd` peut exploiter les informations qu'il a inscrites sur disque lors de l'arrêt du système. Dans le cas contraire, `dhcpcd` lance la séquence du protocole DHCP décrite à la section [“Mode de fonctionnement du protocole DHCP” à la page 177](#). Le client est en mesure ainsi d'obtenir de nouvelles données de configuration réseau.

## Activation et désactivation d'un client DHCP

Pour activer le client DHCP sur un système qui exécute déjà Oracle Solaris sans le service DHCP, vous devez d'abord annuler la configuration du système. Au démarrage du système, vous devez ensuite exécuter plusieurs commandes afin de configurer le système et d'activer le client DHCP.

---

**Remarque** – Dans de nombreux déploiements, il est d'usage de configurer des parties vitales de l'infrastructure en fonction d'adresses IP statiques, au lieu de faire appel au service DHCP. Les raisons pour lesquelles il est préférable de désigner comme clients des périphériques du réseau (routeurs et certains serveurs, par exemple) sortent du cadre de ce manuel.

---

### ▼ Procédure d'activation du client DHCP

Cette procédure est uniquement nécessaire si le protocole DHCPv4 n'a pas été activé lors de l'installation d'Oracle Solaris. Elle ne présente aucun intérêt pour DHCPv6.

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil DHCP Management.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section “[Configuration de l'accès utilisateur aux commandes DHCP](#)” à la page 183.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Reconfigurez le système.**

Choisissez une des méthodes de configuration ci-dessous :

- **Reconfigurez interactivement le système.**

```
# sysconfig configure
```

Lorsque l'outil System Configuration Interactive (SCI) Tool démarre, sélectionnez la configuration automatique du réseau sur l'écran Réseau.

- **Reconfigurez de manière non interactive le système.**

```
# sysconfig configure -c sc_profile
```

Reportez-vous à la page de manuel [sysconfig\(1M\)](#) pour plus d'informations sur l'utilisation du fichier de configuration `sc_profile`.

## ▼ Procédure de désactivation d'un client DHCP

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle ou un nom d'utilisateur assigné au profil DHCP Management.**

Pour plus d'informations au sujet de ce profil, reportez-vous à la section “[Configuration de l'accès utilisateur aux commandes DHCP](#)” à la page 183.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Reconfigurez le système.**

Choisissez une des méthodes de configuration ci-dessous :

- **Reconfigurez interactivement le système.**

```
# sysconfig configure
```

Lorsque SCI Tool démarre, sélectionnez soit Manuelle, soit Aucune pour la configuration réseau dans l'écran Réseau.

- **Reconfigurez de manière non interactive le système.**

```
# sysconfig configure -c sc_profile
```

Reportez-vous à la page de manuel [sysconfig\(1M\)](#) pour plus d'informations sur l'utilisation du fichier de configuration `sc_profile`.

## Administration du client DHCP

Le logiciel client DHCP n'exige pas d'opérations d'administration dans des conditions normales d'utilisation. Le démon `dhcpcd` démarre automatiquement au redémarrage du système, rénégocie les baux et s'interrompt à l'arrêt du système. Vous ne pouvez pas lancer et interrompre manuellement le démon `dhcpcd`. En revanche, en tant que superutilisateur sur le système client, vous pouvez utiliser la commande `ipadm` pour changer la façon dont `dhcpcd` gère l'interface réseau, si nécessaire.

## Options de la commande `ipadm` utilisées par le client DHCP

Cette section récapitule les options de commande décrites dans la page de manuel [ipadm\(1M\)](#).

La commande `ipadm` vous permet de réaliser les opérations suivantes :

- **Créer l'interface IP** : la commande `ipadm create-ip` crée l'interface IP que vous configurez ensuite avec les adresses IP. Les adresses peuvent être statiques ou dynamiques. La création de l'interface IP est une commande prérequis avant d'affecter les adresses.
- **Exécuter le client DHCP** : la commande `ipadm create-addr -T dhcp dhcp-addrobj` lance l'interaction entre `dhcpcd` et le serveur DHCP en vue d'obtenir l'adresse IP et un nouveau jeu d'options de configuration. L'intérêt de cette commande est évident lorsque vous modifiez des informations que vous souhaitez appliquer immédiatement à un client, par exemple lorsque vous ajoutez des adresses IP ou changez le masque de sous-réseau.
- **Demander uniquement des informations de configuration réseau** : la commande `ipadm refresh-addr -i dhcp-addrobj` fait en sorte que `dhcpcd` émette une demande en vue d'obtenir les paramètres de configuration, adresse IP mise à part. Cette commande est pratique lorsque l'interface réseau possède une adresse IP statique, mais que le système client exige la mise à jour des options réseau. Vous ferez appel à cette commande si vous n'avez pas besoin de DHCP pour gérer les adresses IP, mais que vous l'utilisez pour configurer les hôtes sur le réseau.
- **Demander une extension de bail** : la commande `ipadm refresh-addr dhcp-addrobj` provoque l'émission d'une demande de renouvellement du bail par `dhcpcd`. Le client requiert automatiquement le renouvellement des baux. Cependant, vous pouvez faire appel à cette commande si vous modifiez la durée du bail et souhaitez qu'elle soit appliquée aux clients sans attendre le renouvellement de bail suivant.

- **Libérer l'adresse IP** : la commande `ipadm delete-addr -r dhcp-addrobj` demande à dhcpagent d'abandonner l'adresse IP utilisée par l'interface réseau. La libération de l'adresse IP a automatiquement lieu à l'expiration du bail. Il est possible d'émettre cette commande depuis un ordinateur portable, par exemple, lorsque vous quittez un réseau et comptez lancer le système sur un nouveau réseau. Voir aussi la propriété `RELEASE_ON_SIGTERM` du fichier de configuration `/etc/default/dhcpagent`.
- **Abandonner l'adresse IP** : la commande `ipadm delete-addr dhcp-addrobj` demande à dhcpagent d'arrêter l'interface réseau sans informer le serveur DHCP et de mettre en cache le bail dans le système de fichiers. Cette commande permet au client d'utiliser la même adresse IP sans devoir redémarrer.

---

**Remarque** – Actuellement, la commande `ipadm` ne possède pas de fonctionnalité équivalente pour la commande `ifconfig [inet6] interface status`.

---

## Définition des paramètres de configuration du client DHCP

Le fichier `/etc/default/dhcpagent` qui se trouve sur le système client contient des paramètres ajustables pour dhcpagent. Vous pouvez utiliser un éditeur de texte pour modifier plusieurs paramètres ayant une incidence sur le fonctionnement du client. Le fichier `/etc/default/dhcpagent` est bien documenté, aussi pour plus d'informations, reportez-vous au fichier ainsi qu'à la page du manuel [dhcpagent\(1M\)](#).

Par défaut, le client DHCP est configuré comme suit :

### Pour DHCPv4

- Le système client ne nécessite aucun nom d'hôte particulier.  
Si vous voulez qu'un client porte un nom d'hôte spécifique, reportez-vous à la section [“Noms d'hôtes du client DHCPv4”](#) à la page 200.
- Des requêtes par défaut pour le client sont attribuées dans `/etc/default/dhcpagent` et portent sur le serveur DNS, le domaine DNS et l'adresse de diffusion.  
Le fichier des paramètres du client DHCP peut être configuré pour obtenir des options supplémentaires avec le mot-clé `PARAM_REQUEST_LIST` figurant dans le fichier `/etc/default/dhcpagent`. Le serveur DHCP peut être configuré afin de fournir des options qui n'ont pas été demandées de manière spécifique. Reportez-vous à la page de manuel [dhcpd\(8\)](#) et à la section [“Utilisation des macros DHCP \(liste des tâches\)”](#) du manuel [Guide d'administration système : services IP](#) pour plus d'informations sur l'utilisation des macros du serveur DHCP afin d'envoyer des informations aux clients.

## Pour DHCPv4 et DHCPv6

- Le système client utilise DHCP sur une interface réseau physique.  
Si vous voulez exploiter DHCP sur plusieurs interfaces réseau physiques, reportez-vous à la section [“Systèmes clients DHCP avec plusieurs interfaces réseau” à la page 199](#).
- Le client n'est pas automatiquement configuré en tant que client de service de noms si le client DHCP a été configuré après l'installation d'Oracle Solaris.  
Pour plus d'informations sur l'utilisation des services de noms avec les clients DHCP, reportez-vous à la section [“Systèmes clients DHCP et services de noms” à la page 201](#).

## Systèmes clients DHCP avec plusieurs interfaces réseau

Le client DHCP peut gérer simultanément plusieurs interfaces sur un même système. Il peut s'agir d'interfaces physiques comme d'interfaces logiques. Chaque interface possède sa propre adresse IP et sa propre durée de bail. Si plusieurs interfaces réseau sont configurées pour DHCP, le client émet des demandes distinctes pour les configurer. Le client conserve alors un jeu de paramètres de configuration réseau pour chaque interface. Bien que les paramètres soient stockés indépendamment les uns des autres, certains d'entre eux ont un caractère général. Les paramètres globaux s'appliquent à l'ensemble du système plutôt qu'à une interface réseau particulière.

Le nom d'hôte, le nom de domaine NIS et le fuseau horaire sont des exemples de paramètres globaux. Les paramètres globaux ont, en principe, des valeurs différentes pour chaque interface. Cependant, une seule valeur peut être utilisée pour chaque paramètre global associé à chaque système. Pour éviter qu'une requête portant sur un paramètre global ne génère plusieurs réponses, seuls les paramètres de l'interface réseau principale sont pris en compte.

Le client DHCP procède de la même manière pour gérer les baux des interfaces logiques et des interfaces physiques, à l'exception de la limitation suivante pour les interfaces logiques :

- Le client DHCP ne gère pas les routes par défaut associées aux interfaces logiques.  
Le noyau Oracle Solaris associe les routes aux interfaces physiques, et non pas aux interfaces logiques. Lors de l'établissement de l'adresse IP d'une interface physique, il est essentiel que les routes par défaut appropriées soient placées dans la table de routage. Si vous avez recours par la suite à DHCP pour configurer une interface logique associée à cette interface physique, les routes nécessaires doivent déjà être en place. L'interface logique utilise les mêmes routes.  
Lors de l'expiration d'un bail sur une interface physique, le client DHCP supprime les routes par défaut associées à l'interface. Lors de l'expiration d'un bail sur une interface logique, le client DHCP n'efface pas les routes par défaut associées à l'interface. L'interface physique associée et les autres interfaces logiques devront éventuellement utiliser les mêmes routes.

Si vous avez besoin d'ajouter ou de supprimer les routes par défaut associées à une interface sous le contrôle de DHCP, vous pouvez faire appel au mécanisme de script d'événement du client DHCP. Voir [“Scripts d'événement client DHCP” à la page 203](#).

## Noms d'hôtes du client DHCPv4

Par défaut, le client DHCPv4 ne fournit pas son propre nom d'hôte, car il s'attend à ce qu'il soit proposé par le serveur DHCP. Le serveur DHCPv4 est configuré par défaut de manière à fournir des noms d'hôtes aux clients DHCPv4. Lorsque vous utilisez le serveur et le client DHCPv4 ensemble, ces comportements par défaut ne posent pas de problème. En revanche, lorsque vous utilisez le client DHCPv4 avec des serveurs DHCP tiers, il est possible que le client ne reçoive pas de nom d'hôte du serveur. Si le client DHCP n'obtient pas de nom d'hôte via DHCP, le système client vérifie s'il existe un nom pouvant servir de nom d'hôte dans la propriété `config/nodename` du service `svc:/system/identity:node`. Si le fichier est vide, le nom d'hôte prend la valeur `unknown`.

Si le serveur DHCP fournit un nom dans l'option DHCP `Hostname`, le client utilise ce nom d'hôte, même si une autre valeur figure dans la propriété `config/nodename` du service `svc:/system/identity:node`. Si vous souhaitez que le client utilise un nom d'hôte spécifique, vous pouvez activer le client de façon à ce qu'il réclame ce nom, comme cela est décrit dans la procédure suivante.

---

**Remarque** – La procédure présentée ci-après ne s'applique pas à tous les serveurs DHCP. Elle implique l'envoi d'un nom d'hôte spécifique au serveur DHCP par le client, lequel s'attend en retour à recevoir le même nom.

Le serveur DHCP n'est pas tenu, cependant, de respecter cette demande. C'est d'ailleurs ce qui se produit dans de nombreux cas. Il se contente souvent de renvoyer un autre nom.

---

### ▼ Activation d'un client DHCPv4 pour qu'il demande un nom d'hôte spécifique

Les étapes à réaliser diffèrent selon qu'il existe déjà ou non une interface IP avec une adresse DHCP.

- 1 Si l'interface IP avec une adresse DHCP existe déjà, procédez comme suit :
  - a. Supprimez l'adresse DHCP existante.  

```
# ipadm delete-addr -r dhcp-addrobj
```
  - b. Enregistrez une nouvelle adresse DHCP avec le nom d'hôte spécifique de votre choix.  

```
# ipadm create-addr -T dhcp -h hostname dhcp-addrobj
```



**2 Si l'interface IP n'existe pas, procédez comme suit :**

**a. Créez l'interface IP.**

```
# ipadm create-ip interface
```

**b. Enregistrez une adresse DHCP avec le nom d'hôte spécifique de votre choix.**

```
# ipadm create-addr -T dhcp -h hostname dhcp-addrobj
```

## Systèmes clients DHCP et services de noms

Les systèmes Oracle Solaris prennent en charge les services de noms suivants : DNS, NIS et un magasin de fichiers local (`/etc/inet/hosts`). Pour être exploitable, chaque service de noms exige un certain niveau de configuration. Le service SMF `name-service/switch` doit également être configuré de manière adéquate. Pour plus d'informations, reportez-vous à la page de manuel [nsswitch.conf\(4\)](#).

Pour qu'un système client DHCP utilise un service de noms, il est indispensable de configurer le système en tant que client du service de noms. Par défaut, sauf si vous en avez décidé autrement lors de l'installation du système, seuls les fichiers locaux sont pris en compte.

Le tableau suivant récapitule les problèmes ayant trait à chaque service de noms et à DHCP. Il propose des références croisées vers de la documentation contenant des informations utiles sur la configuration des clients pour chaque service de noms.

TABLEAU 12-1 Informations sur la configuration des services de noms pour les systèmes clients DHCP

Service de noms	Informations relatives à la configuration du client
NIS	<p>Si vous utilisez un service DHCP pour envoyer des informations concernant l'installation d'un réseau Oracle Solaris à un système client, vous pouvez utiliser une macro de configuration contenant les options NISservs et NISdmain. Ces options ont pour effet de transmettre les adresses IP des serveurs NIS et du nom de domaine NIS au client. Le client devient ensuite automatiquement un client NIS.</p> <p>Si un système client DHCP exécute déjà Oracle Solaris, le client NIS n'est pas automatiquement configuré sur ce système lorsque le serveur DHCP envoie les informations NIS au client.</p> <p>Si le serveur DHCP est configuré pour communiquer des informations NIS au système client DHCP, vous pouvez connaître les valeurs transmises au client si vous utilisez la commande <code>dhcpcinfo</code> sur le client de la façon suivante :</p> <pre># /usr/sbin/dhcpcinfo NISdmain</pre> <pre># /usr/sbin/dhcpcinfo NISServs</pre> <p><b>Remarque</b> – Pour DHCPv6, veuillez à inclure -v6 ainsi que divers mots-clés de protocole dans la commande, comme suit :</p> <pre># /usr/sbin/dhcpcinfo -v6 NISDomain</pre> <pre># /usr/sbin/dhcpcinfo -v6 NISServers</pre> <p>Utilisez les valeurs renvoyées pour le nom de domaine NIS et les serveurs NIS lorsque vous configurez le système en tant que client NIS.</p> <p>Pour configurer un client NIS pour un système client DHCP, procédez de manière habituelle comme indiqué au <a href="#">Chapitre 6, “Setting Up and Configuring NIS (Tasks)”</a> du manuel <i>Oracle Solaris Administration: Naming and Directory Services</i>.</p> <p><b>Astuce</b> – Vous pouvez créer un script en y faisant figurer les commandes <code>dhcpcinfo</code> et <code>ypinit</code> afin d'automatiser la configuration du client NIS sur des systèmes clients DHCP.</p>
/etc/inet/hosts	<p>Vous devez configurer le fichier <code>/etc/inet/hosts</code> d'un système client DHCP devant utiliser <code>/etc/inet/hosts</code> pour son service de noms.</p> <p>Le nom d'hôte du système client DHCP est ajouté à son propre fichier <code>/etc/inet/hosts</code> par les outils DHCP. Il convient, cependant, d'ajouter manuellement le nom d'hôte aux fichiers <code>/etc/inet/hosts</code> des autres systèmes dans le réseau. Si le système serveur DHCP utilise <code>/etc/inet/hosts</code> pour la résolution de nom, vous devez également insérer manuellement le nom d'hôte du client sur le système.</p>
DNS	<p>Si le système client DHCP reçoit le nom de domaine DNS via DHCP, les propriétés du service SMF de <code>dns/client</code> sont configurées automatiquement. Pour plus d'informations au sujet de DNS, reportez-vous au manuel <i>Oracle Solaris Administration: Naming and Directory Services</i>.</p>

## Scripts d'événement client DHCP

Il est possible de configurer le client DHCP de façon à l'utiliser comme un programme exécutable ou un script en vue d'effectuer des actions appropriées pour le système client. Le programme ou le script, appelé *script d'événement*, est exécuté automatiquement dès que certains événements liés au bail DHCP se produisent. Vous pouvez vous servir du script d'événement pour exécuter d'autres commandes, programmes ou scripts en réponse à des événements de bail spécifiques. Pour ce faire, vous devez fournir votre propre script d'événement.

Les mots-clés d'événement suivants sont utilisés par dhcpcagent pour signifier des événements de bail DHCP :

Mot-clé d'événement	Description
BOUND et BOUND6	L'interface est configurée pour DHCP. Le client reçoit l'accusé de réception (DHCPv4 ACK) ou (DHCPv6 Reply) du serveur DHCP, qui lui accorde la demande de bail pour une adresse IP. Le script d'événement est appelé immédiatement après la configuration de l'interface.
EXTEND et EXTEND6	Le client prolonge le bail de la ligne spécialisée. Le script d'événement est appelé dès que le client reçoit l'accusé de réception du serveur DHCP ayant trait à la demande de renouvellement.
EXPIRE et EXPIRE6	Le bail expire à la date butoir fixée. Pour DHCPv4, le script d'événement est appelé avant la suppression de l'adresse louée de l'interface et l'interface est signalée comme arrêtée. Pour DHCPv6, le script d'événement est appelé avant la suppression des dernières adresses louées de l'interface.
DROP et DROP6	Le client abandonne la ligne spécialisée pour retirer l'interface du contrôle de DHCP. Le script d'événement est appelé juste avant que l'interface n'échappe au contrôle de DHCP.
RELEASE et RELEASE6	Le client libère l'adresse IP. Le script d'événement est appelé juste avant que le client ne libère l'adresse sur l'interface et n'envoie le paquet DHCPv4 RELEASE ou DHCPv6 Release au serveur DHCP.
INFORM et INFORM6	Une interface se procure des données de configuration nouvelles ou mises à jour à partir d'un serveur DHCP par l'intermédiaire du paquet DHCPv4 INFORM ou du message DHCPv6 Information-Request. Ces événements se produisent si le client DHCP obtient uniquement les paramètres de configuration du serveur, mais pas le bail d'une adresse IP.
LOSS6	Pendant la phase d'expiration, lorsqu'il reste un ou plusieurs baux valides, le script d'événement est appelé juste avant la suppression

des adresses expirées. Les adresses effacées sont signalées par l'indicateur `IFF_DEPRECATED`.

Pour chacun de ces événements, `dhcpcagent` exécute la commande suivante :

```
/etc/dhcp/eventhook interface event
```

où *interface* représente l'interface faisant appel à DHCP et *event* correspond à un des mots-clés d'événement décrits précédemment. Par exemple, la première fois que vous configurez l'interface pour DHCP, `dhcpcagent` appelle le script d'événement de la façon suivante :

```
/etc/dhcp/eventhook net0 BOUND
```

Pour utiliser la fonction de script d'événement, vous devez effectuer les opérations suivantes :

- Donner le nom `/etc/dhcp/eventhook` au fichier exécutable.
- Définir `root` comme propriétaire du fichier.
- Configurer les permissions sur 755 (`rwxr-xr-x`).
- Ecrire le script ou le programme afin de réaliser une série d'actions en réponse à un des événements documentés. Comme Sun est susceptible d'ajouter de nouveaux événements, le programme doit ignorer, en silence, les événements qui ne sont pas reconnus ou qui n'exigent aucune action. Le programme ou le script peut, par exemple, inscrire des informations dans un fichier journal en présence de l'événement `RELEASE`, et ignorer tous les autres événements.
- Rendre le script ou le programme non interactif. Avant de recourir au script d'événement, `stdin`, `stdout` et `stderr` se connectent à `/dev/null`. Pour afficher la sortie ou les erreurs, vous devez la/les rediriger vers un fichier.

Le script d'événement hérite son environnement de programme de `dhcpcagent` et s'exécute avec les privilèges `root`. Il peut faire appel à l'utilitaire `dhcpcinfo` pour obtenir des informations supplémentaires au sujet de l'interface, si cela est nécessaire. Pour plus d'informations, reportez-vous à la page de manuel [dhcpcinfo\(1\)](#).

Le démon `dhcpcagent` attend que le script d'événement prenne fin pour tous les événements. Si le script d'événement ne se termine au bout de 55 secondes, `dhcpcagent` envoie un signal `SIGTERM` au processus du script. Si le processus ne se termine pas au bout de trois secondes supplémentaires, le démon envoie un signal `SIGKILL` pour interrompre le processus.

Vous trouverez un exemple de script d'événement dans la page de manuel [dhcpcagent\(1M\)](#).

## Commandes et fichiers DHCP (référence)

Ce chapitre décrit les relations entre les commandes DHCP et les fichiers DHCP. Il n'explique pas, cependant, comment utiliser les commandes.

Ce chapitre contient les informations suivantes :

- “Commandes DHCP” à la page 205
- “Fichiers utilisés par le service DHCP” à la page 207
- “Services SMF utilisés par le service DHCP” à la page 208

### Commandes DHCP

Le tableau suivant présente les commandes prévues pour gérer le protocole DHCP sur votre réseau.

TABLEAU 13-1 Commandes utilisées dans DHCP

Commande	Description
<code>/usr/lib/inet/dhcd</code>	DHCP ISC uniquement : démon de serveur DHCP ISC. Pour plus d'informations, reportez-vous à la page de manuel <code>dhcd(8)</code> .
<code>/usr/lib/inet/dhcrelay</code>	DHCP ISC uniquement : moyen de relayer les demandes DHCP et BOOTP d'un client sur un réseau sans serveurs DHCP vers des serveurs appartenant à d'autres réseaux. Pour plus d'informations, reportez-vous à la page de manuel <code>dhcrelay(8)</code> .
<code>/usr/lib/inet/in.dhcd</code>	DHCP Sun hérité uniquement : démon de serveur DHCP Sun hérité. exécuté au démarrage du système. Il est déconseillé de lancer directement le démon du serveur. Pour démarrer ou arrêter le démon, utilisez le gestionnaire DHCP, la commande <code>svcadm</code> ou la commande <code>dhcpcfg</code> . Faites appel directement au démon uniquement lorsque vous souhaitez exécuter le serveur en mode de débogage en vue de résoudre des problèmes. Pour plus d'informations, reportez-vous à la page de manuel <code>in.dhcd(1M)</code> .

TABLEAU 13-1 Commandes utilisées dans DHCP (Suite)

Commande	Description
<code>/usr/sadm/admin/bin/dhcpmgr</code>	DHCP Sun hérité uniquement : correspond au gestionnaire DHCP, une interface utilisateur graphique (IG) utilisée spécialement pour configurer et gérer le service DHCP. Le gestionnaire DHCP est l'outil d'administration DHCP recommandé. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpmgr(1M)</a> .
<code>/usr/sbin/dhcpagent</code>	Démon client DHCP prévu pour implémenter le côté client du protocole DHCP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpagent(1M)</a> .
<code>/usr/sbin/dhcpconfig</code>	DHCP Sun hérité uniquement : moyen de configurer des serveurs DHCP et les agents de relais BOOTP et d'annuler la configuration lorsque cela est nécessaire. Cette commande sert également à effectuer une conversion vers un autre format de magasin de données et à importer/exporter les données de configuration DHCP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpconfig(1M)</a> .
<code>/usr/sbin/dhcpinfo</code>	DHCP Sun hérité uniquement : permet aux scripts de démarrage système des systèmes clients Oracle Solaris d'obtenir un certain nombre d'informations (comme le nom de l'hôte) à partir du démon du client DHCP <code>dhcpagent</code> . Vous pouvez également utiliser la commande <code>dhcpinfo</code> dans des scripts ou dans la ligne de commande afin d'obtenir les valeurs des paramètres qui vous intéressent. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpinfo(1)</a> .
<code>/usr/sbin/dhtadm</code>	DHCP Sun hérité uniquement : permet d'apporter des modifications aux options et macros dans la table <code>dhcptab</code> . Cette commande est particulièrement utile dans les scripts que vous créez pour automatiser les changements de vos informations DHCP. Associez la commande <code>dhtadm</code> à l'option <code>-P</code> et traitez la sortie avec la commande <code>grep</code> de manière à rechercher des valeurs d'option particulières dans la table <code>dhcptab</code> . Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhtadm(1M)</a> .
<code>/usr/sbin/ipadm</code>	Permet d'attribuer des adresses IP aux interfaces réseau et/ou de configurer les paramètres d'interface réseau à l'initialisation du système. Sur un client DHCP, la commande <code>ipadm</code> permet de démarrer le service DHCP pour obtenir les paramètres nécessaires (y compris l'adresse IP) à la configuration d'une interface réseau. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">ipadm(1M)</a> .
<code>/usr/sbin/omshell</code>	DHCP ISC uniquement : moyen d'interroger et de modifier l'état du serveur DHCP ISC à l'aide de l'API Object Management (OMAPI). Pour plus d'informations, reportez-vous à la page de manuel <a href="#">omshell(1)</a> .
<code>/usr/sbin/pntadm</code>	DHCP Sun hérité uniquement : permet d'apporter des modifications aux tables de réseau DHCP établissant la correspondance entre ID de client et adresses IP et, éventuellement, d'associer les données de configuration aux adresses IP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">pntadm(1M)</a> .
<code>/usr/sbin/snoop</code>	Permet de capturer et d'afficher le contenu des paquets transmis sur le réseau. <code>snoop</code> est très pratique pour résoudre les problèmes liés au service DHCP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">snoop(1M)</a> .

# Fichiers utilisés par le service DHCP

Le tableau suivant répertorie les fichiers associés à DHCP.

**TABLEAU 13-2** Fichiers et tables utilisés par les démons et les commandes DHCP

Nom du fichier ou de la table	Description
dhcptab	DHCP Sun hérité uniquement : terme générique désignant la table des données de configuration DHCP stockées sous forme d'options avec des valeurs attribuées, lesquelles sont ensuite regroupées dans des macros. Le nom de la table <code>dhcptab</code> et son emplacement sont déterminés par le magasin de données réservé aux informations DHCP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcptab(4)</a> .
Table de réseau DHCP	DHCP Sun hérité uniquement : établit la correspondance entre les adresses IP et les ID de client et les options de configuration. Les tables de réseau DHCP sont nommées d'après l'adresse IP du réseau (10.21.32.0, par exemple). Il n'existe aucun fichier appelé <code>dhcp_network</code> . Le nom et l'emplacement des tables de réseau DHCP sont fonction du magasin de données utilisé pour les informations DHCP. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcp_network(4)</a> .
/etc/dhcp/eventhook	DHCP Sun hérité uniquement : script ou fichier exécutable que le démon <code>dhcpgent</code> peut automatiquement exécuter. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpgent(1M)</a> .
/etc/inet/dhcpd4.conf /etc/inet/dhcpd6.conf	DHCP ISC uniquement : contient des informations de configuration pour le serveur DHCP ISC, <code>dhcpd</code> . Pour plus d'informations, reportez-vous à la page de manuel <code>dhcpd.conf(5)</code> .
/etc/inet/dhcpsvc.conf	DHCP Sun hérité uniquement : stocke les options de démarrage du démon DHCP et les informations du magasin de données. Il est interdit d'éditer ce fichier de façon manuelle. Servez-vous de la commande <code>dhcpconfig</code> pour changer les options de démarrage. Pour plus d'informations, reportez-vous à la page de manuel <a href="#">dhcpsvc.conf(4)</a> .
/etc/dhcp/interface.dhc /etc/dhcp/interface.dh6	Contient les paramètres de configuration obtenus à partir de DHCP pour l'interface réseau indiquée. Le nom de fichier pour DHCPv4 se termine par <code>dhc</code> . Le nom de fichier pour DHCPv6 se termine par <code>dh6</code> . Le client met en mémoire cache les données de configuration actuelles dans le fichier <code>/etc/dhcp/interface.dhc</code> dès que cesse le bail de l'adresse IP de l'interface. En cas d'utilisation du service DHCP sur l'interface <code>qe0</code> , par exemple, <code>dhcpgent</code> met en cache les données de configuration dans <code>/etc/dhcp/qe0.dhc</code> . Lors du prochain démarrage du service DHCP sur l'interface, le client adresse une requête au serveur DHCP afin d'exploiter la configuration mise en mémoire cache (à condition que le bail n'ait pas expiré). Si le serveur DHCP rejette la requête, le client lance le processus standard de négociation du bail DHCP.
/etc/default/dhcpgent	Définit les valeurs des paramètres pour le démon client <code>dhcpgent</code> . Pour plus d'informations sur les paramètres, reportez-vous au fichier <code>/etc/default/dhcpgent</code> ou à la page de manuel <a href="#">dhcpgent(1M)</a> .

TABLEAU 13-2 Fichiers et tables utilisés par les démons et les commandes DHCP (Suite)

Nom du fichier ou de la table	Description
/etc/dhcp/inittab /etc/dhcp/inittab6	DHCP Sun hérité uniquement : définit certains aspects des codes d'options DHCP, tels que le type de données, et affecte des étiquettes mnémoniques. Pour plus d'informations sur la syntaxe du fichier, voir la page de manuel <a href="#">dhcp_inittab(4)</a> . Le fichier /etc/dhcp/inittab6 est utilisé par les clients DHCPv6.  Au niveau du client, les informations provenant du fichier /etc/dhcp/inittab permettent à la commande <code>dhcpinfo</code> d'aider les utilisateurs à mieux comprendre la signification de ces informations. Au niveau du système du serveur DHCP, c'est le démon DHCP et les outils de gestion qui utilisent ce fichier pour obtenir des informations relatives aux options DHCP.  Le fichier /etc/dhcp/inittab remplace le fichier /etc/dhcp/dhcptags utilisé dans les versions précédentes.
/var/db/isc-dhcp/dhcp4.leases /var/db/isc-dhcp/dhcp4.leases- /var/db/isc-dhcp/dhcp6.leases /var/db/isc-dhcp/dhcp6.leases-	DHCP ISC uniquement : répertorie les baux pour les serveurs DHCPv4 et DHCPv6. Les fichiers dont le nom se termine par un "-" sont des copies précédentes.

## Services SMF utilisés par le service DHCP

Le tableau suivant répertorie les services SMF associés à DHCP.

TABLEAU 13-3 Services SMF utilisés par les démons et les commandes DHCP

Nom du service SMF	Description
svc:/network/dhcp-server:default	Contient des informations concernant le périphérique DHCP Sun hérité.
svc:/network/dhcp/server:ipv4 svc:/network/dhcp/server:ipv6	Contient des informations concernant le périphérique DHCP ISC.
svc:/network/dhcp/relay:ipv4 svc:/network/dhcp/relay:ipv6	Contient des informations pour le service qui peut relayer les demandes DHCP et BOOTP vers un serveur DHCP ISC.
svc:/network/dns/client	Contient des informations permettant de résoudre les demandes DNS. Ce service SMF est consulté lors de la configuration du serveur DHCP pour vérifier le domaine DNS et le serveur DNS.
svc:/system/name-service/switch	Indique l'emplacement des bases de données de services de noms et l'ordre de recherche des services de noms pour différents types d'information. Ce service fournit des informations de configuration précises pour un service DHCP.



## PARTIE III

# IPsec

Cette section met l'accent sur la sécurité à l'échelle du réseau. L'architecture IPsec (IP security) protège le réseau au niveau du paquet. IKE (Internet Key Exchange, échange de clé Internet) gère les clés pour IPsec. La fonctionnalité IP Filter d'Oracle Solaris fournit un pare-feu.



## Architecture IPsec (présentation)

---

L'architecture IPsec (IP security) offre la protection cryptographique des datagrammes IP dans les paquets réseau IPv4 et IPv6.

Le présent chapitre contient les informations suivantes :

- “Introduction à IPsec” à la page 211
- “Flux de paquets IPsec” à la page 214
- “Associations de sécurité IPsec” à la page 217
- “Mécanismes de protection IPsec” à la page 218
- “Stratégies de protection IPsec” à la page 221
- “Modes Transport et Tunnel dans IPsec” à la page 222
- “Réseaux privés virtuels et IPsec” à la page 224
- “Passage de la translation d'adresses et IPsec” à la page 225
- “IPsec et SCTP” à la page 226
- “IPsec et les zones Oracle Solaris” à la page 226
- “IPsec et domaines logiques” à la page 226
- “Fichiers et utilitaires IPsec” à la page 227

Pour implémenter IPsec sur votre réseau, reportez-vous au [Chapitre 15, “Configuration d'IPsec \(tâches\)”](#). Pour des informations de référence, reportez-vous au [Chapitre 16, “Architecture IPsec \(référence\)”](#).

## Introduction à IPsec

Pour protéger les paquets IP, IPsec les chiffre et/ou les authentifie. IPsec s'exécute dans le module IP. Par conséquent, une application Internet peut tirer profit d'IPsec sans pour autant avoir à modifier sa configuration. Une utilisation à bon escient d'IPsec en fait un outil efficace de sécurisation du trafic réseau.

La protection IPsec implique les composants principaux suivants :

- **Protocoles de sécurité** : les mécanismes de protection de datagramme IP. L'**en-tête d'authentification** (AH) inclut un hachage du paquet IP et garantit l'intégrité. Bien que le contenu du datagramme ne soit pas chiffré, le destinataire est sûr que le contenu du paquet n'a subi aucune modification et que l'expéditeur a envoyé les paquets. **protocole ESP** chiffre les données IP et obscurcit, par conséquent, le contenu des paquets lors de leur transmission. ESP garantit également l'intégrité des données par le biais d'une option d'algorithme d'authentification.
- **Associations de sécurité (SA)** : paramètres cryptographiques et protocole de sécurité IP pour un flux spécifique de trafic réseau. Chaque SA dispose d'une référence unique appelée SPI (security parameter index, index de paramètres de sécurité).
- **Base de données des associations de sécurité (SADB)** : base de données qui associe un protocole de sécurité à une adresse IP de destination et un numéro d'indexation. Ce numéro d'indexation est appelé **index du paramètre de sécurité**. Ces trois éléments (protocole de sécurité, adresse de destination et SPI) identifient un seul paquet IPsec légitime. La base de données garantit que le paquet protégé est reconnu par le récepteur à son arrivée. Elle permet également au récepteur de déchiffrer la communication, de vérifier que les paquets n'ont pas été altérés, de rassembler les paquets et de livrer les paquets à leur destination finale.
- **Gestion des clés** : génération et distribution des clés des algorithmes cryptographiques et de SPI.
- **Mécanismes de sécurité** : algorithmes de chiffrement et d'authentification qui protègent les données des datagrammes IP.
- **SPD (Security Policy Database, base de données de stratégie de sécurité)** : base de données indiquant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP et identifie le mode de traitement des paquets. Un paquet peut être rejeté, passé au clair ou protégé à l'aide d'IPsec. En ce qui concerne les paquets sortants, les bases de données SPD et SADB déterminent le niveau de protection à appliquer. Pour les paquets entrants, la base de données SPD permet de déterminer l'acceptabilité du niveau de protection. Si le paquet est protégé par IPsec, une consultation de la base de données SPD est effectuée après déchiffrement et vérification du paquet.

IPsec applique les mécanismes de sécurité aux datagrammes IP circulant en direction de l'adresse IP de destination. A l'aide des informations contenues dans la base de données SADB, le destinataire vérifie que les paquets entrants sont légitimes et les déchiffre. Les applications peuvent appeler IPsec pour appliquer les mécanismes aux datagrammes IP au niveau de chaque socket.

Lorsque la stratégie IPsec est appliquée à un port sur lequel un socket est déjà connecté, le trafic qui utilise ce socket ne bénéficie pas de la protection IPsec. Bien sûr, les sockets ouverts sur un port *après* l'application de la stratégie IPsec en bénéficient aussi.

## RFC IPsec

Le groupe IETF (Internet Engineering Task Force) a publié un certain nombre de documents RFC (Request for Comments, demande de commentaires) décrivant l'architecture de sécurité de la couche IP. Tous les RFC constituent la propriété intellectuelle de l'Internet Society. Pour plus d'informations sur les RFC, reportez-vous au site Web <http://www.ietf.org/>. Les références de sécurité IP les plus générales sont couvertes par les RFC suivants :

- RFC 2411, "IP Security Document Roadmap", novembre 1998
- RFC 2401, "Security Architecture for the Internet Protocol", novembre 1998
- RFC 2402, "IP Authentication Header", novembre 1998
- RFC 2406, "IP Encapsulating Security Payload (ESP)", novembre 1998
- RFC 2408, "Internet Security Association and Key Management Protocol (ISAKMP)", novembre 1998
- RFC 2407, "The Internet IP Security Domain of Interpretation for ISAKMP", novembre 1998
- RFC 2409, "The Internet Key Exchange (IKE)", novembre 1998
- RFC 3554, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec," juillet 2003

## Terminologie IPsec

Les documents RFC IPsec définissent un certain nombre de termes qui s'avèrent utiles lors de l'implémentation d'IPsec sur des systèmes. Les tableaux suivants répertorient les termes IPsec, leur acronyme et leur définition. Le [Tableau 14-1](#) dresse la liste des termes de négociation de clés.

**TABLEAU 14-1** Termes IPsec, acronymes et usages

Terme IPsec	Acronymes	Définition
Association de sécurité	SA (Security Association)	Paramètres cryptographiques et protocole de sécurité IP appliqués à un flux spécifique de trafic réseau. Le SA est défini par un triplé : protocole de sécurité, SPI unique et IP de destination.
Base de données d'associations de sécurité	SADB (Security Associations Database)	Base de données contenant toutes les associations de sécurité actives.
Index de paramètre de sécurité	SPI (Security Parameter Index)	Valeur d'indexation d'une association de sécurité. Une SPI est une valeur 32 bits qui différencie les SA partageant une destination IP et un protocole de sécurité.

**TABEAU 14–1** Termes IPsec, acronymes et usages (Suite)

Terme IPsec	Acronymes	Définition
Base de données de stratégie de sécurité	SPD (Security Policy Database)	Base de données déterminant si les paquets entrants et sortants présentent le niveau de protection spécifié.
Echange de clés		Processus de génération de clés utilisant des algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont RSA et Diffie-Hellman.
Diffie-Hellman	DH	Algorithme d'échange de clés permettant la génération et l'authentification de clés. souvent appelé <i>échange de clés authentifiées</i> .
RSA	RSA	Algorithme d'échange de clés permettant la génération et la distribution de clés. Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Association de sécurité Internet et protocole de gestion des clés	ISAKMP (Internet Security Association and Key Management Protocol)	Structure courante d'établissement du format des attributs SA, et de négociation, modification et suppression des SA. ISAKMP est le standard IETF de gestion d'échanges IKE.

## Flux de paquets IPsec

La [Figure 14–1](#) illustre la procédure suivie par un paquet avec adresse IP, en tant que partie intégrante d'un [datagramme IP](#) lors d'un appel IPsec sur un paquet sortant. Le diagramme du flux indique l'endroit auquel les en-têtes d'authentification AH et les associations de sécurité ESP sont susceptibles d'être appliqués au paquet. Les méthodes d'application de ces entités et de sélection des algorithmes sont décrites dans les sections suivantes.

La [Figure 14–2](#) illustre le processus entrant IPsec.

FIGURE 14-1 Application d'IPsec au processus de paquet sortant

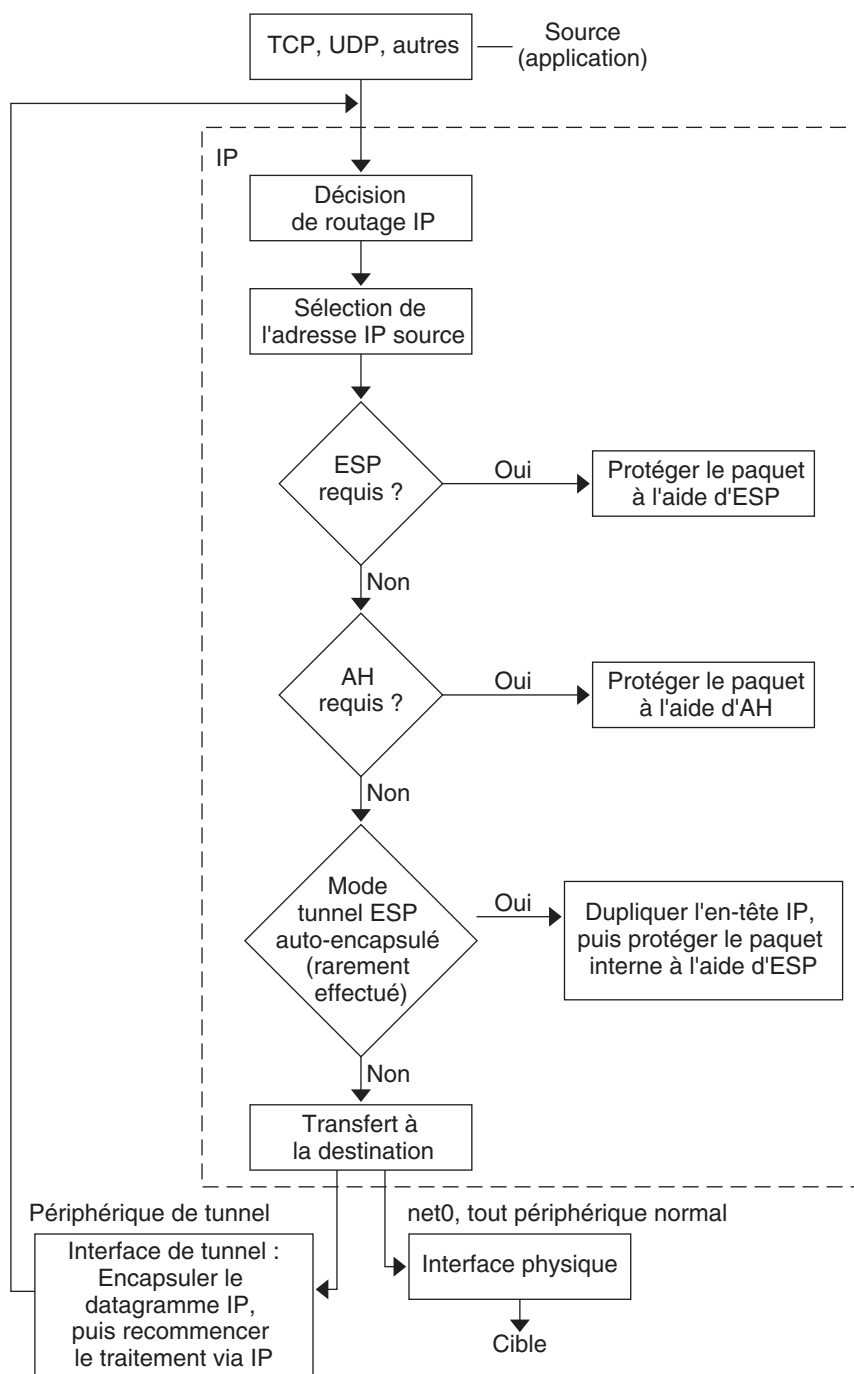
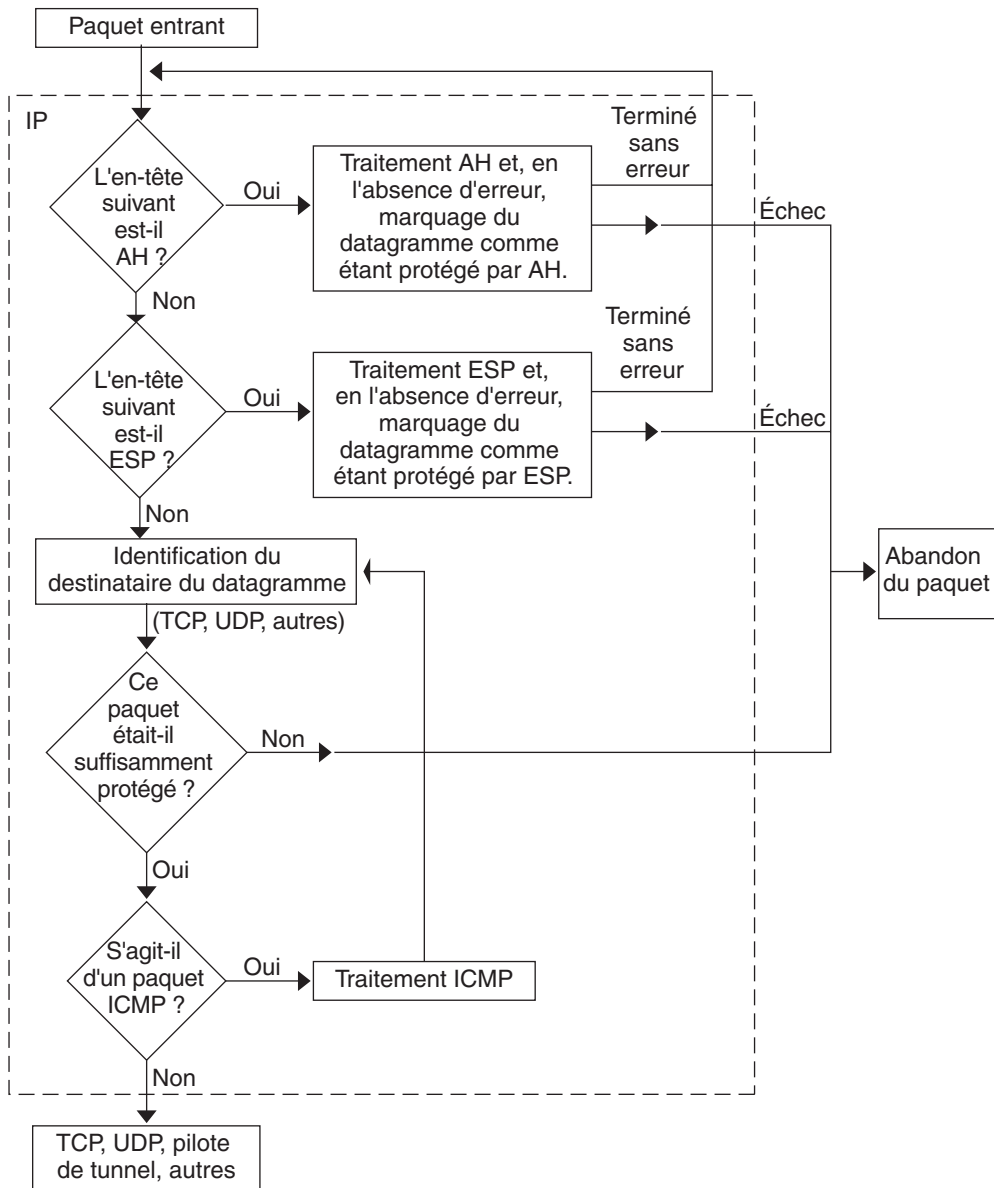


FIGURE 14-2 Application d'IPsec au processus de paquet entrant





## Associations de sécurité IPsec

Une *association de sécurité* (SA, Security Association) IPsec spécifie les propriétés de sécurité que reconnaissent les hôtes lors de la communication. Une seule SA protège les données dans une direction. La protection s'applique à un seul hôte ou à une adresse de groupe (multidiffusion). La communication s'effectuant généralement entre homologues ou entre client et serveur, la sécurité du trafic dans les deux directions requiert la présence de deux SA.

Les trois éléments suivants identifient une SA IPsec de manière unique :

- Le protocole de sécurité (AH ou ESP)
- L'adresse IP de destination
- L'[index du paramètre de sécurité](#)

Le SPI, valeur arbitraire 32 bits, est transmis avec un paquet AH ou ESP. Les pages de manuel [ipsecah\(7P\)](#) et [ipsecesp\(7P\)](#) expliquent l'étendue de la protection AH et ESP. Une somme de contrôle d'intégrité permet d'authentifier un paquet. En cas d'échec de l'authentification, le paquet est rejeté.

Les associations de sécurité sont stockées dans une *base de données d'associations de sécurité* (SADB). Une interface d'administration socket, l'interface PF\_KEY, autorise les applications privilégiées à gérer la base de données. Par exemple, l'application IKE et la commande `ipseckey` font appel à l'interface socket PF\_KEY.

- Pour une description détaillée de la SADB IPsec, reportez-vous à la section “[Base de données des associations de sécurité IPsec](#)” à la page 255.
- Pour plus d'informations sur la gestion de la SADB, consultez la page de manuel [pf\\_key\(7P\)](#).

## Gestion des clés dans IPsec

Les associations de sécurité (SA) requièrent des numéros de clé pour l'authentification et le chiffrement. La gestion de ces numéros de clés s'appelle *gestion des clés*. Le protocole IKE (Internet Key Exchange, échange de clé Internet) gère les clés automatiquement. La commande `ipseckey` permet la gestion manuelle des clés.

Les SA sur les paquets IPv4 et IPv6 peuvent recourir à chacune des méthodes. Il est recommandé d'utiliser IKE à moins d'avoir une bonne raison de préférer la gestion manuelle.

La fonctionnalité d'utilitaire de gestion des services (SMF) d'Oracle Solaris fournit les services de gestion des clés suivants pour IPsec :

- Service `svc:/network/ipsec/ike:default` : service SMF de gestion automatique des clés. Le service `ike` exécute le démon `in.iked` pour la gestion automatique des clés. Le [Chapitre 17, “Protocole IKE \(présentation\)”](#) propose une description du protocole IKE. Pour plus d'informations sur le démon `in.iked`, reportez-vous à la page de manuel [in.iked\(1M\)](#). Pour plus d'informations sur le service `ike`, reportez-vous à la section “Service IKE” à la page 301.
- Service `svc:/network/ipsec/manual-key:default` : service SMF de gestion manuelle des clés. Le service `manual-key` exécute la commande `ipseckey` avec de nombreuses options pour gérer les clés manuellement. Pour obtenir une description de la commande `ipseckey`, reportez-vous à la section “Utilitaires de génération de clés SA dans IPsec” à la page 255. Pour obtenir une description détaillée des options de la commande `ipseckey`, reportez-vous à la page de manuel [ipseckey\(1M\)](#).

# Mécanismes de protection IPsec

IPsec offre deux protocoles de sécurité dans le cadre de la protection des données :

- AH (Authentication Header, en-tête d'authentification)
- ESP (Encapsulating Security Payload, association de sécurité)

AH protège les données à l'aide d'un algorithme d'authentification. ESP protège les données à l'aide d'un algorithme de chiffrement, mais ESP peut et doit être utilisé avec un mécanisme d'authentification. Si vous ne traversez pas de NAT, vous pouvez combiner ESP à AH. Autrement, vous pouvez utiliser un algorithme d'authentification et un mécanisme de chiffrement avec ESP. Un algorithme en mode combiné tel que AES-GCM fournit le chiffrement et l'authentification dans un seul algorithme.

## En-tête Authentification

L'[en-tête d'authentification](#) offre l'authentification des données, un niveau élevé d'intégrité et la protection de rediffusion des datagrammes IP. AH protège la majeure partie du datagramme IP. Comme l'illustre la figure suivante, AH est inséré entre l'en-tête IP et l'en-tête de transport.

En-tête IP	AH	En-tête TCP	
------------	----	-------------	--

L'en-tête de transport peut être TCP, UDP, SCTP ou ICMP. Dans le cas de l'utilisation d'un [tunnel](#), l'en-tête de transport peut être un autre en-tête IP.

## ESP (Encapsulating Security Payload, association de sécurité)

Le module [protocole ESP](#) assure la confidentialité des encapsulations ESP. ESP propose également les services AH. Toutefois, ESP n'offre sa protection qu'à la partie des datagrammes d'encapsulation ESP. ESP fournit des services d'authentification facultatifs afin d'assurer l'intégrité du paquet protégé. Du fait qu'ESP utilise une technologie de chiffrement, un système fournissant ESP peut être soumis à des lois sur le contrôle des importations et exportations.

ESP encapsule ses données de sorte à protéger uniquement les données figurant à la suite de son commencement dans le datagramme, comme illustré ci-dessous.



### Chiffre

Dans un paquet TCP, ESP encapsule uniquement l'en-tête TCP et ses données. Si le paquet est un datagramme IP-in-IP, ESP protège le datagramme IP interne. La stratégie par socket permet l'*auto-encapsulation*. Ainsi, ESP peut encapsuler les options IP, le cas échéant.

Lorsque l'auto-encapsulation est définie, l'en-tête IP est copié afin de créer un datagramme IP-in-IP. Par exemple, lorsque l'auto-encapsulation n'est pas définie sur un socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) options + TCP + data ]
```

Lorsque l'auto-encapsulation est définie sur ce socket TCP, le datagramme est envoyé dans le format suivant :

```
[ IP(a -> b) + ESP [ IP(a -> b) options + TCP + data ] ]
```

Pour plus d'informations, reportez-vous à la section [“Modes Transport et Tunnel dans IPsec” à la page 222](#).

## Considérations de sécurité lors de l'utilisation de AH et ESP

Le tableau suivant permet de comparer les protections AH et ESP.

TABLEAU 14–2 Protections assurées par AH et ESP dans IPsec

Protocole	Paquets protégés	Protection	Attaques contrées
AH	Protection des paquets de l'en-tête IP jusqu'à l'en-tête de transport	Intégrité élevée, authentification des données : <ul style="list-style-type: none"><li>■ réception garantie des données exactes envoyées par l'expéditeur</li><li>■ attaques par rejeu possibles lorsqu'un AH n'active pas la protection par rejeu</li></ul>	Rejeu, couper-coller
fournisseur de services aux entreprises	Protection des paquets figurant à la suite du début d'ESP dans le datagramme	Chiffrement de la charge utile IP à l'aide de l'option de chiffrement Confidentialité garantie	Ecoute électronique
		Protection identique à la protection AH à l'aide de l'option d'authentification	Rejeu, couper-coller
		Intégrité élevée, authentification des données et confidentialité à l'aide des deux options	Rejeu, couper-coller, écoute électronique

## Authentification et chiffrement dans IPsec

Les protocoles de sécurité IPsec font appel à deux types d'algorithmes : les algorithmes d'authentification et les algorithmes de chiffrement. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut utiliser aussi bien les algorithmes d'authentification que les algorithmes de chiffrement. La commande `ipsecacls` affiche la liste des algorithmes présents sur le système, ainsi que leurs propriétés. Pour plus d'informations, reportez-vous à la page de manuel [ipsecacls\(1M\)](#). Vous pouvez aussi utiliser les fonctions décrites dans la page de manuel [getipsecaclbyname\(3NSL\)](#) pour obtenir les propriétés des algorithmes.

IPsec utilise la fonction de structure cryptographique d'Oracle Solaris pour accéder aux algorithmes. Celle-ci offre un référentiel central d'algorithmes, en plus d'autres services. Elle permet à IPsec de tirer profit des accélérateurs cryptographiques hautes performances et

Pour plus d'informations, consultez les références suivantes :

- Chapitre 11, “Structure cryptographique (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Chapitre 8, “Introduction to the Oracle Solaris Cryptographic Framework” du manuel *Developer's Guide to Oracle Solaris 11 Security*

## Algorithmes d'authentification dans IPsec

Les algorithmes d'authentification génèrent une valeur de somme de contrôle d'intégrité, *digest*, à partir des données et d'une clé. Le module AH recourt aux algorithmes d'authentification. Le module ESP peut également y avoir recours.

## Algorithmes de chiffrement dans IPsec

Les algorithmes de chiffrement chiffrent les données à l'aide d'une clé. Dans IPsec, le module ESP fait appel aux algorithmes de chiffrement. Les algorithmes agissent sur les données dans des unités d'une *taille de bloc*.

## Stratégies de protection IPsec

Les stratégies de protection IPsec peuvent recourir aux mécanismes de sécurité, quels qu'ils soient. Vous pouvez appliquer les stratégies IPsec aux niveaux suivants :

- A l'échelle du système
- Par socket

IPsec applique la stratégie à l'échelle du système aux datagrammes entrants et sortants. Les datagrammes sortants sont envoyés avec ou sans protection. Si la protection est appliquée, les algorithmes sont soit spécifiques, soit non spécifiques. Vous pouvez appliquer d'autres règles aux datagrammes sortants, en raison des données supplémentaires connues du système. Les datagrammes sortants peuvent être acceptés ou rejetés. La décision d'accepter ou de rejeter un datagramme sortant est fonction de plusieurs critères qui peuvent se chevaucher et être contradictoires. Pour résoudre les conflits éventuels, il faut identifier la règle à analyser en premier. Le trafic est accepté automatiquement, sauf si une entrée de stratégie indique qu'il doit ignorer toutes les autres stratégies.

La stratégie qui protège normalement un datagramme peut être ignorée. Vous pouvez spécifier une exception dans la stratégie à l'échelle du système ou demander un contournement dans la stratégie par socket. Au niveau du trafic système, les stratégies sont mises en oeuvre, mais les mécanismes de sécurité à proprement parler ne sont pas appliqués. En revanche, la stratégie sortante sur un paquet interne au système se traduit par un paquet sortant auquel ces mécanismes ont été appliqués.

La configuration des stratégies IPsec s'effectue à l'aide du fichier `ipsecinit.conf` et de la commande `ipsecconf`. La page de manuel [ipsecconf\(1M\)](#) contient des exemples et des explications complémentaires.

## Modes Transport et Tunnel dans IPsec

Les normes IPsec définissent deux modes distincts d'opération IPsec : le *mode Transport* et le *mode Tunnel*. Ces modes n'ont aucune incidence sur le codage des paquets. Les paquets sont protégés par AH, ESP ou ces deux protocoles dans chaque mode. L'application de la stratégie des modes est différente lorsque le paquet interne est un paquet IP :

- En mode Transport, l'en-tête extérieur détermine la stratégie IPsec qui protège le paquet IP interne.
- En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

En mode Transport, l'en-tête extérieur ainsi que l'en-tête suivant et tout port pris en charge par celui-ci permettent de déterminer la stratégie IPsec. En fait, IPsec peut mettre en oeuvre différentes stratégies en mode Transport entre deux adresses IP au niveau d'un seul port. Par exemple, si l'en-tête suivant est un en-tête TCP, qui prend en charge les ports, la stratégie IPsec peut alors être définie pour un port TCP de l'adresse IP externe. De même, si l'en-tête suivant est IP, l'en-tête extérieur et l'en-tête IP intérieur permettent de déterminer la stratégie IPsec.

Le mode Tunnel ne fonctionne que pour les datagrammes IP-in-IP. La mise sous tunnel en mode Tunnel peut s'avérer utile lorsque des personnes travaillant à domicile se connectent à un emplacement central. En mode Tunnel, la stratégie IPsec est mise en oeuvre sur le contenu du datagramme IP interne. Différentes stratégies IPsec peuvent être mises en oeuvre pour différentes adresses IP internes. En d'autres termes, l'en-tête IP interne, ainsi que son en-tête suivant et les ports que ce dernier prend en charge, peuvent mettre en oeuvre une stratégie. Contrairement au mode Transport, le mode Tunnel ne permet pas à l'en-tête IP extérieur de dicter la stratégie de son datagramme IP interne.

Par conséquent, en mode Tunnel, la stratégie IPsec peut être spécifiée pour les sous-réseaux d'un LAN derrière un routeur et pour les ports de ces sous-réseaux. La stratégie IPsec peut également être spécifiée pour des adresses IP données (des hôtes) sur ces sous-réseaux. Les ports de ces hôtes peuvent aussi avoir une stratégie IPsec spécifique. Toutefois, si un protocole de routage dynamique est exécuté sur un tunnel, veillez à ne pas utiliser de sélection de sous-réseau ou d'adresse, car la vue de la topologie réseau sur le réseau homologue pourrait être modifiée. Les modifications annuleraient la stratégie IPsec statique. La section [“Protection d'un VPN à l'aide d'IPsec” à la page 236](#) contient des exemples de mises en tunnel comprenant la configuration de routes statiques.

Dans Oracle Solaris, le mode Tunnel ne peut être mis en oeuvre que sur une interface réseau de mise en tunnel IP. Pour obtenir des informations sur les interfaces de mise en tunnel, reportez-vous au [Chapitre 6, “Configuration de tunnels IP”](#). La commande `ipseconf` fournit un mot-clé `tunnel` pour sélectionner une interface réseau de mise en tunnel IP. Lorsque le mot-clé `tunnel` figure dans une règle, tous les sélecteurs spécifiés dans cette règle s'appliquent au paquet interne.

En mode Transport, ESP et/ou AH peuvent protéger le datagramme.

La figure suivante illustre un en-tête IP avec un paquet TCP non protégé.

FIGURE 14-3 Paquet IP non protégé transportant des informations TCP



En mode Transport, ESP protège les données, comme illustré ci-dessous. La zone ombrée indique la partie chiffrée du paquet.

FIGURE 14-4 Paquet IP protégé transportant des informations TCP



 Chiffré

En mode Transport, AH protège les données comme illustré ci-dessous.

FIGURE 14-5 Paquet protégé par un en-tête d'authentification



La protection AH, même en mode Transport, porte sur la majeure partie de l'en-tête IP.

En mode Tunnel, l'intégralité du datagramme figure à l'intérieur de la protection d'un en-tête IPsec. Le datagramme de la [Figure 14-3](#) est protégé en mode Tunnel par un en-tête IPsec externe, ESP dans ce cas, comme indiqué sur l'illustration suivante.

FIGURE 14-6 Paquet IPsec protégé en mode Tunnel



 Chiffré

La commande `ipsecconf` inclut des mots-clés permettant de définir des tunnels en mode Tunnel ou Transport.

- Pour plus d'informations sur la stratégie par socket, reportez-vous à la page de manuel [ipsec\(7P\)](#).
- La section “[Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.](#)” à la page 233 comprend un exemple de stratégie par socket.

- Pour plus d'informations sur les tunnels, reportez-vous à la page de manuel [ipseconf\(1M\)](#).
- La section “[Procédure de protection d'un VPN avec IPsec en mode Tunnel](#)” à la page 239 contient un exemple de configuration de tunnel.

## Réseaux privés virtuels et IPsec

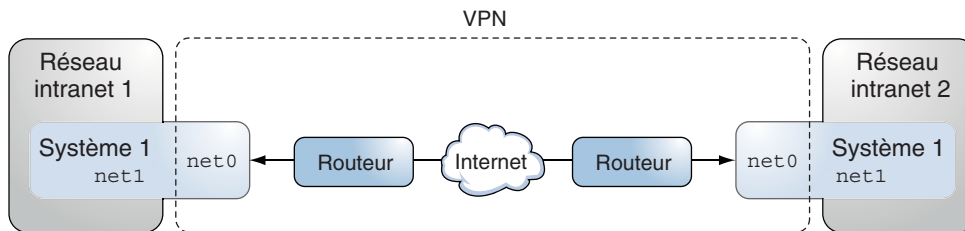
Un tunnel configuré est une interface point-à-point. Le tunnel permet l'encapsulation d'un paquet IP dans un autre paquet IP. Un tunnel correctement configuré requiert une source et une destination. Pour plus d'informations, reportez-vous à la section “[Création et configuration d'un tunnel IP](#)” à la page 127.

Un tunnel crée une [interface physique](#) liée à IP. L'intégrité du lien physique est fonction des protocoles de sécurité sous-jacents. La configuration sécurisée des associations de sécurité (SA) rend le tunnel digne de confiance. Les paquets sortant du tunnel doivent provenir de l'homologue spécifié dans la destination de tunnel. Si la confiance est établie, vous pouvez avoir recours au transfert IP par interface pour créer un [VPN](#).

Vous pouvez ajouter des protections IPsec à un VPN. IPsec sécurise la connexion. Par exemple, une organisation ayant recours à la technologie VPN pour connecter deux bureaux de réseaux distincts peut ajouter IPsec pour sécuriser le trafic entre ces deux bureaux.

La figure suivante illustre comment deux bureaux forment un VPN avec IPsec déployé sur leurs systèmes de réseau.

FIGURE 14-7 Réseau privé virtuel



Pour voir un exemple détaillé de la procédure de configuration, reportez-vous à la section “[Procédure de protection d'un VPN avec IPsec en mode Tunnel](#)” à la page 239.



## Passage de la translation d'adresses et IPsec

IKE peut négocier des SA IPsec dans une zone [NAT](#). Cela permet aux systèmes de se connecter en toute sécurité à partir d'un réseau distant, même lorsqu'ils résident derrière un périphérique NAT. Par exemple, les employés travaillant à domicile ou se connectant depuis un site de conférence peuvent protéger leur trafic à l'aide d'IPsec.

NAT est l'acronyme de Network Address Translation (translation d'adresse réseau). Un routeur NAT permet d'associer une adresse interne privée à une adresse Internet unique. Les routeurs NAT équipent de nombreux points d'accès publics à Internet, comme ceux qu'on trouve dans les hôtels. Pour plus d'informations, reportez-vous à la section [“Utilisation de la fonctionnalité NAT d'IP Filter”](#) à la page 317.

L'utilisation d'IKE lorsqu'un routeur NAT figure entre les systèmes de communication correspond au NAT-T (NAT traversal). NAT-T présente les restrictions suivantes :

- Le protocole AH dépend d'un en-tête IP permanent, ce qui empêche son fonctionnement avec NAT-T. Le protocole ESP s'utilise avec NAT-T.
- Le routeur NAT n'applique pas de règles de traitement particulières. Un routeur NAT obéissant à des règles de traitement IPsec pourrait intervenir dans l'implémentation de NAT-T.
- NAT-T fonctionne uniquement lorsque l'initiateur IKE est le système derrière le routeur NAT. Un répondeur IKE ne peut pas se trouver derrière un routeur NAT, à moins que celui-ci ne soit programmé pour transférer des paquets IKE au système adéquat figurant derrière lui.

Les documents RFC suivants décrivent la fonctionnalité NAT et les restrictions de NAT-T. Vous pouvez obtenir des copies des RFC à l'adresse suivante : <http://www.rfc-editor.org>.

- RFC 3022, "Traditional IP Network Address Translator (Traditional NAT)", janvier 2001
- RFC 3715, "IPsec-Network Address Translation (NAT) Compatibility Requirements", mars 2004
- RFC 3947, "Negotiation of NAT-Traversal in the IKE", janvier 2005
- RFC 3948, "UDP Encapsulation of IPsec Packets", janvier 2005

Pour une utilisation conjointe d'IPsec et NAT, reportez-vous à la section [“Configuration du protocole IKE pour les systèmes portables \(liste des tâches\)”](#) à la page 291.

## IPsec et SCTP

Oracle Solaris prend en charge le protocole SCTP (Streams Control Transmission Protocol). Bien que prise en charge, l'utilisation du protocole SCTP et du numéro de port SCTP dans le cadre de la spécification de la stratégie IPsec n'est pas stable. Les extensions IPsec pour SCTP spécifiées dans le document RFC 3554 ne sont pas encore implémentées. Ces restrictions peuvent être source de complications lors de la création de la stratégie IPsec pour SCPT.

SCTP peut avoir recours à plusieurs adresses source et cible dans le cadre d'une association SCTP unique. Lorsque la stratégie IPsec est appliquée à une seule adresse source ou cible, la communication peut échouer si SCTP change l'adresse source ou cible de cette association. La stratégie IPsec reconnaît uniquement l'adresse d'origine. Pour plus d'informations sur le protocole SCTP, consultez les documents RFC et la section [“Protocol SCTP” du manuel \*Guide d'administration système : services IP\*](#).

## IPsec et les zones Oracle Solaris

Pour les zones IP partagées, la stratégie IPsec est configurée à partir de la zone globale. Le fichier de configuration de la stratégie IPsec, `ipsecinit.conf`, existe uniquement dans la zone globale. Le fichier peut contenir des entrées s'appliquant aux zones non globales et des entrées s'appliquant à la zone globale.

Pour les zones IP exclusives, IPsec est configurée par zone non globale.

Pour plus d'informations à propos de l'utilisation d'IPsec avec des zones, reportez-vous à la section [“Protection du trafic à l'aide d'IPsec” à la page 229](#). Pour obtenir des informations sur les zones, reportez-vous au [Chapitre 15, “Introduction à Oracle Solaris Zones” du manuel \*Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources\*](#).

## IPsec et domaines logiques

Le protocole IPsec fonctionne avec des domaines logiques. Le domaine logique doit exécuter une version d'Oracle Solaris comprenant le protocole IPsec, comme la version Oracle Solaris 10.

Pour créer des domaines logiques, vous devez utiliser Oracle VM Server for SPARC. Cette application s'appelait auparavant Sun Logical Domains. Pour savoir comment configurer des domaines logiques, reportez-vous au manuel [Guide d'administration d'Oracle VM Server for SPARC 2.1](#) ou au manuel *Oracle VM Server for SPARC 2.0 Administration Guide*.

## Fichiers et utilitaires IPsec

Le [Tableau 14–3](#) décrit les fichiers, commandes et identificateurs de service utilisés pour configurer et gérer IPsec. Exhaustif, ce tableau inclut les commandes et fichiers de gestion des clés.

Pour plus d'informations sur les identificateurs de services, reportez-vous au [Chapitre 6](#), “Gestion des services (présentation)” du manuel *Administration d'Oracle Solaris : Tâches courantes*.

- Pour obtenir des instructions sur la mise en oeuvre d'IPsec sur votre réseau, reportez-vous à la section “Protection du trafic à l'aide d'IPsec” à la page 229.
- Pour plus d'informations sur les fichiers et utilitaires IPsec, reportez-vous au [Chapitre 16](#), “Architecture IPsec (référence)”.

TABLEAU 14–3 Liste des utilitaires et fichiers IPsec sélectionnés

Utilitaire IPsec, fichier ou service	Description	Page de manuel
<code>svc:/network/ipsec/ipsecalgs</code>	Service SMF qui gère les algorithmes IPsec.	<a href="#">ipsecalgs(1M)</a>
<code>svc:/network/ipsec/manual-key</code>	Service SMF qui gère les SA IPsec dont les clés sont spécifiées manuellement.	<a href="#">ipseckey(1M)</a>
<code>svc:/network/ipsec/policy</code>	Service SMF qui gère la stratégie IPsec.	<a href="#">smf(5)</a> , <a href="#">ipseconf(1M)</a>
<code>svc:/network/ipsec/ike</code>	Service SMF pour la gestion automatique des SA IPsec à l'aide d'IKE.	<a href="#">smf(5)</a> , <a href="#">in.iked(1M)</a>
Fichier <code>/etc/inet/ipsecinit.conf</code>	Fichier de stratégie IPsec.  Le service <code>policy</code> de SMF utilise ce fichier pour configurer la stratégie IPsec à l'initialisation du système.	<a href="#">ipseconf(1M)</a>
Commande <code>ipseconf</code>	Commande de stratégie IPsec. Utile pour afficher et modifier la stratégie IPsec actuelle, ainsi que pour effectuer des tests.  Le service <code>policy</code> de SMF s'en sert pour configurer la stratégie IPsec lors de l'initialisation du système.	<a href="#">ipseconf(1M)</a>
Interface socket <code>PF_KEY</code>	SADB (Interface for Security Associations Database, interface de la base de données des associations de sécurité). Responsable de la gestion manuelle et automatique des clés.	<a href="#">pf_key(7P)</a>
Commande <code>ipseckey</code>	Commandes de génération de clés pour les SA IPsec <code>ipseckey</code> est un point d'entrée de commandes de l'interface <code>PF_KEY</code> . <code>ipseckey</code> permet de créer, supprimer ou modifier les SA.	<a href="#">ipseckey(1M)</a>

TABLEAU 14-3 Liste des utilitaires et fichiers IPsec sélectionnés (Suite)

Utilitaire IPsec, fichier ou service	Description	Page de manuel
Fichier <code>/etc/inet/secret/ipseckey</code> s	Contient des SA dotés de clés attribuées manuellement.  Le service <code>manual-key</code> de SMF s'en sert pour configurer les SA lors de l'initialisation du système.	
Commande <code>ipsecalgs</code>	Commande d'algorithmes IPsec. Utile pour l'affichage et la modification de la liste d'algorithmes IPsec et de leurs propriétés.  Le service <code>ipsecalgs</code> de SMF s'en sert pour synchroniser les algorithmes IPsec connus avec le noyau lors de l'initialisation du système.	<a href="#">ipsecalgs(1M)</a>
Fichier <code>/etc/inet/ipsecalgs</code>	Contient les définitions d'algorithmes et les protocoles IPsec configurés. Ce fichier est géré par la commande <code>ipsecalgs</code> et ne doit jamais être modifié manuellement.	
Fichier <code>/etc/inet/ike/config</code>	Fichier de configuration et de stratégie IKE. Par défaut, ce fichier n'existe pas. La gestion se base sur des règles et des paramètres généraux figurant dans le fichier <code>/etc/inet/ike/config</code> . Reportez-vous à la section “Utilitaires et fichiers IKE” à la page 263.  Si ce fichier existe, le service <code>svc:/network/ipsec/ike</code> démarre le démon IKE, <code>in.iked</code> , pour la gestion automatique des clés.	<a href="#">ike.config(4)</a>

## Configuration d'IPsec (tâches)

---

Ce chapitre fournit les procédures d'implémentation d'IPsec sur votre réseau. Ces procédures sont décrites dans les sections suivantes :

- “Protection du trafic à l'aide d'IPsec” à la page 229
- “Protection d'un VPN à l'aide d'IPsec” à la page 236
- “Gestion d'IPsec et d'IKE” à la page 242

Vous trouverez une présentation d'IPsec au [Chapitre 14, “Architecture IPsec \(présentation\)”](#). Des informations de référence sur IPsec sont fournies au [Chapitre 16, “Architecture IPsec \(référence\)”](#).

### Protection du trafic à l'aide d'IPsec

Cette section décrit les procédures permettant de sécuriser le trafic entre deux systèmes et de sécuriser un serveur Web. Pour protéger un VPN (Virtual Private Network, réseau privé virtuel), reportez-vous à la section “[Protection d'un VPN à l'aide d'IPsec](#)” à la page 236. Pour obtenir des informations sur les procédures supplémentaires de gestion d'IPsec et sur l'utilisation des commandes SMF avec IPsec et IKE, reportez-vous à la section “[Gestion d'IPsec et d'IKE](#)” à la page 242.

Les informations ci-dessous s'appliquent à toutes les tâches de configuration IPsec :

- **IPsec et zones** : pour gérer les clés et la stratégie IPsec dans le cas d'une zone non globale IP partagée, créez le fichier de stratégie IPsec dans la zone globale, puis exécutez les commandes de configuration IPsec à partir de la zone globale. Utilisez l'adresse source correspondant à la zone non globale à configurer. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.
- **IPsec et RBAC** : pour utiliser les rôles afin d'administrer IPsec, reportez-vous au [Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. La section “Configuration d'un rôle pour la sécurité réseau” à la page 245 présente un exemple.

- **IPsec et SCTP** : vous pouvez utiliser IPsec pour protéger les associations SCTP (Streams Control Transmission Protocol, protocole de transmission de contrôle de flux), mais avec prudence. Pour plus d'informations, reportez-vous à la section [“IPsec et SCTP”](#) à la page 226.
- **IPsec et étiquettes Trusted Extensions** : sur les systèmes configurés avec la fonctionnalité Trusted Extensions d'Oracle Solaris, il est possible d'ajouter des étiquettes aux paquets IPsec. Pour plus d'informations, reportez-vous à la section [“Administration d'IPsec avec étiquettes”](#) du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.
- **Adresses IPv4 et IPv6** : l'exemple IPsec dans ce guide utilise des adresses IPv4. Oracle Solaris prend également en charge les adresses IPv6. Pour configurer IPsec pour un réseau IPv6, remplacez les adresses des exemples par des adresses IPv6. Lorsque vous protégez des tunnels avec IPsec, vous pouvez utiliser des adresses IPv4 et IPv6 en guise d'adresses internes et externes. Une telle configuration vous permet d'acheminer IPv6 via tunnel sur un réseau IPv4, par exemple.

La liste des tâches ci-dessous répertorie les procédures de configuration d'IPsec sur un ou plusieurs systèmes. Les pages de manuel [ipseconf\(1M\)](#), [ipseckey\(1M\)](#) et [ipadm\(1M\)](#) décrivent également des procédures utiles dans leurs sections d'exemples respectives.

Tâche	Description	Voir
Sécurisation du trafic entre deux systèmes	Protège les paquets transmis d'un système à un autre.	<a href="#">“Sécurisation du trafic entre deux systèmes à l'aide d'IPsec”</a> à la page 231
Sécurisation d'un serveur Web à l'aide de la stratégie IPsec	Requiert un trafic non-Web pour utiliser IPsec. Les clients Web sont identifiés par des ports particuliers : les vérifications IPsec sont ignorées.	<a href="#">“Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.”</a> à la page 233
Affichage des stratégies IPsec	Affiche les stratégies IP actuellement mises en oeuvre, dans l'ordre de mise en oeuvre.	<a href="#">“Affichage des stratégies IPsec”</a> à la page 235
Utilisation d'IKE pour créer automatiquement des numéros de clés pour les SA IPsec.	Fournit les données brutes des associations de sécurité.	<a href="#">“Configuration du protocole IKE (liste des tâches)”</a> à la page 267
Configuration d'un réseau privé virtuel (VPN, Virtual Private Network) sécurisé	Définit IPsec entre deux systèmes sur Internet.	<a href="#">“Protection d'un VPN à l'aide d'IPsec”</a> à la page 236

## ▼ Sécurisation du trafic entre deux systèmes à l'aide d'IPsec

Cette procédure correspond à la configuration suivante :

- Les systèmes s'appellent *enigma* et *partym*.
- Chaque système dispose d'une adresse IP. Il peut d'agir d'une adresse IPv4, IPv6 ou les deux.
- Chaque système nécessite le chiffrement ESP avec l'algorithme AES, qui requiert une clé de 128 bits, ainsi que l'authentification ESP avec la synthèse des messages SHA-2, qui requiert une clé de 512 bits.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).  
Avec les SA partagées, une seule paire de SA est suffisante pour protéger les deux systèmes.

---

**Remarque** – Pour utiliser IPsec avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section [“Procédure d'application des protections IPsec dans un réseau Trusted Extensions multiniveau”](#) du manuel *Configuration et administration d'Oracle Solaris Trusted Extensions*.

---

### Avant de commencer

La stratégie IPsec peut être configurée dans la zone globale ou dans une zone de pile IP en mode exclusif. La stratégie pour une zone de pile IP en mode partagé doit être configurée dans la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

#### 2 Sur chaque système, ajoutez des entrées d'hôte au fichier `/etc/inet/hosts`.

Cette étape permet au SMF d'utiliser le système de noms sans dépendre de services de noms inexistants. Pour plus d'informations, reportez-vous à la page de manuel [smf\(5\)](#).

##### a. Sur un système appelé *partym*, saisissez les lignes suivantes dans le fichier `hosts` :

```
# Secure communication with enigma
192.168.116.16 enigma
```

##### b. Sur un système appelé *enigma*, saisissez les lignes suivantes dans le fichier `hosts` :

```
# Secure communication with partym
192.168.13.213 partym
```

**3 Sur chaque système, créez le fichier de stratégie IPsec.**

Le nom de fichier est `/etc/inet/ipsecinit.conf`. Vous en trouverez un exemple dans le fichier `/etc/inet/ipsecinit.sample`.

**4 Ajoutez une entrée de stratégie IPsec au fichier `ipsecinit.conf`.****a. Sur le système `enigma`, ajoutez la stratégie ci-dessous :**

```
{laddr enigma raddr partym} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

**b. Sur le système `partym`, ajoutez la même stratégie :**

```
{laddr partym raddr enigma} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

La syntaxe des entrées de stratégie IPsec est décrite dans la page de manuel [ipseconf\(1M\)](#).

**5 Dans chaque système, configurez IKE afin d'ajouter une paire de SA IPsec entre les deux systèmes.**

Configurez IKE en suivant l'une des procédures de configuration décrites à la section “[Configuration du protocole IKE \(liste des tâches\)](#)” à la page 267. La syntaxe du fichier de configuration IKE est décrite à la page de manuel [ike.config\(4\)](#).

---

**Remarque** – Si vous devez générer et maintenir vos clés manuellement, reportez-vous à la section “[Création manuelle de clés IPsec](#)” à la page 243.

---

**6 Vérifiez la syntaxe du fichier de stratégie IPsec.**

```
# ipseconf -c -f /etc/inet/ipsecinit.conf
```

Corrigez les éventuelles erreurs, vérifiez la syntaxe du fichier, puis continuez.

**7 Actualisez la stratégie IPsec.**

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La stratégie IPsec est activée par défaut. *Actualisez-la*. Si vous avez désactivé la stratégie IPsec, activez-la.

```
# svcadm enable svc:/network/ipsec/policy:default
```

**8 Activez les clés pour IPsec.****■ Si le service `ike` n'est pas activé, activez-le.**

```
# svcadm enable svc:/network/ipsec/ike:default
```

**■ Si le service `ike` est activé, redémarrez-le.**

```
# svcadm restart svc:/network/ipsec/ike:default
```

Si vous avez configuré les clés manuellement à l'[Étape 5](#), suivez la procédure de la section “[Création manuelle de clés IPsec](#)” à la page 243 pour activer les clés.



## 9 Assurez-vous que les paquets sont protégés.

La procédure est décrite à la section “[Vérification de la protection des paquets par IPsec](#)” à la page 248.

### Exemple 15–1 Ajout d'une stratégie IPsec lors de l'utilisation d'une connexion ssh

Dans cet exemple, l'administrateur ayant le rôle root configure la stratégie et les clés IPsec sur deux systèmes en utilisant la commande `ssh` pour atteindre le second système. Pour plus d'informations, reportez-vous à la page de manuel [ssh\(1\)](#).

- Tout d'abord, l'administrateur configure le premier système en effectuant les étapes [Étape 2](#) à [Étape 6](#) de la procédure précédente.
- Ensuite, dans une autre fenêtre de terminal, l'administrateur utilise la commande `ssh` pour se connecter au deuxième système.

```
local-system # ssh other-system
other-system #
```

- Dans la fenêtre de terminal de la session `ssh`, l'administrateur configure la stratégie IPsec et les clés du second système en effectuant les étapes [Étape 2](#) à [Étape 8](#).
- Ensuite, l'administrateur met fin à la session `ssh`.

```
other-system # exit
local-system #
```

- Enfin, l'administrateur active la stratégie IPsec sur le premier système en suivant les procédures de l'[Étape 7](#) et de l'[Étape 8](#).

La prochaine fois que les deux systèmes communiquent, y compris par le biais d'une connexion `ssh`, la communication est protégée par IPsec.

## ▼ Utilisation d'IPsec pour protéger un serveur Web du trafic non-web.

Un serveur Web sécurisé permet aux clients Web de communiquer avec le service Web. Sur un serveur Web sécurisé, le trafic non Web *doit* passer des tests de sécurité. La procédure suivante inclut les contournements pour le trafic Web. En outre, ce serveur Web peut effectuer des requêtes client DNS non sécurisées. Tout autre trafic requiert ESP avec les algorithmes AES et SHA-2.

### Avant de commencer

Vous devez configurer la stratégie IPsec dans la zone globale. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale. Vous avez effectué les étapes de la section “[Sécurisation du trafic entre deux systèmes à l'aide d'IPsec](#)” à la page 231 afin que les conditions suivantes soient remplies :

- La communication entre les deux systèmes est protégée par IPsec.

- Les numéros de clés sont générés par IKE.
- Vous avez vérifié que les paquets sont protégés.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

### 2 Déterminez les services qui doivent ignorer les vérifications de stratégie de sécurité.

Pour un serveur Web, ces services incluent les ports TCP 80 (HTTP) et 443 (HTTP sécurisé). Si le serveur Web assure la recherche de noms DNS, le serveur doit peut-être inclure également le port 53 pour TCP et UDP.

### 3 Ajoutez la stratégie du serveur Web au fichier de stratégie IPsec.

Ajoutez les lignes suivantes dans le fichier `/etc/inet/ipsecinit.conf` :

```
# Web traffic that web server should bypass.
{lport 80 ulp tcp dir both} bypass {}
{lport 443 ulp tcp dir both} bypass {}

# Outbound DNS lookups should also be bypassed.
{rport 53 dir both} bypass {}

# Require all other traffic to use ESP with AES and SHA-2.
# Use a unique SA for outbound traffic from the port
{} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Cette configuration permet uniquement au trafic sécurisé d'accéder au système, avec les exceptions de contournement décrites à l'[Étape 2](#).

### 4 Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

### 5 Actualisez la stratégie IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

### 6 Actualisez les clés pour IPsec.

Redémarrez le service `ike`.

```
# svcadm restart svc:/network/ipsec/ike
```

Si vous avez configuré les clés manuellement, suivez les instructions de la section [“Création manuelle de clés IPsec”](#) à la page 243.

Votre installation est terminée. Si vous le souhaitez, vous pouvez effectuer l'[Étape 7](#).

## 7 (Facultatif) Autorisez un système distant à communiquer avec le serveur Web pour le trafic non-Web.

Ajoutez les lignes suivantes dans un fichier `/etc/inet/ipsecinit.conf` stocké sur le système distant :

```
# Communicate with web server about nonweb stuff
#
{laddr webserver} ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

Vérifiez la syntaxe, puis actualisez la stratégie IPsec pour l'activer.

```
remote-system # ipseccnf -c -f /etc/inet/ipsecinit.conf
remote-system # svcadm refresh svc:/network/ipsec/policy:default
```

Un système distant peut communiquer de manière sécurisée avec le serveur Web pour le trafic non-Web uniquement lorsque les stratégies IPsec des systèmes sont identiques.

## ▼ Affichage des stratégies IPsec

Vous pouvez afficher les stratégies configurées dans le système lorsque vous exécutez la commande `ipseccnf` sans argument.

### Avant de commencer

Vous devez exécuter la commande `ipseccnf` dans la zone globale. Dans une zone IP exclusive, vous devez exécuter la commande `ipseccnf` dans la zone non globale.

### 1 Prenez un rôle bénéficiant du profil Network IPsec Management (gestion IPsec du réseau).

Pour créer un rôle discret pour la sécurité réseau et attribuer ce rôle à un utilisateur, reportez-vous à la section [“Configuration d'un rôle pour la sécurité réseau”](#) à la page 245.

### 2 Affichage des stratégies IPsec

- Affichez les entrées de stratégie IPsec globales dans l'ordre dans lequel les entrées ont été insérées.

```
$ ipseccnf
```

La commande affiche chaque entrée avec un *index* suivi d'un numéro.

- Affichez les entrées de stratégie IPsec dans l'ordre dans lequel les correspondances sont repérées.

```
$ ipseccnf -l -n
```

- Affichez les entrées de stratégie IPsec, y compris les entrées définies par tunnel, dans l'ordre dans lequel les correspondances sont repérées.

```
$ ipseccnf -L -n
```

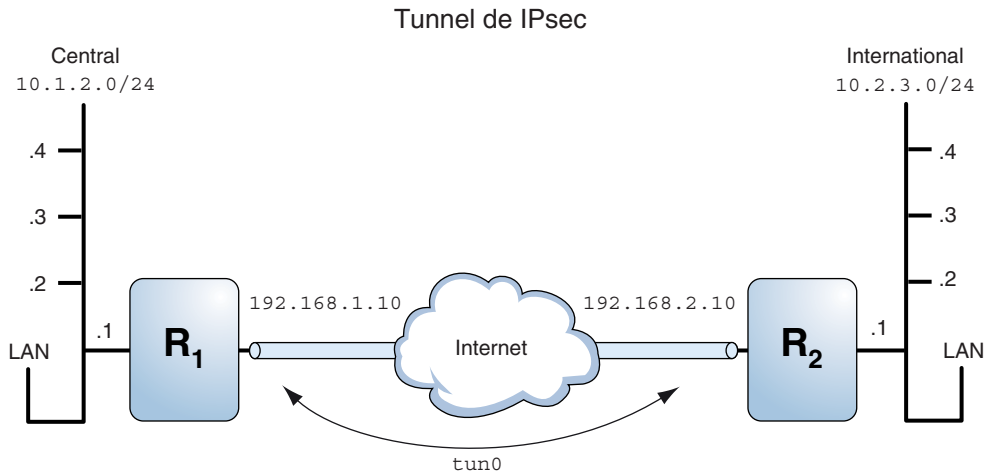
## Protection d'un VPN à l'aide d'IPsec

Oracle Solaris peut configurer un réseau privé virtuel (VPN) protégé par IPsec. Vous pouvez créer des tunnels en *mode Tunnel* ou en *mode Transport*. Pour plus d'informations, reportez-vous à la section [“Modes Transport et Tunnel dans IPsec”](#) à la page 222. Les exemples et procédures de cette section utilisent des adresses IPv4, mais les exemples et procédures s'appliquent également aux réseaux privés virtuels IPv6. Pour une courte explication, reportez-vous à la section [“Protection du trafic à l'aide d'IPsec”](#) à la page 229.

Des exemples de stratégies IPsec pour les tunnels en mode Tunnel sont fournis à la section [“Protection d'un VPN à l'aide d'IPsec en mode Tunnel \(exemples\)”](#) à la page 236.

## Protection d'un VPN à l'aide d'IPsec en mode Tunnel (exemples)

FIGURE 15-1 Tunnel protégé par IPsec



Les exemples ci-dessous considèrent que le tunnel est configuré pour tous les sous-réseaux des LAN :

```
## Tunnel configuration ##
# Tunnel name is tun0
# Intranet point for the source is 10.1.2.1
# Intranet point for the destination is 10.2.3.1
# Tunnel source is 192.168.1.10
# Tunnel destination is 192.168.2.10
```

```
# Tunnel name address object is tun0/to-central
# Tunnel name address object is tun0/to-overseas
```

#### EXEMPLE 15-2 Création d'un tunnel utilisable par tous les sous-réseaux

Dans cet exemple, la totalité du trafic des LAN locaux du LAN central de la [Figure 15-1](#) peut être mise en tunnel du routeur 1 au routeur 2, puis fournie à tous les LAN locaux du LAN Overseas. Le trafic est chiffré à l'aide d'AES.

```
## IPsec policy ##
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

#### EXEMPLE 15-3 Création d'un tunnel connectant deux sous-réseaux

Dans cet exemple, seul le trafic entre le sous-réseau 10.1.2.0/24 du LAN Central et le sous-réseau 10.2.3.0/24 du LAN Overseas est mis en tunnel et chiffré. En l'absence d'autres stratégies IPsec pour Central, si le LAN Central tente de transmettre des données pour d'autres LAN via ce tunnel, le trafic est abandonné au niveau du routeur 1.

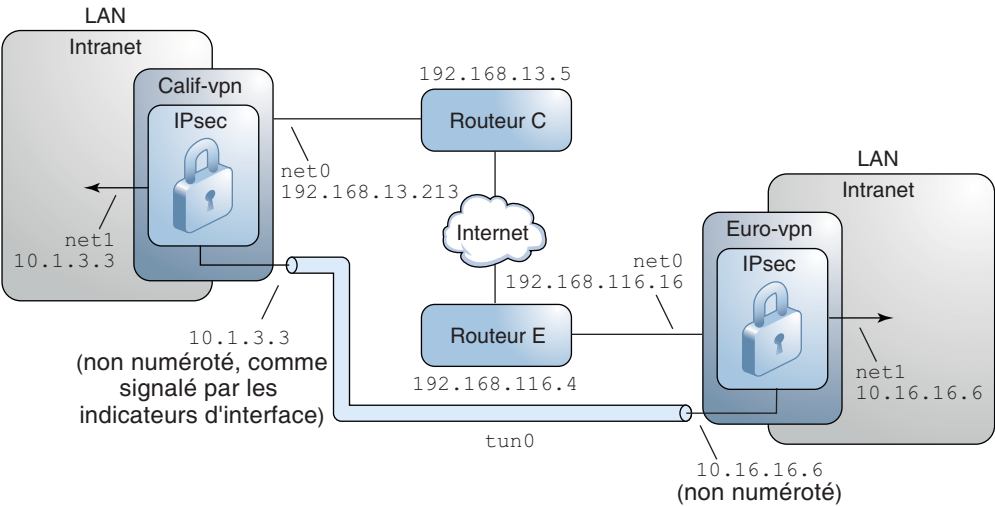
```
## IPsec policy ##
{tunnel tun0 negotiate tunnel laddr 10.1.2.0/24 raddr 10.2.3.0/24}
ipsec {encr_algs aes encr_auth_algs sha512 shared}
```

## Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN

Les procédures suivant cette section sont définies pour la configuration ci-dessous. Le réseau est illustré dans la [Figure 15-2](#).

- Chaque système utilise un espace d'adressage IPv4.
- Chaque système possède deux interfaces. L'interface net0 se connecte à Internet. Dans cet exemple, les adresses IP Internet commencent par 192.168. L'interface net1 se connecte au LAN de la société, son intranet. Dans cet exemple, les adresses IP intranet commencent par le numéro 10.
- Chaque système nécessite l'authentification ESP avec l'algorithme SHA-2. Dans cet exemple, l'algorithme SHA-2 requiert une clé de 512 bits.
- Chaque système nécessite le chiffrement ESP avec l'algorithme AES. L'algorithme AES utilise une clé de 128 ou 256 bits.
- Chaque système peut se connecter à un routeur bénéficiant d'un accès direct à Internet.
- Chaque système utilise des associations de sécurité partagées (SA, Security Associations).

FIGURE 15-2 Exemple de VPN entre plusieurs sites connectés à Internet



Dans l'illustration précédente, les procédures utilisent les paramètres de configuration suivants.

Paramètre	Europe	Californie
Nom du système	euro-vpn	calif-vpn
Interface intranet du système	net1	net1
Adresse intranet du réseau, dite également adresse <i>-point</i> à l'Étape 7	10.16.16.6	10.1.3.3
Objet d'adresse intranet du système	net1/inside	net1/inside
Interface Internet du système	net0	net0
Adresse Internet du système, dite également adresse <i>tsrc</i> à l'Étape 7	192.168.116.16	192.168.13.213
Nom du routeur Internet	router-E	router-C
Adresse du routeur Internet	192.168.116.4	192.168.13.5
Nom du tunnel	tun0	tun0
Objet d'adresse de nom de tunnel	tun0/v4tunaddr	tun0/v4tunaddr

Pour obtenir des informations sur les noms de tunnel, reportez-vous à la section “[Configuration et administration du tunnel avec la commande dladm](#)” à la page 126. Pour obtenir des informations sur les objets d'adresse, reportez-vous à la section “[Procédure de configuration d'une interface IP](#)” à la page 47 et à la page de manuel [ipadm\(1M\)](#).

## ▼ Procédure de protection d'un VPN avec IPsec en mode Tunnel

En mode Tunnel, le paquet IP interne détermine la stratégie IPsec qui protège son contenu.

Cette procédure prolonge la procédure [“Sécurisation du trafic entre deux systèmes à l'aide d'IPsec” à la page 231](#). La configuration est décrite à la section [“Description de la topologie réseau requise par les tâches IPsec afin de protéger un VPN” à la page 237](#).

Pour une description plus détaillée des raisons pour lesquelles certaines commandes doivent être exécutées, reportez-vous aux étapes correspondantes à la section [“Sécurisation du trafic entre deux systèmes à l'aide d'IPsec” à la page 231](#).

---

**Remarque** – Effectuez cette procédure sur les deux systèmes.

---

Outre la connexion de deux systèmes, vous connectez deux intranets qui leur sont connectés. Les systèmes de cette procédure fonctionnent comme des passerelles.

---

**Remarque** – Pour utiliser IPsec en mode Tunnel avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section [“Procédure de configuration d'un tunnel au sein d'un réseau non autorisé” du manuel \*Configuration et administration d'Oracle Solaris Trusted Extensions\*](#).

---

### Avant de commencer

Vous devez vous trouver dans la zone globale pour configurer la stratégie IPsec pour le système ou pour une zone IP partagée. Dans une zone IP exclusive, vous devez configurer la stratégie IPsec dans la zone non globale.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#). Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

#### 2 Contrôlez le flux de paquets avant de configurer IPsec.

##### a. Désactivez la transmission IP et le routage d'IP dynamique.

```
# routeadm -d ipv4-routing
# ipadm set-prop -p forwarding=off ipv4
# routeadm -u
```

La désactivation de la transmission IP empêche le transfert de paquets d'un réseau vers un autre par l'intermédiaire de ce système. La commande `routeadm` est décrite à la page de manuel [routeadm\(1M\)](#).

**b. Activez le multiréseau IP strict.**

```
# ipadm set-prop -p hostmodel=strong ipv4
```

L'activation du multiréseau IP strict requiert que les paquets de l'une des adresses de destination du système arrivent à l'adresse de destination adéquate.

Lorsque le paramètre `hostmodel` est défini sur `strong`, les paquets arrivant sur une interface particulière doivent être adressés à l'une des adresses IP locales de cette interface. Tous les autres paquets sont abandonnés, même les paquets envoyés vers d'autres adresses locales du système.

**c. Assurez-vous que la plupart des services réseau sont désactivés.**

Vérifiez que les montages en loopback et le service `ssh` sont en cours d'exécution.

```
# svcs | grep network
online          Aug_02   svc:/network/loopback:default
...
online          Aug_09   svc:/network/ssh:default
```

**3 Ajoutez une stratégie IPsec.**

Modifiez le fichier `/etc/inet/ipsecinit.conf` afin d'ajouter la stratégie IPsec pour le VPN. Pour obtenir des exemples supplémentaires, reportez-vous à la section [“Protection d'un VPN à l'aide d'IPsec en mode Tunnel \(exemples\)”](#) à la page 236.

Dans cette stratégie, la protection IPsec n'est pas requise entre les systèmes du réseau local et l'adresse IP interne de la passerelle, d'où l'ajout d'une déclaration `bypass`.

**a. Dans le système `euro-vpn`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :**

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.16.16.6 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-2.
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

**b. Sur le système `calif-vpn`, saisissez l'entrée suivante dans le fichier `ipsecinit.conf` :**

```
# LAN traffic to and from this host can bypass IPsec.
{laddr 10.1.3.3 dir both} bypass {}

# WAN traffic uses ESP with AES and SHA-2.
{tunnel tun0 negotiate tunnel}
ipsec {encr_algs aes encr_auth_algs sha512 sa shared}
```

**4 Sur chaque système, configurez IKE afin d'ajouter une paire de SA IPsec entre les deux systèmes.**

Configurez IKE en suivant l'une des procédures de configuration décrites à la section [“Configuration du protocole IKE \(liste des tâches\)”](#) à la page 267. La syntaxe du fichier de configuration IKE est décrite à la page de manuel `ike.config(4)`.



---

**Remarque** – Si vous devez générer et maintenir vos clés manuellement, reportez-vous à la section [“Création manuelle de clés IPsec”](#) à la page 243.

---

## 5 Vérifiez la syntaxe du fichier de stratégie IPsec.

```
# ipsecconf -c -f /etc/inet/ipsecinit.conf
```

Corrigez les éventuelles erreurs, vérifiez la syntaxe du fichier, puis continuez.

## 6 Actualisez la stratégie IPsec.

```
# svcadm refresh svc:/network/ipsec/policy:default
```

La stratégie IPsec est activée par défaut. *Actualisez-la*. Si vous avez désactivé la stratégie IPsec, activez-la.

```
# svcadm enable svc:/network/ipsec/policy:default
```

## 7 Créez et configurez le tunnel, *nom-tunnel*.

Les commandes suivantes configurent les interfaces internes et externes, créent le tunnel tun0 et attribuent des adresses IP au tunnel.

### a. Sur le système calif-vpn, créez le tunnel et configurez-le.

Si l'interface net1 n'existe pas, la première commande la crée.

```
# ipadm create-addr -T static -a local=10.1.3.3 net1/inside
# dladm create-iptun -T ipv4 -a local=10.1.3.3,remote=10.16.16.6 tun0
# ipadm create-addr -T static \
-a local=192.168.13.213,remote=192.168.116.16 tun0/v4tunaddr
```

### b. Sur le système euro-vpn, créez le tunnel et configurez-le.

```
# ipadm create-addr -T static -a local=10.16.16.6 net1/inside
# dladm create-iptun -T ipv4 -a local=10.16.16.6,remote=10.1.3.3 tun0
# ipadm create-addr -T static \
-a local=192.168.116.16,remote=192.168.13.213 tun0/v4tunaddr
```

---

**Remarque** – L'option -T de la commande ipadm spécifie le type d'adresse à créer. L'option -T de la commande dladm spécifie le tunnel.

---

Pour obtenir des informations à propos de ces commandes, consultez les pages de manuel [dladm\(1M\)](#) et [ipadm\(1M\)](#), ainsi que la section [“Procédure de configuration d'une interface IP”](#) à la page 47. Pour obtenir des informations sur les noms personnalisés, reportez-vous à la section [“Noms des périphériques réseau et des liaisons de données”](#) du manuel *Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau*.

## 8 Sur chaque système, configurez le transfert.

```
# ipadm set-ifprop -m ipv4 -p forwarding=on net1
# ipadm set-ifprop -m ipv4 -p forwarding=off net0
```

Le transfert IP signifie que les paquets arrivant peuvent être transférés. Le transfert IP signifie également que les paquets quittant l'interface peuvent provenir d'un autre emplacement. Pour que le transfert de paquet s'effectue sans erreur, vous devez activer le transfert IP à la fois sur l'interface réceptrice et sur l'interface émettrice.

Etant donné que l'interface `net1` se trouve *dans* l'intranet, le transfert IP doit être activé pour `net1`. Comme `tun0` connecte les deux systèmes via Internet, la transmission IP doit être activée pour `tun0`. Le transfert IP de l'interface `net0` est désactivé afin d'éviter toute injection de paquets par un concurrent *externe* dans l'intranet protégé. Le terme *externe* fait référence à Internet.

**9 Sur chaque système, empêchez la publication de l'interface privée.**

```
# ipadm set-addrprop -p private=on net0
```

Même si le transfert de l'IP de `net0` est désactivé, l'implémentation d'un protocole de routage peut permettre d'annoncer l'interface. Par exemple, le protocole `in.routed` peut encore annoncer que `net0` est disponible pour transférer des paquets à ses homologues dans l'intranet. Pour éviter ces annonces, définissez l'indicateur *private* de l'interface.

**10 Redémarrez les services réseau.**

```
# svcadm restart svc:/network/initial:default
```

**11 Ajoutez manuellement une route par défaut sur l'interface `net0`.**

La route par défaut doit correspondre à un routeur bénéficiant d'un accès direct à Internet.

**a. Sur le système `calif-vpn` ajoutez la route suivante :**

```
# route -p add net default 192.168.13.5
```

**b. Sur le système `euro-vpn`, ajoutez la route suivante :**

```
# route -p add net default 192.168.116.4
```

Même si l'interface `net0` ne fait pas partie de l'intranet, `net0` n'a pas besoin de passer par Internet pour atteindre le système homologue. Pour trouver son homologue, `net0` requiert des informations sur le routage Internet. Pour le reste d'Internet, le système VPN apparaît comme étant un hôte, non un routeur. Par conséquent, vous pouvez utiliser un routeur par défaut ou exécuter le protocole de recherche de routeur pour rechercher le système. Pour plus d'informations, reportez-vous aux pages de manuel [route\(1M\)](#) et [in.routed\(1M\)](#).

## Gestion d'IPsec et d'IKE

La liste des tâches suivantes fait référence à des tâches utiles dans le cadre de la gestion d'IPsec.

Tâche	Description	Voir
Création et remplacement manuels des associations de sécurité	Fournit les données brutes des associations de sécurité : <ul style="list-style-type: none"> <li>■ Nom d'algorithme IPsec et numéros de clé</li> <li>■ Index de paramètre de sécurité (SPI)</li> <li>■ Source IP et adresses de destination, et autres paramètres</li> </ul>	<a href="#">“Création manuelle de clés IPsec” à la page 243</a>
Création d'un rôle de sécurité réseau	Crée un rôle pouvant configurer un réseau sécurisé, mais possédant moins de permissions que le rôle root.	<a href="#">“Configuration d'un rôle pour la sécurité réseau” à la page 245</a>
Gestion d'IPsec et des numéros de clés en tant qu'ensemble de services SMF	Décrit quand et comment utiliser les commandes permettant d'activer, de désactiver, d'actualiser et de redémarrer les services. Décrit également les commandes permettant de modifier les valeurs de propriété des services.	<a href="#">“Procédure de gestion des services IKE et IPsec” à la page 246</a>
Vérification de la protection des paquets par IPsec	Recherche des en-têtes spécifiques indiquant la méthode de protection des datagrammes IP dans la sortie de commande snoop.	<a href="#">“Vérification de la protection des paquets par IPsec” à la page 248</a>

## ▼ Création manuelle de clés IPsec

La procédure suivante fournit les numéros de clés de l'[Étape 5](#) de la section [“Sécurisation du trafic entre deux systèmes à l'aide d'IPsec” à la page 231](#). Vous générez des clés pour deux systèmes, partym et enigma. Vous générez des clés sur un système, puis utilisez les clés du premier système sur les deux systèmes.

### Avant de commencer

La gestion manuelle des numéros de clé pour une zone non globale s'effectue dans la zone globale.

### 1 Générez les numéros de clé pour les SA.

#### a. Déterminez les clés nécessaires.

Il vous faut trois numéros aléatoires hexadécimaux pour le trafic sortant et trois autres numéros aléatoires hexadécimaux pour le trafic entrant. Un système doit donc générer les numéros suivants :

- Deux numéros aléatoires hexadécimaux comme valeur du mot-clé spi : un numéro pour le trafic sortant et un numéro pour le trafic entrant. Chaque numéro peut comporter huit caractères maximum.
- Deux numéros aléatoires hexadécimaux pour l'algorithme SHA-2 pour AH. Chacun des numéros doit comporter 512 caractères. L'un d'eux est dédié à dst enigma, l'autre à dst partym.

- Deux numéros aléatoires hexadécimaux pour l'algorithme 3DES pour ESP. Chacun des numéros doit comporter 168 caractères. L'un d'eux est dédié à dst enigma, l'autre à dst partym.

**b. Générez les clés requises.**

- Si un générateur de nombres aléatoires est disponible sur votre site, utilisez-le.
- Utilisez la commande `pktool` comme indiqué dans la section [“Procédure de génération d’une clé symétrique à l’aide de la commande pktool” du manuel Administration d’Oracle Solaris : services de sécurité](#) et l'exemple IPsec de cette section.

**2 Dans le rôle root sur chaque système, ajoutez les clés au fichier de clés manuelles pour IPsec.**

**a. Modifiez le fichier `/etc/inet/secret/ipseckeys` sur le système enigma pour qu'il soit similaire à ce qui suit :**

```
# ipseckeys - This file takes the file format documented in
# ipseckey(1m).
# Note that naming services might not be available when this file
# loads, just like ipsecinit.conf.
#
# Backslashes indicate command continuation.
#
# for outbound packets on enigma
add esp spi 0x8bcd1407 \
    src 192.168.116.16 dst 192.168.13.213 \
    encr_alg 3des \
    auth_alg sha512 \
    encrkey d41fb74470271826a8e7a80d343cc5aa... \
    authkey e896f8df7f78d6cab36c94ccf293f031...
#
# for inbound packets
add esp spi 0x122a43e4 \
    src 192.168.13.213 dst 192.168.116.16 \
    encr_alg 3des \
    auth_alg sha512 \
    encrkey dd325c5c137fb4739a55c9b3a1747baa... \
    authkey ad9ced7ad5f255c9a8605fba5eb4d2fd...
```

**b. Protégez le fichier à l'aide d'autorisations de lecture seule.**

```
# chmod 400 /etc/inet/secret/ipseckeys
```

**c. Vérifiez la syntaxe du fichier.**

```
# ipseckey -c -f /etc/inet/secret/ipseckeys
```

---

**Remarque** – Les numéros de clés utilisés sur chacun des systèmes *doivent* être identiques.

---

### 3 Activez les clés pour IPsec.

- Si le service `manual-key` n'est pas activé, activez-le.  
`# svcadm enable svc:/network/ipsec/manual-key:default`
- Si le service `manual-key` est activé, actualisez-le.  
`# svcadm refresh ipsec/manual-key`

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## ▼ Configuration d'un rôle pour la sécurité réseau

Si vous administrez vos systèmes à l'aide de la fonctionnalité RBAC (Role-Based Access Control, contrôle d'accès à base de rôles) d'Oracle Solaris, suivez cette procédure pour générer un rôle de gestion ou de sécurité du réseau.

### 1 Répertoriez les profils de droits disponibles relatifs au réseau.

```
% getent prof_attr | grep Network | more
Console User:RO::Manage System as the Console User...
Network Management:RO::Manage the host and network configuration...
Network Autoconf Admin:RO::Manage Network Auto-Magic configuration via nwamd...
Network Autoconf User:RO::Network Auto-Magic User...
Network ILB:RO::Manage ILB configuration via ilbadm...
Network LLDP:RO::Manage LLDP agents via lldpadm...
Network VRRP:RO::Manage VRRP instances...
Network Observability:RO::Allow access to observability devices...
Network Security:RO::Manage network and host security...:profiles=Network Wifi
Security,Network Link Security,Network IPsec Management...
Network Wifi Management:RO::Manage wifi network configuration...
Network Wifi Security:RO::Manage wifi network security...
Network Link Security:RO::Manage network link security...
Network IPsec Management:RO::Manage IPsec and IKE...
System Administrator:RO::Can perform most non-security administrative tasks:profiles=...Network Management...
Information Security:RO::Maintains MAC and DAC security policies:profiles=...Network Security...
```

Le profil de gestion du réseau est un profil supplémentaire inclus dans le profil d'administrateur système. Si vous avez attribué le profil de droits d'administrateur système à un rôle, alors ce dernier permet d'exécuter les commandes définies dans le profil de gestion du réseau.

### 2 Répertoriez les commandes dans le profil de droits Network Management.

```
% getent exec_attr | grep "Network Management"
...
Network Management:solaris:cmd:::/sbin/dlstat:euid=dladm;egid=sys
...
Network Management:solaris:cmd:::/usr/sbin/snoop:privs=net_observability
Network Management:solaris:cmd:::/usr/sbin/spray:euid=0 ...
```

### 3 Choisissez l'étendue des rôles de sécurité réseau sur votre site.

Basez votre choix sur les profils de droits définis au cours de l'[Étape 1](#).

- Pour créer un rôle qui gère l'ensemble de la sécurité du réseau, utilisez le profil de droits Network Security.
- Pour créer un rôle qui gère IPsec et IKE uniquement, utilisez le profil de droits Network IPsec Management.

#### 4 Créez un rôle de sécurité réseau incluant le profil de droits Network Management.

Un rôle auquel est appliqué le profil de droits Network Security ou Network IPsec Management, en plus du profil Network Management, peut exécuter les commandes `ipadm`, `ipseckey` et `snoop` entre autres, avec les privilèges appropriés.

Pour créer le rôle, l'attribuer à un utilisateur et en enregistrer les modifications auprès du service de noms, reportez-vous à la section "[Configuration initiale RBAC \(liste des tâches\)](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

### Exemple 15–4 Répartition des responsabilités de sécurité réseau entre les rôles

Dans cet exemple, l'administrateur répartit les responsabilités de sécurité réseau entre deux rôles. Un rôle peut administrer la sécurité des connexions Wi-Fi et des liens et un autre rôle administrer IPsec et IKE. Chaque rôle est assigné à trois personnes, une personne par période de travail.

Ces rôles sont créés par l'administrateur comme suit :

- L'administrateur nomme le premier rôle LinkWifi.
  - L'administrateur attribue au rôle les profils de droits Network Wifi, Network Link Security et Network Management.
  - Ensuite, l'administrateur attribue le rôle LinkWifi aux utilisateurs appropriés.
- L'administrateur nomme le deuxième rôle Administrateur IPsec.
  - L'administrateur attribue au rôle les profils de droits Network IPsec Management et Network Management.
  - Ensuite, l'administrateur attribue le rôle d'administrateur IPsec aux utilisateurs appropriés.

## ▼ Procédure de gestion des services IKE et IPsec

Les étapes suivantes présentent les utilisations les plus probables des services SMF pour IPsec, IKE et la gestion manuelle des clés. Par défaut, les services `policy` et `ipsecalgs` sont activés. Également par défaut, les services `ike` et `manual-key` sont désactivés.

## 1 Pour gérer la stratégie IPsec, effectuez l'une des opérations suivantes :

- Après l'ajout de nouvelles stratégies au fichier `.conf`, actualisez le service `policy`.

```
# svcadm refresh svc:/network/ipsec/policy
```

- Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service `policy`.

```
# svccfg -s policy setprop config/config_file=/etc/inet/MyIpsecinit.conf
# svccfg -s policy listprop config/config_file
config/config_file astring /etc/inet/MyIpsecinit.conf
# svcadm refresh svc:/network/ipsec/policy
# svcadm restart svc:/network/ipsec/policy
```

## 2 Pour gérer automatiquement les clés, effectuez l'une des opérations suivantes :

- Après l'ajout d'entrées dans le fichier `/etc/inet/ike/config`, activez le service `ike`.

```
# svcadm enable svc:/network/ipsec/ike
```

- Après avoir modifié les entrées dans le fichier `/etc/inet/ike/config`, actualisez le service `ike`.

```
# svcadm restart svc:/network/ipsec/ike:default
```

- Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.

```
# svccfg -s ike setprop config/admin_privilege = astring: "modkeys"
# svccfg -s ike listprop config/admin_privilege
config/admin_privilege astring modkeys
# svcadm refresh svc:/network/ipsec/ike
# svcadm restart svc:/network/ipsec/ike
```

- Pour arrêter le service `ike`, désactivez-le.

```
# svcadm disable svc:/network/ipsec/ike
```

## 3 Pour gérer manuellement les clés, effectuez l'une des opérations suivantes :

- Après l'ajout d'entrées pour le fichier `/etc/inet/secret/ipseckeys`, activez le service `manual-key`.

```
# svcadm enable svc:/network/ipsec/manual-key:default
```

- Une fois que vous avez modifié le fichier `ipseckeys`, actualisez le service.

```
# svcadm refresh manual-key
```

- Après la modification de la valeur d'une propriété du service, affichez la valeur de la propriété, puis actualisez et redémarrez le service.

```
# svccfg -s manual-key setprop config/config_file=/etc/inet/secret/MyIpseckeyfile
# svccfg -s manual-key listprop config/config_file
config/config_file astring /etc/inet/secret/MyIpseckeyfile
```

```
# svcadm refresh svc:/network/ipsec/manual-key
# svcadm restart svc:/network/ipsec/manual-key
```

- Pour empêcher la gestion manuelle des clés, désactivez le service `manual-key`.

```
# svcadm disable svc:/network/ipsec/manual-key
```

- 4 Si vous modifiez le tableau des protocoles IPsec et des algorithmes, actualisez le service `ipsecalgs`.

```
# svcadm refresh svc:/network/ipsec/ipsecalgs
```

### Erreurs fréquentes

Pour connaître l'état d'un service, utilisez la commande de `service svcs`. Si le service est en mode maintenance, suivez les suggestions de débogage dans la sortie de la commande de `service svcs -X`.

## ▼ Vérification de la protection des paquets par IPsec

Pour vérifier que les paquets sont protégés, testez la connexion à l'aide de la commande `snoop`. Les préfixes suivants peuvent apparaître dans la sortie `snoop` :

- Le préfixe `AH` : indique que `AH` protège les en-têtes. `AH` : s'affiche si le trafic est protégé à l'aide d'`auth_alg`.
- Le préfixe `ESP` : indique le transfert de données chiffrées. `ESP` : s'affiche si le trafic est protégé à l'aide d'`encr_auth_alg` ou d'`encr_alg`.

### Avant de commencer

Vous devez prendre le rôle `root` pour créer la sortie `snoop`. Vous devez avoir accès aux deux systèmes afin de tester la connexion.

- 1 Sur un système, par exemple `partym`, prenez le rôle de `root`.

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

- 2 A partir du système `partym`, préparez l'analyse des paquets à l'aide de la commande `snoop` à partir d'un système distant.

Dans une fenêtre de terminal sur `partym`, analysez les paquets du système `enigma`.

```
# snoop -d net0 -v enigma
Using device /dev/bge (promiscuous mode)
```



### 3 Envoyez un paquet à partir du système distant.

Dans une autre fenêtre de terminal, connectez-vous à distance au système enigma. Tapez le mot de passe. Ensuite, prenez le rôle root et envoyez un paquet à partir du système enigma au système partym. Le paquet doit être capturé à l'aide de la commande snoop -v enigma.

```
% ssh enigma
Password:      Type your password
% su -
Password:      Type root password
# ping partym
```

### 4 Examinez la sortie de la commande snoop.

Sur le système partym, la sortie devrait contenir les informations AH et ESP après les informations d'en-tête IP initiales. Les informations AH et ESP semblables à l'exemple ci-dessous indiquent que les paquets sont protégés :

```
IP:   Time to live = 64 seconds/hops
IP:   Protocol = 51 (AH)
IP:   Header checksum = 4e0e
IP:   Source address = 192.168.116.16, enigma
IP:   Destination address = 192.168.13.213, partym
IP:   No options
IP:
AH:   ----- Authentication Header -----
AH:
AH:   Next header = 50 (ESP)
AH:   AH length = 4 (24 bytes)
AH:   <Reserved field = 0x0>
AH:   SPI = 0xb3a8d714
AH:   Replay = 52
AH:   ICV = c653901433ef5a7d77c76eaa
AH:
ESP:   ----- Encapsulating Security Payload -----
ESP:
ESP:   SPI = 0xd4f40a61
ESP:   Replay = 52
ESP:   ....ENCRYPTED DATA....

ETHER:   ----- Ether Header -----
...
```



## Architecture IPsec (référence)

---

Ce chapitre contient les informations de référence suivante :

- “Services IPsec” à la page 251
- “Commande ipseconf” à la page 252
- “Fichier ipsecinit.conf” à la page 252
- “Commande ipsecalg” à la page 254
- “Base de données des associations de sécurité IPsec” à la page 255
- “Utilitaires de génération de clés SA dans IPsec” à la page 255
- “IPsec et commande snoop” à la page 257

Pour obtenir les instructions relatives à l'implémentation d'IPsec sur votre réseau, reportez-vous au [Chapitre 15, “Configuration d'IPsec \(tâches\)”](#). Pour une présentation d'IPsec, reportez-vous au [Chapitre 14, “Architecture IPsec \(présentation\)”](#).

## Services IPsec

L'utilitaire de gestion des services (SMF) fournit les services suivants pour IPsec :

- Service `svc:/network/ipsec/policy` : gère la stratégie IPsec. Par défaut, ce service est activé. La valeur de la propriété `config_file` détermine l'emplacement du fichier `ipsecinit.conf`. La valeur initiale est `/etc/inet/ipsecinit.conf`.
- Service `svc:/network/ipsec/ipsecalg` : gère les algorithmes disponibles pour IPsec. Par défaut, ce service est activé.
- Service `svc:/network/ipsec/manual-key` : active la gestion manuelle des clés. Par défaut, ce service est désactivé. La valeur de la propriété `config_file` détermine l'emplacement du fichier de configuration `ipseckeys`. La valeur initiale est `/etc/inet/secret/ipseckeys`.
- Service `svc:/network/ipsec/ike` : gère IKE. Par défaut, ce service est désactivé. Pour les propriétés configurables, reportez-vous à la section “[Service IKE](#)” à la page 301.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*. Voir aussi les pages de manuel [smf\(5\)](#), [svcadm\(1M\)](#) et [svccfg\(1M\)](#).

## Commande ipsecconf

Utilisez la commande `ipsecconf` pour configurer la stratégie IPsec pour un hôte. À l'exécution de la commande de configuration de la stratégie, le système crée des entrées de stratégie IPsec dans le noyau. Elles lui permettent de vérifier la stratégie appliquée à tous les datagrammes IP entrants et sortants. Les datagrammes transférés ne sont pas soumis aux vérifications de stratégie ajoutées à l'aide de cette commande. La commande `ipsecconf` configure également la base de données de stratégie de sécurité (SPD, Security Policy Database). Pour consulter les options de stratégie IPsec, reportez-vous à la page de manuel [ipsecconf\(1M\)](#).

Vous devez prendre le rôle `root` pour exécuter la commande `ipsecconf`. La commande accepte les entrées qui protègent le trafic bidirectionnel. Elle accepte également celles qui protègent le trafic unidirectionnel.

Les entrées de stratégie au format d'adresse locale et d'adresse distante peuvent protéger le trafic dans les deux directions à l'aide d'une entrée de stratégie unique. Par exemple, les entrées de modèles `laddr host1` et `raddr host2` protègent le trafic dans les deux directions quand aucune direction n'est spécifiée pour l'hôte nommé. Par conséquent, une seule entrée de stratégie est nécessaire pour chaque hôte.

Les entrées de stratégie ajoutées par le biais de la commande `ipsecconf` ne sont pas conservées après la réinitialisation du système. Pour vous assurer que la stratégie IPsec est active lorsque le système démarre, ajoutez l'entrée de stratégie au fichier `/etc/inet/ipsecinit.conf`, puis actualisez ou activez le service `policy`. Pour obtenir des exemples, reportez-vous à la section [“Protection du trafic à l'aide d'IPsec”](#) à la page 229.

## Fichier ipsecinit.conf

Pour activer la stratégie de sécurité IPsec lorsque vous démarrez Oracle Solaris, vous créez un fichier de configuration pour initialiser IPsec avec vos entrées de stratégie IPsec spécifiques. Le nom par défaut de ce fichier est `/etc/inet/ipsecinit.conf`. Reportez-vous à la page de manuel [ipsecconf\(1M\)](#) pour plus d'informations sur les entrées d'une stratégie et leur format. Une fois la stratégie configurée, vous pouvez l'actualiser avec la commande `svcadm refresh ipsec/policy`.

## Fichier exemple ipsecinit.conf

Le logiciel Oracle Solaris inclut un exemple de fichier de stratégie IPsec, `ipsecinit.sample`. Vous pouvez l'utiliser comme modèle pour créer votre propre fichier `ipsecinit.conf`. Le fichier `ipsecinit.sample` contient les exemples suivants :

```
...
# In the following simple example, outbound network traffic between the local
# host and a remote host will be encrypted. Inbound network traffic between
# these addresses is required to be encrypted as well.
#
# This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
# and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#

{laddr 10.0.0.1 raddr 10.0.0.2} ipsec
    {encr_algs aes encr_auth_algs sha256 sa shared}

# The policy syntax supports IPv4 and IPv6 addresses as well as symbolic names.
# Refer to the ipseconf(1M) man page for warnings on using symbolic names and
# many more examples, configuration options and supported algorithms.
#
# This example assumes that 10.0.0.1 is the IPv4 address of this host (laddr)
# and 10.0.0.2 is the IPv4 address of the remote host (raddr).
#
# The remote host will also need an IPsec (and IKE) configuration that mirrors
# this one.
#
# The following line will allow ssh(1) traffic to pass without IPsec protection:

{lport 22 dir both} bypass {}

#
# {laddr 10.0.0.1 dir in} drop {}
#
# Uncommenting the above line will drop all network traffic to this host unless
# it matches the rules above. Leaving this rule commented out will allow
# network packets that does not match the above rules to pass up the IP
# network stack. , , ,
```

## Considérations de sécurité pour les commandes ipsecinit.conf et ipseconf

La stratégie IPsec ne peut être modifiée pour les connexions établies. Un socket dont la stratégie ne peut pas être modifiée est appelé un *socket verrouillé*. Les nouvelles entrées de stratégie ne protègent pas les sockets qui sont déjà verrouillés. Pour plus d'informations, reportez-vous aux pages de manuel [connect\(3SOCKET\)](#) et [accept\(3SOCKET\)](#). En cas de doute, redémarrez la connexion.

Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.

- Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
- Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande `ipseconf` avec prudence. La commande `ssh`, une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.

## Commande ipsecalgsh

La fonction de structure cryptographique d'Oracle Solaris fournit des algorithmes d'authentification et de chiffrement à IPsec. La commande `ipsecalgs` permet d'établir la liste des algorithmes pris en charge par chacun des protocoles IPsec. La configuration `ipsecalgs` est stockée dans le fichier `/etc/inet/ipsecalgs`. En général, ce fichier n'a pas besoin d'être modifié. Cependant, si le fichier doit être modifié, utilisez la commande `ipsecalgs`. Le fichier ne doit jamais être édité directement. Les algorithmes pris en charge sont synchronisés avec le noyau à l'initialisation du système par le service `svc:/network/ipsec/ipsecalgsh:default`.

Les protocoles et algorithmes IPsec valides sont décrits par le DOI, ISAKMP, traité dans le document RFC 2407. Au sens global, un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.

En particulier, le DOI ISAKMP définit les conventions d'attribution de nom et de numéro aux algorithmes IPsec valides et à leurs protocoles, `PROTO_IPSEC_AH` et `PROTO_IPSEC_ESP`. Chaque algorithme est associé à exactement un protocole. Ces définitions DOI ISAKMP figurent dans le fichier `/etc/inet/ipsecalgs`. Les numéros d'algorithme et de protocole sont définis par l'IANA (Internet Assigned Numbers Authority). La commande `ipsecalgs` permet d'allonger la liste des algorithmes IPsec.

Pour plus d'informations sur les algorithmes, reportez-vous à la page de manuel [ipsecalgs\(1M\)](#) Pour plus d'informations sur la structure cryptographique, reportez-vous au Chapitre 11, “Structure cryptographique (présentation)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

## Base de données des associations de sécurité IPsec

Les informations sur les numéros de clés des services de sécurité IPsec sont conservées dans la base de données des associations de sécurité ([SADB](#)). Les associations de sécurité (SA) protègent les paquets entrants et sortants. Les SADB sont gérées par un processus utilisateur, éventuellement par plusieurs processus de coopération, qui envoient des messages sur un socket de type spécial. Ce mode de gestion des SADB s'apparente à la méthode décrite à la page de manuel [route\(7P\)](#). Seul le rôle `root` peut accéder à la base de données.

Le démon `in.iked` et la commande `ipseckey` utilisent l'interface socket `PF_KEY` dans le cadre de la gestion des SADB. Pour plus d'informations sur la gestion des requêtes et des messages par les SADB, reportez-vous à la page de manuel [pf\\_key\(7P\)](#).

## Utilitaires de génération de clés SA dans IPsec

Le protocole IKE permet la gestion automatique des clés pour les adresses IPv4 et IPv6. Pour obtenir les instructions relatives à la configuration IKE, reportez-vous au [Chapitre 18](#), “[Configuration du protocole IKE \(tâches\)](#)”. L'utilitaire de génération manuelle de clés est la commande `ipseckey` et sa description est disponible dans la page de manuel [ipseckey\(1M\)](#).

Utilisez la commande `ipseckey` pour remplir manuellement la base de données des associations de sécurité (SADB). En règle générale, les SA sont générées manuellement lorsqu'IKE n'est pas disponible pour une raison quelconque. Cependant, si les valeurs SPI sont uniques, la génération manuelle des SA et IKE peuvent être utilisés en même temps.

La commande `ipseckey` peut être utilisée pour afficher tous les SA connus du système, que les clés aient été ajoutées manuellement ou par IKE. Avec l'option `-c`, la commande `ipseckey` vérifie la syntaxe du fichier de clés que vous avez fourni en tant qu'argument.

Les SA IPsec qui sont ajoutées par le biais de la commande `ipseckey` ne sont pas conservées après la réinitialisation du système. Pour activer manuellement les SA ajoutées à l'initialisation du système, ajoutez des entrées au fichier `/etc/inet/secret/ipseckey`, puis activez le service `svc:/network/ipsec/manual-key:default`. Pour la procédure, reportez-vous à la section “[Création manuelle de clés IPsec](#)” à la page 243.

Bien qu'elle présente un nombre limité d'options générales, la commande `ipseckey` prend en charge un langage de commande enrichi. Si vous le souhaitez, une interface de programmation de génération manuelle de clés peut transmettre les requêtes. Pour plus d'informations, reportez-vous à la page de manuel [pf\\_key\(7P\)](#).

## Considérations de sécurité pour la commande ipseckey

La commande ipseckey permet à un rôle auquel a été attribué le profil de droits Network Security ou Network IPsec Management de saisir des informations de clés cryptographiques confidentielles. Un utilisateur malintentionné accédant à ces informations peut compromettre la sécurité du trafic IPsec.

---

**Remarque** – Si possible, utilisez IKE avec ipseckey plutôt que la génération de clés manuelle.

---

Prenez en considération les points suivants lorsque vous gérez des informations de génération de clés à l'aide de la commande ipseckey :

- Avez-vous actualisé les informations relatives à la génération de clés ? L'actualisation périodique des clés est une pratique de sécurité essentielle. Elle permet de prémunir les éventuelles défaillances de l'algorithme et des clés, et de limiter les dommages subis par une clé exposée.
- Le TTY est-il connecté à un réseau ? La commande ipseckey est-elle en mode interactif ?
  - En mode interactif, la sécurité des informations de génération de clés constitue celle du chemin d'accès au réseau pour le trafic du TTY. Evitez d'exécuter la commande ipseckey lors d'une session rlogin ou telnet en clair.
  - Même les fenêtres locales sont vulnérables aux attaques d'un programme caché qui intercepte les événements de fenêtre.
- Avez-vous utilisé l'option -f ? Le fichier est-il en cours d'accès sur le réseau ? Le fichier est-il accessible en lecture par tout utilisateur ?
  - Un utilisateur malintentionné est en mesure de lire un fichier monté sur le réseau lorsque ce fichier est en cours de lecture. Le fichier contenant les informations de génération de clés ne doit pas être lisible par tous.
  - Protégez votre système d'attribution de nom. Lorsque les deux conditions suivantes sont vérifiées, vos noms d'hôtes ne sont plus fiables.
    - Votre adresse source est un hôte que vous pouvez rechercher sur le réseau.
    - Votre système d'attribution de nom est compromis.

Les défaillances de sécurité proviennent souvent d'une mauvaise utilisation des outils, non des outils eux-mêmes. Utilisez la commande ipseckey avec prudence. La commande ssh, une console ou autre TTY connecté offrent les modes d'opération les plus sûrs.



## IPsec et commande snoop

La commande snoop permet l'analyse des en-têtes ESP et AH. En raison du chiffrement des données ESP, la commande snoop ne détecte pas les en-têtes chiffrés et protégés par ESP. AH ne chiffre pas les données. Par conséquent, la commande snoop peut contrôler le trafic protégé par AH. L'option -V de la commande signale l'utilisation d'AH sur un paquet. Pour plus d'informations, reportez-vous à la page de manuel [snoop\(1M\)](#).

La section “[Vérification de la protection des paquets par IPsec](#)” à la page 248 contient un exemple détaillé de sortie snoop sur un paquet protégé.

Des analyseurs de réseau tiers sont également disponibles, notamment le logiciel open-source [Wireshark](http://www.wireshark.org/about.html) (<http://www.wireshark.org/about.html>) qui est intégré à cette version.



## Protocole IKE (présentation)

---

Le protocole IKE (Internet Key Exchange, échange de clé Internet) automatise la gestion des clés pour IPsec. Oracle Solaris implémente IKEv1. Ce chapitre aborde les sujets suivants :

- “Gestion des clés avec IKE” à la page 259
- “Négociation des clés IKE” à la page 260
- “Choix de configuration IKE” à la page 261
- “Utilitaires et fichiers IKE” à la page 263

Pour connaître les instructions d'implémentation d'IKE, reportez-vous au [Chapitre 18](#), “[Configuration du protocole IKE \(tâches\)](#)”. Pour obtenir des informations de référence, reportez-vous au [Chapitre 19](#), “[Protocole IKE \(référence\)](#)”. Pour plus d'informations sur les protocoles IPsec, reportez-vous au [Chapitre 14](#), “[Architecture IPsec \(présentation\)](#)”.

## Gestion des clés avec IKE

La gestion des numéros de clé des associations de sécurité (Security Associations, SA) pour IPsec est appelée *gestion des clés*. La gestion automatique des clés requiert un canal de communication sécurisé pour la création, l'authentification et l'échange des clés. Oracle Solaris utilise IKE version 1 pour automatiser la gestion des clés. IKE s'intègre facilement dans les environnement à grande échelle et peut fournir un canal sécurisé pour un grand volume de trafic. Les associations de sécurité IPsec sur paquets IPv4 et IPv6 peuvent utiliser le protocole IKE.

IKE peut profiter de l'accélération matérielle disponible et stocker sur des composants matériels. Les accélérateurs matériels permettent aux opérations de clés intensives d'être gérées hors du système. Le stockage des clés sur des composants matériels fournit une couche de protection supplémentaire.

# Négociation des clés IKE

Le démon IKE, `in.iked`, négocie et authentifie de manière sécurisée le matériel de génération de clés pour les SA IPsec. Il utilise des germes de sécurité aléatoires pour les clés des fonctions internes fournies par le SE. Le protocole IKE assure une confidentialité de transmission parfaite (PFS, perfect forward secrecy). En mode PFS, les clés qui protègent la transmission des données ne sont pas utilisées pour générer des clés complémentaires. Les germes de sécurité employés pour créer des clés de transmission de données ne sont pas réutilisés. Reportez-vous à la page de manuel `in.iked(1M)`.

## Terminologie relative aux clés IKE

Le tableau ci-dessous répertorie les termes utilisés dans la négociation des clés et les acronymes les plus couramment employés. Vous y trouverez également une définition de chacun de ces termes ainsi que leur contexte d'utilisation.

TABEAU 17-1 Terminologie de négociation des clés, acronymes et utilisation

Terminologie de négociation des clés	Acronymes	Définition et utilisation
Echange de clés		Processus de génération de clés pour les algorithmes cryptographiques asymétriques. Les principales méthodes utilisées sont les protocoles RSA et Diffie-Hellman.
Algorithme Diffie-Hellman	DH	Algorithme d'échange de clés permettant la génération et l'authentification de clés. souvent appelé <i>échange de clés authentifiées</i> .
Protocole RSA	RSA	Algorithme d'échange de clés permettant la génération et le transport de clés. Ce protocole porte le nom de ses trois créateurs : Rivest, Shamir et Adleman.
Confidentialité de transmission parfaite	PFS (perfect forward secrecy)	Ne s'applique qu'à l'échange de clés authentifiées. Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.
Groupe Oakley		Méthode de création sécurisée de clés pour la phase 2. La méthode Oakley s'emploie pour négocier des PFS.

## Phase 1 d'IKE

La phase 1 est connue sous le nom de *Main Mode* (mode principal). Pendant la phase 1, IKE utilise des méthodes de chiffrement de clé publique pour s'authentifier auprès d'entités IKE homologues. Il en résulte une association de sécurité (SA, security association) ISAKMP (Internet Security Association and Key Management Protocol). Une SA ISAKMP est un canal

sécurisé sur lequel IKE négocie les numéros de clé des datagrammes IP. Contrairement aux SA IPsec, les SA ISAKMP sont bidirectionnelles. Il n'est donc pas nécessaire de disposer de plus d'une association de sécurité.

La façon dont IKE négocie les numéros de clé lors de la phase 1 peut être configurée. IKE lit les informations concernant la configuration dans le fichier `/etc/inet/ike/config`. Ces informations incluent :

- Des paramètres généraux tels que le nom des certificats de clés publiques
- L'activation ou non du mode de confidentialité de transmission parfaite (PFS)
- Les interfaces concernées
- Les protocoles de sécurité et leurs algorithmes
- La méthode d'authentification

Les deux méthodes d'authentification utilisent respectivement les clés prépartagées et les certificats de clés publiques. Les certificats de clés publiques peuvent être autosignés ou émis par l'[autorité de certification \(CA\)](#) d'un fournisseur d'infrastructures de clés publiques (PKI).

## Phase 2 d'IKE

La phase 2 est connue sous le nom de *Quick Mode* (mode rapide). Lors de la phase 2, IKE crée et gère les SA IPsec entre les systèmes qui exécutent le démon IKE. IKE utilise le canal sécurisé qui a été créé lors de la phase 1 pour protéger la transmission des numéros de clé. Le démon IKE crée les clés à partir d'un générateur de nombres aléatoires à l'aide du périphérique `/dev/random`. Le démon actualise les clés à une fréquence qui peut être configurée. Les numéros de clé sont accessibles aux algorithmes spécifiés dans le fichier de configuration `ipsecinit.conf` de la stratégie IPsec.

## Choix de configuration IKE

Le fichier de configuration `/etc/inet/ike/config` contient des entrées de stratégie IKE. Pour que deux démons IKE puissent s'authentifier mutuellement, les entrées doivent être valides et les numéros de clé doivent être disponibles. Les entrées des fichiers de configuration déterminent la façon dont les numéros de clé seront utilisés pour authentifier l'échange qui a lieu lors de la phase 1. Il y a deux possibilités : les clés prépartagées ou les certificats de clés publiques.

Si l'entrée est `auth_method preshared`, ce sont les clés prépartagées qui sont utilisées pour authentifier l'échange. Si `auth_method` possède une valeur autre que `preshared`, l'authentification s'effectue à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou installés par un fournisseur de PKI. Pour plus d'informations, reportez-vous à la page de manuel [ike.config\(4\)](#).

## IKE avec l'authentification des clés prépartagées

Les clés prépartagées servent à authentifier deux systèmes homologues. La clé prépartagée est un nombre hexadécimal ou une chaîne ASCII créée par un administrateur sur un système. Cette clé est ensuite partagée de manière sécurisée entre les différents administrateurs du système homologue. Si la clé prépartagée est interceptée par un utilisateur malintentionné, celui-ci peut alors se faire passer pour l'un des systèmes homologues.

La clé prépartagée sur les systèmes homologues qui utilisent cette méthode d'authentification doit être identique. Les clés sont liées à une adresse IP donnée ou à une plage d'adresses. Les clés sont placées dans le fichier `/etc/inet/secret/ike.preshared` de chaque système. Pour plus d'informations, reportez-vous à la page de manuel [ike.preshared\(4\)](#).

## IKE avec certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Les clés publiques utilisent l'[algorithme Diffie-Hellman](#) pour authentifier et négocier les clés. Les certificats de clés publiques peuvent être soit autosignés, soit certifiés par une [autorité de certification \(CA\)](#).

Les certificats de clés publiques autosignés sont créés par l'administrateur. La commande `ikecert cert local -ks` permet de créer la partie privée des bclés du système. Le certificat autosigné est ensuite émis, au format X.509, par le système distant. Le certificat du système distant est entré à l'aide de la commande `ikecert cert db` pour la partie publique de la clé. Les certificats autosignés résident dans le répertoire `/etc/inet/ike/publickeys` des systèmes communicants. Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté.

Les certificats autosignés sont à mi-chemin entre les clés prépartagées et les CA. Contrairement aux clés prépartagées, les certificats autosignés peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté. Pour autosigner un certificat pour un système n'ayant pas de numéro fixe, utilisez un nom alternatif de DNS (`www.example.org`) ou d'email (`root@domain.org`).

Les clés publiques peuvent être délivrées par un fournisseur de PKI ou une CA. Elles doivent être installées, avec les certificats CA qui les accompagnent, dans le répertoire `/etc/inet/ike/publickeys`. Lorsque vous utilisez l'option `-T`, les certificats résident sur le matériel connecté. Les fournisseurs émettent également des listes des certificats révoqués (CRL). Outre les clés et les certificats CA, vous devez également installer les CRL dans le répertoire `/etc/inet/ike/crls`.

Les certificats CA présentent l'avantage d'être certifiés par une organisation externe, et non par l'administrateur du site. Il s'agit en quelque sorte de certificats "certifiés". Comme les certificats autosignés, les certificats CA peuvent être utilisés sur une machine portable ou sur un système

susceptible d'être renuméroté. Contrairement aux certificats autosignés, ils s'intègrent facilement aux environnements à grande échelle afin de protéger un grand nombre de systèmes communicants.

## Utilitaires et fichiers IKE

Vous trouverez, dans le tableau ci-dessous, une liste des fichiers de configuration de la stratégie IKE, les emplacements de stockage des clés IKE et les différentes commandes et divers services permettant d'implémenter IKE. Pour plus d'informations sur les services, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

**TABEAU 17-2** Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services

Fichier, emplacement, commande ou service	Description	Page de manuel
<code>svc:/network/ipsec/ike</code>	Service SMF qui gère IKE.	<a href="#">smf(5)</a>
<code>/usr/lib/inet/in.iked</code>	Démon IKE (Internet Key Exchange). Permet la gestion des clés automatique lorsque le service <code>ike</code> est actif.	<a href="#">in.iked(1M)</a>
<code>/usr/sbin/ikeadm</code>	Commande d'administration IKE permettant d'afficher et de modifier la stratégie IKE. Permet à l'utilisateur d'afficher les objets administratifs IKE, tels que les algorithmes de phase 1 et les groupes Diffie-Hellman disponibles.	<a href="#">ikeadm(1M)</a>
<code>/usr/sbin/ikecert</code>	Commande de gestion de bases de données de certificats permettant de manipuler les bases de données locales détentrices de certificats de clés publiques. Les bases de données peuvent également être stockées sur le matériel connecté.	<a href="#">ikecert(1M)</a>
<code>/etc/inet/ike/config</code>	Fichier de configuration par défaut de la stratégie IKE. Contient les règles du site pour la concordance des requêtes IKE entrantes et la préparation des requêtes IKE sortantes.  Si le fichier existe, le démon <code>in.iked</code> démarre lorsque le service <code>ike</code> est activé. L'emplacement de ce fichier peut être modifié à l'aide de la commande <code>svccfg</code> .	<a href="#">ike.config(4)</a>
<code>ike.preshared</code>	Fichier de clés prépartagées du répertoire <code>/etc/inet/secret</code> . Contient des numéros de clé secrets destinés à l'authentification pendant la phase 1. Ce fichier s'utilise lorsque IKE est configuré avec des clés prépartagées.	<a href="#">ike.preshared(4)</a>
<code>ike.privatekeys</code>	Répertoire de clés privées de <code>/etc/inet/secret</code> . Contient les clés privées de la bclé.	<a href="#">ikecert(1M)</a>
Répertoire <code>publickeys</code>	Répertoire de <code>/etc/inet/ike</code> contenant les fichiers de certificats et clés publiques. Contient la clé publique de la bclé.	<a href="#">ikecert(1M)</a>

TABLEAU 17-2 Fichiers de configuration IKE, emplacements de stockage des clés, commandes et services (Suite)

Fichier, emplacement, commande ou service	Description	Page de manuel
Répertoire <code>cr1s</code>	Répertoire de <code>/etc/inet/ike</code> contenant les listes de révocation des clés publiques et des fichiers de certificats.	<a href="#">ikecert(1M)</a>
Carte Sun Crypto Accelerator 6000	Matériel accélérant les opérations de clés publiques en les déchargeant du système d'exploitation. Les clés publiques, les clés privées et les certificats de clés publiques peuvent également être stockés sur cette carte. La carte Sun Crypto Accelerator 6000 est un périphérique certifié FIPS 140-2 Niveau 3.	<a href="#">ikecert(1M)</a>



## Configuration du protocole IKE (tâches)

---

Ce chapitre décrit la procédure de configuration du protocole Internet Key Exchange (IKE) sur vos systèmes. Une fois configuré, ce protocole génère automatiquement les numéros de clé IPsec sur votre réseau. Le présent chapitre contient les informations suivantes :

- “Affichage des informations IKE” à la page 265
- “Configuration du protocole IKE (liste des tâches)” à la page 267
- “Configuration du protocole IKE avec des clés prépartagées (liste des tâches)” à la page 268
- “Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)” à la page 273
- “Configuration du protocole IKE pour les systèmes portables (liste des tâches)” à la page 291
- “Configuration du protocole IKE en vue de l'utilisation du matériel connecté” à la page 298

Pour voir une présentation du protocole IKE, reportez-vous au [Chapitre 17, “Protocole IKE \(présentation\)”](#). Pour obtenir des informations de référence sur le protocole IKE, reportez-vous au [Chapitre 19, “Protocole IKE \(référence\)”](#). Pour consulter d'autres procédures, reportez-vous aux sections Exemples des pages de manuel `ikeadm(1M)`, `ikecert(1M)` et `ike.config(4)`.

### Affichage des informations IKE

Vous pouvez afficher les algorithmes et les groupes qui peuvent servir aux négociations IKE de la phase 1.

#### ▼ Procédure d'affichage des groupes et algorithmes disponibles pour les échanges IKE de la phase 1

Dans cette procédure, vous déterminez quels groupes Diffie-Hellman peuvent être utilisés dans les échanges IKE de la phase 1. Vous pouvez afficher les algorithmes de chiffrement et

d'authentification qui peuvent servir aux échanges IKE de la phase 1. Les valeurs numériques correspondent aux valeurs spécifiées pour ces algorithmes par l'[IANA](#) (Internet Assigned Numbers Authority).

### 1 Affichage de la liste des groupes Diffie-Hellman qu'IKE peut utiliser dans la phase 1.

Les groupes Diffie-Hellman définis configurent les SA IKE.

```
# ikeadm dump groups
Value Strength Description
1      66      ietf-ike-grp-modp-768
2      77      ietf-ike-grp-modp-1024
5      91      ietf-ike-grp-modp-1536
14     110     ietf-ike-grp-modp-2048
15     130     ietf-ike-grp-modp-3072
16     150     ietf-ike-grp-modp-4096
17     170     ietf-ike-grp-modp-6144
18     190     ietf-ike-grp-modp-8192
```

Completed dump of groups

Vous pouvez utiliser l'une de ces valeurs comme argument du paramètre `oakley_group` dans une plate-forme IKE de la phase 1, comme dans :

```
p1_xform
{ auth_method preshared oakley_group 15 auth_alg sha encr_alg aes }
```

### 2 Affichage de la liste des algorithmes d'authentification qu'IKE peut utiliser dans la phase 1.

```
# ikeadm dump authalgs
Value Name
1      md5
2      sha1
4      sha256
5      sha384
6      sha512
```

Completed dump of authalgs

Vous pouvez utiliser l'un de ces noms comme argument du paramètre `auth_alg` dans une plate-forme IKE de la phase 1, comme dans :

```
p1_xform
{ auth_method preshared oakley_group 15 auth_alg sha256 encr_alg 3des }
```

### 3 Affichage de la liste des algorithmes de chiffrement qu'IKE peut utiliser dans la phase 1.

```
# ikeadm dump encralgs
Value Name
3      blowfish-cbc
5      3des-cbc
1      des-cbc
7      aes-cbc
```

Completed dump of encralgs

Vous pouvez utiliser l'un de ces noms comme argument du paramètre `encr_alg` dans une plate-forme IKE de la phase 1, comme dans :

```
pl_xform
{ auth_method preshared oakley_group 15 auth_alg sha256 encr_alg aes }
```

**Voir aussi** Pour effectuer des tâches de configuration de règles IKE nécessitant ces valeurs, reportez-vous à la section [“Configuration du protocole IKE \(liste des tâches\)”](#) à la page 267.

## Configuration du protocole IKE (liste des tâches)

L'authentification du protocole IKE peut s'effectuer à l'aide de clés prépartagées ou de certificats autosignés ou émanant d'autorités de certifications (CA). Les méthodes d'authentification IKE sont liées par une règle aux points d'extrémité protégés. Vous pouvez donc utiliser toutes les méthodes d'authentification IKE ou une seule d'entre elles sur un système. Un pointeur menant à une bibliothèque PKCS #11 permet à IKE d'utiliser un accélérateur matériel connecté.

Une fois le protocole IKE configuré, vous devez effectuer les tâches IPsec qui utilisent cette configuration. Le tableau ci-dessous répertorie les tâches correspondant aux différentes configurations IKE.

Tâche	Description	Voir
Configuration d'IKE avec des clés prépartagées	Protégez les communications entre deux systèmes en faisant en sorte qu'ils partagent une clé secrète.	<a href="#">“Configuration du protocole IKE avec des clés prépartagées (liste des tâches)”</a> à la page 268
Configuration d'IKE avec des certificats de clés publiques	Protégez les communications à l'aide de certificats de clés publiques. Ces certificats peuvent être autosignés ou attestés par un fournisseur de PKI.	<a href="#">“Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)”</a> à la page 273
Franchissement d'un boîtier NAT	Configurez les protocoles IPsec et IKE pour communiquer avec un système portable	<a href="#">“Configuration du protocole IKE pour les systèmes portables (liste des tâches)”</a> à la page 291
Configuration d'IKE pour qu'il utilise un keystore matériel pour générer une paire de certificats	Activez une carte Sun Crypto Accelerator 6000 pour accélérer les opérations IKE et stocker des certificats de clés publiques.	<a href="#">“Configuration du protocole IKE en vue de l'utilisation du matériel connecté”</a> à la page 298

# Configuration du protocole IKE avec des clés prépartagées (liste des tâches)

Le tableau ci-dessous répertorie les procédures de configuration et de maintenance du protocole IKE avec des clés prépartagées.

Tâche	Description	Voir
Configuration d'IKE avec des clés prépartagées	Créez un fichier de configuration IKE ainsi qu'une clé à partager.	<a href="#">“Configuration du protocole IKE avec des clés prépartagées” à la page 268</a>
Ajout de clés prépartagées à un système IKE en cours d'exécution.	Ajoutez une nouvelle entrée de stratégie IKE et de nouveaux numéros de clé à un système appliquant actuellement la stratégie IKE.	<a href="#">“Procédure de configuration d'IKE pour un nouveau système homologue” à la page 271</a>

## Configuration du protocole IKE avec des clés prépartagées

Les clés prépartagées sont la méthode d'authentification la plus simple pour IKE. Elles s'utilisent notamment lors de la configuration du protocole IKE sur deux systèmes homologues gérés par le même administrateur. N'oubliez cependant pas que, contrairement aux certificats de clés publiques, les clés prépartagées sont liées à des adresses IP. Les clés prépartagées peuvent être associées à des adresses IP ou des plages d'adresses IP spécifiques, et ne peuvent pas s'utiliser avec des systèmes portables ou des systèmes susceptibles d'être renumérotés, à moins que la renumérotation soit incluse dans la plage d'adresses IP spécifiée.

### ▼ Configuration du protocole IKE avec des clés prépartagées

La longueur des clés des algorithmes d'implémentation du protocole IKE est variable. Elle dépend du niveau de sécurité dont vous souhaitez doter le site. En règle générale, la longueur des clés est proportionnelle au niveau de sécurité.

Dans cette procédure, vous générez des clés au format ASCII.

Les noms de systèmes choisis pour illustrer cette procédure sont : enigma et partym. Remplacez enigma et partym par les noms de vos systèmes.

---

**Remarque** – Pour utiliser IPsec avec des étiquettes sur un système Trusted Extensions, reportez-vous aux étapes supplémentaires indiquées à la section “[Procédure d’application des protections IPsec dans un réseau Trusted Extensions multiniveau](#)” du manuel *Configuration et administration d’Oracle Solaris Trusted Extensions*.

---

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d’informations, reportez-vous à la section “[Procédure d’obtention des droits d’administration](#)” du manuel *Administration d’Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l’[Exemple 15-1](#).

### 2 Sur chaque système, créez un fichier `/etc/inet/ike/config`.

Vous pouvez utiliser le fichier `/etc/inet/ike/config.sample` comme modèle.

### 3 Entrez les règles et paramètres globaux dans le fichier `ike/config` sur chacun des systèmes.

Les règles et paramètres globaux de ce fichier doivent garantir le fonctionnement de la stratégie IPsec du fichier `ipsecinit.conf`. Les exemples de configuration IKE ci-dessous vont de pair avec les exemples `ipsecinit.conf` de la section “[Sécurisation du trafic entre deux systèmes à l’aide d’IPsec](#)” à la page 231.

#### a. Modifiez par exemple le fichier `/etc/inet/ike/config` sur le système `enigma`:

```
### ike/config file on enigma, 192.168.116.16

## Global parameters
#
## Defaults that individual rules can override.
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
#
## The rule to communicate with partym
# Label must be unique
{ label "enigma-partym"
  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes }
  p2_pfs 5
}
```

#### b. Modifiez le fichier `/etc/inet/ike/config` sur le système `partym`:

```
### ike/config file on partym, 192.168.13.213
## Global Parameters
#
p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha encr_alg 3des }
p2_pfs 2
```

```
## The rule to communicate with enigma
# Label must be unique
{ label "partym-enigma"
  local_addr 192.168.13.213
  remote_addr 192.168.116.16
  p1_xform
  { auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes }
  p2_pfs 5
}
```

**4 Sur chaque système, vérifiez la syntaxe du fichier.**

```
# /usr/lib/inet/in.iked -c -f /etc/inet/ike/config
```

**5 Créez un fichier /etc/inet/secret/ike.preshare sur chacun des systèmes.**

Placez la clé prépartagée dans chacun des fichiers.

**a. Sur le système enigma par exemple, le fichier ike.preshared se présente comme suit :**

```
# ike.preshared on enigma, 192.168.116.16
#...
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.13.213
  # The preshared key can also be represented in hex
# as in 0xf47cb0f432e14480951095f82b
# key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
}
```

**b. Sur le système partym, le fichier ike.preshared se présente comme suit :**

```
# ike.preshared on partym, 192.168.13.213
#...
{ localidtype IP
  localid 192.168.13.213
  remoteidtype IP
  remoteid 192.168.116.16
  # The preshared key can also be represented in hex
# as in 0xf47cb0f432e14480951095f82b
  key "This is an ASCII Cqret phrAz, use str0ng p@ssword tekniques"
}
```

**6 Activez le service IKE.**

```
# svcadm enable ipsec/ike
```

### Exemple 18-1 Actualisation d'une clé prépartagée IKE

Lorsqu'un administrateur IKE souhaite actualiser la clé prépartagée, il modifie les fichiers sur ses systèmes homologues et redémarre le démon `in.iked`.

Il commence par ajouter l'entrée de clé partagée, valide pour n'importe quel hôte sur le sous-réseau `192.168.13.0/24`.

```
#...
{ localidtype IP
  localid 192.168.116.0/24
  remoteidtype IP
  remoteid 192.168.13.0/24
  # enigma and partym's shared passphrase for keying material
  key "L0ooong key Th@t m^st Be Ch*angEd \"reguLarLy)"
}
```

Ensuite, l'administrateur redémarre le service IKE sur chaque système.

```
# svcadm enable ipsec/ike
```

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## ▼ Procédure de configuration d'IKE pour un nouveau système homologue

Si vous ajoutez des entrées de stratégie IPsec à une configuration de travail entre des systèmes homologues, vous devez actualiser le service de stratégie IPsec. Il n'est pas nécessaire de reconfigurer ou de redémarrer IKE.

Si vous ajoutez un nouveau système homologue à la stratégie IPsec, vous devez modifier non seulement IPsec, mais aussi la configuration IKE.

**Avant de commencer** Vous avez mis à jour le fichier `ipsecinit.conf` et actualisé la stratégie IPsec pour les systèmes homologues.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#). Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

### 2 Créez une règle pour la gestion des clés par IKE, pour le nouveau système qui utilise IPsec.

#### a. Par exemple, sur le système *enigma*, ajoutez la règle suivante au fichier `/etc/inet/ike/config`:

```
### ike/config file on enigma, 192.168.116.16

## The rule to communicate with ada

{label "enigma-to-ada"
  local_addr 192.168.116.16
```

```
remote_addr 192.168.15.7
pl_xform
{auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes}
p2_pfs 5
}
```

**b. Sur le système ada, ajoutez la règle suivante :**

```
### ike/config file on ada, 192.168.15.7

## The rule to communicate with enigma

{label "ada-to-enigma"
 local_addr 192.168.15.7
 remote_addr 192.168.116.16
 pl_xform
 {auth_method preshared oakley_group 5 auth_alg sha256 encr_alg aes}
 p2_pfs 5
}
```

**3 Créez une clé prépartagée IKE pour les systèmes homologues.**

**a. Sur le système enigma, ajoutez les informations suivantes au fichier**

**/etc/inet/secret/ike.preshared :**

```
# ike.preshared on enigma for the ada interface
#
{ localidtype IP
  localid 192.168.116.16
  remoteidtype IP
  remoteid 192.168.15.7
  # enigma and ada's shared key
  key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
}
```

**b. Sur le système ada, ajoutez les informations suivantes au fichier ike.preshared :**

```
# ike.preshared on ada for the enigma interface
#
{ localidtype IP
  localid 192.168.15.7
  remoteidtype IP
  remoteid 192.168.116.16
  # ada and enigma's shared key
  key "Twas brillig and the slivey toves did *s0mEtHiNg* be CareFULL hEEEr"
}
```

**4 Sur chaque système, actualisez le service ike.**

```
# svcadm refresh ike
```

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.



# Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches)

Le tableau ci-dessous répertorie les procédures de création de certificats de clés publiques pour IKE. Ces procédures incluent l'accélération et le stockage de certificats sur le matériel connecté.

Un certificat public doit être unique, ainsi le créateur d'un certificat de clé publique génère un nom unique et arbitraire pour ce certificat. En règle générale, on crée un nom distinctif X.509. Un autre nom peut également servir à l'identification. Le format de ces noms est *tag=value*. Les valeurs sont arbitraires, mais leur format doit correspondre au type de balise. Par exemple, le format de la balise email est *name@domain.suffix*.

Tâche	Description	Voir
Configuration du protocole IKE avec des certificats de clés publiques autosignés	Créez et placez deux certificats sur chaque système : <ul style="list-style-type: none"> <li>■ Un certificat autosigné</li> <li>■ Certificat de clé publique du système homologue</li> </ul>	<a href="#">“Configuration du protocole IKE avec des certificats de clés publiques autosignés” à la page 274</a>
Configuration du protocole IKE avec un certificat PKI émanant d'une autorité de certification	Créez une demande de certificat et placez trois certificats sur chacun des systèmes : <ul style="list-style-type: none"> <li>■ Le certificat créé par l'autorité de certification (CA) suite à votre demande</li> <li>■ Le certificat de clé publique de la CA</li> <li>■ la CRL de la CA.</li> </ul>	<a href="#">“Configuration du protocole IKE avec des certificats signés par une CA” à la page 279</a>
Configuration de certificats de clés publiques sur le matériel local	Procédez de l'une des manières suivantes : <ul style="list-style-type: none"> <li>■ Générez un certificat autosigné sur le matériel local et ajoutez la clé publique d'un système distant sur le matériel.</li> <li>■ Générez une demande de certificat dans le matériel local et ajoutez les certificats de clés publiques de la CA dans le matériel.</li> </ul>	<a href="#">“Génération et stockage de certificats de clés publiques dans le matériel” à la page 285</a>
Mise à jour de la liste des certificats révoqués (CRL) d'une PKI	Accédez à la CRL depuis un point de distribution central.	<a href="#">“Traitement des listes des certificats révoqués” à la page 288</a>

---

**Remarque** – Pour étiqueter les paquets et les négociations IKE sur un système Trusted Extensions, effectuez les procédures décrites à la section [“Configuration d’IPsec avec étiquettes \(liste des tâches\)” du manuel \*Configuration et administration d’Oracle Solaris Trusted Extensions\*](#).

Les certificats de clés publiques sont gérés dans la zone globale sur les systèmes Trusted Extensions. Trusted Extensions ne change pas la manière dont les certificats sont gérés et stockés.

---

## Configuration du protocole IKE avec des certificats de clés publiques

Grâce aux certificats de clés publiques, les systèmes communicants n'ont plus besoin de partager de numéros de clé secrets hors bande. Contrairement aux clés prépartagées, les certificats de clés publiques peuvent être utilisés sur une machine portable ou sur un système susceptible d'être renuméroté.

Les certificats de clés publiques peuvent également être stockés dans le matériel connecté. Pour la procédure, reportez-vous à la section [“Configuration du protocole IKE en vue de l'utilisation du matériel connecté” à la page 298](#).

### ▼ Configuration du protocole IKE avec des certificats de clés publiques autosignés

Dans cette procédure, vous créez une paire de certificats. La clé privée est stockée sur le disque, dans la base de données de certificats locale, et peut être référencée par la sous-commande `cert local`. La portion publique de la paire de certificats est stockée dans la base de données des certificats publics. Elle peut être référencée par la sous-commande `cert db`. Vous échangez la portion publique avec un système homologue. La combinaison des deux certificats sert à authentifier les transmissions IKE.

Les certificats autosignés nécessitent un temps système inférieur à celui des certificats publics émanant d'une CA, mais s'intègrent plus difficilement dans un environnement à grande échelle. A la différence des certificats émis par une CA, les certificats autosignés doivent être vérifiés hors bande.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#). Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

## 2 Créez un certificat autosigné dans la base de données `ike.privatekeys`.

```
# ikecert certlocal -ks -m keysize -t keytype \
-D dname -A altname \
[-S validity-start-time] [-F validity-end-time] [-T token-ID]
```

-ks	Crée un certificat autosigné.
-m keysize	Taille de la clé. La <i>keysize</i> peut être 512, 1 024, 2 048, 3 072 ou 4 096.
-t keytype	Spécifie le type d'algorithme à utiliser. Le <i>keytype</i> (type de clé) peut être <code>rsa-sha1</code> , <code>rsa-md5</code> ou <code>dsa-sha1</code> .
-D dname	Nom distinctif X.509 de l'objet du certificat. <i>dname</i> se présente de la manière suivante : <code>C=country</code> (pays), <code>O=organization</code> (organisation), <code>OU=organizational unit</code> , (unité d'organisation) <code>CN=common name</code> (nom commun). Les balises valides sont C, O, OU et CN.
-A altname	Nom alternatif du certificat. <i>altname</i> se présente de la manière suivante : <code>tag=value</code> . Les balises valides sont IP, DNS, email et DN.
-S, validity-start-time	Indique la date de début de validité absolue ou relative du certificat.
-F, validity-end-time	Indique la date de fin de validité absolue ou relative du certificat.
-T token-ID	Permet à un jeton matériel PKCS #11 de générer les clés. Les certificats sont alors stockés sur le matériel.

### a. Exécutée par exemple sur le système `partym`, la commande se présente comme suit :

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=partym" \
-A IP=192.168.13.213
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE-----
```

---

**Remarque** – Les valeurs des options `-D` et `-A` sont arbitraires. Ces valeurs servent uniquement à identifier le certificat. Elles ne permettent pas d'identifier un système, comme 192.168.13.213. Il s'agit en réalité de valeurs idiosyncrasiques, vous devez donc vérifier hors bande que le certificat correct est installé sur les systèmes homologues.

---

### b. Exécutée sur le système `enigma`, elle se présente de la manière suivante :

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
-D "O=exampleco, OU=IT, C=US, CN=enigma" \
-A IP=192.168.116.16
Creating private key.
Certificate added to database.
-----BEGIN X509 CERTIFICATE-----
```

```
MIIC1TCCAb2gAwIBAgIEB15JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

### 3 Enregistrez le certificat et envoyez-le au système distant.

La sortie est une version codée de la portion publique du certificat. Vous pouvez coller en toute sécurité ce certificat dans un e-mail. La partie réceptrice doit vérifier hors bande que le certificat correct est installé, comme indiqué dans l'[Étape b](#).

#### a. Par exemple, vous transmettez la portion publique du certificat par `tym` à l'administrateur de `enigma`.

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEfdZgKjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
a...+
zBGi4QkNdI3f
-----END X509 CERTIFICATE-----
```

#### b. L'administrateur de `enigma` vous transmet la portion publique du certificat `enigma`.

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MIIC1TCCAb2gAwIBAgIEB15JnjANBgkqhkiG9w0BAQUFADAaMRgwFgYDVQQDEw9T
...
y85m6LHJYtC6
-----END X509 CERTIFICATE-----
```

### 4 Sur chaque système, ajoutez le certificat que vous avez reçu à la base de données de clés publiques.

#### a. Enregistrez l'e-mail de l'administrateur dans un fichier lisible par `root`.

#### b. Redirigez le fichier vers la commande `ikecert`.

```
# ikecert certdb -a < /tmp/certificate.eml
```

La commande importe le texte entre les balises `BEGIN` et `END`.

### 5 Vérifiez auprès de l'autre administrateur que ce certificat est bien de lui.

Par exemple, vous pouvez téléphoner à l'autre administrateur afin de vérifier que le hachage de son certificat public, que vous possédez, correspond au hachage de son certificat privé, que seul lui possède.

#### a. Répertoriez les certificats stockés sur `partym`.

Dans l'exemple suivant, la remarque 1 indique le nom distinctif du certificat dans l'emplacement 0. Le certificat privé de l'emplacement 0 possède le même hachage, ces

certificats appartiennent donc à la même paire de certificats. Pour que les certificats publics fonctionnent, vous devez posséder une paire correspondante. La sous-commande `certdb` répertorie la portion publique, tandis que la sous-commande `certlocal` répertorie la portion privée.

```
partym # ikecert certdb -l
```

```
Certificate Slot Name: 0   Key Type: rsa
  (Private key in certlocal slot 0)
  Subject Name: <O=exampleco, OU=IT, C=US, CN=partym>   Note 1
  Key Size: 2048
  Public key hash: 80829EC52FC5BA910F4764076C20FDCF
```

```
Certificate Slot Name: 1   Key Type: rsa
  (Private key in certlocal slot 1)
  Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
  Key Size: 2048
  Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
partym # ikecert certlocal -l
```

```
Local ID Slot Name: 0   Key Type: rsa
  Key Size: 2048
  Public key hash: 80829EC52FC5BA910F4764076C20FDCF   Note 3
```

```
Local ID Slot Name: 1   Key Type: rsa-sha1
  Key Size: 2048
  Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
Local ID Slot Name: 2   Key Type: rsa
  Key Size: 2048
  Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

Cette vérification a permis de confirmer que le système `partym` possédait une paire de certificats valide.

#### b. Vérifiez que le système `enigma` possède le certificat public de `partym`.

Vous pouvez communiquer la valeur de hachage par téléphone.

Comparez les hachages de la remarque 3 sur `partym` indiquée dans l'étape précédente avec la remarque 4 sur `enigma`.

```
enigma # ikecert certdb -l
```

```
Certificate Slot Name: 0   Key Type: rsa
  (Private key in certlocal slot 0)
  Subject Name: <O=exampleco, OU=IT, C=US, CN=Ada>
  Key Size: 2048
  Public key hash: 2239A6A127F88EE0CB40F7C24A65B818
```

```
Certificate Slot Name: 1   Key Type: rsa
  (Private key in certlocal slot 1)
  Subject Name: <O=exampleco, OU=IT, C=US, CN=enigma>
```

```
Key Size: 2048
Public key hash: FEA65C5387BBF3B2C8F16C019FEB388
```

```
Certificate Slot Name: 2   Key Type: rsa
  (Private key in certlocal slot 2)
Subject Name: <O=exampleco, OU=IT, C=US, CN=partym>
Key Size: 2048
Public key hash: 80829EC52FC5BA910F4764076C20FDCF   Note 4
```

Le hachage de clé publique et le nom du sujet du dernier certificat stocké dans la base de données de certificats publics de enigma correspond au hachage du certificat privé de partym issu de l'étape précédente.

## 6 Approuvez les deux certificats sur chacun des systèmes.

Editez le fichier `/etc/inet/ike/config` pour reconnaître les certificats.

L'administrateur du système distant fournit la valeur des paramètres `cert_trust`, `remote_addr` et `remote_id`.

### a. Sur le système partym par exemple, le fichier `ike/config` se présente de la manière suivante :

```
# Explicitly trust the self-signed certs
# that we verified out of band. The local certificate
# is implicitly trusted because we have access to the private key.

cert_trust "O=exampleco, OU=IT, C=US, CN=enigma"

# We could also use the Alternate name of the certificate,
# if it was created with one. In this example, the Alternate Name
# is in the format of an IP address:
# cert_trust "192.168.116.16"

## Parameters that may also show up in rules.

p1_xform
{ auth_method preshared oakley_group 5 auth_alg sha256 encr_alg 3des }
p2_pfs 5

{
  label "US-partym to JA-enigmax"
  local_id type dn
  local_id "O=exampleco, OU=IT, C=US, CN=partym"
  remote_id "O=exampleco, OU=IT, C=US, CN=enigma"

  local_addr 192.168.13.213
  # We could explicitly enter the peer's IP address here, but we don't need
  # to do this with certificates, so use a wildcard address. The wildcard
  # allows the remote device to be mobile or behind a NAT box
  remote_addr 0.0.0.0/0

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

**b. Sur le système enigma, ajoutez les valeurs de enigma des paramètres locaux dans le fichier `ike/config`.**

Pour les paramètres distants, utilisez les valeurs de `partym`. Assurez-vous que la valeur du mot-clé `label` est unique sur le système local.

```
...
{
  label "JA-enigmax to US-partym"
  local_id_type dn
  local_id "O=exampleco, OU=IT, C=US, CN=enigma"
  remote_id "O=exampleco, OU=IT, C=US, CN=partym"

  local_addr 192.168.116.16
  remote_addr 0.0.0.0/0
...

```

**7 Sur les systèmes homologues, activez IKE.**

```
partym # svcadm enable ipsec/ike
```

```
enigma # svcadm enable ipsec/ike
```

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## ▼ Configuration du protocole IKE avec des certificats signés par une CA

Les certificats publics émanant d'autorités de certification (CA) requièrent une négociation avec une organisation externe. Ces certificats s'intègrent très facilement dans les environnements à grande échelle afin protéger un grand nombre de systèmes communicants.

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section "[Procédure d'obtention des droits d'administration](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

## 2 La commande `ikecert certlocal -kc` permet de créer une demande de certificat.

Pour consulter la description des arguments de cette commande, reportez-vous à l'[Étape b](#) de la section “[Configuration du protocole IKE avec des certificats de clés publiques autosignés](#)” à la page 274.

```
# ikecert certlocal -kc -m keysize -t keytype \  
-D dname -A altname
```

### a. La commande suivante permet par exemple de créer une demande de certificats sur le système partym :

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \  
> -D "C=US, O=PartyCompany\, Inc., OU=US-Partym, CN=Partym" \  
> -A "DN=C=US, O=PartyCompany\, Inc., OU=US-Partym" \  
Creating software private keys. \  
Writing private key to file /etc/inet/secret/ike.privatekeys/2. \  
Enabling external key providers - done. \  
Certificate Request: \  
Proceeding with the signing operation. \  
Certificate request generated successfully (.../publickeys/0) \  
Finished successfully. \  
-----BEGIN CERTIFICATE REQUEST----- \  
MIIBYjCCATMCAQAwUzELMAkGA1UEBhMCVVMxHTAbBgNVBAoTTFEV4YW1wbGVDb21w \  
... \  
lcM+tw0ThRrfuJX9t/Qa1R/KxRlMA3zckO80mO9X \  
-----END CERTIFICATE REQUEST-----
```

### b. La commande suivante permet de créer une demande de certificat sur le système enigma :

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \  
> -D "C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax, CN=Enigmax" \  
> -A "DN=C=JA, O=EnigmaCo\, Inc., OU=JA-Enigmax" \  
Creating software private keys. \  
... \  
Finished successfully. \  
-----BEGIN CERTIFICATE REQUEST----- \  
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu \  
... \  
8qlqdjaStLGfhd00 \  
-----END CERTIFICATE REQUEST-----
```

## 3 Soumettez la demande de certificat à un fournisseur de PKI.



Le fournisseur de PKI vous indiquera la procédure de soumission des demandes de certificat. Dans la plupart des cas, celle-ci s'effectue en remplissant un formulaire directement sur le site Web du fournisseur. Dans ce formulaire, vous devrez notamment indiquer la preuve de la légitimité de votre demande. Il suffit généralement de coller votre certificat dans le formulaire. Après avoir vérifié votre demande, le fournisseur émet les deux objets de certificats suivants et une liste des certificats révoqués :

- Votre certificat de clé publique : ce certificat est basé sur la demande que vous avez envoyée au fournisseur. Cette demande est intégrée au certificat, qui vous identifie de manière unique.
- Un certificat CA : la signature du fournisseur. La CA vérifie que votre certificat de clé publique est légitime.
- Une liste des certificats révoqués (CRL) : la liste la plus récente des certificats révoqués par le fournisseur. Cette liste n'est pas expédiée sous la forme d'un objet de certificat séparé si l'accès à la CRL est intégré au certificat de clé publique.

Si un URI de CRL est intégré au certificat de clé publique, IKE peut récupérer automatiquement la CRL. De la même façon, si une entrée de DN (nom de répertoire sur un serveur LDAP) est intégrée au certificat de clé publique, IKE peut récupérer la CRL sur un serveur LDAP que vous avez spécifié et la mettre en cache.

Pour consulter un exemple d'URI et d'entrée de DN intégrés à un certificat de clé publique, reportez-vous à la section [“Traitement des listes des certificats révoqués”](#) à la page 288.

#### 4 Ajoutez tous les certificats sur votre système.

L'option -a de la commande `ikecert certdb -a` ajoute l'objet collé à la base de données de certificats correspondante de votre système. Pour plus d'informations, reportez-vous à la section [“IKE avec certificats de clés publiques”](#) à la page 262.

##### a. Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

##### b. Ajoutez le certificat de clé publique que vous avez reçu du fournisseur de PKI.

```
# ikecert certdb -a < /tmp/PKIcert.eml
```

##### c. Ajoutez le certificat CA émanant du fournisseur de PKI.

```
# ikecert certdb -a < /tmp/PKIca.eml
```

- d. Si le fournisseur de PKI vous a envoyé une liste des certificats révoqués, ajoutez-la à la base de données `cert_rldb` :

```
# ikecert cert_rldb -a
  Press the Return key
  Paste the CRL:
-----BEGIN CRL-----
...
-----END CRL-----
  Press the Return key
<Control>-D
```

- 5 Le mot-clé `cert_root` permet d'identifier le fournisseur de PKI dans le fichier `/etc/inet/ike/config`.

Utilisez le nom que le fournisseur de PKI vous a indiqué.

- a. Sur le système `partym`, par exemple, le fichier `ike/config` peut se présenter de la manière suivante :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

## Parameters that may also show up in rules.

p1_xform
{ auth_method rsa_sig oakley_group 1 auth_alg sha384 encr_alg aes}
p2_pfs 2

{
  label "US-partym to JA-enigmax - Example PKI"
  local_id type dn
  local_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"
  remote_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"

  local_addr 192.168.13.213
  remote_addr 192.168.116.16

  p1_xform
  {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

---

**Remarque** – Tous les arguments du paramètre `auth_method` doivent se trouver sur la même ligne.

---

- b. Créez un fichier similaire sur le système `enigma`.

Le fichier `enigma ike/config` doit :

- Inclure la même valeur `cert_root`.
- Utiliser les valeurs de `enigma` pour les paramètres locaux.
- Utiliser les valeurs de `partym` pour les paramètres distants.
- Créer une valeur unique pour le mot-clé `label`. Elle doit différer de la valeur `label` du système distant.

```
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"
...
{
  label "JA-enigmax to US-partym - Example PKI"
  local_id_type dn
  local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
  remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

  local_addr 192.168.116.16
  remote_addr 192.168.13.213
  ...
}
```

## 6 Spécifiez le mode de traitement des CRL par le protocole IKE.

Choisissez l'option appropriée :

### ■ Pas de CRL disponible

Si le fournisseur de PKI ne fournit pas de CRL, ajoutez le mot-clé `ignore_crls` au fichier `ike/config`.

```
# Trusted root cert
...
cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, ...
ignore_crls
...
```

Le mot-clé `ignore_crls` indique au protocole IKE de ne pas chercher de CRL.

### ■ CRL disponible

Si le fournisseur de PKI vous communique un point de distribution central pour les CRL, vous pouvez modifier le fichier `ike/config` de manière à ce qu'il pointe sur cet emplacement.

Pour consulter des exemples de ce type de configuration, reportez-vous à la section [“Traitement des listes des certificats révoqués” à la page 288](#).

**Exemple 18-2** Utilisation de `rsa_encrypt` lors de la configuration du protocole IKE

Lorsque vous utilisez `auth_method rsa_encrypt` dans le fichier `ike/config`, vous devez ajouter le certificat homologue à la base de données `publickeys`.

1. Envoyez ce certificat à l'administrateur du système distant.

Vous pouvez le coller dans un e-mail.

L'administrateur de `party` envoie le message suivant :

```
To: admin@ja.enigmaexample.com
From: admin@us.partyexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII...
-----END X509 CERTIFICATE-----
```

L'administrateur de `enigma` envoie l'e-mail suivant :

```
To: admin@us.partyexample.com
From: admin@ja.enigmaexample.com
Message: -----BEGIN X509 CERTIFICATE-----
MII
...
-----END X509 CERTIFICATE-----
```

2. Sur chacun des systèmes, ajoutez à la base de données `publickeys` locale le certificat envoyé par e-mail.

```
# ikcert certdb -a < /tmp/saved.cert.eml
```

En cachant les identités à l'aide du protocole IKE, la méthode d'authentification utilisée en chiffrement RSA prévient les risques d'écoute électronique. Etant donné que la méthode `rsa_encrypt` cache l'identité de l'homologue, le protocole IKE ne peut récupérer son certificat. La méthode `rsa_encrypt` requiert donc que les homologues IKE connaissent leurs clés publiques respectives.

C'est pourquoi vous devez ajouter le certificat de l'homologue à la base de données `publickeys` lorsque vous utilisez la méthode `auth_method` de `rsa_encrypt` dans le fichier `/etc/inet/ike/config`. La base de données `publickeys` détient alors trois certificats pour chaque couple de systèmes communicants :

- Votre certificat de clé publique
- Le certificat CA
- Le certificat de clé publique de l'homologue

**Dépannage** la charge du protocole IKE, qui inclut les trois certificats, peut s'avérer trop importante pour le chiffrement via `rsa_encrypt`. L'apparition d'erreurs indiquant que l'autorisation a échoué ou que la charge n'est pas conforme peut signifier que la méthode `rsa_encrypt` est incapable de chiffrer la totalité de la charge. Pour réduire la charge, utilisez une autre méthode (par exemple, `rsa_sig`, qui ne requiert que deux certificats).

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## ▼ Génération et stockage de certificats de clés publiques dans le matériel

Le processus de génération et de stockage de certificats de clés publiques sur du matériel est similaire au processus de génération et de stockage de certificats de clés publiques sur un système. Dans le premier cas, il convient d'identifier le matériel à l'aide des commandes `ikecert certlocal` et `ikecert certdb`, accompagnées de l'option `-T` et de l'ID de jeton.

### Avant de commencer

- Le matériel doit être configuré.
- Excepté si le mot-clé `pkcs11_path` du fichier `/etc/inet/ike/config` pointe sur une autre bibliothèque, le matériel utilise `/usr/lib/libpkcs11.so`. Cette bibliothèque doit être implémentée conformément aux standards suivants : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki), c'est-à-dire une bibliothèque PKCS #11.

Pour consulter les instructions de paramétrage, reportez-vous à la section [“Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 6000”](#) à la page 298.

### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

### 2 Générez un certificat autosigné ou une demande de certificat et spécifiez l'ID de jeton.

Procédez de l'une des manières suivantes :

---

**Remarque** – Pour RSA, la carte Sun Crypto Accelerator 6000 prend en charge des clés d'une longueur maximum de 2 048 bits. Pour DSA, la longueur maximum des clés est de 1 024 bits.

---

- Pour un certificat autosigné, utilisez la syntaxe suivante :

```
# ikecert certlocal -ks -m 2048 -t rsa-sha1 \
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \
> -a -T dca0-accel-stor IP=192.168.116.16
Creating hardware private keys.
Enter PIN for PKCS#11 token:      Type user:password
```

L'argument de l'option `-T` est l'ID de jeton de la carte Sun Crypto Accelerator 6000 connectée.

- **Pour une demande de certificat, utilisez la syntaxe suivante :**

```
# ikecert certlocal -kc -m 2048 -t rsa-sha1 \  
> -D "C=US, O=PartyCompany, OU=US-Partym, CN=Partym" \  
> -a -T dca0-accel-stor IP=192.168.116.16  
Creating hardware private keys.  
Enter PIN for PKCS#11 token:      Type user:password
```

Pour obtenir une description des arguments de la commande `ikecert`, reportez-vous à la page de manuel [ikecert\(1M\)](#).

- 3 Lorsque vous êtes invité à saisir le PIN, entrez le nom de l'utilisateur de la carte Sun Crypto Accelerator 6000 suivi de deux-points et du mot de passe de l'utilisateur.**

Si la carte Sun Crypto Accelerator 6000 possède un utilisateur `ikemgr` dont le mot de passe est `rgm4tigt`, entrez :

Enter PIN for PKCS#11 token: **ikemgr:rgm4tigt**

---

**Remarque** – La réponse est stockée en *texte en clair* sur le disque.

---

Après entrée du mot de passe, le certificat s'imprime :

```
Enter PIN for PKCS#11 token: ikemgr:rgm4tigt  
-----BEGIN X509 CERTIFICATE-----  
MIIBuDCCASECAQAwSTELMAkGA1UEBhMCVVMxFTATBgNVBAoTDFBhcnR5Q29tcGFu  
...  
oKUDBbZ90/pLwYGr  
-----END X509 CERTIFICATE-----
```

- 4 Envoyez votre certificat aux personnes concernées.**

Procédez de l'une des manières suivantes :

- **Envoyez le certificat autosigné au système distant.**

Vous pouvez le coller dans un e-mail.

- **Envoyez la demande de certificat à un fournisseur de PKI.**

Pour ce faire, suivez les instructions du fournisseur de PKI. Pour plus d'informations, reportez-vous à l'[Étape 3](#) de la section "[Configuration du protocole IKE avec des certificats signés par une CA](#)" à la page 279.

## 5 Editez le fichier `/etc/inet/ike/config` sur votre système pour reconnaître les certificats.

Procédez de l'une des manières suivantes :

### ■ Certificat autosigné

Utilisez les valeurs fournies par l'administrateur du système distant pour les paramètres `cert_trust`, `remote_id` et `remote_addr`. Sur le système enigma par exemple, le fichier `ike/config` se présente comme suit :

```
# Explicitly trust the following self-signed certs
# Use the Subject Alternate Name to identify the cert

cert_trust "192.168.116.16"      Local system's certificate Subject Alt Name
cert_trust "192.168.13.213"    Remote system's certificate Subject Alt name

...
{
    label "JA-enigmax to US-party"
    local_id_type dn
    local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
    remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

    local_addr 192.168.116.16
    remote_addr 192.168.13.213

    pl_xform
    {auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

### ■ Demande de certificat

Entrez le nom que le fournisseur de PKI vous a communiqué comme valeur du mot-clé `cert_root`. Sur le système enigma par exemple, le fichier `ike/config` peut se présenter comme suit :

```
# Trusted root cert
# This certificate is from Example PKI
# This is the X.509 distinguished name for the CA that it issues.

cert_root "C=US, O=ExamplePKI\, Inc., OU=PKI-Example, CN=Example PKI"

...
{
    label "JA-enigmax to US-party - Example PKI"
    local_id_type dn
    local_id "C=JA, O=EnigmaCo, OU=JA-Enigmax, CN=Enigmax"
    remote_id "C=US, O=PartyCompany, OU=US-Partym, CN=Partym"

    local_addr 192.168.116.16
    remote_addr 192.168.13.213

    pl_xform
```

```
{auth_method rsa_sig oakley_group 2 auth_alg sha256 encr_alg aes}
}
```

## 6 Placez les certificats de l'autre partie sur le matériel.

Répondez à la demande de PIN comme vous l'avez fait au cours de l'[Étape 3](#).

---

**Remarque** – Vous *devez* ajouter les certificats de clés publiques au matériel connecté qui a généré votre clé privée.

---

### ■ Certificat autosigné.

Ajoutez le certificat autosigné du système distant. Dans cet exemple, il est stocké dans le fichier `DCA.ACCEL.STOR.CERT`.

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

Si le certificat autosigné a utilisé `rsa_encrypt` comme valeur du paramètre `auth_method`, ajoutez le certificat de l'homologue au magasin du matériel.

### ■ Certificats émanant d'un fournisseur de PKI.

Ajoutez le certificat généré par le fournisseur suite à votre demande et ajoutez la CA.

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

```
# ikecert certdb -a -T dca0-accel-stor < DCA.ACCEL.STOR.CA.CERT
Enter PIN for PKCS#11 token:      Type user:password
```

Pour ajouter une liste des certificats révoqués (CRL) communiquée par un fournisseur de PKI, reportez-vous à la section “[Traitement des listes des certificats révoqués](#)” à la page 288.

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## ▼ Traitement des listes des certificats révoqués

Les listes des certificats révoqués (CRL) sont émises par une autorité de certification et contiennent les certificats périmés ou compromis. Vous pouvez traiter les CRL de quatre façons :

- Vous devez faire en sorte que le protocole IKE ignore les listes des certificats révoqués si votre CA n'en émet pas. Pour plus d'informations, reportez-vous à l'[Étape 6](#) de la section “[Configuration du protocole IKE avec des certificats signés par une CA](#)” à la page 279.



- Vous pouvez faire en sorte que le protocole IKE accède aux CRL à partir d'un URI (uniform resource indicator, identificateur universel de ressources) dont l'adresse est intégrée au certificat de clé publique de la CA.
- Vous pouvez faire en sorte que le protocole IKE accède aux CRL à partir d'un serveur LDAP dont l'entrée de nom de répertoire (DN, directory name) est intégrée au certificat de clé publique de la CA.
- Vous pouvez traiter les CRL comme des arguments de la commande `ikecert certldb`. Voir l'[Exemple 18-3](#).

La section ci-dessous décrit la procédure permettant de paramétrer l'utilisation des CRL à partir d'un point de distribution central dans le protocole IKE.

## 1 Affichez le certificat que vous avez reçu de la CA.

```
# ikecert certldb -lv certspec
```

-l            Liste les certificats dans la base de données de certificats IKE.

-v            Liste les certificats en mode détaillé. Utilisez cette option avec précaution.

*certspec*    Modèle permettant de rechercher les certificats correspondants dans la base de données de certificats IKE.

Par exemple, le certificat suivant a été émis par Oracle. (les détails ont été modifiés).

```
# ikecert certldb -lv example-protect.oracle.com
```

```
Certificate Slot Name: 0    Type: dsa-sha1
```

```
(Private key in certlocal slot 0)
```

```
Subject Name: <O=Oracle, CN=example-protect.oracle.com>
```

```
Issuer Name: <CN=Oracle CA (Cl B), O=Oracle>
```

```
SerialNumber: 14000D93
```

```
Validity:
```

```
Not Valid Before: 2011 Sep 19th, 21:11:11 GMT
```

```
Not Valid After: 2015 Sep 18th, 21:11:11 GMT
```

```
Public Key Info:
```

```
Public Modulus (n) (2048 bits): C575A...A5
```

```
Public Exponent (e) ( 24 bits): 010001
```

```
Extensions:
```

```
Subject Alternative Names:
```

```
DNS = example-protect.oracle.com
```

```
Key Usage: DigitalSignature KeyEncipherment
```

```
[CRITICAL]
```

```
CRL Distribution Points:
```

```
Full Name:
```

```
URI = #Ihttp://www.oracle.com/pki/pkismica.crl#i
```

```
DN = <CN=Oracle CA (Cl B), O=Oracle>
```

```
CRL Issuer:
```

```
Authority Key ID:
```

```
Key ID:                    4F ... 6B
```

```
SubjectKeyID:            A5 ... FD
```

```
Certificate Policies
```

```
Authority Information Access
```

Notez l'entrée `CRL Distribution Points`. L'entrée `URI` indique que la CRL de cette organisation est disponible sur le Web. L'entrée `DN` indique que la CRL est disponible sur un serveur LDAP. Après que le protocole IKE a accédé à la CRL, celle-ci est mise en cache en vue de futures utilisations.

Pour accéder à la CRL, vous devez tout d'abord accéder à un point de distribution.

## 2 Choisissez l'une des méthodes suivantes pour accéder à la CRL depuis un point de distribution central.

### ■ Utilisez l'URI.

Ajoutez le mot-clé `use_http` au fichier `/etc/inet/ike/config` de l'hôte. Le fichier `ike/config` se présente comme suit :

```
# Use CRL from organization's URI
use_http
...
```

### ■ Utilisez un proxy Web.

Ajoutez le mot-clé `proxy` au fichier `ike/config`. Le mot-clé `proxy` adopte une URL comme argument, comme indiqué ci-dessous :

```
# Use own web proxy
proxy "http://proxy1:8080"
```

### ■ Utilisez un serveur LDAP.

Utilisez le nom du serveur LDAP comme argument du mot-clé `ldap-list` dans le fichier `/etc/inet/ike/config` de l'hôte. Le nom du serveur LDAP est fourni par votre organisation. L'entrée dans le fichier `ike/config` se présente comme suit :

```
# Use CRL from organization's LDAP
ldap-list "ldap1.oracle.com:389,ldap2.oracle.com"
...
```

Le protocole IKE récupère la CRL et la met en cache jusqu'à ce que le certificat expire.

## Exemple 18-3 Ajout d'une CRL à la base de données `certltdb` locale

Si la CRL du fournisseur de PKI n'est pas disponible à partir d'un point de distribution central, vous pouvez ajouter cette liste manuellement à la base de données `certltdb` locale. Pour extraire la CRL dans un fichier, suivez les instructions du fournisseur de PKI, puis ajoutez la CRL à la base de données à l'aide de la commande `ikecert certltdb -a`.

```
# ikcert certltdb -a < Oracle.Cert.CRL
```

# Configuration du protocole IKE pour les systèmes portables (liste des tâches)

Le tableau ci-dessous décrit les procédures permettant de configurer le protocole IKE pour gérer des systèmes qui se connectent à distance à un site central.

Tâche	Description	Voir
Etablissement de la communication avec un site central depuis un lieu hors site	Permettez aux systèmes hors site de communiquer avec un site central. Ces systèmes peuvent être portables.	<a href="#">“Configuration du protocole IKE pour les systèmes hors site” à la page 291</a>
Utilisation d'un certificat public d'une CA et du protocole IKE sur un système central acceptant le trafic des systèmes mobiles	Configurez un système de passerelle pour accepter le trafic IPsec d'un système ne possédant pas d'adresse IP fixe.	<a href="#">Exemple 18-4</a>
Utilisation d'un certificat public d'une CA et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez le système portable de manière à protéger son trafic avec le site central (par exemple, le siège de l'entreprise).	<a href="#">Exemple 18-5</a>
Utilisation de certificats autosignés et du protocole IKE sur un système central acceptant le trafic de systèmes mobiles	Configurez un système de passerelle avec des certificats autosignés pour accepter le trafic IPsec d'un système portable.	<a href="#">Exemple 18-6</a>
Utilisation de certificats autosignés et du protocole IKE sur un système ne possédant pas d'adresse IP fixe	Configurez un système portable avec des certificats autosignés pour protéger son trafic avec un site central.	<a href="#">Exemple 18-7</a>

## Configuration du protocole IKE pour les systèmes portables

Lorsqu'ils sont configurés correctement, les ordinateurs portables peuvent communiquer avec les ordinateurs centraux de l'entreprise via IPsec et IKE. L'utilisation combinée d'une stratégie IPsec globale et d'une méthode d'authentification de clé publique permet de protéger le trafic des systèmes hors site avec le système central.

### ▼ Configuration du protocole IKE pour les systèmes hors site

Les protocoles IPsec et IKE requièrent un ID unique pour identifier la source et la destination. Pour les systèmes portables hors site ne possédant pas d'adresse IP unique, vous devez utiliser un autre type d'ID permettant d'identifier un système de manière unique (par exemple, DNS, DN ou email).

Il est toujours préférable de configurer les systèmes portables ou hors site possédant une adresse IP unique avec un autre type d'ID. Par exemple, si ces systèmes tentent de se connecter à un site central par l'intermédiaire d'un boîtier NAT, leur adresse unique n'est pas utilisée. Le boîtier NAT leur assigne une adresse IP arbitraire que le système central ne reconnaît pas.

Les clés prépartagées ne sont pas, elles non plus, un moyen d'authentification approprié pour les systèmes portables, car elles requièrent une adresse IP fixe. Les certificats autosignés ou les certificats PKI permettent par contre aux systèmes portables de communiquer avec le site central.

## 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#). Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

## 2 Configurez le système central de manière à ce qu'il reconnaisse les systèmes portables.

### a. Configurez le fichier `ipsecinit.conf`.

Le système central nécessite une stratégie autorisant une plage étendue d'adresses IP. Les certificats de la stratégie IKE garantissent ultérieurement la légitimité des systèmes connectés.

```
# /etc/inet/ipsecinit.conf on central
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}
```

### b. Configurez le fichier de configuration IKE.

Le DNS identifie le système central et les certificats permettent d'authentifier le système.

```
## /etc/inet/ike/ike.config on central
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# List self-signed certificates - trust server and enumerated others
#cert_trust "DNS=central.domain.org"
#cert_trust "DNS=mobile.domain.org"
#cert_trust "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust "email=root@central.domain.org"
```

```
#cert_trust    "email=user1@mobile.domain.org"
#

# Rule for mobile systems with certificate
{
    label "Mobile systems with certificate"
    local_id type DNS
    # CA's public certificate ensures trust,
    # so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

### 3 Connectez-vous à chacun des systèmes portables et configurez-les de manière à ce qu'ils trouvent le système central.

#### a. Configurez le fichier `/etc/hosts`.

Le fichier `/etc/hosts` n'a pas besoin d'une adresse pour le système mobile, mais peut en fournir une. Il doit contenir une adresse IP publique pour le système central.

```
# /etc/hosts on mobile
central 192.xxx.xxx.x
```

#### b. Configurez le fichier `ipsecinit.conf`.

Le système portable doit être capable de trouver le système central à partir de son adresse IP publique. Les deux systèmes doivent avoir la même stratégie IPsec.

```
# /etc/inet/ipsecinit.conf on mobile
# Find central
{raddr 192.xxx.xxx.x} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}
```

#### c. Configurez le fichier de configuration IKE.

L'identificateur ne peut pas être une adresse IP. Pour les systèmes portables, les identificateurs valides sont les suivants :

- `DN=nom-répertoire-ldap`
- `DNS=adresse-DNS`
- `email=adresse-e-mail`

Les certificats permettent d'authentifier le système portable.

```
## /etc/inet/ike/ike.config on mobile
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
```

```
# Use web proxy
proxy "http://somecache.domain:port/"
#
# Use LDAP server
ldap_server "ldap-server1.domain.org,ldap2.domain.org:port"
#
# List CA-signed certificates
cert_root "C=US, O=Domain Org, CN=Domain STATE"
#
# Self-signed certificates - trust me and enumerated others
#cert_trust "DNS=mobile.domain.org"
#cert_trust "DNS=central.domain.org"
#cert_trust "DN=CN=Domain Org STATE (CLASS), O=Domain Org"
#cert_trust "email=user1@domain.org"
#cert_trust "email=root@central.domain.org"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile with certificate"
    local_id_type DNS

# NAT-T can translate local_addr into any public IP address
# central knows me by my DNS

    local_id "mobile.domain.org"
    local_addr 0.0.0.0/0

# Find central and trust the root certificate
    remote_id "central.domain.org"
    remote_addr 192.xxx.xxx.x

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

#### 4 Activez le service ike.

```
# svcadm enable svc:/network/ipsec/ike
```

### Exemple 18–4 Configuration d'un ordinateur central pour qu'il accepte le trafic IPsec d'un système portable

Le protocole IKE peut commencer les négociations derrière un boîtier NAT, mais il est préférable de ne pas faire intervenir de boîtier de ce type. Dans l'exemple ci-dessous, le certificat public d'une CA a été placé sur le système mobile et sur le système central. Le système central accepte les négociations IPsec émanant d'un système situé derrière un boîtier NAT. main1 est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'[Exemple 18–5](#).

```
## /etc/hosts on main1
main1 192.168.0.100
```

```

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
    label "Off-site system with root certificate"
    local_id_type DNS
    local_id "main1.domain.org"
    local_addr 192.168.0.100

# CA's public certificate ensures trust,
# so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256}
}

```

### Exemple 18–5 Configuration d'un système situé derrière un boîtier NAT avec IPsec

Dans l'exemple ci-dessous, le certificat public d'une CA a été placé sur le système mobile et sur le système central. `mobile1` se connecte au siège de l'entreprise depuis son domicile. Le réseau du FAI (fournisseur d'accès Internet) utilise un boîtier NAT pour pouvoir assigner une adresse privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres nœuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'[Exemple 18–4](#).

```

## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

```

```
## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters
#
# Find CRLs by URI, URL, or LDAP
# Use CRL from organization's URI
use_http
#
# Use web proxy
proxy "http://cache1.domain.org:8080/"
#
# Use LDAP server
ldap_server "ldap1.domain.org,ldap2.domain.org:389"
#
# List CA-signed certificate
cert_root "C=US, O=ExamplePKI Inc, OU=PKI-Example, CN=Example PKI"
#
# Rule for off-site systems with root certificate
{
    label "Off-site mobile1 with root certificate"
    local_id_type DNS
    local_id "mobile1.domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the root certificate
    remote_id "main1.domain.org"
    remote_addr 192.168.0.100

p2_pfs 5

pl_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

### Exemple 18-6 Acceptation de certificats autosignés émanant d'un système portable

Dans l'exemple ci-dessous, les certificats autosignés ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. main1 est le système acceptant les connexions de systèmes hors site. Pour paramétrer les systèmes hors site, reportez-vous à l'[Exemple 18-7](#).

```
## /etc/hosts on main1
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on main1
# Keep everyone out unless they use this IPsec policy:
{} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on main1
# Global parameters
#
# Self-signed certificates - trust me and enumerated others
```



```

cert_trust      "DNS=main1.domain.org"
cert_trust      "jdoe@domain.org"
cert_trust      "user2@domain.org"
cert_trust      "user3@domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site systems with trusted certificates"
    local_id_type DNS
    local_id "main1.domain.org"
    local_addr 192.168.0.100

# Trust the self-signed certificates
# so allow any remote_id and any remote IP address.
    remote_id ""
    remote_addr 0.0.0.0/0

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}

```

### Exemple 18–7 Utilisation de certificats autosignés pour contacter un système central

Dans l'exemple ci-dessous, `mobile1` se connecte au siège de l'entreprise depuis un domicile privé. Les certificats ont été émis par le système portable et le système central, et ont été placés sur les deux systèmes. Le réseau du FAI utilise un boîtier NAT pour assigner une adresse privée à `mobile1`. Le boîtier NAT convertit l'adresse privée en une adresse IP publique partagée par d'autres noeuds du réseau du FAI. Le siège de l'entreprise ne se trouve pas derrière un boîtier NAT. Pour paramétrer l'ordinateur du siège de l'entreprise, reportez-vous à l'[Exemple 18–6](#).

```

## /etc/hosts on mobile1
mobile1 10.1.3.3
main1 192.168.0.100

## /etc/inet/ipsecinit.conf on mobile1
# Find main1
{raddr 192.168.0.100} ipsec {encr_algs aes encr_auth_algs sha256 sa shared}

## /etc/inet/ike/ike.config on mobile1
# Global parameters

# Self-signed certificates - trust me and the central system
cert_trust      "jdoe@domain.org"
cert_trust      "DNS=main1.domain.org"
#
# Rule for off-site systems with trusted certificate
{
    label "Off-site mobile1 with trusted certificate"
    local_id_type email
    local_id "jdoe@domain.org"
    local_addr 0.0.0.0/0

# Find main1 and trust the certificate

```

```
remote_id "main1.domain.org"
remote_addr 192.168.0.100

p2_pfs 5

p1_xform
{auth_method rsa_sig oakley_group 5 encr_alg aes auth_alg sha256 }
}
```

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.

## Configuration du protocole IKE en vue de l'utilisation du matériel connecté

Les certificats de clés publiques peuvent également être stockés sur du matériel connecté. La carte Sun Crypto Accelerator 6000 permet de stocker et de décharger les opérations de clés publiques du système.

### ▼ Configuration du protocole IKE en vue de l'utilisation d'une carte Sun Crypto Accelerator 6000

**Avant de commencer** La procédure suivante suppose que la carte Sun Crypto Accelerator 6000 est connectée au système, et que le ou les logiciels correspondants ont été installés et configurés. Pour obtenir des instructions, reportez-vous au *Sun Crypto Accelerator 6000 Board Version 1.1 User's Guide*.

#### 1 Connectez-vous en tant qu'administrateur.

Pour plus d'informations, reportez-vous à la section [“Procédure d'obtention des droits d'administration”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*. Si vous vous connectez à distance, exécutez la commande `ssh` pour que votre connexion soit sécurisée. Voir l'[Exemple 15-1](#).

#### 2 Assurez-vous que la bibliothèque PKCS #11 est liée.

IKE utilise les routines de la bibliothèque pour gérer la génération des clés et leur stockage sur la carte Sun Crypto Accelerator 6000. Entrez la commande suivante pour déterminer si une bibliothèque PKCS #11 a été liée :

```
$ ikeadm get stats
...
PKCS#11 library linked in from /usr/lib/libpkcs11.so
$
```

### 3 Déterminez l'ID de jeton pour la carte Sun Crypto Accelerator 6000 connectée.

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot"
```

La bibliothèque renvoie un ID de jeton, également appelé [nom du keystore](#), de 32 caractères. Dans l'exemple ci-dessous, vous pouvez utiliser le jeton Sun Metaslot avec la commande `ikecert` pour stocker et accélérer les clés IKE.

Pour plus d'informations sur l'utilisation du jeton, reportez-vous à la section [“Génération et stockage de certificats de clés publiques dans le matériel”](#) à la page 285.

Les espaces situés à la fin sont automatiquement remplis par la commande `ikecert`.

#### Exemple 18–8 Découverte et utilisation de jetons metaslot

Les jetons peuvent être stockés sur le disque, sur une carte connectée ou dans le keystore softtoken fourni par la structure cryptographique. L'ID de jeton du keystore de softtoken peut se présenter comme suit :

```
$ ikecert tokens
Available tokens with library "/usr/lib/libpkcs11.so":

"Sun Metaslot"
```

Pour créer une phrase de passe pour un keystore de softtoken, reportez-vous à la page de manuel [pktool\(1\)](#).

La commande ci-dessous permet d'ajouter un certificat au keystore de softtoken. `Sun.Metaslot.cert` est le fichier contenant le certificat CA.

```
# ikecert certdb -a -T "Sun Metaslot" < Sun.Metaslot.cert
Enter PIN for PKCS#11 token:      Type user:passphrase
```

**Étapes suivantes** Si vous n'avez pas terminé d'établir la stratégie IPsec, effectuez de nouveau la procédure IPsec pour activer ou actualiser la stratégie IPsec.



## Protocole IKE (référence)

---

Ce chapitre aborde les sujets suivants :

- “Service IKE” à la page 301
- “Démon IKE” à la page 302
- “Fichier de configuration IKE” à la page 302
- “Commande `ikeadm`” à la page 303
- “Fichiers de clés prépartagées IKE” à la page 304
- “Commandes et bases de données de clés publiques IKE” à la page 304

Pour plus d'informations sur l'implémentation du protocole IKE, reportez-vous au [Chapitre 18](#), “Configuration du protocole IKE (tâches)”. Pour obtenir une présentation du protocole, reportez-vous au [Chapitre 17](#), “Protocole IKE (présentation)”.

## Service IKE

**Service** `svc:/network/ipsec/ike:default` : l'utilitaire de gestion des services (SMF) fournit le service `ike` qui permet de gérer IKE. Par défaut, ce service est désactivé. Avant d'activer ce service, vous devez créer un fichier de configuration IKE, `/etc/inet/ike/config`.

Les propriétés de service `ike` suivantes sont configurables :

- **Propriété** `config_file` : emplacement du fichier de configuration IKE. La valeur initiale est `/etc/inet/ike/config`.
- **Propriété** `debug_level` : niveau de débogage du démon `in.iked`. La valeur initiale est `op`, ce qui signifie opérationnelle. Pour connaître les valeurs possibles, reportez-vous au tableau sur les niveaux de débogage sous *Object Types* de la page de manuel [ikeadm\(1M\)](#).
- **Propriété** `admin_privilege` : niveau de privilège du démon `in.iked`. La valeur initiale est `base`. Les autres valeurs sont `modkeys` et `keymat`. Pour plus d'informations, reportez-vous à la section “Commande `ikeadm`” à la page 303.

Pour plus d'informations sur l'utilitaire SMF, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*. Voir aussi les pages de manuel [smf\(5\)](#), [svcadm\(1M\)](#) et [svccfg\(1M\)](#).

## Démon IKE

Le démon `in.iiked` automatise la gestion des clés cryptographiques pour IPsec sur les systèmes Oracle Solaris. Il négocie avec un système distant exécutant le même protocole pour fournir, de manière protégée, des numéros de clé authentifiés destinés aux associations de sécurité (SA). Le démon doit s'exécuter sur tous les systèmes qui sont censés communiquer en toute sécurité.

Par défaut, le service `svc:/network/ipsec/ike:default` n'est pas activé. Après que vous avez configuré le fichier `/etc/inet/ike/config` et activé le service `ike`, le démon `in.iiked` se lance à l'initialisation du système.

Une fois le démon IKE en cours d'exécution, le système s'authentifie auprès de son entité IKE homologue lors de la phase 1. L'homologue, ainsi que les méthodes d'authentification, sont définis dans le fichier de stratégie IKE. Le démon crée alors les clés pour la phase 2. Les clés IKE sont actualisées automatiquement à un intervalle spécifié dans le fichier de stratégie. Le démon `in.iiked` est à l'écoute des demandes IKE entrantes émanant du réseau et des demandes de trafic hors bande via le socket `PF_KEY`. Pour plus d'informations, reportez-vous à la page de manuel [pf\\_key\(7P\)](#).

Le démon IKE est pris en charge par deux commandes. La commande `ikeadm` peut être utilisée pour afficher et modifier temporairement la stratégie IKE. Pour modifier de manière définitive la stratégie IKE, vous devez modifier les propriétés du service `ike`. Pour modifier les propriétés du service IKE, reportez-vous à la section [“Procédure de gestion des services IKE et IPsec”](#) à la page 246. La commande `ikeadm` peut également servir à afficher les SA Phase 1, les règles de stratégie, les clés prépartagées, les groupes Diffie-Hellman disponibles, les algorithmes d'authentification et de chiffrement Phase 1, et le cache de certificat.

et la commande `ikecert` d'afficher et de gérer les bases de données de clés publiques. Cette dernière gère les bases de données `ike.privatekeys` et `publickeys` locales, ainsi que les opérations de clés publiques et le stockage de ces clés sur du matériel.

## Fichier de configuration IKE

Le fichier de configuration IKE, `/etc/inet/ike/config`, gère les clés des interfaces protégées dans le fichier de stratégie IPsec, `/etc/inet/ipsecinit.conf`.

La gestion des clés avec IKE inclut des règles et des paramètres globaux. Les règles IKE identifient les systèmes ou réseaux sécurisés par les numéros de clé. Elles spécifient également la méthode d'authentification. Les paramètres globaux incluent des éléments tels que le chemin

vers un accélérateur matériel connecté. Pour consulter des exemples de fichiers de stratégie IKE, reportez-vous à la section “[Configuration du protocole IKE avec des clés prépartagées \(liste des tâches\)](#)” à la page 268. Pour des exemples et une description des entrées de stratégies IKE, consultez la page de manuel [ike.config\(4\)](#).

Les SA IPsec prises en charge par IKE protègent les datagrammes IP conformément aux stratégies paramétrées dans le fichier de configuration des stratégies IPsec, `/etc/inet/ipsecinit.conf`. Le fichier de stratégie IKE détermine si la confidentialité de transmission parfaite (PFS, perfect forward security) est utilisée lors de la création des SA IPsec.

Le fichier `/etc/inet/ike/config` peut inclure le chemin vers une bibliothèque implémentée conformément au standard suivant : RSA Security Inc. PKCS #11 Cryptographic Token Interface (Cryptoki). IKE utilise la bibliothèque PKCS #11 pour accéder au matériel d'accélération et de stockage des clés.

En matière de sécurité, les considérations concernant le fichier `ike/config` sont similaires à celles concernant le fichier `ipsecinit.conf`. Pour plus d'informations, reportez-vous à la section “[Considérations de sécurité pour les commandes ipsecinit.conf et ipsecconf](#)” à la page 253.

## Commande ikeadm

La commande `ikeadm` permet d'effectuer les opérations suivantes :

- Afficher les différents aspects de l'état d'IKE
- Modifier les propriétés du démon IKE.
- Afficher les statistiques concernant la création de SA pendant la phase 1.
- Déboguer les échanges du protocole IKE.
- Affiche les objets du démon IKE tels que les SA Phase 1, les règles de stratégie, les clés prépartagées, les groupes Diffie-Hellman disponibles, les algorithmes d'authentification et de chiffrement Phase 1, et le cache de certificat.

Pour consulter des exemples et une description complète des options de cette commande, reportez-vous à la page de manuel [ikeadm\(1M\)](#)

Le niveau de privilège du démon IKE en cours d'exécution détermine les aspects du démon IKE susceptibles d'être affichés et modifiés. Trois niveaux de privilège sont possibles.

Niveau base	Vous ne pouvez ni afficher ni modifier les numéros de clé. Le niveau base est le niveau de privilège par défaut.
Niveau modkeys	A ce niveau, vous pouvez supprimer, modifier et ajouter des clés prépartagées.
Niveau keymat	Ce niveau vous permet d'afficher les numéros de clé actuels à l'aide de la commande <code>ikeadm</code> .

Pour modifier temporairement un privilège, vous pouvez utiliser la commande `ikeadm`. Pour une modification permanente, modifiez la propriété `admin_privilege` du service `ike`. Pour la procédure, reportez-vous à la section [“Procédure de gestion des services IKE et IPsec”](#) à la page 246.

En matière de sécurité, les considérations concernant la commande `ikeadm` sont similaires à celles concernant la commande `ipseckey`. Pour plus d'informations, reportez-vous à la section [“Considérations de sécurité pour la commande ipseckey”](#) à la page 256.

## Fichiers de clés prépartagées IKE

Lorsque vous créez des clés manuellement, elles sont stockées dans des fichiers du répertoire `/etc/inet/secret`. Le fichier `ike.preshared` contient les clés prépartagées des SA ISAKMP (Internet Security Association and Key Management Protocol) et le fichier `ipseckey` contient les clés prépartagées des SA IPsec. Ces fichiers sont protégés en mode `0600` et le répertoire `secret` en mode `0700`.

- Lorsque vous configurez le fichier `ike/config` pour demander des clés prépartagées, vous créez un fichier `ike.preshared`. Vous entrez les numéros de clé des SA ISAKMP, c'est-à-dire de l'authentification IKE, dans le fichier `ike.preshared`. Les clés prépartagées étant utilisées pour authentifier la phase 1, le fichier doit être valide avant le démarrage du démon `in.iked`.
- Le fichier `ipseckey` contient les numéros de clé des SA IPsec. Pour consulter des exemples de gestion manuelle de ce fichier, reportez-vous à la section [“Création manuelle de clés IPsec”](#) à la page 243. Le démon IKE n'utilise pas ce fichier. Les numéros de clé générés par IKE pour les SA IPsec sont stockés dans le noyau.

## Commandes et bases de données de clés publiques IKE

La commande `ikecert` permet de manipuler les bases de données de clés publiques du système local. Utilisez-la lorsque le fichier `ike/config` requiert des certificats de clés publiques. Ces bases de données étant utilisées par IKE pour authentifier la phase 1 de l'échange, elles doivent être alimentées avant l'activation du démon `in.iked`. Trois sous-commandes permettent de gérer chacune des trois bases de données : `certlocal`, `certdb` et `certldb`.

La commande `ikecert` permet aussi de gérer le stockage des clés. Les clés peuvent être stockées sur disque, sur une carte Sun Crypto Accelerator 6000 connectée ou dans un fichier `keystore` de clés `softtoken`. Ce fichier est disponible lorsque le metaslot de la structure cryptographique est utilisé pour communiquer avec le matériel. La commande `ikecert` utilise la bibliothèque PKCS #11 pour localiser le lieu de stockage des clés.



Pour plus d'informations, consultez la page de manuel [ikecert\(1M\)](#) Pour plus d'informations sur le metaslot et sur le fichier keystore de clés softtoken, reportez-vous à la page de manuel [cryptoadm\(1M\)](#).

## Commande `ikecert tokens`

L'argument `tokens` répertorie les ID de jetons disponibles. Les ID de jetons permettent aux commandes `ikecert certlocal` et `ikecert certdb` de générer des certificats de clés publiques et des demandes de certificats. Ces certificats et demandes de certificats peuvent également être stockés par la structure cryptographique dans le fichier keystore de clés softtoken ou sur une carte Sun Crypto Accelerator 6000 connectée. La commande `ikecert` utilise la bibliothèque PKCS #11 pour déterminer l'emplacement de stockage des certificats.

## Commande `ikecert certlocal`

La sous-commande `certlocal` gère la base de données des clés privées. Les options de cette sous-commande permettent d'ajouter, d'afficher et de supprimer des clés privées. Cette sous-commande permet également de créer un certificat autosigné ou une demande de certificat. L'option `-ks` crée un certificat autosigné et l'option `-kc` une demande de certificat. Les clés sont stockées sur le système, dans le répertoire `/etc/inet/secret/ike.privatekeys`, ou sur un composant matériel connecté (option `-T`).

Lorsque vous créez une clé privée, les options de la commande `ikecert certlocal` doivent avoir des entrées connexes dans le fichier `ike/config`. Le tableau ci-dessous détaille les correspondances entre les options `ikecert` et les entrées `ike/config`.

TABLEAU 19-1 Correspondances entre les options `ikecert` et les entrées `ike/config`

Option <code>ikecert</code>	Entrée <code>ike/config</code>	Description
<code>-A nom-alternatif-sujet</code>	<code>cert_trust nom-alternatif-sujet</code>	Pseudonyme identifiant le certificat de manière unique. Il peut s'agir d'une adresse IP, d'une adresse e-mail ou d'un nom de domaine.
<code>-D, nom-distinctif-X.509</code>	<code>nom-distinctif-X.509</code>	Nom complet de l'autorité de certification, incluant le pays (C), le nom de l'organisation (ON), l'unité d'organisation (OU) et le nom commun (CN).
<code>-t dsa-sha1</code>	<code>auth_method dsa_sig</code>	Méthode d'authentification légèrement plus lente que <a href="#">RSA</a> .

TABLEAU 19-1 Correspondances entre les options `ikecert` et les entrées `ike/config` (Suite)

Option <code>ikecert</code>	Entrée <code>ike/config</code>	Description
<code>-t rsa-md5</code> et <code>-t rsa-sha1</code>	<code>auth_method rsa_sig</code>	Méthode d'authentification légèrement plus rapide que la méthode <a href="#">DSA</a> .  La clé publique RSA doit être suffisamment importante pour chiffrer la <a href="#">charge utile</a> la plus lourde. Les charges les plus lourdes sont habituellement les données d'identité (par exemple, le nom distinctif X.509).
<code>-t rsa-md5</code> et <code>-t rsa-sha1</code>	<code>auth_method rsa_encrypt</code>	Le chiffrement RSA met les identités d'IKE à l'abri des écoutes électroniques, mais implique que les homologues IKE connaissent leurs clés publiques respectives.

Lorsque vous émettez une demande de certificat à l'aide de la commande `ikecert certlocal -kc`, vous envoyez la sortie de cette commande à un fournisseur de PKI ou à une CA. Si votre entreprise possède sa propre PKI, vous envoyez cette sortie à votre administrateur de PKI. Le fournisseur de PKI, la CA ou votre administrateur de PKI crée alors les certificats. Ceux qui vous sont transmis par le fournisseur de PKI ou la CA sont entrés dans la sous-commande `certdb`. La liste des certificats révoqués (CRL) que le fournisseur de PKI vous envoie est entrée dans la sous-commande `certrlb`.

## Commande `ikecert certdb`

La sous-commande `certdb` gère la base de données des clés publiques. Les options de cette sous-commande vous permettent d'ajouter, d'afficher et de supprimer des certificats et des clés publiques. Cette sous-commande accepte l'entrée de certificats générés par la commande `ikecert certlocal -ks` sur un système distant. Pour plus d'informations sur cette procédure, reportez-vous à la section [“Configuration du protocole IKE avec des certificats de clés publiques autosignés” à la page 274](#). Cette commande accepte également l'entrée de certificats émanant de fournisseurs PKI ou de la CA. Pour plus d'informations sur cette procédure, reportez-vous à la section [“Configuration du protocole IKE avec des certificats signés par une CA” à la page 279](#).

Les certificats et les clés publiques sont stockés sur le système, dans le répertoire `/etc/inet/ike/publickeys`. L'option `-T` permet de stocker les certificats, les clés privées et les clés publiques sur les composants matériels connectés.

## Commande `ikecert certdb`

La sous-commande `certrlb` gère la base de données des listes des certificats révoqués (CRL), `/etc/inet/ike/crls`. Cette base de données met à jour les listes de révocation des clés publiques. Les certificats qui ne sont plus valides figurent dans ces listes. Lorsqu'un fournisseur de PKI vous fait parvenir une CRL, vous pouvez l'installer dans cette base de données à l'aide de

la commande `ikecert certrl db`. Pour plus d'informations sur cette procédure, reportez-vous à la section [“Traitement des listes des certificats révoqués”](#) à la page 288.

## Répertoire `/etc/inet/ike/publickeys`

Le répertoire `/etc/inet/ike/publickeys` contient la partie publique des bclés et leur certificat, qui sont stockés dans des fichiers ou à des *emplacements*. Ce répertoire est protégé en mode `0755` et peut être alimenté à l'aide de la commande `ikecert cert db`. L'option `-T` permet de stocker les clés sur une carte Sun Crypto Accelerator 6000 plutôt que dans le répertoire `publickeys`.

Les emplacements contiennent, sous forme chiffrée, le nom distinctif X.509 des certificats qui ont été générés sur un autre système. Si vous utilisez des certificats autosignés, vous devez indiquer le certificat que l'administrateur du système distant vous a envoyé comme entrée de commande. Si vous utilisez des certificats d'une CA, vous installez deux certificats signés d'une CA dans la base de données. Vous installez un certificat basé sur la requête de signature de certificat envoyée à la CA. Vous installez également un certificat de la CA.

## Répertoire `/etc/inet/secret/ike.privatekeys`

Le répertoire `/etc/inet/secret/ike.privatekeys` contient des fichiers de clés privées qui font partie de bclés. Ce répertoire est protégé en mode `0700`. La commande `ikecert cert local` remplit le répertoire `ike.privatekeys`. Les clés privées sont effectives uniquement lors de l'installation de leur clé publique homologue, de certificats autosignés ou de certificats CA. Les clés publiques homologues sont stockées dans le répertoire `/etc/inet/ike/publickeys` ou sur du matériel pris en charge.

## Répertoire `/etc/inet/ike/crls`

Le répertoire `/etc/inet/ike/crls` contient les fichiers des listes des certificats révoqués (CRL). Chaque fichier correspond à un fichier de certificat public du répertoire `/etc/inet/ike/publickeys`. Les fournisseurs de PKI fournissent les CRL correspondant à leurs certificats. La commande `ikecert certrl db` permet d'alimenter la base de données.



## IP Filter dans Oracle Solaris (présentation)

---

Ce chapitre fournit une présentation d'IP Filter, une fonction d'Oracle Solaris. Les tâches IP Filter sont décrites au [Chapitre 21, “IP Filter \(tâches\)”](#).

Le présent chapitre contient les informations suivantes :

- “Introduction à IP Filter” à la page 309
- “Traitement des paquets avec IP Filter” à la page 310
- “Recommandations relatives à l'utilisation d'IP Filter” à la page 313
- “Utilisation des fichiers de configuration IP Filter” à la page 314
- “Utilisation d'ensembles de règles IP Filter” à la page 314
- “Crochets de filtre de paquets” à la page 320
- “IPv6 pour IP Filter” à la page 320
- “Pages de manuel IP Filter” à la page 321

### Introduction à IP Filter

La fonction IP Filter d'Oracle Solaris remplace le pare-feu SunScreen dans le système d'exploitation. Tout comme le pare-feu SunScreen, IP Filter assure un filtrage de paquets avec état, ainsi que la translation d'adresse réseau (NAT, Network Address Translation). IP Filter permet également le filtrage de paquets sans état, ainsi que la création et la gestion des pools d'adresses.

Le filtrage de paquets assure une protection de base contre les attaques potentielles via le réseau. IP Filter peut filtrer les paquets par adresse IP, port, protocole, interface réseau et direction du trafic. IP Filter peut également filtrer en fonction d'une adresse IP source individuelle, d'une adresse IP de destination, d'une plage d'adresses IP ou par pools d'adresses.

IP Filter est dérivé du logiciel Open Source IP Filter. Les conditions de licence, attribution et déclarations de copyright pour Open Source IP Filter sont accessibles via le chemin par défaut

`/usr/lib/ipf/IPFILTER.LICENCE`. Si vous avez installé Oracle Solaris dans un autre emplacement que celui par défaut, modifiez le chemin afin d'accéder au fichier se trouvant à l'emplacement de l'installation.

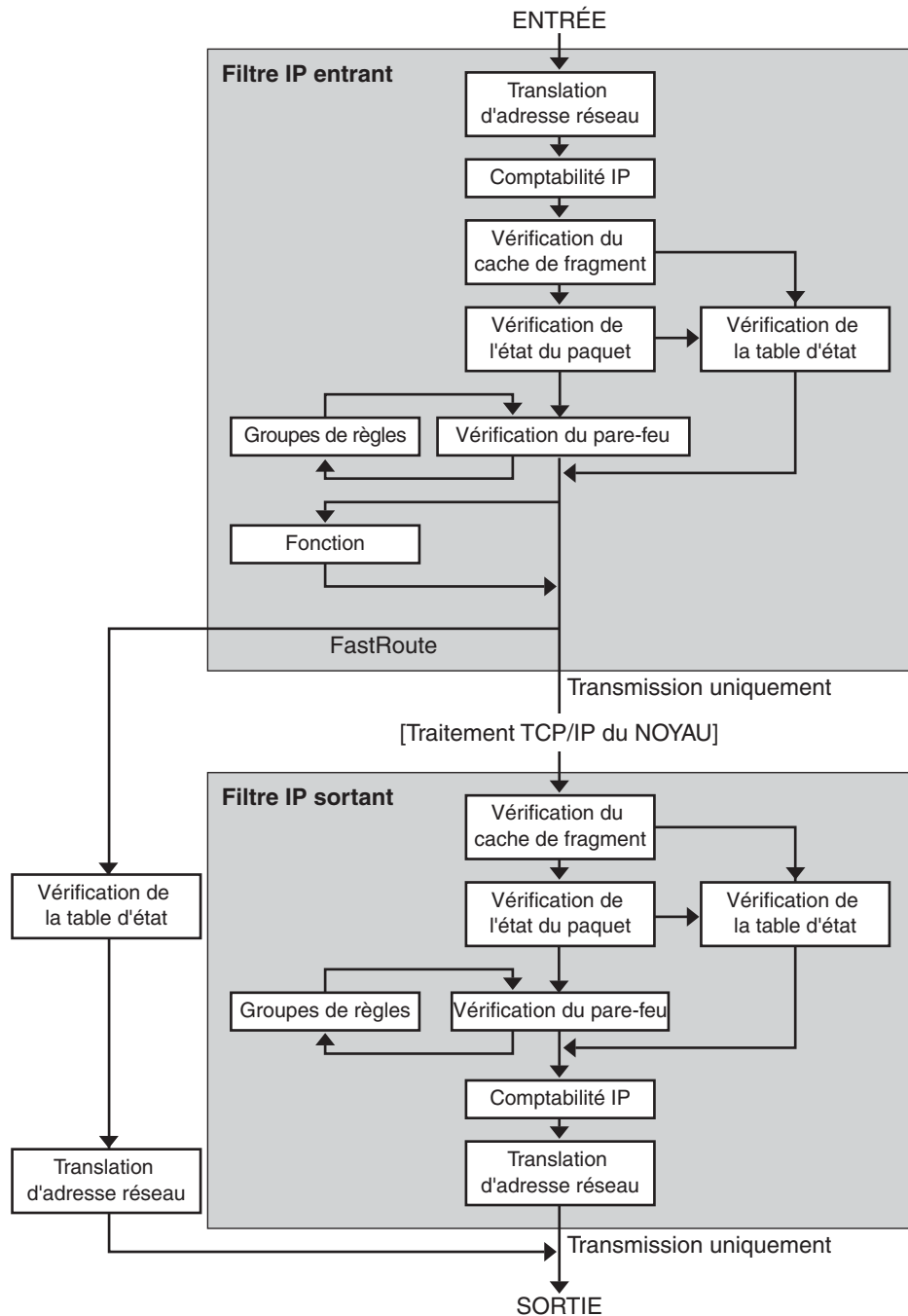
## Sources d'informations pour Open Source IP Filter

La page d'accueil du logiciel Open Source IP Filter de Darren Reed se trouve à l'adresse <http://coombs.anu.edu.au/~avalon/ip-filter.html>. Ce site Web fournit des informations relatives au logiciel Open Source IP Filter, notamment un lien vers le didacticiel “IP Filter Based Firewalls HOWTO” (Brendan Conoboy et Erik Fichtner, 2002). Vous trouverez dans ce didacticiel les instructions de construction de pare-feux dans un environnement BSD UNIX, expliquées pas à pas. Bien qu'il soit destiné à un environnement BSD UNIX, ce didacticiel est également applicable à la configuration d'IP Filter.

## Traitement des paquets avec IP Filter

Au cours du traitement d'un paquet, IP Filter exécute une séquence d'étapes. Le diagramme ci-dessous illustre les étapes du traitement d'un paquet et l'intégration du filtrage à la pile de protocole TCP/IP.

FIGURE 20-1 Séquence de traitement d'un paquet



Le traitement d'un paquet inclut les opérations suivantes :

- **Translation d'adresse réseau (NAT)**

Translation d'une adresse IP privée vers une adresse publique, ou définition d'alias pour plusieurs adresses privées vers une adresse publique unique. NAT (Network Address Translation, translation d'adresse réseau) permet à une organisation de résoudre le problème d'épuisement des adresses IP lorsqu'elle utilise un réseau et requiert l'accès à Internet.

- **Comptabilité IP**

Les règles d'entrée et de sortie peuvent être configurées séparément, avec enregistrement du nombre d'octets transmis. En cas de correspondance d'une règle, le nombre d'octets du paquet est ajouté à la règle et des statistiques en cascade sont rassemblées.

- **Vérification du cache de fragment**

Si un paquet du trafic en cours constitue un fragment et que le paquet précédent a été autorisé, le fragment de paquet est également autorisé, sans consultation de la table d'état ni vérification de règle.

- **Vérification de l'état du paquet**

Si la règle contient l'instruction `keep state`, tous les paquets d'une session spécifiée sont automatiquement transmis ou bloqués, selon la spécification de la règle : `pass` (transmettre) ou `block` (bloquer).

- **Vérification du pare-feu**

Les règles d'entrée et de sortie peuvent être configurées séparément, afin d'autoriser ou non la transmission d'un paquet, via IP Filter, vers les routines TCP/IP du noyau ou vers le réseau.

- **Groupes**

Les groupes permettent d'écrire des ensembles de règles selon une structure arborescente.

- **Fonction**

Une fonction correspond à l'action à réaliser. Les fonctions sont, par exemple, `block` (bloquer), `pass` (transmettre), `literal` (littéral) et `send ICMP response` (envoyer une réponse ICMP).

- **FastRoute**

FastRoute indique à IP Filter de ne pas transmettre le paquet vers la pile UNIX IP pour le routage, ce qui entraîne une réduction TTL.

- **Authentification IP**

Les paquets authentifiés ne sont transmis via les boucles du pare-feu qu'une seule fois, afin d'éviter le traitement multiple de certains paquets.



## Recommandations relatives à l'utilisation d'IP Filter

- IP Filter est géré par les services SMF `svc:/network/pfil` et `svc:/network/ipfilter`. Pour une présentation complète de l'utilitaire SMF, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*. Pour une présentation pas à pas des procédures associées à SMF, reportez-vous au [Chapitre 7, “Gestion des services \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.
- IP Filter requiert la modification directe des fichiers de configuration.
- IP Filter est installé en tant que composant d'Oracle Solaris. Par défaut, IP Filter n'est pas activé lorsque vous venez de procéder à l'installation. Pour configurer le filtrage, vous devez modifier les fichiers de configuration et activer manuellement IP Filter. Pour activer le filtrage, réinitialisez le système ou montez les interfaces à l'aide de la commande `ipadm`. Pour plus d'informations, reportez-vous à la page de manuel [ipadm\(1M\)](#). Pour obtenir la description des tâches associées à l'activation d'IP Filter, reportez-vous à la section “Configuration d'IP Filter” à la page 323.
- Pour gérer IP Filter, connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter. Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “Configuration initiale RBAC (liste des tâches)” du manuel *Administration d'Oracle Solaris : services de sécurité*.
- IPMP (IP Network Multipathing, multipathing sur réseau IP) ne prend en charge que le filtrage sans état.  
 Si vous souhaitez qu'IP Filter effectue un filtrage sans état du trafic en provenance et à destination d'un groupe IPMP, définissez le paramètre `ipmp_hook_emulation`. Par défaut, la valeur est définie sur zéro (0), ce qui signifie qu'IP Filter ne peut pas effectuer une inspection avec état des paquets du trafic sur les interfaces physiques appartenant à un groupe IPMP. Pour activer le filtrage de paquets IPMP, saisissez la commande suivante :  

```
ndd -set /dev/ip ipmp_hook_emulation 1
```
- Le logiciel Oracle Solaris Cluster ne prend pas en charge le filtrage IP Filter pour les services évolutifs. En revanche, IP Filter est pris en charge pour les services de basculement. Pour connaître les recommandations et restrictions relatives à IP Filter dans un cluster, reportez-vous à la section “Restrictions concernant les fonctions du SE Oracle Solaris” du manuel *Guide d'installation du logiciel Oracle Solaris Cluster*.
- Le filtrage interzones est pris en charge à condition que les règles IP Filter soient implémentées dans une zone qui fonctionne en tant que routeur virtuel pour les autres zones du système.

## Utilisation des fichiers de configuration IP Filter

IP Filter peut assurer des services de pare-feu ou de translation d'adresse réseau (NAT, Network Address Translation). Vous pouvez implémenter IP Filter à l'aide de fichiers de configuration chargeables. IP Filter contient un répertoire appelé `/etc/ipf`. Vous pouvez créer et enregistrer les fichiers de configuration `ipf.conf`, `ipnat.conf` et `ippool.conf` dans le répertoire `/etc/ipf`. Si ces fichiers existent dans le répertoire `/etc/ipf`, ils sont automatiquement chargés à l'initialisation. Il est également possible d'enregistrer les fichiers de configuration à un autre emplacement, puis de les charger manuellement. Pour obtenir des exemples de fichiers de configuration, reportez-vous à la section [“Création et modification des fichiers de configuration IP Filter”](#) à la page 348.

## Utilisation d'ensembles de règles IP Filter

Pour gérer le pare-feu, vous devez spécifier des ensembles de règles à l'aide d'IP Filter, puis filtrer le trafic réseau en fonction de ces ensembles de règles. Les types d'ensembles de règles suivants sont disponibles :

- Ensembles de règles de filtrage de paquets
- Ensembles de règles NAT (Network Address Translation, translation d'adresse réseau)

Par ailleurs, il est possible de créer des pools d'adresses pour référencer des groupes d'adresses IP. Ensuite, ces pools peuvent être utilisés dans un ensemble de règles. Les pools d'adresses permettent d'accélérer le traitement des règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

## Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter

Vous pouvez configurer le filtrage de paquets à l'aide des ensembles de règles de filtrage de paquets. La commande `ipf` permet d'utiliser les ensembles de règles de filtrage de paquets. Pour plus d'informations sur la commande `ipf`, reportez-vous à la page de manuel [ipf\(1M\)](#).

Vous pouvez créer des règles de filtrage de paquets via la ligne de commande, à l'aide de la commande `ipf` ou dans un fichier de configuration de filtrage de paquets. Si vous souhaitez charger les règles de filtrage de paquets à l'initialisation, créez le fichier de configuration `/etc/ipf/ipf.conf` pour y insérer les règles de filtrage de paquets. Dans le cas contraire, placez le fichier `ipf.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ipf`.

Avec IP Filter, deux ensembles de règles de filtrage de paquets peuvent coexister : l'ensemble de règles actif et l'ensemble de règles inactif. Dans la plupart des cas, vous utiliserez l'ensemble de règles actif. Toutefois, la commande `ipf -I` permet d'appliquer une commande à la liste de

règles inactives. La liste de règles inactives n'est pas employée par IP Filter, sauf si vous la sélectionnez. La liste de règles inactives constitue l'emplacement auquel vous pouvez enregistrer des règles sans affecter le filtrage de paquets actif.

IP Filter traite les règles de la liste de règles du début à la fin de la liste de règles configurée, puis transmet ou bloque le paquet. Un indicateur permet à IP Filter de déterminer si un paquet doit être transmis ou non. Il parcourt l'intégralité de l'ensemble de règles et détermine si le paquet doit être transmis ou bloqué, en fonction de la dernière règle correspondante.

Il existe deux exceptions à ce processus. D'une part, si le paquet correspondant à une règle contenant le mot-clé `quick`, Si une règle inclut le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées. D'autre part, si le paquet correspond à une règle contenant le mot-clé `group`, seules les règles portant l'indicateur de ce `group` sont vérifiées.

## Configuration des règles de filtrage de paquets

Appliquez la syntaxe suivante pour créer des règles de filtrage de paquets :

*action* [*in|out*] *option* *mot-clé*, *mot-clé*...

1. Chaque règle commence par une action. IP Filter applique l'action au paquet si celui-ci correspond à la règle. Les actions habituellement appliquées aux paquets sont répertoriées ci-dessous.

<code>block</code>	Empêche le paquet de traverser le filtre.
<code>pass</code>	Permet au paquet de traverser le filtre.
<code>log</code>	Consigne le paquet sans déterminer s'il est bloqué ou transmis. Exécutez la commande <code>ipmon</code> pour afficher le journal.
<code>count</code>	Inclut le paquet dans les statistiques du filtre. Exécutez la commande <code>ipfstat</code> pour afficher les statistiques.
<code>skip nombre</code>	Le filtre saute <i>nombre</i> règles de filtrage.
<code>auth</code>	Le paquet est authentifié par un programme utilisateur qui valide les informations qu'il contient. Le programme détermine si le paquet est transmis ou bloqué.

2. Le mot suivant est `in` ou `out`. Votre choix détermine si la règle de filtrage de paquets est appliquée à un paquet entrant (`in`) ou à un paquet sortant (`out`).
3. Ensuite, vous pouvez insérer toute une liste d'options. Si vous en utilisez plusieurs, elles doivent être dans l'ordre indiqué ci-dessous.

<code>log</code>	Consigne le paquet si la règle constitue la dernière règle correspondante. Exécutez la commande <code>ipmon</code> pour afficher le journal.
------------------	--

- |                                   |  |
|-----------------------------------|--|
| <code>quick</code>                | Exécute la règle contenant l'option <code>quick</code> si un paquet lui correspond. Toute vérification de règle subséquente est interrompue. |
| <code>on nom-interface</code>     | Applique la règle uniquement si le paquet entre ou sort via l'interface spécifiée.   |
| <code>dup-to nom-interface</code> | Copie le paquet et envoie la copie sur <i>nom-interface</i> vers une adresse IP éventuellement spécifiée.                                    |
| <code>to nom-interface</code>     | Déplace le paquet vers une file d'attente sortante sur <i>nom-interface</i> .  |
4. Une fois les options spécifiées, vous avez le choix entre plusieurs mots-clés afin de déterminer si le paquet correspond à la règle. Les mots-clés doivent être utilisés dans l'ordre indiqué ci-dessous.

---

**Remarque** – Par défaut, le filtre autorise la transmission de tout paquet ne correspondant à aucune règle du fichier de configuration.

---

- |                               |  |
|-------------------------------|--|
| <code>tos</code>              | Filtre les paquets en fonction de leur type de service, exprimé sous forme d'entier décimal ou hexadécimal.  |
| <code>ttl</code>              | Filtre les paquets en fonction de leur durée de vie. La durée de vie d'un paquet est une valeur enregistrée dans celui-ci qui indique la durée pendant laquelle le paquet peut se trouver sur le réseau avant d'être abandonné.  |
| <code>proto</code>            | Les paquets correspondant à la règle sont déterminés en fonction d'un protocole spécifique. Vous pouvez employer l'un des noms de protocole spécifiés dans le fichier <code>/etc/protocols</code> ou un nombre décimal représentant le protocole. Le mot-clé <code>tcp/udp</code> peut être utilisé pour filtrer les paquets TCP ou UDP. |
| <code>from/to/all/ any</code> | Filtre les paquets en fonction des éléments suivants : l'adresse IP source, l'adresse IP de destination et le numéro de port. Le mot-clé <code>all</code> permet d'accepter tous les paquets, quelles que soient leur source et leur destination.  |
| <code>with</code>             | Les paquets correspondant à la règle sont ceux qui sont associés à des attributs spécifiques. Insérez le mot <code>not</code> ou <code>no</code> devant le mot-clé pour indiquer qu'un paquet ne correspond à la règle qu'en l'absence de l'option.  |

<code>flags</code>	Employé pour TCP afin de filtrer les paquets en fonction des indicateurs TCP définis. Pour plus d'informations sur les indicateurs TCP, reportez-vous à la page de manuel <a href="#">ipf(4)</a> .
<code>icmp-type</code>	Filtre les paquets en fonction du type d'ICMP. Ce mot-clé n'est employé que si l'option <code>proto</code> est définie sur <code>icmp</code> et que l'option <code>flags</code> n'est pas utilisée.
<code>keep options-à-conserver</code>	Détermine les informations conservées pour le paquet. Les options <code>state</code> et <code>flags</code> sont disponibles comme <i>options-à-conserver</i> . L'option <code>state</code> conserve les informations relatives à la session et peuvent être conservées sur les paquets TCP, UDP et ICMP. L'option <code>flags</code> permet de conserver les informations sur les fragments de paquets et d'appliquer les informations aux fragments suivants. Les <i>options-à-conserver</i> permettent la transmission des paquets correspondant à la règle sans passer par la liste de contrôle d'accès.
<code>head numéro</code>	Crée un groupe pour les règles de filtrage, désigné par le numéro <i>numéro</i> .
<code>group numéro</code>	Ajoute la règle au groupe de numéro <i>numéro</i> au lieu du groupe par défaut. Toutes les règles de filtrage sont placées dans le groupe 0 si aucun autre groupe n'est spécifié.

L'exemple suivant illustre la constitution d'une syntaxe de règle de filtrage de paquets pour créer une règle. Pour bloquer le trafic entrant à partir de l'adresse IP 192.168.0.0/16, ajoutez la règle suivante à la liste de règles :

```
block in quick from 192.168.0.0/16 to any
```

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles de filtrage de paquets, reportez-vous à la page de manuel [ipf\(4\)](#) Pour une description des tâches associées au filtrage de paquets, reportez-vous à la section “[Gérez les ensembles de règles de filtrage de paquets d'IP Filter](#)” à la page 330. Pour une explication du schéma d'adresse IP (192.168.0.0/16) de l'exemple, reportez-vous au [Chapitre 1](#), “[Planification du développement du réseau](#)”.

## Utilisation de la fonctionnalité NAT d'IP Filter

NAT configure des règles de mappage qui réalisent la translation des adresses IP source et de destination vers d'autres adresses Internet ou intranet. Ces règles modifient les adresses source et de destination des paquets IP entrants et sortants et envoient les paquets. Vous pouvez également utiliser NAT pour rediriger le trafic d'un port à un autre. NAT assure l'intégrité du paquet en cas de modification ou de redirection de celui-ci.

Exécutez la commande `ipnat` pour utiliser les listes de règles NAT. Pour plus d'informations sur la commande `ipnat`, reportez-vous à la page de manuel [ipnat\(1M\)](#).

Vous pouvez créer des règles NAT à la ligne de commande, à l'aide de la commande `ipnat` ou dans un fichier de configuration NAT. Les règles de configuration NAT résident dans le fichier `ipnat.conf`. Si vous souhaitez charger les règles NAT à l'initialisation, créez le fichier `/etc/ipf/ipnat.conf` afin d'y insérer les règles NAT. Dans le cas contraire, placez le fichier `ipnat.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ipnat`.

## Configuration des règles NAT

Appliquez la syntaxe ci-dessous pour créer des règles NAT :

*commande nom-interface paramètres*

1. Toute règle commence par l'une des commandes ci-dessous :

<code>map</code>	Mappe une adresse IP ou un réseau IP vers une autre adresse IP ou un autre réseau IP selon un processus circulaire non contrôlé.
<code>rdr</code>	Redirige les paquets d'un couple port-adresse IP vers un autre couple port-adresse IP.
<code>bimap</code>	Etablit une translation d'adresse réseau bidirectionnelle entre une adresse IP externe et une adresse IP interne.
<code>map-block</code>	Etablit la translation basée sur les adresses IP statiques. Cette commande se base sur un algorithme qui force la translation des adresses vers une plage de destination.

2. Le mot suivant correspond au nom de l'interface, par exemple `bge0`.
3. Ensuite, vous avez le choix entre divers paramètres, afin de définir la configuration NAT. Les paramètres suivants sont disponibles :

<code>ipmask</code>	Désigne le masque réseau.
<code>dstipmask</code>	Désigne l'adresse cible de la translation de <code>ipmask</code> .
<code>mapport</code>	Désigne les protocoles <code>tcp</code> , <code>udp</code> ou <code>tcp/udp</code> , ainsi qu'une plage de numéros de port.

L'exemple suivant illustre la constitution d'une syntaxe de règle NAT pour créer une règle NAT. Pour réécrire un paquet sortant sur le périphérique `de0` avec l'adresse source `192.168.1.0/24` et pour afficher son adresse source comme étant `10.1.0.0/16`, ajoutez la règle ci-dessous à l'ensemble de règles NAT :

```
map de0 192.168.1.0/24 -> 10.1.0.0/16
```

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles NAT, reportez-vous à la page de manuel [ipnat\(4\)](#).

## Utilisation de la fonctionnalité de pools d'adresses d'IP Filter

Les pools d'adresses constituent une référence unique pour nommer un groupe de paires adresse/masque de réseau. Les processus fournis pas les pools d'adresses permettent de trouver plus rapidement les adresses IP correspondant aux règles. En outre, ils facilitent la gestion des grands groupes d'adresses.

Les règles de configuration de pool d'adresses sont définies dans le fichier `ippool.conf`. Si vous souhaitez charger le fichier de règles de pool d'adresses à l'initialisation, créez le fichier `/etc/ipf/ippool.conf` afin d'y insérer les règles de pool. Dans le cas contraire, placez le fichier `ippool.conf` à un autre endroit, puis activez manuellement le filtrage de paquets à l'aide de la commande `ippool`.

### Configuration des pools d'adresses

Pour créer un pool d'adresses, appliquez la syntaxe suivante :

```
table role = role-name type = storage-format number = reference-number
```

**table** Définit la référence des adresses.

**role** Spécifie le rôle du pool dans IP Filter. A ce stade, vous ne pouvez faire référence qu'au rôle `ipf`.

**type** Spécifie le format de stockage du pool.

**numéro** Spécifie le numéro de référence utilisé par la règle de filtrage.

Par exemple, pour faire référence aux groupes d'adresses `10.1.1.1` et `10.1.1.2` et au réseau `192.16.1.0` à l'aide du numéro de pool 13, insérez la règle suivante dans le fichier de configuration de pool d'adresses :

```
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24 };
```

Ensuite, pour faire référence au numéro de pool 13 dans une règle de filtrage, élaborer une règle similaire à la suivante :

```
pass in from pool/13 to any
```

Vous devez charger le fichier de pool avant de charger les règles contenant une référence au pool. Dans le cas contraire, le pool n'est pas défini, comme indiqué dans la sortie suivante :

```
# ipfstat -io  
empty list for ipfilter(out)  
block in from pool/13(!) to any
```

Si vous ajoutez le pool par la suite, l'ensemble de règle du noyau n'est pas mis à jour. Vous devez également recharger le fichier de règles faisant référence au pool.

Pour obtenir la syntaxe et la grammaire complètes utilisées pour écrire des règles de filtrage de paquets, reportez-vous à la page de manuel [ippool\(4\)](#).

## Crochets de filtre de paquets

Dans la version en cours, les crochets de filtre de paquets remplacent le module `pfil` pour activer IP Filter. Dans les versions précédentes, une étape supplémentaire dédiée à la configuration du module `pfil` était requise pour configurer Solaris IP Filter. Cette exigence de configuration supplémentaire augmentait les risques d'erreurs entraînant le dysfonctionnement d'IP Filter. L'insertion du module STREAMS `pfil` entre IP et le pilote de périphérique affectait également les performances. Enfin, le module `pfil` ne pouvait pas intercepter les paquets entre les zones.

Les crochets de filtre de paquets optimisent la procédure d'activation d'IP Filter. Grâce à ces crochets, IP Filter contrôle les flux de paquet entrants et sortants du système Oracle Solaris à l'aide de seuils de filtre de préROUTAGE (entrants) et de postROUTAGE (sortants).

Avec les crochets de filtre de paquets, le module `pfil` devient inutile. Par conséquent, les composants suivants associés au module sont également supprimés.

- Pilote `pfil`
- Démon `pfil`
- Service SMF `svc:/network/pfil`

Pour obtenir une description des tâches associées à l'activation d'IP Filter, reportez-vous au [Chapitre 21, “IP Filter \(tâches\)”](#).

## IPv6 pour IP Filter

A partir de la version 6/06, IPv6 est pris en charge avec Solaris IP Filter. Ce filtrage peut se baser sur l'adresse IPv6 source/de destination, sur les pools contenant des adresses IPv6 et sur les en-têtes d'extension IPv6.

De nombreux aspects d'IPv6 sont similaires à IPv4. Toutefois, les en-têtes et tailles des paquets ne sont pas identiques dans les deux versions d'IP, ce qui constitue une considération de poids pour IP Filter. Les paquets IPv6 appelés *jumbogrammes* contiennent un datagramme de longueur supérieure à 65 535 octets. IP Filter ne prend pas en charge les jumbogrammes IPv6.



Pour en savoir plus sur les autres fonctionnalités IPv6, reportez-vous à la section “[Fonctions principales d’IPv6](#)” du manuel *Guide d’administration système : services IP*.

---

**Remarque** – Pour plus d’informations sur les jumbogrammes, reportez-vous au document IPv6 Jumbograms, RFC 2675 de l’IETF (Internet Engineering Task Force, groupe d’étude d’ingénierie Internet). [<http://www.ietf.org/rfc/rfc2675.txt>]

---

Les tâches IP Filter associées à IPv6 ne sont pas très différentes d’IPv4. La différence la plus notable est l’emploi de l’option -6 avec certaines commandes. Les commandes `ipf` et `ipfstat` incluent l’option -6 à utiliser avec le filtrage de paquets IPv6. Appliquez l’option -6 avec la commande `ipf` pour charger et vider les règles de filtrage de paquets IPv6. Pour afficher les statistiques IPv6, utilisez l’option -6 avec la commande `ipfstat`. Les commandes `ipmon` et `ippool` prennent également en charge IPv6, même si aucune option n’est associée à la prise en charge d’IPv6. La commande `ipmon` a été optimisée pour autoriser la journalisation des paquets IPv6. La commande `ippool` prend en charge les pools avec les adresses IPv6. Vous pouvez créer des pools d’adresses IPv4, des pools d’adresses IPv6 et des pools contenant à la fois des adresses IPv4 et IPv6.

Vous pouvez utiliser le fichier `ipf6.conf` pour créer des jeux de règles de filtrage de paquets pour IPv6. Par défaut, le fichier de configuration `ipf6.conf` figure dans le répertoire `/etc/ipf`. Comme pour les autres fichiers de configuration de filtrage, le fichier `ipf6.conf` se charge automatiquement au cours du processus d’initialisation s’il est stocké dans le répertoire `/etc/ipf`. Vous pouvez également créer un fichier de configuration IPv6, le conserver à un autre emplacement et le charger manuellement.

Une fois les règles de filtrage de paquets pour IPv6 configurées, activez les capacités de filtrage de paquets IPv6 en créant l’interface.

Pour plus d’information sur IPv6, reportez-vous au [Chapitre 3, “Présentation d’IPv6”](#) du manuel *Guide d’administration système : services IP*. Pour obtenir une description des tâches associées à IP Filter, reportez-vous au [Chapitre 21, “IP Filter \(tâches\)”](#).

## Pages de manuel IP Filter

Le tableau ci-dessous répertorie les pages de manuel applicables à IP Filter.

Page de manuel	Description
<a href="#">ipf(1M)</a>	Exécutez la commande <code>ipf</code> pour effectuer les tâches suivantes : <ul style="list-style-type: none"><li>■ Utiliser les ensembles de règles de filtrage de paquets.</li><li>■ Désactiver et activer le filtrage.</li><li>■ Réinitialiser les statistiques et resynchroniser la liste d'interface du noyau avec la liste de statut d'interface actuelle.</li></ul>
<a href="#">ipf(4)</a>	Contient la grammaire et la syntaxe de création des règles de filtrage de paquets IP Filter.
<a href="#">ipfilter(5)</a>	Fournit les informations d'octroi de licence du logiciel Open Source IP Filter.
<a href="#">ipfs(1M)</a>	Exécutez la commande <code>ipfs</code> pour enregistrer et restaurer les informations NAT et les informations de table d'état lors des réinitialisations.
<a href="#">ipfstat(1M)</a>	Exécutez la commande <code>ipfstat</code> pour récupérer et afficher les statistiques relatives au traitement des paquets.
<a href="#">ipmon(1M)</a>	Exécutez la commande <code>ipmon</code> pour ouvrir le périphérique du journal et afficher les paquets consignés pour le filtrage de paquets et pour NAT.
<a href="#">ipnat(1M)</a>	Exécutez la commande <code>ipnat</code> pour effectuer les tâches suivantes : <ul style="list-style-type: none"><li>■ Utiliser les règles NAT</li><li>■ Récupérer et afficher les statistiques NAT.</li></ul>
<a href="#">ipnat(4)</a>	Contient la grammaire et la syntaxe pour la création de règles NAT.
<a href="#">ippool(1M)</a>	Exécutez la commande <code>ippool</code> pour créer et gérer les pools d'adresses.
<a href="#">ippool(4)</a>	Contient la grammaire et la syntaxe de création des pools d'adresses IP Filter.
<a href="#">nnd(1M)</a>	Affiche les paramètres de filtrage actuels du module STREAMS <code>pfil</code> et les valeurs courantes des paramètres réglables.

## IP Filter (tâches)

---

Ce chapitre fournit les instructions relatives à chaque étape des tâches. Pour obtenir des informations générales sur IP Filter, reportez-vous au [Chapitre 20, “IP Filter dans Oracle Solaris \(présentation\)”](#).

Le présent chapitre contient les informations suivantes :

- [“Configuration d'IP Filter” à la page 323](#)
- [“Désactivation d'IP Filter” à la page 327](#)
- [“Utilisation des ensembles de règles IP Filter” à la page 329](#)
- [“Affichage des statistiques et des informations relatives à IP Filter” à la page 341](#)
- [“Utilisation des fichiers journaux IP Filter” à la page 344](#)
- [“Création et modification des fichiers de configuration IP Filter” à la page 348](#)

## Configuration d'IP Filter

La liste des tâches ci-dessous identifie les procédures associées à la configuration d'IP Filter.

TABLEAU 21-1 Configuration d'IP Filter (liste des tâches)

Tâche	Description	Voir
Activation initiale d'IP Filter	IP Filter n'est pas activé par défaut. Activez-le manuellement ou à l'aide des fichiers de configuration disponibles dans le répertoire <code>/etc/ipf/</code> , puis réinitialisez le système. Les crochets de filtre de paquets remplacent le module <code>pfil</code> pour activer IP Filter.	<a href="#">“Activation d'IP Filter” à la page 324</a>

**TABEAU 21-1** Configuration d'IP Filter (liste des tâches) *(Suite)*

Tâche	Description	Voir
Réactivation d'IP Filter	Si IP Filter est désactivé, vous pouvez le réactiver soit en réinitialisant le système, soit en exécutant la commande <code>ipf</code> .	<a href="#">“Réactivation d'IP Filter” à la page 325</a>
Activation du filtrage de loopback	Disponible en option, le filtrage de loopback permet, par exemple, de filtrer le trafic entre les zones.	<a href="#">“Activation du filtrage de loopback” à la page 326</a>

## ▼ Activation d'IP Filter

**1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

**2 Créez un ensemble de règles de filtrage de paquets.**

L'ensemble de règles de filtrage de paquets contient les règles de filtrage de paquets utilisées par IP Filter. Pour charger les règles de filtrage de paquets à l'initialisation, modifiez le fichier `/etc/ipf/ipf.conf` afin d'implémenter le filtrage de paquets IPv4. Utilisez le fichier `/etc/ipf/ipf6.conf` pour les règles de filtrage de paquets IPv6. Si vous ne souhaitez pas charger les règles de filtrage de paquets à l'initialisation, insérez-les dans le fichier de votre choix, puis activez manuellement le filtrage de paquets. Pour plus d'informations sur le filtrage de paquets, reportez-vous à la section [“Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter” à la page 314](#). Pour plus d'informations sur l'utilisation des fichiers de configuration, reportez-vous à la section [“Création et modification des fichiers de configuration IP Filter” à la page 348](#).

**3 (Facultatif) Créez un fichier de configuration NAT (Network Address Translation, translation d'adresse réseau).**

---

**Remarque** – NAT ne prend pas en charge IPv6.

---

Créez le fichier `ipnat.conf` si vous souhaitez utiliser la translation d'adresse réseau. Si vous souhaitez charger les règles NAT à l'initialisation, créez le fichier `/etc/ipf/ipnat.conf` afin d'y insérer les règles NAT. Si vous ne souhaitez pas charger les règles NAT à l'initialisation, placez le fichier `ipnat.conf` dans le répertoire de votre choix, puis activez manuellement les règles NAT.

Pour plus d'informations sur NAT, reportez-vous à la section [“Utilisation de la fonctionnalité NAT d'IP Filter” à la page 317](#).

#### 4 (Facultatif) Créez un fichier de configuration de pool d'adresses.

Créez un fichier `ipool.conf` si vous souhaitez référencer un groupe d'adresses sous la forme d'un pool d'adresses unique. Pour charger le fichier de configuration de pool d'adresses à l'initialisation, créez le fichier `/etc/ipf/ippool.conf` afin d'y insérer le pool d'adresses. Si vous ne souhaitez pas charger le fichier de configuration de pool d'adresses à l'initialisation, placez le fichier `ippool.conf` dans le répertoire de votre choix, puis activez manuellement les règles.

Un pool d'adresses peut contenir exclusivement des adresses IPv4 ou exclusivement des adresses IPv6. Il peut également contenir à la fois des adresses IPv4 et des adresses IPv6.

Pour plus d'informations sur les pools d'adresses, reportez-vous à la section [“Utilisation de la fonctionnalité de pools d'adresses d'IP Filter”](#) à la page 319.

#### 5 (Facultatif) Activez le filtrage de trafic en loopback.

Pour filtrer le trafic entre les zones configurées sur le système, le cas échéant, activez le filtrage de loopback. Reportez-vous à la section [“Activation du filtrage de loopback”](#) à la page 326. Vous devez également définir les ensembles de règles adéquats applicables aux zones.

#### 6 Activez IP Filter.

```
# svcadm enable network/ipfilter
```

## ▼ Réactivation d'IP Filter

Si le filtrage de paquets a été temporairement désactivé, vous pouvez le réactiver.

#### 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Activez IP Filter et le filtrage selon l'une des méthodes ci-dessous :

- Redémarrez l'ordinateur.

```
# reboot
```

---

**Remarque** – Lorsque IP Filter est activé, les fichiers suivants sont chargés après une réinitialisation s'ils sont présents : le fichier `/etc/ipf/ipf.conf`, le fichier `/etc/ipf/ipf6.conf` en cas d'utilisation d'IPv6 ou le fichier `/etc/ipf/ipnat.conf`.

---

- Exécutez les commandes suivantes pour activer IP Filter et le filtrage :
  - a. Activez IP Filter.

```
# ipf -E
```

- b. Activez le filtrage de paquets.

```
# ipf -f filename
```

- c. (Facultatif) Activez NAT.

```
# ipnat -f filename
```

---

Remarque – NAT ne prend pas en charge IPv6.

---

## ▼ Activation du filtrage de loopback

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "[Configuration initiale RBAC \(liste des tâches\)](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Le cas échéant, arrêtez IP Filter.**

```
# svcadm disable network/ipfilter
```

- 3 **Ajoutez la ligne suivante au début du fichier `/etc/ipf.conf` ou `/etc/ipf6.conf` :**

```
set intercept_loopback true;
```

Cette ligne doit précéder toutes les règles IP Filter définies dans le fichier. Toutefois, vous pouvez insérer des commentaires avant la ligne, comme dans l'exemple ci-dessous :

```
#
# Enable loopback filtering to filter between zones
#
set intercept_loopback true;
#
# Define policy
#
block in all
block out all
<other rules>
...
```

- 4 **Lancez IP Filter.**

```
# svcadm enable network/ipfilter
```

- 5 **Pour vérifier le statut du filtrage de loopback, exécutez la commande ci-dessous :**

```
# ipf -T ipf_loopback
ipf_loopback    min 0    max 0x1 current 1
#
```

Si le filtrage de loopback est désactivé, la commande génère la sortie suivante :

```
ipf_loopback    min 0    max 0x1 current 0
```

## Désactivation d'IP Filter

Vous pouvez désactiver le filtrage de paquets et NAT pour :

- Réaliser des tests
- Dépanner des problèmes système dont IP Filter semble être à l'origine

La liste des tâches ci-dessous identifie les procédures associées à la désactivation des fonctions IP Filter.

TABLEAU 21-2 Désactivation d'IP Filter (liste des tâches)

Tâche	Description	Voir
Désactivation du filtrage de paquets.	Désactivez le filtrage de paquets à l'aide de la commande <code>ipf</code> .	<a href="#">“Désactivation du filtrage de paquets” à la page 327</a>
Désactivation de NAT.	Désactivez NAT à l'aide de la commande <code>ipnat</code> .	<a href="#">“Désactivation de NAT” à la page 328</a>
Désactivation du filtrage de paquets et de NAT.	Désactivez le filtrage de paquets et NAT à l'aide de la commande <code>ipf</code> .	<a href="#">“Désactivation du filtrage de paquets” à la page 328</a>

### ▼ Désactivation du filtrage de paquets

La procédure ci-dessous permet de désactiver le filtrage de paquets IP Filter en vidant les règles de filtrage de paquets de l'ensemble de règles de filtrage actif. La procédure ne désactive pas IP Filter. Vous pouvez réactiver IP Filter en ajoutant des règles à l'ensemble de règles.

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Pour désactiver les règles IP Filter, vous avez le choix entre les méthodes suivantes :**

- Supprimez du noyau l'ensemble de règles actif.

# `ipf -Fa`

Cette commande désactive toutes les règles de filtrage de paquets.

- Supprimez les règles de filtrage appliquées aux paquets entrants.

```
# ipf -Fi
```

Cette commande désactive les règles de filtrage de paquets appliquées aux paquets entrants.

- Supprimez les règles de filtrage appliquées aux paquets sortants.

```
# ipf -Fo
```

Cette commande désactive les règles de filtrage de paquets appliquées aux paquets sortants.

## ▼ Désactivation de NAT

La procédure ci-dessous permet de désactiver les règles NAT d'IP Filter en les vidant de l'ensemble de règles NAT actif. La procédure ne désactive pas IP Filter. Vous pouvez réactiver IP Filter en ajoutant des règles à l'ensemble de règles.

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel Administration d'Oracle Solaris : services de sécurité](#).

- 2 **Supprimez NAT du noyau.**

```
# ipnat -FC
```

L'option -C permet de supprimer toutes les entrées de la liste de règles NAT actuelle. L'option -F permet de supprimer toutes les entrées actives de la table de translation NAT qui indique les mappages NAT actifs.

## ▼ Désactivation du filtrage de paquets

Lorsque vous exécutez cette procédure, NAT et le filtrage de paquets sont supprimés du noyau. Pour réactiver le filtrage de paquets et NAT après avoir exécuté cette procédure, le cas échéant, vous devez réactiver IP Filter. Pour plus d'informations, reportez-vous à la section [“Réactivation d'IP Filter” à la page 325](#).

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel Administration d'Oracle Solaris : services de sécurité](#).

- 2 **Désactivez le filtrage de paquets et autorisez la transmission de tous les paquets sur le réseau.**

```
# ipf -D
```



**Remarque** – La commande `ipf -D` vide les règles de l'ensemble de règles. Lorsque vous réactivez le filtrage, vous devez ajouter des règles à l'ensemble de règles.

## Utilisation des ensembles de règles IP Filter

La liste des tâches ci-dessous identifie les procédures associées aux ensembles de règles IP Filter.

**TABEAU 21-3** Utilisation des ensembles de règles IP Filter (liste des tâches)

Tâche	Description	Voir
Gestion, affichage et modification des ensembles de règles pour le filtrage de paquets IP Filter		“Gérez les ensembles de règles de filtrage de paquets d'IP Filter” à la page 330
	Affichez un ensemble de règles actif pour le filtrage de paquets.	“Affichage de l'ensemble actif de règles de filtrage de paquets” à la page 330
	Affichez un ensemble de règles inactif pour le filtrage de paquets.	“Affichage de l'ensemble inactif de règles de filtrage de paquets” à la page 331
	Activez un nouvel ensemble de règles actif.	“Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour” à la page 331
	Supprimez un ensemble de règles.	“Suppression d'un ensemble de règles de filtrage de paquets” à la page 333
	Ajoutez des règles aux ensembles de règles.	“Ajout de règles à l'ensemble actif de règles de filtrage de paquets” à la page 333 “Ajout de règles à l'ensemble inactif de règles de filtrage de paquets” à la page 334
	Basculez entre les ensembles de règles actif et inactif.	“Basculement entre les ensembles actif et inactif de règles de filtrage de paquets” à la page 335
	Supprimez du noyau un ensemble de règles inactif.	“Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau” à la page 336

**TABLEAU 21-3** Utilisation des ensembles de règles IP Filter (liste des tâches) (Suite)

Tâche	Description	Voir
Gérez, affichez et modifiez les règles NAT IP Filter		“Gestion des règles NAT d'IP Filter” à la page 337
	Affichez les règles NAT actives.	“Affichage des règles NAT actives” à la page 337
	Supprimez les règles NAT.	“Suppression des règles NAT” à la page 337
	Ajoutez des règles aux règles NAT.	“Ajout de règles aux règles NAT” à la page 338
Gérez, affichez et modifiez les pools d'adresses IP Filter		“Gestion des pools d'adresses d'IP Filter” à la page 339
	Affichez les pools d'adresses actifs.	“Affichage des pools d'adresses actifs” à la page 339
	Supprimez un pool d'adresses.	“Suppression d'un pool d'adresses” à la page 339
	Ajoutez des règles à un pool d'adresses.	“Ajout de règles à un pool d'adresses” à la page 340

## Gérez les ensembles de règles de filtrage de paquets d'IP Filter

Lorsque cette option est activée, les ensembles actif et inactif de règles de filtrage de paquets peuvent résider dans le noyau. L'ensemble de règles actif détermine le filtrage appliqué aux paquets entrants et aux paquets sortants. L'ensemble de règles inactif contient également des règles. Ces règles ne sont pas appliquées, sauf si vous définissez l'ensemble de règles inactif comme l'ensemble de règles actif. Vous pouvez gérer, afficher et modifier les ensembles actif et inactif de règles de filtrage de paquets.

### ▼ Affichage de l'ensemble actif de règles de filtrage de paquets

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Affichez l'ensemble actif de règles de filtrage de paquets chargé dans le noyau.**

**# ipfstat -io**

**Exemple 21–1** Affichage de l'ensemble actif de règles de filtrage de paquets

L'exemple ci-dessous présente la sortie de l'ensemble actif de règles de filtrage de paquets chargé dans le noyau.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe1 from 192.168.1.0/24 to any
pass in all
block in on dmfe1 from 192.168.1.10/32 to any
```

▼ **Affichage de l'ensemble inactif de règles de filtrage de paquets**

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Affichez l'ensemble inactif de règles de filtrage de paquets.**

```
# ipfstat -I -io
```

**Exemple 21–2** Affichage de l'ensemble inactif de règles de filtrage de paquets

L'exemple ci-dessous présente la sortie d'un ensemble inactif de règles de filtrage de paquets.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
```

▼ **Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour**

Effectuez la procédure ci-dessous pour exécuter l'une ou l'autre des tâches suivantes :

- Activation d'un ensemble de règles de filtrage de paquets différent de celui que IP Filter utilise actuellement
- Rechargement du même ensemble de règles de filtrage mis à jour.

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Procédez de l'une des façons suivantes :**

- Si vous souhaitez activer un ensemble de règles complètement différent, créez-le dans un fichier distinct.
- Pour mettre à jour l'ensemble de règles actuel, modifiez le fichier de configuration contenant l'ensemble de règles.

### 3 Supprimez l'ensemble de règles actuel et chargez le nouvel ensemble de règles.

```
# ipf -Fa -f filename
```

La variable *filename* peut correspondre à un fichier contenant un ensemble de règles complètement différent, ou au fichier contenant l'ensemble de règles actif, mis à jour.

L'ensemble de règles actif est supprimé du noyau. Les règles du fichier *filename* constituent dorénavant l'ensemble de règles actif.

---

**Remarque** – Même si vous rechargez le fichier de configuration actuel, vous devez exécuter la commande. Dans le cas contraire, le système ignore l'ensemble de règles modifié défini dans le fichier de configuration mis à jour et continue d'appliquer l'ancien ensemble de règles.

N'utilisez pas de commandes telles que `ipf -D` ou `svcadm restart` pour charger l'ensemble de règles mis à jour. Ces commandes affectent la sécurité du réseau, car elles désactivent le pare-feu avant de charger le nouvel ensemble de règles.

---

#### Exemple 21–3 Activation d'un nouvel ensemble de règles de filtrage de paquets

Dans l'exemple ci-dessous, un ensemble de règles de filtrage de paquets est remplacé par un autre ensemble se trouvant dans un fichier de configuration distinct, `/etc/ipf/ipf.conf`.

```
# ipfstat -io
empty list for ipfilter(out)
pass in quick on dmfe all
# ipf -Fa -f /etc/ipf/ipf.conf
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
```

#### Exemple 21–4 Rechargement d'un ensemble de règles de filtrage de paquets mis à jour

Dans l'exemple ci-dessous, un ensemble de règles de filtrage de paquets actuellement actif est rechargé suite à sa mise à jour. Dans cet exemple, le fichier utilisé est `/etc/ipf/ipf.conf`.

```
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any

(Edit the /etc/ipf/ipf.conf configuration file.)

# ipf -Fa -f /etc/ipf/ipf.conf
```

```
# ipfstat -io (Optional)
empty list for ipfilter (out)
block in log quick from 10.0.0.0/8 to any
block in quick on elx10 from 192.168.0.0/12 to any
```

## ▼ Suppression d'un ensemble de règles de filtrage de paquets

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Supprimez l'ensemble de règles.

```
# ipf -F [a|i|o]
```

- a Supprime toutes les règles de filtrage de l'ensemble de règles.
- i Supprime les règles de filtrage pour les paquets entrants.
- o Supprime les règles de filtrage pour les paquets sortants.

### Exemple 21–5 Suppression d'un ensemble de règles de filtrage de paquets

Dans l'exemple ci-dessous, toutes les règles de filtrage sont supprimées de l'ensemble de règles de filtrage actif.

```
# ipfstat -io
block out log on dmf0 all
block in log quick from 10.0.0.0/8 to any
# ipf -Fa
# ipfstat -io
empty list for ipfilter(out)
empty list for ipfilter(in)
```

## ▼ Ajout de règles à l'ensemble actif de règles de filtrage de paquets

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :

- Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `ipf -f -`.

```
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
```

- Exécutez les commandes ci-dessous :
  - a. Créez un ensemble de règles dans le fichier de votre choix.
  - b. Ajoutez ces règles à l'ensemble de règles actif.

```
# ipf -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin de l'ensemble de règles actif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

### Exemple 21–6 Ajout de règles à l'ensemble actif de règles de filtrage de paquets

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble actif de règles de filtrage de paquets à partir de la ligne de commande.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
# echo "block in on dmfe1 proto tcp from 10.1.1.1/32 to any" | ipf -f -
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

## ▼ Ajout de règles à l'ensemble inactif de règles de filtrage de paquets

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "[Configuration initiale RBAC \(liste des tâches\)](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Créez un ensemble de règles dans le fichier de votre choix.
- 3 Ajoutez ces règles à l'ensemble de règles inactif.

```
# ipf -I -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin de l'ensemble de règles inactif. IP Filter utilise un algorithme de type "dernière règle correspondante", de sorte que les nouvelles règles déterminent les priorités de filtrage, sauf si l'utilisateur ajoute le mot-clé `quick`. Si le paquet correspond à une règle contenant le mot-clé `quick`, l'action associée à cette règle est exécutée et les règles suivantes sont ignorées.

**Exemple 21–7** Ajout de règles à l'ensemble de règles inactif

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles inactif à partir d'un fichier.

```
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
# ipf -I -f /etc/ipf/ipf.conf
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

▼ **Basculement entre les ensembles actif et inactif de règles de filtrage de paquets**

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 **Basculez entre les ensembles de règles actif et inactif.**

```
# ipf -s
```

Cette commande permet de basculer entre les ensembles de règles actif et inactif dans le noyau. Si l'ensemble de règles inactif est vide, aucun filtrage de paquets n'est effectué.

**Exemple 21–8** Basculement entre les ensembles actif et inactif de règles de filtrage de paquets

Dans l'exemple ci-dessous, la commande `ipf -s` est exécutée. L'ensemble de règles inactif devient alors l'ensemble de règles actif, tandis que l'ensemble de règles actif devient l'ensemble de règles inactif.

- Avant l'exécution de la commande `ipf -s`, la sortie de la commande `ipfstat -I -io` permet d'afficher les règles de l'ensemble de règles inactif. La sortie de la commande `ipfstat -io` affiche les règles de l'ensemble de règles actif.

```
# ipfstat -io
empty list for ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipfstat -I -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
```

- Une fois la commande `ipf -s` exécutée, les sorties des commandes `ipfstat -I -io` et `ipfstat -io` indiquent que le contenu des deux ensembles de règles a été échangé.

```
# ipf -s
Set 1 now inactive
# ipfstat -io
pass out quick on dmfe1 all
pass in quick on dmfe1 all
block in log quick from 10.0.0.0/8 to any
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
```

## ▼ Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "[Configuration initiale RBAC \(liste des tâches\)](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Spécifiez l'ensemble de règles inactif via la commande "`flush all`".

```
# ipf -I -Fa
```

Cette commande vide l'ensemble de règles inactif du noyau.

---

**Remarque** – Si vous exécutez ensuite la commande `ipf -s`, l'ensemble de règles inactif vide devient l'ensemble de règles actif. Si l'ensemble de règles actif est vide, *aucun* filtrage n'est effectué.

---

### Exemple 21–9 Suppression d'un ensemble inactif de règles de filtrage de paquets du noyau

Dans l'exemple ci-dessous, l'ensemble inactif de règles de filtrage de paquets est vidé afin de supprimer toutes les règles.

```
# ipfstat -I -io
empty list for inactive ipfilter(out)
block in log quick from 10.0.0.0/8 to any
block in on dmfe1 proto tcp from 10.1.1.1/32 to any
# ipf -I -Fa
# ipfstat -I -io
empty list for inactive ipfilter(out)
empty list for inactive ipfilter(in)
```



# Gestion des règles NAT d'IP Filter

Appliquez les procédures ci-dessous pour gérer, afficher et modifier les règles NAT.

## ▼ Affichage des règles NAT actives

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Affichez les règles NAT actives.

```
# ipnat -l
```

### Exemple 21–10 Affichage des règles NAT actives

L'exemple ci-dessous présente la sortie de l'ensemble de règles NAT actif.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

## ▼ Suppression des règles NAT

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Supprimez les règles NAT actuelles.

```
# ipnat -C
```

### Exemple 21–11 Suppression des règles NAT

Dans l'exemple ci-dessous, les entrées des règles NAT actuelles sont supprimées.

```
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32
```

```
List of active sessions:
# ipnat -C
1 entries flushed from NAT list
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
```

## ▼ Ajout de règles aux règles NAT

### 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :

- Pour ajouter des règles à l'ensemble de règles NAT via la ligne de commande, exécutez la commande `ipnat -f -`.

```
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
```

- Exécutez les commandes ci-dessous :

- a. Créez des règles NAT supplémentaires dans le fichier de votre choix.
- b. Ajoutez ces règles aux règles NAT actives.

```
# ipnat -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin des règles NAT.

## Exemple 21–12 Ajout de règles à l'ensemble de règles NAT

Dans l'exemple ci-dessous, une règle est ajoutée à l'ensemble de règles NAT via la ligne de commande.

```
# ipnat -l
List of active MAP/Redirect filters:

List of active sessions:
# echo "map dmfe0 192.168.1.0/24 -> 20.20.20.1/32" | ipnat -f -
# ipnat -l
List of active MAP/Redirect filters:
map dmfe0 192.168.1.0/24 -> 20.20.20.1/32

List of active sessions:
```

# Gestion des pools d'adresses d'IP Filter

Appliquez les procédures ci-dessous pour gérer, afficher et modifier les pools d'adresses.

## ▼ Affichage des pools d'adresses actifs

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Affichez le pool d'adresses actif.

```
# ippool -l
```

### Exemple 21-13 Affichage du pool d'adresses actif

Dans l'exemple ci-dessous, le contenu du pool d'adresses actif est affiché.

```
# ippool -l
table role = ipf type = tree number = 13
      { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

## ▼ Suppression d'un pool d'adresses

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Supprimez les entrées du pool d'adresses actuel.

```
# ippool -F
```

### Exemple 21-14 Suppression d'un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est supprimé.

```
# ippool -l
table role = ipf type = tree number = 13
      { 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# ippool -F
```

```
1 object flushed
# ippool -l
```

## ▼ Ajout de règles à un pool d'adresses

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Appliquez l'une des méthodes ci-dessous pour ajouter des règles à l'ensemble de règles actif :

- Pour ajouter des règles à l'ensemble de règles via la ligne de commande, exécutez la commande `ippool -f -`.

```
# echo "table role = ipf type = tree number = 13
{10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24};" | ippool -f -
```

- Exécutez les commandes ci-dessous :

- a. Créez des pools d'adresses supplémentaires dans le fichier de votre choix.
- b. Ajoutez ces règles au pool d'adresses actif.

```
# ippool -f filename
```

Les règles présentes dans le fichier *filename* sont ajoutées à la fin du pool d'adresses actif.

### Exemple 21–15 Ajout de règles à un pool d'adresses

Dans l'exemple ci-dessous, un pool d'adresses est ajouté à l'ensemble de règles de pool d'adresses via la ligne de commande.

```
# ippool -l
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
# echo "table role = ipf type = tree number = 100
{10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24};" | ippool -f -
# ippool -l
table role = ipf type = tree number = 100
{ 10.0.0.0/32, 172.16.1.2/32, 192.168.1.0/24; };
table role = ipf type = tree number = 13
{ 10.1.1.1/32, 10.1.1.2/32, 192.168.1.0/24; };
```

# Affichage des statistiques et des informations relatives à IP Filter

TABEAU 21-4 Affichage des statistiques et informations IP Filter (liste des tâches)

Tâche	Description	Voir
Affichage des tables d'état	Affichez les tables d'état pour obtenir des informations sur le filtrage de paquets à l'aide de la commande ipfstat.	<a href="#">“Affichage des tables d'état d'IP Filter” à la page 341</a>
Affichage des statistiques d'état	Affichez les statistiques relatives à l'état des paquets à l'aide de la commande ipfstat - s.	<a href="#">“Affichage des statistiques d'état d'IP Filter” à la page 342</a>
Affichage des statistiques NAT	Affichez les statistiques NAT à l'aide de la commande ipnat - s.	<a href="#">“Affichage des statistiques NAT d'IP Filter” à la page 343</a>
Affichage des statistiques de pool d'adresses	Affichez les statistiques de pool d'adresses à l'aide de la commande ippool - s.	<a href="#">“Affichage des statistiques de pool d'adresses d'IP Filter” à la page 343</a>

## ▼ Affichage des tables d'état d'IP Filter

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel Administration d'Oracle Solaris : services de sécurité.](#)

- 2 **Affichez la table d'état.**

# ipfstat

Remarque – L'option - t permet d'afficher la table d'état au format de l'utilitaire top.

### Exemple 21-16 Affichage des tables d'état d'IP Filter

Dans l'exemple ci-dessous, une table d'état est affichée.

```
# ipfstat
bad packets:           in 0    out 0
  input packets:      blocked 160 passed 11 nomatch 1 counted 0 short 0
  output packets:     blocked 0  passed 13681 nomatch 6844 counted 0 short 0
```

```

input packets logged:  blocked 0 passed 0
output packets logged: blocked 0 passed 0
packets logged:        input 0 output 0
log failures:          input 0 output 0
fragment state(in):    kept 0  lost 0
fragment state(out):   kept 0  lost 0
packet state(in):      kept 0  lost 0
packet state(out):     kept 0  lost 0
ICMP replies:          0      TCP RSTs sent: 0
Invalid source(in):    0
Result cache hits(in): 152      (out): 6837
IN Pullups succeeded:  0      failed: 0
OUT Pullups succeeded: 0      failed: 0
Fastroute successes:  0      failures: 0
TCP cksum fails(in):  0      (out): 0
IPF Ticks:             14341469
Packet log flags set: (0)
                      none

```

## ▼ Affichage des statistiques d'état d'IP Filter

- 1 **Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

- 2 **Affichez les statistiques d'état.**

```
# ipfstat -s
```

### Exemple 21–17 Affichage des statistiques d'état d'IP Filter

Dans l'exemple ci-dessous, les statistiques d'état sont affichées.

```

# ipfstat -s
IP states added:
    0 TCP
    0 UDP
    0 ICMP
    0 hits
    0 misses
    0 maximum
    0 no memory
    0 max bucket
    0 active
    0 expired
    0 closed
State logging enabled

State table bucket statistics:
    0 in use

```

```
0.00% bucket usage
0 minimal length
0 maximal length
0.000 average length
```

## ▼ Affichage des statistiques NAT d'IP Filter

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Affichage des statistiques NAT

```
# ipnat -s
```

### Exemple 21–18 Affichage des statistiques NAT d'IP Filter

Dans l'exemple ci-dessous, les statistiques NAT sont affichées.

```
# ipnat -s
mapped in      0      out      0
added  0      expired 0
no memory      0      bad nat 0
inuse  0
rules   1
wilds   0
```

## ▼ Affichage des statistiques de pool d'adresses d'IP Filter

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Affichage des statistiques de pool d'adresses

```
# ippool -s
```

### Exemple 21–19 Affichage des statistiques de pool d'adresses d'IP Filter

Dans l'exemple ci-dessous, les statistiques de pool d'adresses sont affichées.

```
# ippool -s
Pools: 3
Hash Tables: 0
Nodes: 0
```

# Utilisation des fichiers journaux IP Filter

TABLEAU 21-5 Utilisation des fichiers journaux IP Filter (liste des tâches)

Tâche	Description	Voir
Création d'un fichier journal	Créez un fichier journal IP Filter distinct.	<a href="#">“Configuration d'un fichier journal d'IP Filter” à la page 344</a>
Affichage des fichiers journaux	Affichez le fichier journal normal et les fichiers journaux d'état et NAT à l'aide de la commande ipmon.	<a href="#">“Affichage des fichiers journaux IP Filter” à la page 345</a>
Vidage du tampon de journalisation des paquets	Supprimez le contenu du tampon de journalisation des paquets à l'aide de la commande ipmon - F.	<a href="#">“Vidage du fichier journal de paquets” à la page 346</a>
Enregistrement des paquets consignés dans un fichier	Les paquets consignés peuvent être enregistrés dans un fichier afin d'être consultés par la suite.	<a href="#">“Enregistrement dans un fichier des paquets consignés” à la page 347</a>

## ▼ Configuration d'un fichier journal d'IP Filter

Par défaut, toutes les informations de journal IP Filter sont enregistrées dans le fichier syslogd. Configurez un fichier journal afin de séparer les informations de trafic IP Filter enregistrées des autres données susceptibles d'être consignées dans le fichier journal par défaut. Procédez comme suit.

- 1
- Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**  
  
Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel Administration d'Oracle Solaris : services de sécurité.](#)

- 2
- Ajoutez les lignes suivantes au fichier /etc/syslog.conf :**

```
# Save IP Filter log output to its own file
local0.debug /var/log/log-name
```



---

**Remarque** – Sur la deuxième ligne, séparez `local0.debug` de `/var/log/log-name` à l'aide de la touche de tabulation (non la barre d'espace).

---

**3 Créez le fichier journal.**

```
# touch /var/log/log-name
```

**4 Redémarrez le service de journal système.**

```
# svcadm restart system-log
```

### Exemple 21–20 Création d'un journal IP Filter

L'exemple suivant crée le fichier `ipmon.log` pour archiver les informations IP Filter.

Dans `/etc/syslog.conf` :

```
# Save IP Filter log output to its own file
local0.debug          /var/log/ipmon.log
```

Sur la ligne de commande :

```
# touch /var/log/ipmon.log
# svcadm restart system-log
```

## ▼ Affichage des fichiers journaux IP Filter

### Avant de commencer

Il est conseillé de créer un fichier journal distinct pour enregistrer les données IP Filter. Reportez-vous à la section [“Configuration d'un fichier journal d'IP Filter”](#) à la page 344.

**1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.**

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Affichez le fichier journal normal, le fichier journal NAT ou le fichier journal d'état. Pour afficher un fichier journal, tapez la commande ci-dessous, conjointement avec l'option adéquate :**

```
# ipmon -o [S|N|I] filename
```

S     Affiche le fichier journal d'état.

N     Affiche le fichier journal NAT.

I     Affiche le fichier journal IP normal.

Pour afficher le fichier journal normal et les fichiers journaux d'état et NAT, appliquez les options :

```
# ipmon -o SNI filename
```

- Si vous avez arrêté manuellement le démon `ipmon`, vous pouvez également exécuter la commande ci-dessous pour afficher le fichier journal IP Filter et les fichiers journaux d'état et NAT :

```
# ipmon -a filename
```

---

**Remarque** – N'utilisez pas la syntaxe `ipmon -a` si le démon `ipmon` est en cours d'exécution. Normalement, le démon démarre automatiquement à l'initialisation du système. Si vous exécutez la commande `ipmon -a`, une autre copie de `ipmon` s'ouvre également. Dans ce cas, les deux copies lisent les mêmes informations de journal, mais tout message du journal n'est reçu que par l'une d'elles.

---

Pour plus d'informations sur l'affichage des fichiers journaux, reportez-vous à la page de manuel [ipmon\(1M\)](#).

### Exemple 21–21 Affichage des fichiers journaux IP Filter

L'exemple ci-dessous présente la sortie du fichier `/var/ipmon.log`.

```
# ipmon -o SNI /var/ipmon.log
02/09/2004 15:27:20.606626 bge0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

ou

```
# pkill ipmon
# ipmon -aD /var/ipmon.log
02/09/2004 15:27:20.606626 bge0 @0:1 p 129.146.157.149 ->
129.146.157.145 PR icmp len 20 84 icmp echo/0 IN
```

## ▼ Vidage du fichier journal de paquets

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section "[Configuration initiale RBAC \(liste des tâches\)](#)" du manuel *Administration d'Oracle Solaris : services de sécurité*.

## 2 Vidage du tampon de journalisation des paquets

```
# ipmon -F
```

### Exemple 21–22 Vidage du fichier journal de paquets

L'exemple ci-dessous présente la sortie obtenue en cas de suppression d'un fichier journal. Le système génère un rapport même si le fichier journal est vide, comme dans cet exemple.

```
# ipmon -F
0 bytes flushed from log buffer
0 bytes flushed from log buffer
0 bytes flushed from log buffer
```

## ▼ Enregistrement dans un fichier des paquets consignés

### 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)” du manuel \*Administration d'Oracle Solaris : services de sécurité\*](#).

### 2 Enregistrez dans un fichier les paquets consignés.

```
# cat /dev/ipl > filename
```

Continuez la journalisation des paquets dans le fichier *filename* et interrompez la procédure en tapant `Ctrl-C` pour afficher de nouveau l'invite de ligne de commande.

### Exemple 21–23 Enregistrement dans un fichier des paquets consignés

L'exemple ci-dessous présente les résultats obtenus lorsque les paquets consignés sont enregistrés dans un fichier.

```
# cat /dev/ipl > /tmp/logfile
^C#

# ipmon -f /tmp/logfile
02/09/2004 15:30:28.708294 bge0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 52 -S IN
02/09/2004 15:30:28.708708 bge0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.792611 bge0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 70 -AP IN
02/09/2004 15:30:28.872000 bge0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872142 bge0 @0:1 p 129.146.157.149,33923 ->
    129.146.157.145,23 PR tcp len 20 43 -AP IN
```

```
02/09/2004 15:30:28.872808 bge0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
02/09/2004 15:30:28.872951 bge0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 47 -AP IN
02/09/2004 15:30:28.926792 bge0 @0:1 p 129.146.157.149,33923 ->
129.146.157.145,23 PR tcp len 20 40 -A IN
.
.
(output truncated)
```

## Création et modification des fichiers de configuration IP Filter

Vous devez modifier directement les fichiers de configuration afin de créer et modifier les ensembles de règles et les pools d'adresses. Les fichiers de configuration suivent les règles de syntaxe UNIX standard :

- Le signe dièse (#) indique qu'une ligne contient des commentaires.
- Une ligne peut contenir à la fois des commentaires et des règles.
- Vous pouvez ajouter des espaces supplémentaires afin de faciliter la lecture des règles.
- La définition d'une règle peut s'étaler sur plusieurs lignes. Insérez un backslash (\) à la fin d'une ligne pour indiquer que la règle continue sur la ligne suivante.

### ▼ Création d'un fichier de configuration d'IP Filter

La procédure ci-dessous décrit la configuration des :

- Fichiers de configuration de filtrage de paquets
- Fichiers de configuration des règles NAT
- Fichiers de configuration de pool d'adresses

#### 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil des droits de gestion IP Filter.

Vous pouvez créer un rôle et lui attribuer le profil de droits de gestion IP Filter. Pour créer un rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

#### 2 Lancez l'éditeur de fichiers de votre choix. Créez et modifiez le fichier de configuration de la fonction que vous souhaitez configurer.

- Pour créer un fichier de configuration des règles de filtrage de paquets, modifiez le fichier `ipf.conf`.

IP Filter utilise les règles de filtrage de paquets spécifiées dans le fichier `ipf.conf`. Si vous placez le fichier de règles de filtrage de paquets dans le fichier `/etc/ipf/ipf.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement des règles de filtrage à l'initialisation, le cas échéant, placez-les dans le fichier de votre choix. Vous pouvez ensuite activer les règles à l'aide de la commande `ipf`, comme décrit à la section [“Activation d'un nouvel ensemble de règles de filtrage de paquets ou d'un ensemble mis à jour”](#) à la page 331.

Pour plus d'informations sur la création de règles de filtrage de paquets, reportez-vous à la section [“Utilisation de la fonctionnalité de filtrage de paquets d'IP Filter”](#) à la page 314.

---

**Remarque** – Si le fichier `ipf.conf` est vide, aucun filtrage n'est appliqué. Un fichier `ipf.conf` vide correspond à un ensemble de règles défini comme suit :

```
pass in all
pass out all
```

---

- Pour créer un fichier de configuration des règles NAT, modifiez le fichier `ipnat.conf`.  
IP Filter utilise les règles NAT spécifiées dans le fichier `ipnat.conf`. Si vous placez le fichier de règles NAT dans le fichier `>/etc/ipf/ipnat.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement des règles NAT à l'initialisation, le cas échéant, placez le fichier `ipnat.conf` dans le dossier de votre choix. Ensuite, vous pouvez activer les règles NAT à l'aide de la commande `ipnat`.  
Pour plus d'informations sur la création de règles pour NAT, reportez-vous à la section [“Utilisation de la fonctionnalité NAT d'IP Filter”](#) à la page 317.
- Pour créer un fichier de configuration des pools d'adresses, modifiez le fichier `ippool.conf`.  
IP Filter utilise le pool d'adresses spécifié dans le fichier `ippool.conf`. Si vous placez le fichier de règles du pool d'adresses dans le fichier `/etc/ipf/ippool.conf`, ce fichier est chargé à l'initialisation du système. Pour empêcher le chargement du pool d'adresses à l'initialisation, le cas échéant, placez le fichier `ippool.conf` dans le dossier de votre choix. Ensuite, vous pouvez activer le pool d'adresses à l'aide de la commande `ippool`.  
Pour plus d'informations sur la création de pools d'adresses, reportez-vous à la section [“Utilisation de la fonctionnalité de pools d'adresses d'IP Filter”](#) à la page 319.

## Exemples de fichiers de configuration IP Filter

Les exemples ci-dessous illustrent les règles de filtrage de paquets utilisées dans les configurations de filtrage.

### EXEMPLE 21–24 Configuration d'un hôte IP Filter

Cet exemple présente une configuration sur un ordinateur hôte avec une interface réseau bge.

**EXEMPLE 21-24** Configuration d'un hôte IP Filter (Suite)

```
# pass and log everything by default
pass in log on bge0 all
pass out log on bge0 all

# block, but don't log, incoming packets from other reserved addresses
block in quick on bge0 from 10.0.0.0/8 to any
block in quick on bge0 from 172.16.0.0/12 to any

# block and log untrusted internal IPs. 0/32 is notation that replaces
# address of the machine running Solaris IP Filter.
block in log quick from 192.168.1.15 to <thishost>
block in log quick from 192.168.1.43 to <thishost>

# block and log X11 (port 6000) and remote procedure call
# and portmapper (port 111) attempts
block in log quick on bge0 proto tcp from any to bge0/32 port = 6000 keep state
block in log quick on bge0 proto tcp/udp from any to bge0/32 port = 111 keep state
```

Cet ensemble de règles commence par deux règles illimitées qui permettent à tout type de données d'entrer et sortir via l'interface bge. Le deuxième ensemble de règles empêche tout paquet entrant issu des espaces d'adresses privées 10.0.0.0 et 172.16.0.0 de traverser la pare-feu. L'ensemble de règles suivant bloque des adresses internes spécifiques de la machine hôte. Enfin, le dernier ensemble de règles empêche l'entrée des paquets via les ports 6000 et 111.

**EXEMPLE 21-25** Configuration d'un serveur IP Filter

Cet exemple présente la configuration d'une machine hôte tenant lieu de serveur Web. Cet ordinateur possède une interface réseau e1000g.

```
# web server with an e1000g interface
# block and log everything by default;
# then allow specific services
# group 100 - inbound rules
# group 200 - outbound rules
# (0/32) resolves to our IP address)
*** FTP proxy ***

# block short packets which are packets
# fragmented too short to be real.
block in log quick all with short

# block and log inbound and outbound by default,
# group by destination
block in log on e1000g0 from any to any head 100
block out log on e1000g0 from any to any head 200

# web rules that get hit most often
pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = http flags S keep state group 100
```

**EXEMPLE 21-25** Configuration d'un serveur IP Filter (Suite)

```

pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = https flags S keep state group 100

# inbound traffic - ssh, auth
pass in quick on e1000g0 proto tcp from any \
to e1000g0/32 port = 22 flags S keep state group 100
pass in log quick on e1000g0 proto tcp from any \
to e1000g0/32 port = 113 flags S keep state group 100
pass in log quick on e1000g0 proto tcp from any port = 113 \
to e1000g0/32 flags S keep state group 100

# outbound traffic - DNS, auth, NTP, ssh, www, smtp
pass out quick on e1000g0 proto tcp/udp from e1000g0/32 \
to any port = domain flags S keep state group 200
pass in quick on e1000g0 proto udp from any \
port = domain to e1000g0/32 group 100

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = 113 flags S keep state group 200
pass out quick on e1000g0 proto tcp from e1000g0/32 port = 113 \
to any flags S keep state group 200

pass out quick on e1000g0 proto udp from e1000g0/32 to any \
port = ntp group 200
pass in quick on e1000g0 proto udp from any \
port = ntp to e1000g0/32 port = ntp group 100

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = ssh flags S keep state group 200

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = http flags S keep state group 200
pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = https flags S keep state group 200

pass out quick on e1000g0 proto tcp from e1000g0/32 \
to any port = smtp flags S keep state group 200

# pass icmp packets in and out
pass in quick on e1000g0 proto icmp from any to e1000g0/32 keep state group 100
pass out quick on e1000g0 proto icmp from e1000g0/32 to any keep state group 200

# block and ignore NETBIOS packets
block in quick on e1000g0 proto tcp from any \
to any port = 135 flags S keep state group 100

block in quick on e1000g0 proto tcp from any port = 137 \
to any flags S keep state group 100
block in quick on e1000g0 proto udp from any to any port = 137 group 100
block in quick on e1000g0 proto udp from any port = 137 to any group 100

```

**EXEMPLE 21-25** Configuration d'un serveur IP Filter (Suite)

```
block in quick on e1000g0 proto tcp from any port = 138 \
to any flags S keep state group 100
block in quick on e1000g0 proto udp from any port = 138 to any group 100

block in quick on e1000g0 proto tcp from any port = 139 to any flags S keep state
group 100
block in quick on e1000g0 proto udp from any port = 139 to any group 100
```

**EXEMPLE 21-26** Configuration d'un routeur IP Filter

Cet exemple présente la configuration d'un routeur possédant une interface interne, nge0, et une interface externe, ce1.

```
# internal interface is nge0 at 192.168.1.1
# external interface is nge1 IP obtained via DHCP
# block all packets and allow specific services
*** NAT ***
*** POOLS ***

# Short packets which are fragmented too short to be real.
block in log quick all with short

# By default, block and log everything.
block in log on nge0 all
block in log on nge1 all
block out log on nge0 all
block out log on nge1 all

# Packets going in/out of network interfaces that aren't on the loopback
# interface should not exist.
block in log quick on nge0 from 127.0.0.0/8 to any
block in log quick on nge0 from any to 127.0.0.0/8
block in log quick on nge1 from 127.0.0.0/8 to any
block in log quick on nge1 from any to 127.0.0.0/8

# Deny reserved addresses.
block in quick on nge1 from 10.0.0.0/8 to any
block in quick on nge1 from 172.16.0.0/12 to any
block in log quick on nge1 from 192.168.1.0/24 to any
block in quick on nge1 from 192.168.0.0/16 to any

# Allow internal traffic
pass in quick on nge0 from 192.168.1.0/24 to 192.168.1.0/24
pass out quick on nge0 from 192.168.1.0/24 to 192.168.1.0/24

# Allow outgoing DNS requests from our servers on .1, .2, and .3
pass out quick on nge1 proto tcp/udp from nge1/32 to any port = domain keep state
pass in quick on nge0 proto tcp/udp from 192.168.1.2 to any port = domain keep state
```



**EXEMPLE 21-26** Configuration d'un routeur IP Filter (Suite)

```
pass in quick on nge0 proto tcp/udp from 192.168.1.3 to any port = domain keep state
```

```
# Allow NTP from any internal hosts to any external NTP server.
```

```
pass in quick on nge0 proto udp from 192.168.1.0/24 to any port = 123 keep state
```

```
pass out quick on nge1 proto udp from any to any port = 123 keep state
```

```
# Allow incoming mail
```

```
pass in quick on nge1 proto tcp from any to nge1/32 port = smtp keep state
```

```
pass in quick on nge1 proto tcp from any to nge1/32 port = smtp keep state
```

```
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = smtp keep state
```

```
# Allow outgoing connections: SSH, WWW, NNTP, mail, whois
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = 22 keep state
```

```
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 22 keep state
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = 80 keep state
```

```
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 80 keep state
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = 443 keep state
```

```
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = 443 keep state
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = nntp keep state
```

```
block in quick on nge1 proto tcp from any to any port = nntp keep state
```

```
pass out quick on nge1 proto tcp from 192.168.1.0/24 to any port = nntp keep state
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = smtp keep state
```

```
pass in quick on nge0 proto tcp from 192.168.1.0/24 to any port = whois keep state
```

```
pass out quick on nge1 proto tcp from any to any port = whois keep state
```

```
# Allow ssh from offsite
```

```
pass in quick on nge1 proto tcp from any to nge1/32 port = 22 keep state
```

```
# Allow ping out
```

```
pass in quick on nge0 proto icmp all keep state
```

```
pass out quick on nge1 proto icmp all keep state
```

```
# allow auth out
```

```
pass out quick on nge1 proto tcp from nge1/32 to any port = 113 keep state
```

```
pass out quick on nge1 proto tcp from nge1/32 port = 113 to any keep state
```

```
# return rst for incoming auth
```

```
block return-rst in quick on nge1 proto tcp from any to any port = 113 flags S/SA
```

```
# log and return reset for any TCP packets with S/SA
```

```
block return-rst in log on nge1 proto tcp from any to any flags S/SA
```

**EXEMPLE 21-26** Configuration d'un routeur IP Filter (Suite)

```
# return ICMP error packets for invalid UDP packets
block return-icmp(net-unr) in proto udp all
```

## PARTIE IV

# Performances du réseau

Cette partie traite des fonctionnalités de performances de réseau telles que l'équilibrage de charge intégré et le protocole de redondance de routeur virtuel.



## Présentation de l'équilibreur de charge intégré

---

L'équilibreur de charge intégré (ILB, Integrated Load Balancer) est une fonction d'Oracle Solaris qui permet l'équilibrage de charge de type Layer 3 et Layer 4 pour le système Oracle Solaris installé sur les systèmes SPARC et x86. ILB intercepte les demandes entrantes des clients, détermine le serveur d'arrière-plan qui doit gérer la demande en fonction des règles d'équilibrage de charge, puis transfère la demande au serveur sélectionné. ILB peut effectuer des contrôles de l'intégrité du serveur et fournit des données pour les algorithmes d'équilibrage de charge afin de vérifier si le serveur sélectionné peut gérer la demande entrante.

Ce chapitre se compose des sections suivantes :

- [“Terminologie d'ILB” à la page 358](#)
- [“Fonctions d'ILB” à la page 360](#)
- [“Processus d'ILB” à la page 365](#)
- [“Recommandations relatives à l'utilisation d'ILB” à la page 366](#)
- [“ILB et utilitaire de gestion des services” à la page 366](#)
- [“Commandes et sous-commandes ILB” à la page 366](#)

ILB possède les fonctions principales suivantes :

- Prise en charge des modes Direct Server Return (DSR) et Network Address Translation (NAT) sans état pour IPv4 et IPv6
- Interface de ligne de commande pour l'administration ILB
- Surveillance des serveurs par le biais de contrôles de l'intégrité

ILB se compose de trois éléments majeurs :

- Interface de ligne de commande `ilbadm` : vous pouvez utiliser cette interface pour configurer des règles d'équilibrage de charge, effectuer des contrôles de l'intégrité des serveurs.
- Bibliothèque de configuration `libilb` : `ilbadm` et d'autres applications tierces peuvent utiliser la fonctionnalité implémentée dans `libilb` pour l'administration ILB.
- Démon `ilbd` : ce démon exécute les tâches suivantes :

- Gestion de la configuration persistante
- Accès série au module du noyau ILB par le traitement des informations de configuration et l'envoi de ces données en vue de l'exécution au sein du module du noyau ILB
- Contrôles de l'intégrité des serveurs et envoi des résultats au module du noyau ILB afin d'ajuster la distribution de charge

## Terminologie d'ILB

Cette section décrit certains termes utiles à connaître lors de l'implémentation d'ILB sur vos systèmes.

### **Vidange des connexions**

Mécanisme qui empêche toute nouvelle connexion à un serveur désactivé par l'administrateur. Cette fonction est utile car elle arrête les serveurs sans interrompre les connexions ou sessions actives. Les connexions existantes au serveur continuent de fonctionner normalement. Une fois le serveur prêt à gérer les demandes, il peut être de nouveau activé par l'administrateur, et l'équilibreur de charge lui transfèrera les nouvelles connexions. ILB fournit ne fournit cette capacité qu'aux serveurs avec des services virtuels basés sur le mode NAT.

### **Mode Direct Server Return (DSR)**

Désigne le mode qui équilibre la charge des demandes entrantes aux serveurs d'arrière-plan et indique au trafic de retour des serveurs d'ignorer l'équilibreur de charge en envoyant directement les demandes au client. L'implémentation actuelle du mode DSR dans ILB ne fournit pas de suivi des connexions TCP (c.-à-d. sans état).

Avantages :

- Meilleures performances que le mode NAT, car seule l'adresse MAC cible des paquets est modifiée, et les serveurs répondent directement aux clients.
- Entièrement transparent : les serveurs voient une connexion directement à partir de l'adresse IP du client et répondent au client par le biais de la passerelle par défaut.

Inconvénients :

- Le serveur d'arrière-plan doit répondre à la fois à sa propre adresse IP (pour les contrôles de l'intégrité) et à l'adresse IP virtuelle (pour le trafic d'équilibrage de charge).
- Du fait que l'équilibreur de charge ne maintient aucun état de connexion (c.-à-d. sans état), l'ajout ou la suppression de serveurs provoquera l'interruption des connexions.

### **Algorithme d'équilibrage de charge**

Algorithme utilisé par ILB pour sélectionner un serveur d'arrière-plan dans un groupe de serveurs pour une demande entrante.

**Règle d'équilibrage de charge** Dans ILB, un service virtuel est représenté par une règle d'équilibrage de charge et définie par les paramètres suivants :

- Adresse IP virtuelle
- Protocole de transport : TCP ou UDP
- Numéro (ou plage de numéros) de port
- Algorithme d'équilibrage de charge
- Type de mode d'équilibrage de charge (DSR, Full-NAT ou Half-NAT)
- Groupe de serveurs constitué d'un ensemble de serveurs d'arrière-plan
- Contrôles optionnels de l'intégrité des serveurs effectués sur chaque serveur du groupe de serveurs
- Port optionnel pour effectuer les contrôles de l'intégrité

---

**Remarque** – Vous pouvez spécifier des contrôles de l'intégrité sur port particulier, ou sur n'importe quel sélectionné de manière aléatoire par le démon `ilbd`, de la plage de numéros de port associés au serveur.

---

**Equilibrage de charge NAT**

Opération qui consiste à réécrire les informations d'en-tête IP et gérer à la fois le trafic de demande et le trafic de réponse. Il existe deux types de NAT : Half-NAT et Full-NAT. Tous les deux réécrivent l'adresse IP de destination. Cependant, Full-NAT réécrit également l'adresse IP source, et la fait apparaître sur le serveur d'où toutes les connexions sont originaires à partir de l'équilibreur de charge. NAT fournit le suivi des connexions TCP (c.-à-d. avec état).

Avantages :

- Fonctionnement avec tous les serveurs d'arrière-plan en modifiant la passerelle par défaut pour pointer vers l'équilibreur de charge.
- Du fait que l'équilibreur de charge maintient l'état de connexion, l'ajout ou la suppression de serveurs peut avoir lieu sans interruption des connexions.

Inconvénients :

- Des performances plus faibles que DSR, à cause du traitement qui nécessite que l'en-tête IP soit modifié et que les serveurs envoient leurs réponses à l'équilibreur de charge.
- Tous les serveurs d'arrière-plan doivent utiliser l'équilibreur de charge en tant que passerelle par défaut.

**Configuration persistante**

Dans le contexte d'ILB, une configuration persistante dans une configuration (c.-à-d. un ensemble de règles d'équilibrage de charge) qui persiste après la réinitialisation et les mises à jour de packages.

**Source proxy**

La plage d'adresses IP qui peuvent servir de proxy. La plage est limitée à 10 adresses IP. La source proxy est requise uniquement en cas d'implémentation Full NAT.

**session**

Se compose d'un nombre de paquets qui proviennent du même client pendant un intervalle donné et qui prennent du sens dans leur globalité.

<b>Persistence de session</b>	Fonction permettant d'envoyer tous les paquets d'un client au même serveur d'arrière-plan. Egalement désignée sous le nom d'adhérence. Vous pouvez configurer une persistance de session simple (autrement dit, une persistance d'adresse source) pour un service virtuel en spécifiant les options <code>pmask=prefix length</code> et <code>persist-timeout=value</code> in seconds. Une fois la persistance de session établie entre un client et un serveur, tous les paquets allant du client vers le service virtuel sont transférés au même serveur d'arrière-plan pendant toute la durée de la persistance. La longueur du préfixe dans la notation CIDR est une valeur comprise entre 0–32 pour IPv4 et 0–128 pour IPv6.
<b>Groupe de serveurs</b>	Ensemble constitué de zéro ou plusieurs serveurs d'arrière-plan qui doit compter au moins un serveur lorsqu'il sert de service virtuel. Par exemple, si vous souhaitez équilibrer la charge des demandes HTTP, vous devez configurer ILB avec un groupe de serveurs constitué de un ou plusieurs serveurs d'arrière-plan. ILB équilibrera le trafic HTTP à travers l'ensemble des serveurs configurés.
<b>ID de serveur</b>	Nom unique pour l'adresse IP, assigné par le système lorsque le serveur est ajouté au groupe de serveurs.
<b>Adresse IP virtuelle (VIP)</b>	Adresse IP pour un service virtuel.
<b>Service virtuel</b>	Un service que les clients voient sous la forme <code>VIP:port</code> . Exemple : <code>www.foo.com:80</code> . Bien que le service est géré par un groupe de serveurs comprenant plus d'un serveur, les clients du service virtuel ne voient qu'une seule adresse IP <code>address:port</code> pour ce groupe de serveurs. Il est possible d'inclure un serveur dans plus d'un groupe de serveurs afin qu'il serve à plusieurs services virtuels. Un seul groupe de serveurs peut également servir à plusieurs services virtuels.

## Fonctions d'ILB

Cette section décrit les fonctions principales d'ILB.

### Modes de fonctionnement d'ILB

ILB prend en charge les modes DSR et NAT sans état pour IPv4 et IPv6, par le biais de topologies à une ou deux branches.

- **Mode DSR sans état** : dans ce mode, ILB équilibre les demandes entrantes vers les serveurs d'arrière-plan, mais laisse le trafic de retour provenant de ces serveurs et à destination des clients l'ignorer. Cependant, vous pouvez également configurer ILB en tant que routeur pour le serveur d'arrière-plan. Dans ce cas, la réponse du serveur d'arrière-plan au client est routée par l'ordinateur qui exécute ILB. Avec le mode DSR sans état, ILB n'enregistre pas les informations d'état des paquets traités, excepté à des fins statistiques. Etant donné qu'ILB n'enregistre pas d'état dans ce mode, les performances sont comparables aux performances normales assurées en transfert IP. Ce mode s'adapte mieux aux protocoles sans connexion.
- **Mode NAT (Full-NAT et Half-NAT)** : ILB utilise NAT en mode autonome, pour la fonctionnalité d'équilibrage de charge uniquement. Dans ce mode, ILB réécrit les informations d'en-tête et gère le trafic entrant ainsi que le trafic sortant. Le mode NAT offre une sécurité supplémentaire et s'adapte mieux au trafic HTTP (ou SSL).



---

**Remarque** – Le chemin du code NAT implémenté dans ILB diffère de celui de la fonction IP Filter d'Oracle Solaris. N'utilisez *pas* ces deux chemins de code simultanément.

---

## Algorithmes d'ILB

Les algorithmes d'ILB contrôlent les distributions du trafic et fournissent diverses caractéristiques pour la distribution des charges et la sélection des serveurs. ILB fournit les algorithmes suivants pour chaque mode de fonctionnement :

- Round-robin – Dans un algorithme round-robin, l'équilibreur de charge affecte les demandes à une liste de serveurs à tour de rôle. Après l'affectation d'un serveur à une demande, le serveur est déplacé vers la fin de la liste.
- *src IP* hash : avec la méthode source IP hash, l'équilibreur de charge sélectionne un serveur en fonction de la valeur de hachage associée à l'adresse IP source de la demande entrante.
- *src-IP, port* hash : avec la méthode source IP, port hash, l'équilibreur de charge sélectionne un serveur en fonction de la valeur de hachage associée à l'adresse IP source et du port source de la demande entrante.
- *src-IP, VIP* hash : avec la méthode source IP, VIP hash, l'équilibreur de charge sélectionne un serveur en fonction de la valeur de hachage associée à l'adresse IP source et de l'adresse IP cible de la demande entrante.

## Interface de ligne de commande ILB

L'interface de ligne de commande se trouve dans le répertoire `/usr/sbin/ilbadm`. Elle inclut les sous-commandes de configuration des règles d'équilibrage de charge, des groupes de serveurs et des contrôles de l'intégrité des serveurs. Des sous-commandes d'affichage des statistiques et des informations de configuration y sont également disponibles. Les sous-commandes peuvent se diviser en deux catégories :

- Les sous-commandes de configuration qui permettent de réaliser les tâches suivantes :
  - Création et suppression de règles d'équilibrage de charge
  - Activation et désactivation de règles d'équilibrage de charge
  - Création et suppression de groupes de serveurs
  - Ajout et suppression de serveurs dans un groupe de serveurs
  - Activation et désactivation de serveurs d'arrière-plan
  - Création et suppression de contrôles de l'intégrité pour un groupe de serveurs au sein d'une règle d'équilibrage de charge

---

**Remarque** – L'administration de ces sous-commandes de configuration requière des privilèges. Pour les obtenir, accédez à la fonction de contrôle d'accès basé sur les rôles. Pour créer le rôle adéquat et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

---

- Les sous-commandes d'affichage qui permettent de réaliser les tâches suivantes :
  - Affichage des règles d'équilibrage de charge, groupes de serveurs et contrôles de l'intégrité
  - Affichage des statistiques de transfert des paquets
  - Affichage de la table des connexions NAT
  - Affichage des résultats des contrôles de l'intégrité
  - Affichage de la table des correspondances de persistance de session

---

**Remarque** – Vous n'avez pas besoin de privilèges pour administrer les sous-commandes d'affichage.

---

Pour obtenir une liste des sous-commandes `ilbadm`, reportez-vous à la section [“Commandes et sous-commandes ILB”](#) à la page 366. Pour plus d'informations sur les sous-commandes `ipadm`, reportez-vous à la page de manuel `ilbadm(1M)`.

## Fonction ILB de surveillance des serveurs

ILB fournit une fonction de surveillance des serveurs facultative qui permet d'effectuer des contrôles de l'intégrité des serveurs avec les capacités suivantes :

- Tests ping intégrés
- Tests TCP intégrés
- Tests UDP intégrés
- Tests utilisateur pouvant servir de contrôles de l'intégrité

Par défaut, ILB n'effectue aucun contrôle de l'intégrité du serveur. Vous pouvez définir des contrôles de l'intégrité pour chaque groupe de serveurs lors de la création d'une règle d'équilibrage de charge. Vous ne pouvez configurer qu'un contrôle de l'intégrité par règle d'équilibrage de charge. Tant qu'un service virtuel est activé, les contrôles de l'intégrité définis sur le groupe de serveurs associé à ce service virtuel démarrent automatiquement et se répètent de manière périodique. Les contrôles de l'intégrité s'arrêtent dès que le service virtuel est désactivé. Les états précédents des contrôles de l'intégrité ne sont pas maintenus si le service virtuel est réactivé.

Lorsque vous souhaitez vérifier l'intégrité du serveur par le biais d'un test TCP, d'un test UDP ou d'un test personnalisé, ILB envoie un test ping par défaut afin de déterminer si le serveur est accessible, avant d'envoyer le test spécifié au serveur. Le test ping constitue un moyen de surveiller l'intégrité du serveur. Si le test ping échoue, le serveur correspondant est désactivé et l'état unreachable lui est attribué. Si le test ping réussit, alors que le test TCP/UDP/personnalisé échoue, le serveur est désactivé et l'état dead lui est attribué.

---

**Remarque –**

- Vous pouvez désactiver le test ping par défaut.
  - Le test ping par défaut ne peut pas être désactivé pour le test UDP. Par conséquent, pour les contrôles de l'intégrité UDP, le test ping est toujours le test par défaut.
- 

Vous pouvez configurer le contrôle de l'intégrité pour les paramètres affichés dans le tableau suivant.

**TABEAU 22-1** Configuration des paramètres de contrôle de l'intégrité

Paramètres de contrôle de l'intégrité	Description
hc - test	Spécifie le type de contrôle à effectuer.
hc - timeout	Initie un délai d'attente lorsque le contrôle n'est pas terminé.
hc - interval	Spécifie l'intervalle entre plusieurs contrôles consécutifs.  <b>Remarque –</b> Les intervalles sont définis de manière aléatoire entre les valeurs suivantes : $0.5 * hc - interval$ et $1.5 * hc - interval$ .
hc - count	Spécifie le nombre de contrôles consécutifs ayant échoué avant qu'un serveur soit considéré comme défaillant.

---

## Fonctions ILB supplémentaires

Cette section décrit les fonctions supplémentaires d'ILB.

- **Permet aux clients d'effectuer des tests ping sur les adresses IP virtuelles (VIP) :** ILB peut répondre aux demandes d'écho du protocole ICMP (Internet Control Message Protocol) sur les VIP des clients. ILB fournit cette capacité pour les modes de fonctionnement DSR et NAT.
- **Permet d'ajouter et de supprimer des serveurs dans un groupe de serveurs sans interrompre le service :** vous pouvez ajouter et supprimer des serveurs de manière dynamique sans que les connexions existantes avec les serveurs d'arrière-plan soient interrompues. ILB fournit cette capacité pour le mode NAT.

- **Permet de configurer la persistance de session (adhérence)** : dans de nombreuses applications, il est important d'envoyer une série de connexions et/ou de paquets du même client au même serveur d'arrière-plan. Vous pouvez configurer la persistance de session pour un service virtuel en spécifiant le masque de réseau dans la sous-commande `create-rule{[-m persist=<netmask>]}`. Après avoir créé une correspondance persistante, les demandes de connexions et/ou de paquets suivantes sur un service virtuel, avec une adresse IP source du client correspondante, sont transférées au même serveur d'arrière-plan. La prise en charge du mécanisme de persistance de session est disponible pour les modes DSR et NAT.
- **Permet d'effectuer une vidange des connexions** : ILB prend en charge cette capacité uniquement pour les serveurs dont les services virtuels utilisent le mode NAT. Cette fonction empêche les nouvelles connexions d'être envoyées au serveur si celui-ci est désactivé. Les connexions existantes à ce serveur continuent de fonctionner. Une fois toutes les connexions à ce serveur terminées, le serveur peut être arrêté pour maintenance. Une fois le serveur prêt à gérer les demandes, activez-le afin que l'équilibreur de charge lui transfère les nouvelles connexions. Cette fonction permet d'arrêter les serveurs pour maintenance sans interrompre les connexions ou sessions actives.
- **Permet d'équilibrer la charge sur les ports TCP et UDP** : ILB peut équilibrer la charge de tous les ports sur une adresse IP donnée entre différents ensembles de serveurs sans nécessiter la configuration de règles explicites pour chaque port. ILB fournit cette capacité pour les modes de fonctionnement DSR et NAT.
- **Permet de spécifier chaque port pour les services virtuels au sein du même groupe de serveurs** avec cette fonction, ILB vous permet de définir des ports de destination pour différents serveurs appartenant au même groupe de serveurs en mode NAT.
- **Permet d'équilibrer la charge sur une plage simple de numéros de port** : ILB peut équilibrer la charge sur une suite de ports associée à la VIP pour un groupe de serveurs donné. Il est pratique de conserver les adresses IP en équilibrant la charge de différentes plages de numéros de port associées à la même VIP pour différents ensembles de serveurs d'arrière-plan. De plus, lorsque la persistance de session est activée pour le mode NAT, ILB envoie sur le même serveur d'arrière-plan des demandes issues de la même adresse IP client pour différents ports de la même plage.
- **Permet de changer de port et de réduire la plage de ports** : selon la plage de ports d'un serveur définie dans une règle d'équilibrage de charge, vous pouvez changer de port et réduire la plage de ports. Si la plage de ports d'un serveur est différente de la plage de ports VIP, la fonction de basculement entre les ports est automatiquement implémentée. Quant à la fonction de réduction de la plage de ports, elle est implémentée si la plage de ports du serveur n'affiche qu'un port. ILB fournit ces fonctions pour le mode NAT.

## Processus d'ILB

Cette section décrit les processus d'ILB tels que le traitement des paquets client-serveur et serveur-client.

### Traitement des paquets client-serveur :

1. ILB reçoit une demande entrante envoyée par le client à une adresse VIP et compare cette demande avec les règles d'équilibrage de charge.
2. Si ILB trouve une règle d'équilibrage de charge correspondante, il utilise un algorithme d'équilibrage de charge pour transférer la demande au serveur d'arrière-plan en fonction du mode de fonctionnement.
  - En mode DSR, ILB remplace l'en-tête MAC de la demande entrante par l'en-tête MAC du serveur d'arrière-plan sélectionné.
  - En mode Half-NAT, ILB remplace l'adresse IP cible et le numéro du port pour le protocole de transfert de la demande entrante par ceux du serveur d'arrière-plan sélectionné.
  - En mode Full-NAT, ILB remplace l'adresse IP source et le numéro du port pour le protocole de transfert de la demande entrante par l'adresse source NAT de la règle d'équilibrage de charge. ILB remplace également l'adresse IP cible et le numéro du port pour le protocole de transfert de la demande entrante par ceux du serveur d'arrière-plan sélectionné.
3. ILB transfère la demande entrante modifiée au serveur d'arrière-plan sélectionné.

### Traitement des paquets serveur-client :

1. Le serveur d'arrière-plan envoie une réponse à ILB en écho à la demande entrante du client.
2. L'action d'ILB après avoir reçu la réponse du serveur d'arrière-plan dépend du mode de fonctionnement :
  - En mode DSR normal, la réponse du serveur d'arrière-plan ignore ILB et se dirige directement vers le client. Cependant, si ILB sert également de routeur pour le serveur d'arrière-plan, la réponse du serveur d'arrière-plan au client est routée par l'ordinateur qui exécute ILB.
  - En modes Half-NAT et Full-NAT, ILB fait correspondre la réponse du serveur d'arrière-plan avec la demande entrante et remplace l'adresse IP modifiée ainsi que le numéro du port pour le protocole de transfert par ceux de la demande entrante d'origine. ILB transfère alors la réponse au client.

## Recommandations relatives à l'utilisation d'ILB

Les consignes suivantes décrivent la procédure d'utilisation d'ILB :

- Pour gérer ILB, vous devez pouvoir vous connecter en tant que superutilisateur ou prendre un rôle bénéficiant du profil des droits ILB Management. Vous pouvez créer un rôle et lui attribuer le profil de droits ILB Management. Pour créer le rôle et l'attribuer à un utilisateur, reportez-vous à la section [“Configuration initiale RBAC \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Pour activer l'audit des commandes de configuration ILB, vous devez présélectionner la classe d'audit pour l'administration du système entier. Pour ce faire, reportez-vous à la section [“Configuration du service d'audit \(liste des tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.
- Les composants utilisateur d'ILB sont fournis dans un package IPS distinct, dans le référentiel Oracle Solaris, sous un nom commençant par `SUNwlb`. Vous devez télécharger ces packages à partir du référentiel Oracle Solaris à l'aide de la commande `pkg install`. Pour connaître les instructions d'installation d'ILB, reportez-vous à la section [“Installation de l'équilibreur de charge intégré”](#) à la page 369.
- L'implémentation NAT d'ILB en mode autonome est limitée à la fonctionnalité d'équilibrage de charge.
- ILB fournit uniquement une redondance pour les pannes d'ordinateurs et ne gère pas les pannes de commutateurs. Désormais, ILB n'assure plus la synchronisation entre différents ordinateurs qui exécutent ILB.

## ILB et utilitaire de gestion des services

ILB est géré par l'utilitaire de gestion des services SMF (Service Management Facility) `svc:/network/loadbalancer/ilb:default`. Pour avoir une présentation de l'utilitaire SMF, reportez-vous au [Chapitre 6, “Gestion des services \(présentation\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*. Pour connaître les procédures détaillées associées à l'utilitaire SMF, reportez-vous au [Chapitre 7, “Gestion des services \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : Tâches courantes*.

## Commandes et sous-commandes ILB

Vous pouvez utiliser la commande `ilbadm` et ses sous-commandes pour manipuler les règles d'équilibrage de charge. Pour plus d'informations sur les sous-commandes `ipadm`, reportez-vous à la page de manuel [ilbadm\(1M\)](#).

TABLEAU 22-2 Commandes et sous-commandes ILB pour manipuler les règles d'équilibrage de charge

Commande ILB	Description
<code>ilbadm create-rule</code>	Crée un nom de règle ( <code>rule name</code> ) avec les caractéristiques données.
<code>ilbadm show-rule</code>	Affiche les caractéristiques des règles spécifiées ou affiche toutes les règles si aucune règle n'est spécifiée.
<code>ilbadm delete-rule</code>	Supprime toutes les informations appartenant à un <code>rule name</code> . Si le nom ( <code>name</code> ) n'existe pas, la sous-commande échoue.
<code>ilbadm enable-rule</code>	Active une règle nommée, ou active toutes les règles si aucun nom n'est spécifié.
<code>ilbadm disable-rule</code>	Désactive une règle nommée, ou désactive toutes les règles si aucun nom n'est spécifié.
<code>ilbadm show-statistics</code>	Affiche les statistiques. Par exemple, <code>-t</code> avec la sous-commande inclut un horodatage avec chaque en-tête.
<code>ilbadm show-hc-result</code>	Affiche les résultats du contrôle d'intégrité des serveurs associés au nom spécifié de la règle <code>rule-name</code> . Si la règle <code>rule-name</code> n'est pas spécifiée, les résultats du contrôle de l'intégrité des serveurs pour toutes les règles s'affichent.
<code>ilbadm show-nat</code>	Affiche les informations de la table NAT.
<code>ilbadm create-servergroup</code>	Crée d'un groupe de serveurs. Vous pouvez ajouter des serveurs supplémentaires à l'aide de <code>ilbadm add-server</code> .
<code>ilbadm delete-servergroup</code>	Supprime un groupe de serveurs.
<code>ilbadm show-servergroup</code>	Répertorie un groupe de serveurs ou tous les groupes de serveurs, si aucun groupe de serveurs n'est spécifié.
<code>ilbadm enable-server</code>	Active un serveur désactivé.
<code>ilbadm disable-server</code>	Désactive les serveurs spécifiés.
<code>ilbadm add-server</code>	Ajoute les serveurs spécifiés aux groupes de serveurs.
<code>ilbadm show-server</code>	Affiche les serveurs associés aux règles nommées ou tous les serveurs, si aucun nom de règle n'est spécifié.
<code>ilbadm remove-server</code>	Supprime des serveurs d'un groupe de serveurs.
<code>ilbadm create-healthcheck</code>	Configure des informations des contrôles de l'intégrité qui peuvent servir à configurer des règles.
<code>ilbadm show-persist</code>	Affiche de la table des correspondances de persistance de session.

**TABEAU 22-2** Commandes et sous-commandes ILB pour manipuler les règles d'équilibrage de charge  
(Suite)

Commande ILB	Description
<code>ilbadm export-config <i>filename</i></code>	Exporte le fichier de configuration dans un format adapté à l'importation afin de pouvoir l'utiliser avec la commande <code>ilbadm import</code> si nécessaire. Si <i>filename</i> n'est pas spécifié, <code>ilbadm export</code> écrit sur <code>stdout</code> .
<code>ilbadm import-config -p <i>filename</i></code>	Importe un fichier et remplace la configuration existante avec le contenu de ce fichier importé. Si <i>filename</i> n'est pas spécifié, <code>ilbadm import</code> écrit à partir de <code>stdin</code> .



## Configuration de l'équilibreur de charge intégré (tâches)

---

Ce chapitre décrit l'installation et la configuration d'ILB (Integrated Load Balancer, équilibreur de charge intégré) et contient les sections suivantes :

- “Installation de l'équilibreur de charge intégré” à la page 369
- “Activation et désactivation d'ILB” à la page 370
- “Configuration d'ILB” à la page 371
- “Configuration de haute disponibilité ILB (Mode actif/passif uniquement)” à la page 375
- “Configuration de l'autorisation utilisateur pour les sous-commandes de configuration ILB” à la page 380
- “Administration des groupes de serveurs ILB” à la page 381
- “Administration des serveurs d'arrière-plan dans ILB” à la page 382
- “Administration des contrôles de l'intégrité du serveur dans ILB” à la page 384
- “Administration des règles ILB” à la page 387
- “Affichage des statistiques ILB” à la page 389
- “Utilisation des sous-commandes Import et Export” à la page 391

## Installation de l'équilibreur de charge intégré

Cette section décrit l'installation d'ILB.

ILB possède deux portions, le noyau et l'utilisateur. La portion du noyau est automatiquement installée en même temps que Oracle Solaris 11. Mais pour obtenir la portion de l'utilisateur ILB, l'utilisateur doit installer manuellement l'ilb présent dans le package `service/network/load-balancer/ilb`.

# Activation et désactivation d'ILB

Cette section décrit les procédures permettant d'activer et de désactiver ILB.

## ▼ Procédure d'activation d'ILB

### Avant de commencer

Vérifiez que les fichiers d'attribut RBAC (Role Based Access Control, contrôle d'accès basé sur les rôles) du système possèdent les entrées suivantes (si ces entrées sont absentes, ajoutez-les manuellement) :

- Nom de fichier : /etc/security/auth\_attr
  - solaris.network.ilb.config::Network ILB  
Configuration::help=NetworkILBconf.html
  - solaris.network.ilb.enable::Network ILB Enable  
Configuration::help=NetworkILBenable.html
  - solaris.smf.manage.ilb::Manage Integrated Load Balancer Service  
States::help=SmfILBStates.html
- Nom de fichier : /etc/security/prof\_attr
  - Network ILB::Manage ILB configuration via  
ilbadm:auths=solaris.network.ilb.config,solaris.network.ilb.enable;help=RtNetILB.htm
  - L'entrée Network Management du fichier doit inclure solaris.smf.manage.ilb.
- Nom du fichier : /etc/user\_attr
  - daemon:::auths=solaris.smf.manage.ilb,solaris.smf.modify.application

### 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits ILB Management.

Vous pouvez créer un rôle et lui attribuer le profil de droits ILB Management. Pour créer le rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

### 2 Activez le service de transfert adéquat (IPv4 ou IPv6, ou les deux).

```
#svcadm enable svc:/network/ipv4-forwarding
# svcadm enable svc:/network/ipv6-forwarding
```

### 3 Activez le service ILB.

```
# svcadm enable ilb
```

### 4 Vérifiez que le service ILB est activé.

```
# svcs ilb
```

## ▼ Procédure de désactivation d'ILB

- 1 Connectez-vous en tant que superutilisateur ou prenez un rôle bénéficiant du profil de droits ILB Management.

Vous pouvez créer un rôle et lui attribuer le profil de droits ILB Management. Pour créer le rôle et l'attribuer à un utilisateur, reportez-vous à la section “[Configuration initiale RBAC \(liste des tâches\)](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

- 2 Désactivez le service ILB.

```
# svcadm disable ilb
```

- 3 Vérifiez que le service ILB est désactivé.

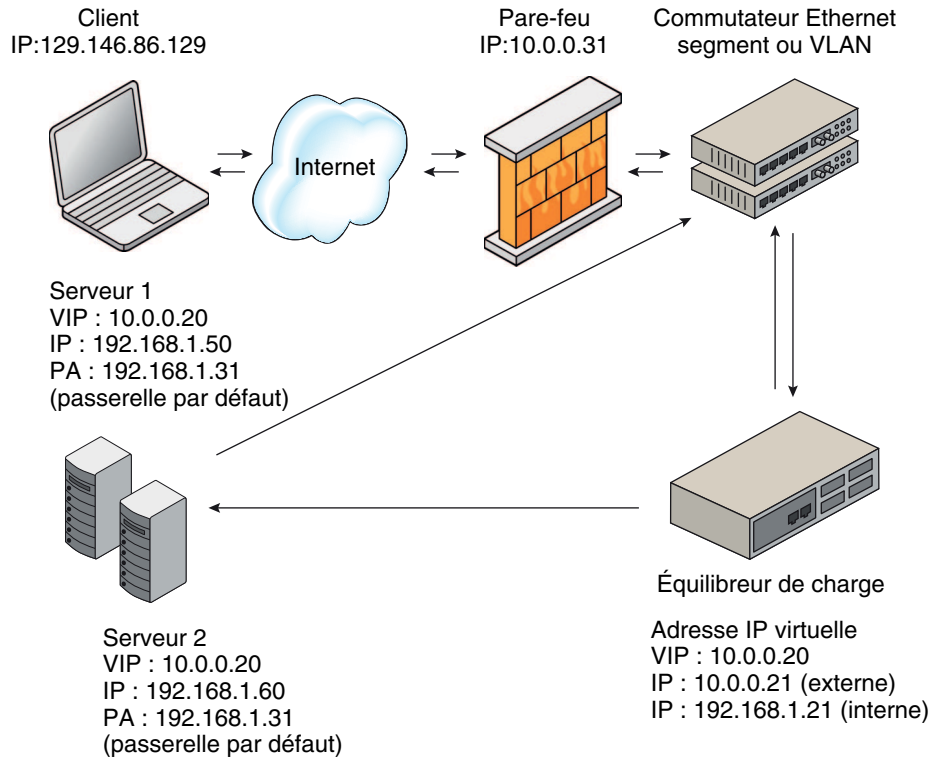
```
# svcs ilb
```

## Configuration d'ILB

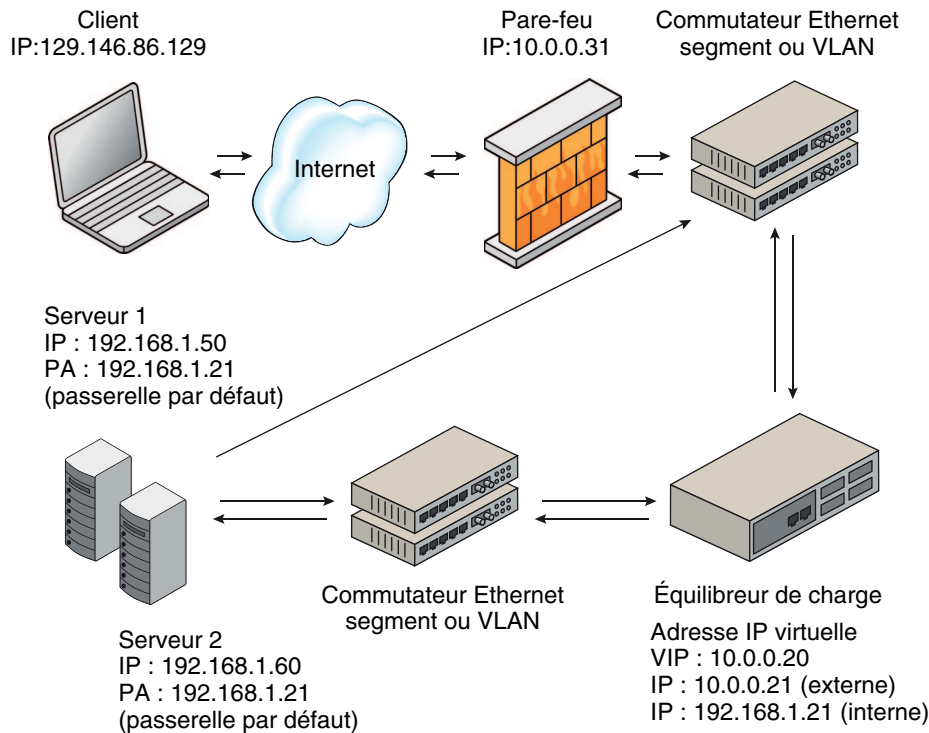
Cette section décrit l'implémentation d'ILB avec les topologies DSR, Half-NAT et Full-NAT.

### Topologies DSR, Full-NAT et Half-NAT

La figure ci-dessous illustre l'implémentation d'ILB avec la topologie DSR.



ILB fonctionne en mode Half-NAT et en mode Full-NAT. L'implémentation générale de la topologie NAT s'affiche comme illustré dans la figure suivante.



## Topologie d'équilibrage de charge Half-NAT

En mode Half-NAT, ILB réécrit uniquement l'adresse IP de destination dans l'en-tête des paquets. Si vous utilisez l'implémentation Half-NAT, vous ne pouvez pas vous connecter à une adresse IP virtuelle (VIP) du service à partir du même sous-réseau sur lequel le serveur réside.

TABLEAU 23-1 Flux de demande et flux de réponse pour l'implémentation Half-NAT

Flux de demande	Adresse IP source	Adresse IP cible
1. Client → Équilibreur de charge	Client	VIP de l'équilibreur de charge
2. Équilibreur de charge → Serveur	Client	Serveur
Flux de réponse		
3. Serveur → Équilibreur de charge	Serveur	Client
4. Équilibreur de charge → Client	VIP de l'équilibreur de charge	Client

Si vous connectez le PC client sur le même réseau que celui des serveurs, le serveur souhaité répond directement au client. La quatrième étape n'a pas lieu et, par conséquent, l'adresse IP

source pour la réponse du serveur au client n'est pas valide. Lorsque le client envoie une demande de connexion à l'équilibreur de charge, la réponse vient du serveur souhaité. Dorénavant, la pile IP du client abandonne correctement toutes les réponses.

Dans ce cas, les flux de demande et de réponse se présentent comme illustré dans le tableau suivant.

TABLEAU 23-2 Flux de demande et flux de réponse pour l'implémentation Half-NAT

Flux de demande	Adresse IP source	Adresse IP cible
1. Client → Equilibreur de charge	Client	VIP de l'équilibreur de charge
2. Equilibreur de charge → Serveur	Client	Serveur
Flux de réponse		
3. Serveur → Client	Serveur	Client

## Topologie d'équilibrage de charge Full-NAT

Dans l'implémentation Full-NAT, les adresses IP source et cible sont réécrites pour permettre au trafic de passer par l'équilibreur de charge dans les deux sens. La topologie Full-NAT permet de se connecter au VIP à partir du même sous-réseau que celui hébergeant les serveurs. Le tableau suivant représente la topologie Full-NAT pour ILB. Aucun routage par défaut n'est requis dans ces serveurs. Le routage par défaut via l'équilibreur de charge est l'adresse du routeur sur le sous-réseau C. Dans ce scénario, l'équilibreur de charge se comporte comme un proxy.

TABLEAU 23-3 Flux de demande et flux de réponse pour l'implémentation Full-NAT

Flux de demande	Adresse IP source	Adresse IP cible
1. Client → Equilibreur de charge	Client	VIP de l'équilibreur de charge
2. Equilibreur de charge → Serveur	Adresse de l'interface de l'équilibreur de charge (sous-réseau C)	Serveur
Flux de réponse		
3. Serveur → Equilibreur de charge	Serveur	Adresse de l'interface de l'équilibreur de charge (sous-réseau C)
4. Equilibreur de charge → Client	VIP de l'équilibreur de charge	Client

## Configuration de haute disponibilité ILB (Mode actif/passif uniquement)

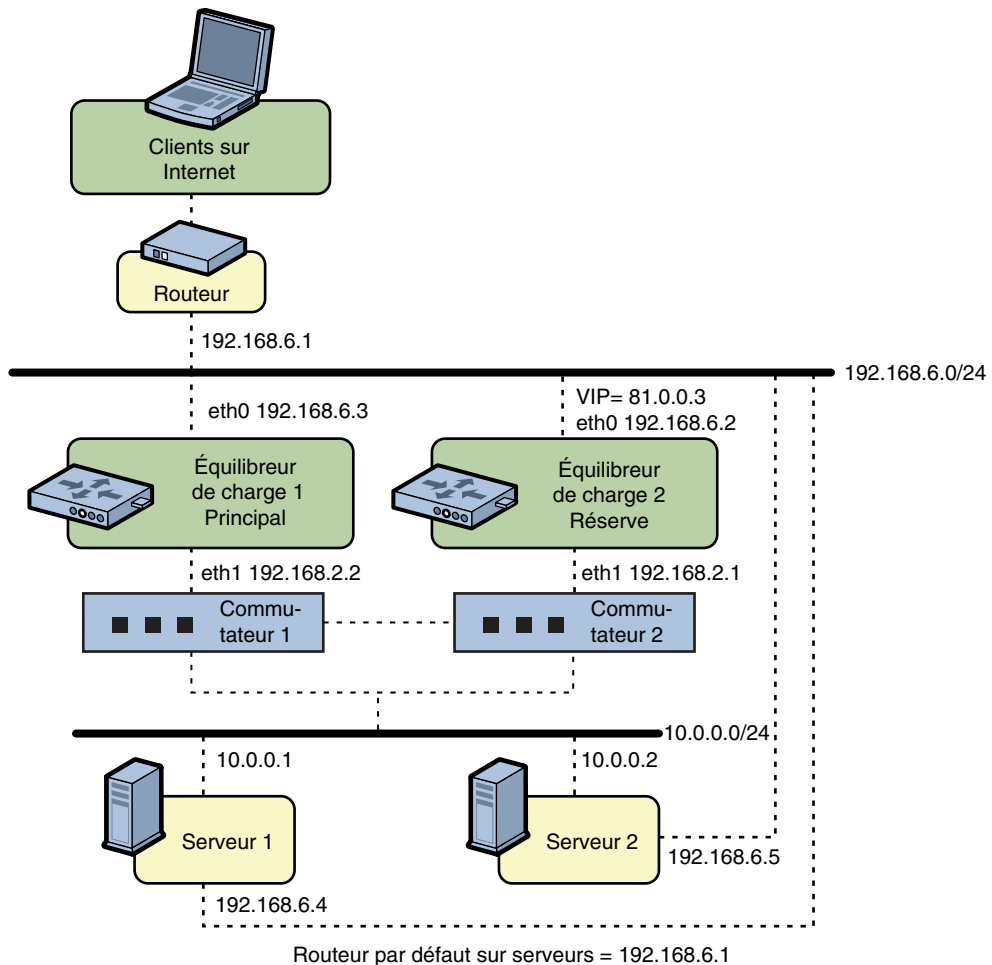
Cette section décrit la configuration à haute disponibilité d'ILB avec les topologies DSR, Half-NAT et Full-NAT.

### Configuration à haute disponibilité d'ILB à l'aide de la topologie DSR

Cette section décrit la procédure de configuration des connexions ILB de manière à atteindre la haute disponibilité à l'aide de la topologie DSR. Vous devez configurer deux équilibres de charge, l'un en tant qu'équilibreur de charge principal, l'autre en tant qu'équilibreur de charge de réserve. En cas de panne de l'équilibreur de charge principal, l'équilibreur de charge de réserve prend sa place.

La figure suivante illustre la topologie DSR pour la configuration des connexions ILB permettant d'atteindre la haute disponibilité.

## Topologie DSR



Toutes les VIP sur équilibreurs de charge sont configurées sur des interfaces tournées vers le sous-réseau 192.168.6.0/24.

## ▼ Procédure de configuration à haute disponibilité d'ILB avec la topologie DSR

- 1 Configurez les deux équilibreurs de charge (principal et réserve) à l'aide des commandes suivantes :

```
# ilbadm create-servergroup -s server=10.0.0.1,10.0.0.2 sg1
# ilbadm create-rule -i vip=81.0.0.3,port=9001 \
-m lbalg=hash-ip-port,type=DSR -o servergroup=sg1 rule1
```



**2 Vérifiez que VIP est configuré sur l'interface lo0 de tous les serveurs.**

```
Server1# ipadm create-addr -T static -d -a 81.0.0.3/24 lo0/server1
Server2# ipadm create-addr -T static -d -a 81.0.0.3/24 lo0/server2
```

**3 Configurez l'équilibreur de charge 1 en tant qu'équilibreur de charge principal.**

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb1
```

**4 Configurez l'équilibreur de charge 2 en tant qu'équilibreur de charge de réserve.**

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb2
```

La configuration précédente fournit une protection contre les scénarios de panne suivants :

- Si l'équilibreur de charge 1 tombe en panne, l'équilibreur de charge 2 prend sa place et gère la résolution d'adresse pour le VIP 81.0.0.3 ainsi que tous les paquets des clients possédant l'adresse IP de destination 81.0.0.3.

Lorsque l'équilibreur de charge 1 est rétabli, l'équilibreur de charge 2 retourne en mode veille.

- Si l'une des interfaces de l'équilibreur de charge 1, ou les deux, tombe en panne, l'équilibreur de charge 2 devient l'équilibreur de charge principal. Par conséquent, l'équilibreur de charge 2 gère la résolution d'adresse pour le VIP 81.0.0.3 ainsi que tous les paquets des clients possédant l'adresse IP de destination 81.0.0.3.

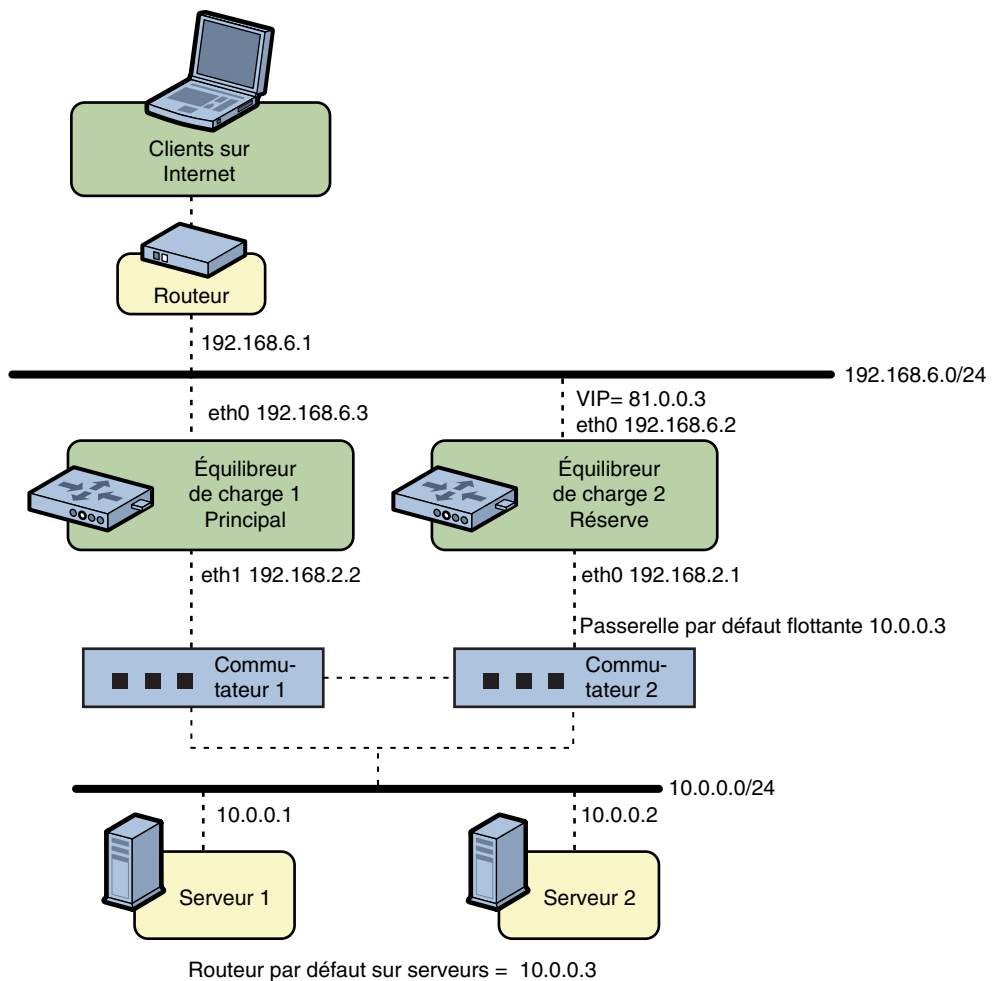
Lorsque les deux interfaces de l'équilibreur de charge 1 retrouvent leur intégrité, l'équilibreur de charge 2 retourne en mode veille.

## Configuration à haute disponibilité ILB avec la topologie Half-NAT

Cette section décrit la procédure de configuration des connexions ILB de manière à atteindre la haute disponibilité à l'aide de la topologie Half-NAT. Vous devez configurer deux équilibreurs de charge, l'un en tant qu'équilibreur de charge principal, l'autre en tant qu'équilibreur de charge de réserve. En cas de panne de l'équilibreur de charge principal, l'équilibreur de charge de réserve prend sa place.

La figure suivante illustre la topologie Half-NAT pour la configuration des connexions ILB permettant d'atteindre la haute disponibilité.

## Topologie Half-NAT



Toutes les VIP sur équilibreurs de charge sont configurées sur des interfaces tournées vers le sous-réseau 192.168.6.0/24.

## ▼ Procédure de configuration à haute disponibilité d'ILB avec la topologie Half-NAT

- 1 Configurez l'équilibreur de charge principal et l'équilibreur de charge de réserve.

```
# ilbadm create servergroup -s server=10.0.0.1,10.0.0.2 sg1
# ilbadm create-rule -ep -i vip=81.0.0.3,port=9001-9006,protocol=udp \
-m lbalg=roundrobin,type=HALF-NAT,pmask=24 \
-h hc-name=hc1,hc-port=9006 \
```

```
-t conn-drain=70,nat-timeout=70,persist-timeout=70 -o servergroup=sg1 rule1
```

## 2 Configurez l'équilibreur de charge 1 en tant qu'équilibreur de charge principal.

```
LB1# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB1# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb1
LB1# vrrpadm create-router -V 1 -A inet -l eth0 -p 255 vrrp1
LB1# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB1# ipadm create-addr -T static -d -a 10.0.0.3/24 vnic2/lb1
LB1# vrrpadm create-router -V 2 -A inet -l eth1 -p 255 vrrp2
```

## 3 Configurez l'équilibreur de charge 2 en tant qu'équilibreur de charge de réserve.

```
LB2# dladm create-vnic -m vrrp -V 1 -A inet -l eth0 vnic1
LB2# ipadm create-addr -T static -d -a 81.0.0.3/24 vnic1/lb2
LB2# vrrpadm create-router -V 1 -A inet -l eth0 -p 100 vrrp1
LB2# dladm create-vnic -m vrrp -V 2 -A inet -l eth1 vnic2
LB2# ipadm create-addr -T static -d -a 10.0.0.3/24 vnic2/lb2
LB2# vrrpadm create-router -V 2 -A inet -l eth1 -p 100 vrrp2
```

## 4 Ajoutez l'adresse IP pour la passerelle flottante par défaut sur les deux serveurs.

```
# route add net 192.168.6.0/24 10.0.0.3
```

La configuration précédente fournit une protection contre les scénarios de panne suivants :

- Si l'équilibreur de charge 1 tombe en panne, l'équilibreur de charge 2 prend sa place et gère la résolution d'adresse pour le VIP 81.0.0.3 ainsi que tous les paquets des clients possédant l'adresse IP de destination 81.0.0.3. Il doit également gérer tous les paquets envoyés à l'adresse 10.0.0.3 de la passerelle flottante.

Lorsque l'équilibreur de charge 1 est rétabli, l'équilibreur de charge 2 retourne en mode veille.

- Si l'une des interfaces de l'équilibreur de charge 1, ou les deux, tombe en panne, l'équilibreur de charge 2 devient l'équilibreur de charge principal. Par conséquent, l'équilibreur de charge 2 gère la résolution d'adresse pour le VIP 81.0.0.3 ainsi que tous les paquets des clients possédant l'adresse IP de destination 81.0.0.3. Il doit également gérer tous les paquets envoyés à l'adresse 10.0.0.3 de la passerelle flottante.

Lorsque les deux interfaces de l'équilibreur de charge 1 retrouvent leur intégrité, l'équilibreur de charge 2 retourne en mode veille.

---

**Remarque** – L'implémentation actuelle d'ILB ne synchronise pas l'équilibreur de charge principal et l'équilibreur de réserve. Lorsque l'équilibreur de charge principal tombe en panne et que l'équilibreur de charge de réserve prend sa place, les connexions existantes échouent. Cependant, la haute disponibilité sans synchronisation reste intéressante dans le cas où l'équilibreur de charge principal tombe en panne.

---

## Configuration de l'autorisation utilisateur pour les sous-commandes de configuration ILB

Vous devez posséder l'autorisation RBAC `solaris.network.ilb.config` pour exécuter les sous-commandes de configuration ILB suivantes :

```
create-servergroup
delete-servergroup groupname
show-servergroup
add-server
remove-server
enable-server
disable-server
show-server
create-healthcheck
show-healthcheck
delete-healthcheck
show-rule
delete-rule
enable-rule
disable-rule
show-statistics
show-hc-result
show-nat
show-persist
export-config
import-config
```

Pour affecter l'autorisation à un utilisateur existant, reportez-vous au [Chapitre 9, “Utilisation du contrôle d'accès basé sur les rôles \(tâches\)”](#) du manuel *Administration d'Oracle Solaris : services de sécurité*.

Vous pouvez également fournir cette autorisation lorsque vous créez un compte utilisateur sur le système. Exemple :

```
useradd -g 10 -u 1210 -A solaris.network.ilb.config ilbadmin
```

La commande `useradd` ajoute un nouvel utilisateur aux fichiers `/etc/passwd`, `/etc/shadow` et `/etc/user_attr`. L'option `-A` affecte l'autorisation à l'utilisateur.

# Administration des groupes de serveurs ILB

Vous pouvez utiliser la commande `ilbadm` pour créer, supprimer et répertorier les groupes de serveurs ILB. Pour connaître la définition d'un groupe de serveurs, reportez-vous à la section “Terminologie d'ILB” à la page 358.

## ▼ Procédure de création d'un groupe de serveurs

- 1 Sélectionnez un nom pour le groupe de serveurs en cours de création.
- 2 Sélectionnez des serveurs à inclure dans le groupe de serveurs.  
Vous pouvez spécifier les serveurs avec leur nom d'hôte ou adresse IP et un port optionnel.
- 3 Créez le groupe de serveurs.  
`# ilbadm create-servergroup -s servers=webserv1,webserv2,webserv3 webgroup`

### Exemple 23–1 Création d'un groupe de serveurs

L'exemple suivant crée un groupe de serveurs appelé `webgroup` et constitué de trois serveurs :

```
# ilbadm create-servergroup -s servers=webserv1,webserv2,webserv3 webgroup
```

## ▼ Procédure de suppression d'un groupe de serveurs

- 1 Sélectionnez le groupe de serveurs que vous souhaitez supprimer.  
Le groupe de serveurs ne doit pas être en cours d'utilisation par une règle active. Dans le cas contraire, la suppression échoue.
- 2 Dans la fenêtre de terminal, supprimez le groupe de serveurs.  
`# ilbadm delete-servergroup webgroup`

### Exemple 23–2 Suppression d'un groupe de serveurs

L'exemple suivant supprime un groupe de serveurs appelé `webgroup` :

```
# ilbadm delete-servergroup webgroup
```

## Affichage d'un groupe de serveurs

Dans une fenêtre de terminal, saisissez la sous-commande `show-servergroup` pour obtenir des informations sur un groupe de serveurs spécifique ou sur tous les groupes de serveurs.

L'exemple suivant fournit des informations détaillées sur tous les groupes de serveurs :

```
# ilbadm show-servergroup -o all
```

sname	serverID	minport	maxport	IP_address
specgroup	_specgroup.0	7001	7001	199.199.67.18
specgroup	_specgroup.1	7001	7001	199.199.67.19
test123	_test123.0	7001	7001	199.199.67.18
test123	_test123.1	7001	7001	199.199.67.19

## Administration des serveurs d'arrière-plan dans ILB

Vous pouvez utiliser la commande `ilbadm` pour ajouter, supprimer, activer et désactiver un ou plusieurs serveurs d'arrière-plan au sein des groupes de serveurs. Des définitions sont disponibles à la section [“Terminologie d'ILB” à la page 358](#).

### ▼ Procédure d'ajout d'un serveur d'arrière-plan à un groupe de serveurs

- Ajoutez un serveur d'arrière-plan à un groupe de serveurs.

Les spécifications liées au serveur doivent inclure un nom d'hôte ou une adresse IP et peuvent également inclure un port ou une plage de numéros de port optionnels. Les entrées de serveur avec la même adresse IP sont désactivées au sein d'un groupe de serveurs.

```
# ilbadm add-server -e -s server=192.168.89.1,192.168.89.2 ftpgroup
# ilbadm add-server -e -s server=[2001:7::feed:6]:8080 sgrp
```

L'option `-e` active les serveurs en plus de les ajouter au groupe.

---

**Remarque** – Les adresses IPv6 doivent être saisies entre crochets.

---

### Exemple 23–3 Ajout d'un serveur d'arrière-plan à un groupe de serveurs

L'exemple suivant ajoute des serveurs aux groupes de serveurs `ftpgroup` et `sgrp`, et les active.

```
# ilbadm add-server -e -s \
server=192.168.89.1,192.168.89.2 ftpgroup
# ilbadm add-server -e -s server=[2001:7::feed:6]:8080 sgrp
```

## ▼ Procédure de suppression d'un serveur d'arrière-plan à un groupe de serveurs

- 1 Pour supprimer un serveur d'un groupe de serveurs spécifique, procédez comme suit :
  - a. Déterminez l'ID du serveur à supprimer d'un groupe de serveurs. L'ID du serveur peut être obtenu à partir de la sortie de la sous-commande `show-servergroup -o all`.
  - b. Supprimez le serveur.
 

```
# ilbadm remove-server -s server=_specgroup.0 specgroup
```
- 2 Pour supprimer un serveur de tous les groupes de serveurs, procédez comme suit :
  - a. Déterminez l'adresse IP et le nom d'hôte du serveur à supprimer.
  - b. Utilisez la sortie de la commande `ilbadm show-servergroup -o all` pour identifier les groupes de serveurs auxquels appartient le serveur.
  - c. Pour chaque groupe de serveurs, exécutez la sous-commande suivante afin de supprimer le serveur du groupe.

### Exemple 23–4 Suppression d'un serveur d'arrière-plan d'un groupe de serveurs

L'exemple suivant supprime le serveur avec l'ID `10.1.1.2` du groupe de serveurs `websg` :

```
# ilbadm remove-server -s server=_specgroup.0 specgroup
```

Prenez note des remarques suivantes :

- Si le serveur est utilisé par une règle NAT ou Half-NAT, désactivez le serveur à l'aide de la sous-commande `disable-server` avant la suppression. Lorsqu'un serveur est désactivé, il prend l'état `connection-draining`. Une fois toutes les connexions vidées, le serveur peut être supprimé à l'aide de la sous-commande `remove-server`. Après l'exécution de la commande `disable-server`, vérifiez périodiquement la table NAT (à l'aide de la commande `show-nat`) pour vous assurer que le serveur en question possède toujours des connexions. Une fois toutes les connexions vidées (le serveur ne s'affiche pas dans la sortie de la commande `show-nat`), le serveur peut alors être supprimé à l'aide de la commande `remove-server`.
- Si la valeur du délai d'attente `conn-drain` est définie, l'état `connection-draining` sera atteint à la fin de ce délai d'attente. La valeur par défaut du délai d'attente `conn-drain` est 0, ce qui signifie que le serveur restera en attente jusqu'à ce qu'une connexion soit fermée.

## ▼ Procédure de réactivation ou désactivation d'un serveur d'arrière-plan

- 1 Déterminez l'adresse IP, le nom d'hôte ou l'ID du serveur à réactiver ou désactiver. Si une adresse IP ou un nom d'hôte est spécifié(e), le serveur sera réactivé ou désactivé pour toutes les règles qui lui sont associées. Si un ID de serveur est spécifié, le serveur sera réactivé ou désactivé spécifiquement pour les règles associées à cet ID de serveur.

---

**Remarque** – Un serveur peut posséder plusieurs ID s'il appartient à plusieurs groupes de serveurs.

---

- 2 Réactivez ou désactivez un serveur.

```
# ilbadm enable-server server
# ilbadm disable-server server
```

### Exemple 23–5 Réactivation et désactivation d'un serveur d'arrière-plan

Dans l'exemple suivant, un serveur avec l'ID `websg.1` est activé, puis désactivé.

```
# ilbadm enable-server websg.1
# ilbadm disable-server websg.1
```

## Administration des contrôles de l'intégrité du serveur dans ILB

ILB fournit à l'utilisateur un choix d'options facultatives permettant de vérifier l'intégrité du serveur :

- Tests ping intégrés
- Tests TCP intégrés
- Tests UDP intégrés
- Tests utilisateur pouvant servir de contrôles de l'intégrité

Par défaut, ILB n'effectue aucun contrôle de l'intégrité du serveur. Vous pouvez définir des contrôles de l'intégrité pour chaque groupe de serveurs lors de la création d'une règle d'équilibrage de charge. Vous ne pouvez configurer qu'un contrôle de l'intégrité par règle d'équilibrage de charge. Tant qu'un service virtuel est activé, les contrôles de l'intégrité définis sur le groupe de serveurs associé à ce service virtuel démarrent automatiquement et se répètent de manière périodique. Les contrôles de l'intégrité s'arrêtent dès que le service virtuel est désactivé. Les états précédents des contrôles de l'intégrité ne sont pas maintenus si le service virtuel est réactivé.



Lorsque vous souhaitez vérifier l'intégrité du serveur par le biais d'un test TCP, d'un test UDP ou d'un test personnalisé, ILB envoie un test ping par défaut afin de déterminer si le serveur est accessible, avant d'envoyer le test spécifié au serveur. Le test ping constitue un moyen de surveiller l'intégrité du serveur. Si le test ping échoue, le serveur correspondant est désactivé et l'état `unreachable` lui est attribué. Si le test ping réussit, alors que le test TCP/UDP/personnalisé échoue, le serveur est désactivé et l'état `dead` lui est attribué.

Vous pouvez utiliser la commande `ilbadm` pour créer, supprimer et répertorier différents contrôles de l'intégrité du serveur. Des définitions sont disponibles à la section [“Terminologie d'ILB” à la page 358](#).

## Création d'un contrôle de l'intégrité

L'exemple suivant crée deux contrôles de l'intégrité nommés *objects*, *hc1* et *hc-myscript*. Le premier contrôle de l'intégrité utilise le test TCP intégré. Le second contrôle de l'intégrité utilise un test personnalisé : `/var/tmp/my-script`.

```
# ilbadm create-healthcheck \
-h hc-timeout=3,hc-count=2,hc-interval=8,hc-test=tcp hc1
# ilbadm create-healthcheck \
-h hc-timeout=3,hc-count=2,hc-interval=8,hc-test=/var/tmp/my-script hc-myscript
```

`hc-test` spécifie le type de contrôle de l'intégrité.

`hc-interval` spécifie l'intervalle qui sépare chaque contrôle de l'intégrité. Pour éviter la synchronisation, l'intervalle réel est défini de manière aléatoire entre  $0,5 * hc-interval$  et  $1,5 * hc-interval$ .

`hc-timeout` spécifie le délai d'attente au-delà duquel le contrôle de l'intégrité, s'il ne s'exécute pas, est considéré comme un échec.

`hc-count` spécifie le nombre de tentatives autorisé pour exécuter le contrôle de l'intégrité `hc-test`.

---

**Remarque** – Le port pour `hc-test` est spécifié avec le mot-clé `hc-port` dans la sous-commande `create-rule`. Pour plus d'informations, reportez-vous à la page de manuel [ilbadm\(1M\)](#).

---

## Détails sur le test utilisateur

Les critères suivants doivent être respectés par le test fourni par l'utilisateur :

- Il peut s'agir d'un fichier binaire ou d'un script.
- Le test peut résider n'importe où sur le système, et son chemin absolu doit être spécifié dans la sous-commande `create-healthcheck`.

Lorsque vous définissez ce test (par exemple `/var/tmp/my-script`) pour le contrôle de l'intégrité dans la sous-commande `create-rule`, le démon `ilbd` daemon clone un processus et exécute le test comme suit :

```
/var/tmp/my-script $1 $2 $3 $4 $5
```

Voici une description des arguments :

\$1 VIP (adresse IPv4 ou IPv6 littérale)

\$2 IP du serveur (adresse IPv4 ou IPv6 littérale)

\$3 Protocole (UDP, TCP en tant que chaîne)

\$4 Plage de numéros de ports (valeur spécifiée par l'utilisateur pour `hc-port`)

\$5 Délai d'attente maximal (en secondes) au-delà duquel le test renvoie un échec. Si le test dépasse ce délai, il peut être arrêté et considéré comme un échec. Cette valeur est définie par l'utilisateur et spécifiée dans `hc-timeout`.

Le test utilisateur *my-script* peut ou non utiliser tous les arguments, mais il *doit* renvoyer l'un des résultats suivants :

- Délai d'aller-retour en microsecondes
- 0 si le test ne calcule pas le délai d'aller-retour
- -1 en cas d'échec

Par défaut, le contrôle de l'intégrité s'exécute avec les privilèges suivants : `PRIV_PROC_FORK`, `RIV_PROC_EXEC`, `RIV_NET_ICMPACCESS` .

Si un ensemble de privilèges plus étendu est requis, vous devez implémenter `setuid` dans le test. Pour plus d'informations sur les privilèges, reportez-vous à la page de manuel [privileges\(5\)](#).

## Suppression d'un contrôle de l'intégrité

L'exemple suivant supprime un contrôle de l'intégrité appelé *hc1* :

```
# ilbadm destroy-healthcheck hc1
```

## Liste des contrôles de l'intégrité

Vous pouvez utiliser la sous-commande `list-healthcheck` pour obtenir des informations détaillées sur les contrôles de l'intégrité configurés. L'exemple suivant répertorie deux contrôles de l'intégrité configurés :

```
# ilbadm list-healthcheck
```

NAME	TIMEOUT	COUNT	INTERVAL	DEF_PING	TEST
hc1	3	2	8	Y	tcp
hc2	3	2	8	N	/var/usr-script

## Affichage des résultats du contrôle de l'intégrité

Vous pouvez utiliser la sous-commande `list-hc-result` pour obtenir les résultats des contrôles de l'intégrité. Si une règle ou un contrôle de l'intégrité n'est pas spécifié(e), la sous-commande répertorie tous les contrôles de l'intégrité.

L'exemple suivant affiche les résultats des contrôles de l'intégrité associés à la règle `rule1` :

```
# ilbadm list-hc-result rule1
```

RULE	HC	SERVERID	TEST	STATUS	FAIL	LAST	NEXT
rule1	hc1	sg1:0	tcp	server-alive	3	11:23:30	11:23:40
rule1	hc1	sg1:1	tcp	server-dead	4	11:23:30	11:23:40

## Administration des règles ILB

Vous pouvez utiliser la commande `ilbadm` pour créer, supprimer et répertorier les règles d'équilibrage de charge. Pour obtenir la définition d'une règle d'équilibrage de charge et connaître les paramètres nécessaires pour créer une règle, reportez-vous à la section [“Terminologie d'ILB” à la page 358](#).

### ▼ Procédure de création d'une règle

- 1 Créez un groupe de serveurs qui inclut les serveurs d'arrière-plan appropriés.

```
# ilbadm create-servergroup -s server=60.0.0.10:6000-6009,60.0.0.11:7000-7009 sg1
```

- 2 Si vous souhaitez associer des contrôles de l'intégrité du serveur à une règle, créez un objet de contrôle de l'intégrité.  

```
# ilbadm create-healthcheck -h hc-test=tcp,hc-timeout=2,hc-count=3,hc-interval=10 hc1
```
- 3 Identifiez le VIP, le port et le protocole optionnel qui seront associés à la règle.
- 4 Sélectionnez l'opération à utiliser (DSR, Full-NAT ou Half-NAT). Si vous sélectionnez NAT, vous devez spécifier la plage d'adresses IP à utiliser en tant qu'adresse proxy-src.
- 5 Sélectionnez l'algorithme d'équilibrage de charge à utiliser.
- 6 Sélectionnez d'autres fonctions facultatives (reportez-vous à la page de manuel [ilbadm\(1M\)](#) pour plus d'informations).
- 7 Sélectionnez un nom de règle.
- 8 Créez et activez la règle.

```
# ilbadm create-rule -e -i vip=81.0.0.10,port=5000-5009,protocol=tcp\  
-m lbalg=rr,type=NAT,proxy-src=60.0.0.101-60.0.0.104,persist=/24 -h hc-name=hc1 -o servergroup=sg1 rule1
```

### Exemple 23-6 Création d'une règle Full-NAT avec une persistance de session de contrôle de l'intégrité

Cet exemple crée un contrôle de l'intégrité appelé hc1 et un groupe de serveurs appelé sg1 (constitué de deux serveurs, chacun avec une plage de numéros de port). La dernière commande crée et active une règle appelée rule1 du mode Full-NAT, et associe cette règle au groupe de serveurs et au contrôle de l'intégrité. Veuillez noter que la création de la règle doit s'effectuer après la création du groupe de serveurs et du contrôle de l'intégrité.

```
ilbadm create-healthcheck -h hc-test=tcp,hc-timeout=2,hc-count=3,hc-interval=10 hc1  
ilbadm create-servergroup -s server=60.0.0.10:6000-6009,60.0.0.11:7000-7009 sg1  
ilbadm create-rule -e -i vip=81.0.0.10,port=5000-5009,protocol=tcp \  
-m lbalg=rr,type=NAT,proxy-src=60.0.0.101-60.0.0.104,persist=/24  
-h hc-name=hc1 -o servergroup=sg1 rule1
```

Lorsque vous créez une règle NAT/Half NAT, il est recommandé de spécifier la valeur du délai d'attente connection-drain. La valeur par défaut du délai d'attente conn-drain est 0, ce qui signifie que le serveur restera en attente jusqu'à ce qu'une connexion soit fermée.

## Suppression d'une règle

Pour supprimer une règle, utilisez la sous-commande `delete-rule`. Si vous voulez supprimer toutes les règles, utilisez l'option `-a`. L'exemple suivant supprime la règle appelée rule1 :

```
# ilbadm delete-rule rule1
```

## Liste des règles

Pour dresser la liste des informations de configuration d'une règle, utilisez la sous-commande `list - rule`. Si aucun nom de règle n'est spécifié, les informations concernent l'ensemble des règles.

```
# ilbadm list-rule
```

Nom de la règle (+ = activée)	LB-alg	Type	Proto	VIP/port
rule-http +	HIPP	H-NAT	TCP	10.0.0.1/http
rule-dns	HIP	DSR	UDP	10.0.0.1/53
rule-abc	RR	NAT	TCP	2003::1/1024
rule-xyz +	HIPV	NAT	TCP	2003::1/2048-2050

## Affichage des statistiques ILB

Vous pouvez utiliser la commande `ilbadm` pour imprimer des statistiques sur un serveur ou une règle, ou afficher la table NAT et la table des correspondances de persistance de session. Des définitions sont disponibles à la section [“Terminologie d'ILB” à la page 358](#).

## Obtention de statistiques à l'aide de la sous-commande `show-statistics`

Utilisez la sous-commande `show-statistics` pour afficher les informations sur la distribution de charge. L'exemple suivant présente l'usage de la sous-commande `show-statistics` :

```
ilbadm show-statics
PKT_P   BYTES_P   PKT_U   BYTES_U   PKT_D   BYTES_D
9       636       0       0       0       0
```

où

- `PKT_P` : paquets traités
- `BYTES_P` : octets traités
- `PKT_U` : paquets non traités
- `BYTES_U` : octets non traités

## Affichage de la table des connexions NAT

Utilisez la sous-commande `show-nat` pour afficher les informations sur la table des connexions NAT. Il n'existe aucun lien entre les positions relatives des éléments et les exécutions consécutives de cette commande. Par exemple, si vous exécutez deux fois `{ ilbadm show-nat 10 }`, rien de vous garantit que vous obtiendrez deux fois les mêmes 10 éléments, en particulier si votre système est occupé. Si vous ne spécifiez pas de nombre, la table des connexions NAT entière s'affiche.

L'exemple suivant présente cinq entrées de la table des connexions NAT.

**EXEMPLE 23-7** Entrées de table des connexions NAT `ilbadm show-nat 5`

```
UDP: 124.106.235.150.53688 > 85.0.0.1.1024 >>> 82.0.0.39.4127 > 82.0.0.56.1024
UDP: 71.159.95.31.61528 > 85.0.0.1.1024 >>> 82.0.0.39.4146 > 82.0.0.55.1024
UDP: 9.213.106.54.19787 > 85.0.0.1.1024 >>> 82.0.0.40.4114 > 82.0.0.55.1024
UDP: 118.148.25.17.26676 > 85.0.0.1.1024 >>> 82.0.0.40.4112 > 82.0.0.56.1024
UDP: 69.219.132.153.56132 > 85.0.0.1.1024 >>> 82.0.0.39.4134 > 82.0.0.55.1024
```

Le format des entrées est le suivant :

T: IP1 > IP2 >>> IP3 > IP4

T: The transport protocol used in this entry.

IP1: The client's IP address and port.

IP2: The VIP and port.

IP3: If half-NAT mode, the client's IP address and port.

If full-NAT mode, the client's IP address and port.

IP4: The back-end server's IP address and port.

## Affichage de la table des correspondances de persistance de session

Utilisez la sous-commande `show-persist` pour afficher la table des correspondances de persistance de session.

**EXEMPLE 23-8** `ilbadm show-persist 5`

L'exemple suivant présente cinq entrées de cette table :

```
rule2: 124.106.235.150 --> 82.0.0.56
rule3: 71.159.95.31 --> 82.0.0.55
rule3: 9.213.106.54 --> 82.0.0.55
rule1: 118.148.25.17 --> 82.0.0.56
rule2: 69.219.132.153 --> 82.0.0.55
```

Le format des entrées est le suivant :

R: IP1 --> IP2

R: The rule that this persistence entry is tied to.

EXEMPLE 23-8 `ilbadm show-persist 5` (Suite)

IP1: The client's IP address.

IP2: The back-end server's IP address.

## Utilisation des sous-commandes Import et Export

La sous-commande `export` exporte la configuration actuelle dans un fichier utilisateur. Ces informations peuvent alors être utilisées en entrées de la sous-commande `import`. La sous-commande `import` supprime la configuration existante avant l'importation, sauf mention contraire. L'omission d'un nom de fichier demande à la commande de lire à partir d'une entrée standard ou d'écrire dans une sortie standard.

Pour exporter une configuration ILB, utilisez la commande `export-config`. L'exemple suivant exporte la configuration actuelle dans le fichier `/var/tmp/ilb_config`, sous un format adapté à l'importation avec la commande `import` :

```
# ilbadm export-config /var/tmp/ilb_config
```

Pour importer une configuration ILB, utilisez la commande `import-config`. L'exemple suivant lit le contenu de configuration du fichier `/var/tmp/ilb_config` et remplace la configuration existante :

```
# ilbadm import-config /var/tmp/ilb_config
```





## Protocole de redondance de routeur virtuel (VRRP) (Présentation)

---

Le protocole de redondance de routeur virtuel (VRRP) est un protocole internet standard spécifié dans le document [Virtual Router Redundancy Protocol Version 3 for IPv4 and IPv6](#) et il est pris en charge dans Oracle Solaris pour fournir une haute disponibilité. Oracle Solaris fournit un outil d'administration qui configure et gère le service VRRP.

Lorsque vous définissez un réseau, un LAN par exemple, il est très important de fournir un service de haute disponibilité. Une manière d'augmenter la fiabilité du réseau consiste à fournir des sauvegardes des composants critiques dans le réseau. L'ajout de composants tels que des routeurs, des commutateurs et des liaisons au réseau assure la continuité du service malgré les défaillances. La fourniture de redondance aux extrémités d'un réseau est une tâche cruciale qui peut être effectuée facilement avec VRRP. Les routeurs virtuels peuvent être introduits dans le LAN à l'aide de VRRP afin d'assurer la restauration après panne pour un routeur.

Pour en savoir plus sur les termes utilisés dans VRRP, reportez-vous à la section [“Terminologie VRRP”](#) à la page 394.

Ce chapitre se compose des sections suivantes :

- [“Terminologie VRRP”](#) à la page 394
- [“Présentation de l'architecture VRRP”](#) à la page 395
- [“Restrictions de VRRP”](#) à la page 397

VRRP est un protocole d'élection qui attribue de façon dynamique les responsabilités d'un routeur virtuel à l'un des routeurs VRRP présents dans le LAN. VRRP fournit un ou plusieurs routeurs secondaires pour un routeur configuré statistiquement sur le LAN.

Un routeur VRRP appelé routeur maître contrôle la ou les adresse(s) IPv4 ou IPv6 associée(s) au routeur virtuel. Le routeur virtuel transmet les paquets envoyés à l'adresse IP du routeur maître.

Le processus d'élection fournit le basculement dynamique tout en transférant les paquets envoyés à ces adresses IP. VRRP élimine le point d'échet unique qui est inhérent à l'environnement statique routé par défaut.

L'utilisation de la fonctionnalité VRRP dans Oracle Solaris permet de disposer d'un chemin d'accès par défaut hautement disponible pour le processus de routage sans avoir à configurer le routage dynamique ou les protocoles de détection de routeur sur chaque hôte final.

## Terminologie VRRP

Cette section décrit certains termes utiles à connaître lors de l'implémentation de VRRP sur vos systèmes.

<b>Routeur de secours</b>	Instance VRRP pour un VRID actif mais pas en état maître. Un VRID peut avoir n'importe quel nombre de routeurs de secours. Un routeur de secours est prêt à prendre le rôle du routeur maître en cas de défaillance de ce dernier.
<b>Routeur maître</b>	Instance VRRP qui assure la fonction de routage pour le routeur virtuel à un moment donné. Un seul routeur maître est actif à la fois pour un VRID donné.
<b>Adresse IP virtuelle</b>	Adresse IP associée à un VRID auprès duquel d'autres hôtes peuvent obtenir un service réseau. La VRIP est gérée par les instances VRRP appartenant à un VRID.
<b>Adresse MAC virtuelle</b>	Adresse MAC prédéfinie utilisée par des instances VRRP tout en s'exécutant dans un média, par exemple Ethernet qui utilise les adresses MAC. Une adresse MAC virtuelle isole le fonctionnement du routeur virtuel du routeur réel qui fournit la fonction de routage et on l'utilise à la place de l'adresse MAC réelle. Une adresse MAC virtuelle est dérivée du VRID.
<b>VRID (ID de routeur virtuel)</b>	Numéro unique utilisé pour identifier un routeur virtuel. Les VRID doivent être uniques sur un segment de réseau donné.
<b>VNIC</b>	Une pseudo interface réseau configurée sur un adaptateur réseau physique également appelée NIC (network interface card, carte d'interface réseau). Une interface physique peut avoir plusieurs VNIC. Les VNIC sont des composants essentiels de la virtualisation de réseau. Pour plus d'informations, reportez-vous à la <a href="#">Partie III, "Virtualisation du réseau et gestion des ressources" du manuel <i>Administration d'Oracle Solaris : interfaces réseau et virtualisation réseau</i></a> .
<b>Instance VRRP</b>	Programme s'exécutant sur un routeur à l'aide de l'implémentation VRRP. Une instance VRRP unique peut fournir des fonctionnalités VRRP à plusieurs routeurs virtuels.
<b>Routeur VRRP</b>	Image de routeur unique créée par le fonctionnement d'un ou plusieurs routeurs qui utilisent VRRP.

# Présentation de l'architecture VRRP

## Routeur VRRP

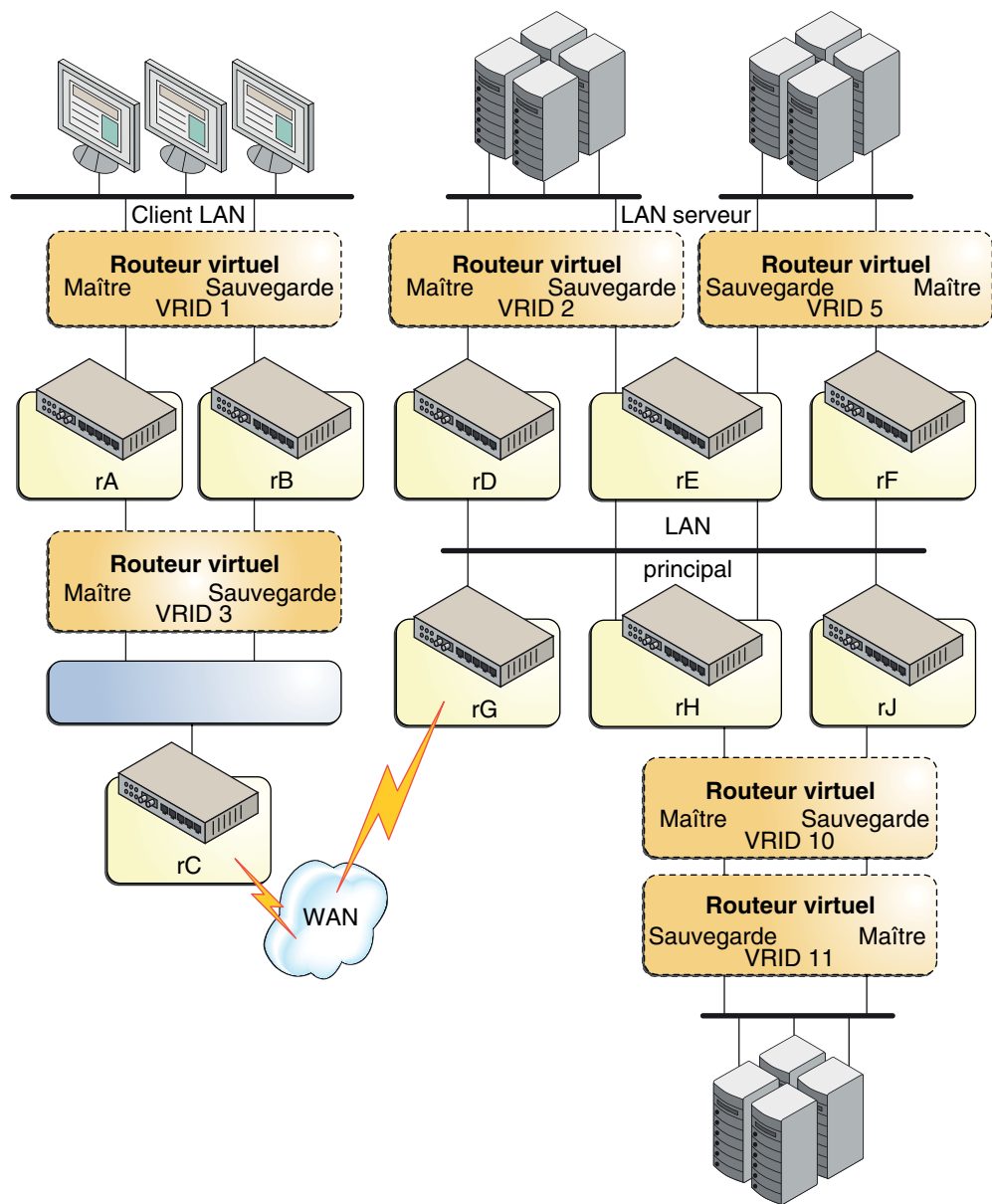
VRRP s'exécute sur chaque routeur VRRP et gère l'état du routeur. Un hôte peut disposer de plusieurs routeurs VRRP configurés, où chaque routeur VRRP appartient à un routeur virtuel différent.

Un routeur VRRP dispose des attributs suivants :

- Nom de routeur : identifiant unique à l'échelle du système
- VRID : identifie le routeur virtuel au sein d'un LAN
- Adresse IP principale : utilisée en tant qu'adresse IP source de la publication VRRP
- Adresses IP virtuelles
- Paramètres VRRP : incluent la priorité, l'intervalle de publication, le mode de préemption et le mode d'acceptation
- Informations d'état et statistiques VRRP

## Processus VRRP

La figure suivante illustre le fonctionnement de VRRP.



Comme illustré dans la figure précédente, VRRP fonctionne en utilisant les composants suivants :

- Le routeur rA est le routeur maître du routeur virtuel VRID 1 et le routeur de secours pour VRID 3. Le routeur rA assure le routage des paquets adressés au VIP pour VRID 1 et il est prêt à prendre le rôle de routage pour VRID 3.
- Le routeur rB est le routeur maître du routeur virtuel VRID 3 et le routeur de secours pour VRID 1. Le routeur rB assure le routage des paquets adressés au VIP pour VRID 3 et il est prêt à prendre le rôle de routage pour VRID 1.
- Le routeur rC ne dispose pas des fonctions VRRP, mais il utilise la VIP pour VRID 3 afin d'atteindre le sous-réseau LAN du client.
- Le routeur rD est le routeur maître pour VRID 2. Le routeur rF est le routeur maître pour VRID 5. Le routeur rE est le routeur de secours pour ces deux VRID. En cas de défaillance de rD ou de rF, rE devient le routeur maître pour ce VRID. rD et rF pourraient tomber en panne en même temps. Le fait qu'un routeur VRRP soit un routeur maître pour un VRID ne l'empêche pas d'être un routeur maître pour un autre VRID.
- Le routeur rG est la passerelle WAN pour le LAN constituant l'épine dorsale. Tous les routeurs connectés à l'épine dorsale partagent des informations de routage avec les routeurs sur le WAN en utilisant un protocole de routage dynamique comme OSPF. VRRP n'est pas impliqué dans ces opérations, mais le routeur rC indique que le chemin d'accès au sous-réseau LAN du client passe par la VIP de VRID 3.
- Le routeur rH est le routeur maître pour VRID 10 et le routeur de secours pour VRID 11. De même, le routeur rJ est le routeur maître pour VRID 11 et le routeur de secours pour VRID 10. Cette configuration de partage de charge VRRP montre que plusieurs VRID peuvent exister sur une interface de routeur unique.

VRRP peut être utilisé en tant que partie d'une conception réseau qui fournit une redondance de routage quasiment totale pour tous les systèmes sur le réseau.

## Restrictions de VRRP

### Prise en charge de zone en mode IP exclusif

Dans chaque zone en mode IP exclusif, le service VRRP `svc:/network/vrrp/default` est activé automatiquement en cas de création de tout routeur VRRP dans cette zone. Le service VRRP gère le routeur VRRP pour cette zone spécifique.

Cependant, la prise en charge d'une zone en mode IP exclusif est limitée pour les raisons suivantes :

- VNIC ne peut pas être créé dans une zone non globale. Par conséquent, commencez par créer la VNIC VRRP dans la zone globale, puis assignez la VNIC à la zone non globale où réside le routeur VRRP. Le routeur VRRP peut alors être créé et démarré dans la zone non globale à l'aide de la commande `vrpadm`.
- Dans un système Oracle Solaris unique, la création de deux routeurs VRRP dans des zones différentes partageant le même routeur virtuel n'est pas possible. En effet, Oracle Solaris ne permet pas de créer deux VNIC avec la même adresse MAC.

## Interopérations avec les autres fonctionnalités réseau

Le service VRRP ne peut pas fonctionner sur une interface IPMP (IP Network Multipathing, multipathing sur réseau IP). En effet, VRRP nécessite des adresses MAC spécifiques à VRRP tandis qu'IPMP fonctionne totalement dans la couche IP.

En outre, les adresses IP virtuelles VRRP peuvent uniquement être configurées de façon statique et ne peuvent pas être configurées automatiquement par les deux outils existants de configuration automatique d'adresses IP : `in.ndpd` pour la configuration automatique IPv6 et `dhcpage` pour la configuration DHCP. Les routeurs VRRP maître et de secours (VNIC) partageant la même adresse MAC, `in.ndpd` et `dhcpage` peuvent être confondus. Des résultats inattendus sont susceptibles de survenir. Par conséquent, la configuration automatique IPv6 et les configurations DHCP ne sont pas prises en charge par les VNIC VRRP. Si vous configurez la configuration automatique IPv6 ou DHCP sur une VNIC VRRP, la tentative d'affichage de l'adresse IP configurée automatiquement échoue, tout comme l'opération de configuration automatique.

## Configuration VRRP - Tâches

---

Un routeur VRRP exécute VRRP et fonctionne avec d'autres routeurs VRRP participant au même routeur virtuel. VRRP dispose d'un jeu d'adresses IP virtuelles

Ce chapitre est constitué des sections suivantes :

- “Création de VNIC VRRP” à la page 400
- “Configuration de vrpadm” à la page 400
- “Considérations de sécurité” à la page 403

Dans un LAN, chaque routeur virtuel est identifié de façon unique par le VRID, la famille d'adresse, et il est associé à un jeu d'adresses IP virtuelles protégées.

Chaque routeur VRRP participant est doté de paramètres supplémentaires comme la priorité, l'intervalle de publication et le mode d'acceptation. Seul un routeur VRRP (le routeur maître) à la fois peut endosser la responsabilité du routeur virtuel et transférer les paquets envoyés aux adresses IP virtuelles.

En cas de défaillance du routeur maître, les autres routeurs VRRP participants détectent son absence et un autre routeur VRRP sera choisi en tant que routeur maître et en assumera les responsabilités.

Tous les routeurs VRRP dotés du même routeur virtuel partagent la même adresse MAC virtuelle VRRP. L'adresse MAC virtuelle est calculée en fonction de la famille d'adresses et du VRID du routeur virtuel (en format hexadécimal dans l'ordre standard de bits Internet).  
Exemple :

IPv4: 00-00-5E-00-01-{VRID}

IPv6: 00-00-5E-00-02-{VRID}

Par conséquent, il faut commencer par créer une VNIC VRRP spéciale avec l'adresse MAC virtuelle pour que le routeur VRRP fonctionne correctement. Toutes les adresses IP résidant sur cette VNIC sont considérées comme des adresses IP virtuelles protégées par le routeur VRRP.

Ces adresses IP virtuelles résident dans le routeur de secours et sont utilisées lorsque le routeur devient le routeur principal, fournissant ainsi une haute disponibilité pour ces adresses IP virtuelles.

## Création de VNIC VRRP

La sous-commande `dladm create-vnic` existante a été étendue afin de vous permettre de créer la VNIC VRRP. La syntaxe est la suivante :

```
# dladm create-vnic [-t] [-R root-dir] [-l link] [-m vrrp -V VRID -A
{inet | inet6}] [-v vlan-id] [-p prop=value[,...]] vnic-link
```

Un nouveau type d'adresse VNIC, `vrrp`, a été introduit. Vous devez spécifier le VRID et la famille d'adresse avec ce nouveau type d'adresse VNIC.

Par conséquent, une VNIC avec une adresse MAC de routeur virtuel bien connu sera créée.

## Configuration de `vrrpadm`

Les sections suivantes récapitulent les sous-commandes `vrrpadm`. Reportez-vous à la page de manuel [vrrpadm\(1M\)](#) pour plus d'informations. Toutes les sous-commandes sont persistantes excepté la sous-commande `vrrpadm show-router`. Par exemple, le routeur VRRP créé par `vrrpadm create-router` est conservé après réinitialisation.

### Sous-commande `vrrpadm create-router`

La sous-commande `vrrpadm create-router` crée un routeur VRRP avec le VRID spécifié et la famille d'adresse avec les paramètres donnés. Une VNIC VRRP spéciale doit être créée pour chaque routeur VRRP et la VNIC peut être créée avec la commande `dladm create-vnic`. Pour plus d'informations, reportez-vous à la page de manuel [vrrpadm\(1M\)](#). La syntaxe est la suivante :

```
# vrrpadm create-router -V vrid -l link -A {inet | inet6} [-p \
priority] [-i adv-interval] [-o flags]router-name
```

L'option `-o` est utilisée pour configurer les modes de préemption et d'acceptation du routeur VRRP. Les valeurs peuvent être les suivantes : `preempt`, `un_preempt`, `accept`, `no_accept`. Par défaut, les deux modes sont définis sur `true`.

La valeur `router-name` est utilisée en tant qu'identifiant unique de ce routeur VRRP et elle est utilisée dans les autres sous-commandes `vrrpadm`. Les caractères autorisés pour les noms de routeur sont : les caractères alphanumériques (a-z, A-Z, 0-9) et le trait de soulignement ('\_'). La longueur maximale du nom d'un routeur est de 31 caractères.



## Sous-commande vrrpadm modify-router

La sous-commande `vrrpadm modify-router` modifie la configuration d'un routeur VRRP spécifié. La syntaxe est la suivante :

```
# vrrpadm modify-router [-p priority] [-i adv-interval] [-o flags] \
router-name
```

## Sous-commande vrrpadm delete-router

La sous-commande `vrrpadm delete-router` supprime un routeur VRRP spécifié. La syntaxe est la suivante :

```
# vrrpadm delete-router router-name
```

## Sous-commande vrrpadm disable-router

Un routeur VRRP ne fonctionne pas tant qu'il n'est pas activé. Par défaut, un routeur VRRP est activé lors de sa création initiale. Cependant, il est parfois utile de désactiver temporairement un routeur VRRP afin de pouvoir effectuer des modifications de configuration, puis de réactiver le routeur. La syntaxe est la suivante :

```
# vrrpadm disable-router router-name
```

## Sous-commande vrrpadm enable-router

Un routeur VRRP désactivé peut être réactivé à l'aide de la sous-commande `enable-router`. La liaison de données sous-jacente sur laquelle le routeur VRRP est créé (spécifiée par l'option `-l` lors de la création du routeur avec `vrrpadm create-router`) et la VNIC du routeur VRRP doivent exister lors de l'activation du routeur. Si ce n'est pas le cas, l'opération d'activation échoue. La syntaxe est la suivante :

```
# vrrpadm enable-router router-name
```

## Sous-commande vrrpadm show-router

La sous-commande `vrrpadm show-router` affiche la configuration et l'état d'un routeur VRRP spécifié. Pour plus d'informations, reportez-vous à la page de manuel [vrrpadm\(1M\)](#). La syntaxe est la suivante :

```
# vrrpadm show-router [-P | -x] [-p] [-o field[,...]] [router-name]
```

Vous trouverez ci-dessous des exemples de sortie `vrrpadm show-router` :

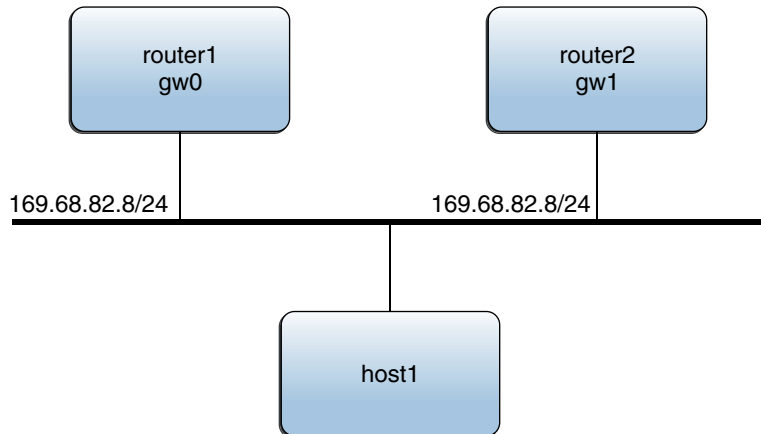
```
# vrrpadm show-router vrrp1
NAME VRID LINK AF PRIO ADV_INTV MODE STATE VNIC
vrrp1 1 bge1 IPv4 100 1000 e-pa- BACK vnic1

# vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK MAST 1m17s vnic1 10.0.0.100 10.0.0.1

# vrrpadm show-router -P vrrp1
NAME PEER P_PRIO P_INTV P_ADV_LAST M_DOWN_INTV
vrrp1 10.0.0.123 120 1000 0.313s 3609
```

#### EXEMPLE 25-1 Exemple de configuration VRRP

La figure suivante illustre une configuration VRRP standard.



Dans cet exemple, l'adresse IP 169.68.82.8 est configurée en tant que passerelle par défaut pour host1. Cette adresse IP est l'adresse IP virtuelle protégée par le routeur virtuel composé de deux routeurs VRRP : router1 et router2. Seul l'un des deux routeurs fait office à tout moment donné de routeur maître, c'est-à-dire qu'il assume les responsabilités du routeur virtuel et transfère les paquets en provenance de host1.

Si l'on suppose que le VRID du routeur virtuel est 12, vous trouverez ci-dessous les étapes utilisées pour réaliser la configuration VRRP précédente sur router1 et router2. Le routeur router1 est le propriétaire de l'adresse IP virtuelle 169.68.82.8 et sa priorité est la valeur par défaut (255). Le routeur router2 est le routeur de secours dont la priorité est 100.

```
router1:
# dladm create-vnic -m vrrp -V 12 -A inet -l gw0 vnic1
# vrrpadm create-router -V 12 -A inet -l gw0 vrrp1
# ipadm create-addr -T static -d -a 169.68.82.8/24 vnic1/router1
```

**EXEMPLE 25-1** Exemple de configuration VRRP (Suite)

```
# ipadm create-addr -T static -d -a 169.68.82.100/24 gw0/router1
# vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MAST BACK 1m17s vnic1 169.68.82.100 169.68.82.8
router2:
# dladm create-vnic -m vrrp -V 12 -A inet -l gw1 vnic1
# vrrpadm create-router -V 12 -A inet -l gw1 -p 100 vrrp1
# ipadm create-addr -T static -d -a 169.68.82.8/24 vnic1/router2
# ipadm create-addr -T static -d -a 169.68.82.101/24 gw0/router2
# vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 BACK INIT 2m32s vnic1 169.68.82.101 169.68.82.8
```

En utilisant la configuration de router1 comme exemple, vous devez configurer au moins une adresse IP sur gw0. Dans l'exemple suivant, cette adresse IP de router1 est l'adresse IP principale qui est utilisée pour envoyer les paquets de publication VRRP :

```
# vrrpadm show-router -x vrrp1
NAME STATE PRV_STAT STAT_LAST VNIC PRIMARY_IP VIRTUAL_IPS
vrrp1 MAST BACK 1m17s vnic1 169.68.82.100 169.68.82.8
```

## Considérations de sécurité

Une nouvelle autorisation `solaris.network.vrrp` a été introduite et elle est requise pour configurer le service VRRP. Notez que l'opération en lecture seule - `vrrpadm showrouter` ne nécessite pas cette autorisation.

L'autorisation `solaris.network.vrrp` a été ajoutée au profil de gestion réseau.



# Implémentation du contrôle de congestion

Ce chapitre décrit l'implémentation du contrôle de congestion dans Oracle Solaris. Des contrôles sont définis afin d'éviter la congestion du trafic TCP et SCTP.

## Congestion du réseau et contrôle de congestion

La congestion du réseau se traduit généralement par des dépassements du tampon du routeur, lorsque les noeuds envoient plus de paquets que le réseau ne peut en gérer. Divers algorithmes empêchent la congestion du trafic en établissant des contrôles sur les systèmes d'envoi. Ces algorithmes sont pris en charge par Oracle Solaris et peuvent être facilement ajoutés ou directement placés dans le système d'exploitation.

Le tableau suivant répertorie et décrit les algorithmes pris en charge.

Algorithme	Nom du SE Oracle Solaris	Description
NewReno	newreno	Algorithme par défaut dans Oracle Solaris. Ce mécanisme de contrôle est basé sur une fenêtre de congestion de l'expéditeur et les mécanismes de Slow Start (démarrage lent) et de Congestion Avoidance (anti-congestion).
HighSpeed	highspeed	L'une des versions modifiées les plus connues et les plus simples de NewReno pour les réseaux rapides.
CUBIC	cubic	Algorithme par défaut actuel dans Linux 2.6. Avec cet algorithme, la phase Congestion Avoidance passe d'une augmentation linéaire du fenêtrage à une fonction cubique.

Algorithme	Nom du SE Oracle Solaris	Description
Vegas	vegas	Algorithme classique basé sur la temporisation, qui tente de prédire la congestion sans déclencher une perte réelle de paquets.

Pour activer le contrôle de congestion dans Oracle Solaris, les propriétés de contrôle TCP suivantes doivent être définies. Bien que ces propriétés concernent le trafic TCP, le mécanisme de contrôle activé par ces propriétés s'applique également au trafic SCTP.

- `cong_enabled` : contient une liste d'algorithmes, séparés par des virgules, actuellement opérationnels dans le système. Vous pouvez ajouter ou supprimer des algorithmes pour n'utiliser que ceux qui vous intéressent.
- `cong_default` : algorithme utilisé par défaut lorsqu'aucun algorithme n'est spécifié explicitement dans les options de socket des applications. Actuellement la valeur de la propriété `cong_default` s'applique aux zones globales et non globales.

Pour définir ces propriétés, vous utilisez la commande `ipadm set-prop`. Vous utilisez le modificateur `+=` pour ajouter un algorithme ou le modificateur `-=` pour en supprimer un.

## ▼ Procédure d'implémentation du contrôle de congestion du réseau TCP et SCTP

**1 Connectez-vous en tant qu'administrateur.**

Pour plus d'informations, reportez-vous à la section “[Procédure d'obtention des droits d'administration](#)” du manuel *Administration d'Oracle Solaris : services de sécurité*.

**2 Affichez les valeurs actuelles des propriétés de contrôle de congestion du protocole TCP.**

```
# ipadm show-prop -p cong_enabled,cong_default tcp
```

Si vous ne spécifiez pas ces propriétés, elles s'affichent toutes.

Cette commande affiche les valeurs actuelles ainsi que les algorithmes possibles qui peuvent être assignés aux propriétés.

**3 Définissez les propriétés de contrôle de congestion du protocole TCP.**

```
# ipadm set-prop -p cong-ctrl-property+=algorithm tcp
```

où

*cong-ctrl-property*      Désigne la propriété `cong_enabled` ou `cong_default`.

*algorithm*                Spécifie l'algorithme que vous définissez pour la propriété. Vous pouvez définir n'importe quel algorithme répertorié sous le champ POSSIBLE, en

début de sortie de la commande `ipadm show-prop`.

**4 (Facultatif) Supprimez un algorithme actuellement activé.**

```
# ipadm set-prop -p cong-ctrl-property-=algorithm tcp
```

---

**Remarque** – L'ajout ou la suppression d'algorithmes n'est soumise à aucune règle de séquence. Vous pouvez supprimer un algorithme avant d'en ajouter d'autres à une propriété. Cependant, vous devez toujours définir un algorithme pour la propriété `cong_default`.

---

**5 (Facultatif) Affichez les nouvelles valeurs des propriétés de contrôle de congestion.**

```
# ipadm show-prop -p cong_enabled,cong_default tcp
```

**Exemple 26–1 Définition des algorithmes pour le contrôle de congestion**

Cet exemple remplace l'algorithme `newreno` défini par défaut pour le protocole TCP par l'algorithme `cubic`. Il supprime également `vegas` de la liste des algorithmes activés.

```
# ipadm show-prop -p cong_default,cong_enabled tcp
PROTO  PROPERTY  PERM  CURRENT          PERSISTENT  DEFAULT  POSSIBLE
tcp     cong_default  rw    newreno          --          newreno  -
tcp     cong_enabled  rw    newreno,cubic,  --          newreno  newreno,cubic,
                                     highspped,    highspped,vegas
                                     vegas

# ipadm set-prop -p cong_enabled-=vegas tcp
# ipadm set-prop -p cong_default=cubic tcp

# ipadm show-prop -p cong_default,cong_enabled tcp
PROTO  PROPERTY  PERM  CURRENT          PERSISTENT  DEFAULT  POSSIBLE
tcp     cong_default  rw    cubic            --          newreno  -
tcp     cong_enabled  rw    newreno,cubic,  --          newreno  newreno,cubic,
                                     highspped    highspped,vegas
```





## PARTIE V

# Qualité de service IP (IPQoS)

Cette partie décrit les tâches et les informations concernant la qualité de service IP (IPQoS) et l'implémentation des services différenciés d'Oracle Solaris.



## Présentation d'IPQoS (généralités)

---

La qualité de service IP (IPQoS) permet de hiérarchiser, de contrôler et de recueillir les statistiques comptables. A l'aide d'IPQoS, vous pouvez fournir des niveaux de service homogènes aux utilisateurs de votre réseau. Cela permet également de gérer le trafic pour éviter la congestion du réseau.

Voici la liste des sujets abordés dans ce chapitre :

- “Principes de base d'IPQoS” à la page 411
- “Livraison d'une qualité de service avec IPQoS” à la page 414
- “Amélioration de l'efficacité du réseau dans IPQoS” à la page 415
- “Modèle de services différenciés” à la page 417
- “Trafic sur un réseau compatible IPQoS” à la page 422

### Principes de base d'IPQoS

IPQoS active l'architecture de services différenciés (Diffserv) qui est défini par le groupe de travail de l'IETF, The Differentiated Services Working Group. Dans Oracle Solaris, le composant IPQoS est implémenté au niveau de l'IP de la pile du protocole TCP/IP.

### Quels sont les services différenciés ?

En activant IPQoS, vous fournissez différents niveaux de service réseau aux clients et aux applications sélectionnés. Les différents niveaux de service sont collectivement désignés sous l'appellation de *services différenciés*. Les services différenciés fournis aux clients peuvent se baser sur la structure des niveaux de service offerts par l'entreprise à ses clients. Vous pouvez également fournir des services différenciés en fonction des priorités définies pour les applications ou les utilisateurs de votre réseau.

Offrir une qualité de service implique les activités suivantes :

- Déléguer des niveaux de service à différents groupes (clients ou services d'une entreprise, par exemple)
- Définir la priorité des services réseau attribuée à certains groupes ou applications
- Discerner et éliminer les goulots d'étranglement ou toute autre forme de congestion
- Contrôler les performances réseau et fournir des statistiques sur les performances
- Réguler la bande passante au vu des ressources réseau

## Fonctions IPQoS

IPQoS possède les fonctions suivantes :

- `ipqosconf`, outil au niveau de la ligne de commande pour configurer la stratégie QoS
- Classificateur sélectionnant les actions, selon les filtres configurant la stratégie QoS de votre organisation
- Module de mesure du trafic réseau conformé au modèle Diffserv
- Différenciation des services basée sur la possibilité de marquer un en-tête IP de paquet avec des informations de transmission
- Module de comptabilisation des flux rassemblant les statistiques des flux de trafic
- Statistiques sur les classes de trafic, via la commande UNIX® `kstat`
- Prise en charge de l'architecture SPARC® et x86
- Prise en charge des adresses IPv4 et IPv6
- Interopérabilité avec l'architecture de sécurité IP (IPsec)
- Prise en charge des marquages de priorité utilisateur 802.1D dans les réseaux locaux virtuels (VLAN)

## Sources d'informations sur la théorie de la qualité de service et les techniques

Vous trouverez des informations sur les services différenciés et la qualité de service dans la documentation papier ou en ligne.

### Ouvrages sur la qualité de service

Pour plus d'informations sur la théorie de la qualité de service et ses applications, reportez-vous aux publications suivantes :

- Ferguson, Paul et Geoff Huston. *Quality of Service*. John Wiley & Sons, Inc., 1998.
- Kilkki, Kalevi. *Differentiated Services for the Internet*. Macmillan Technical Publishing, 1999.

## Documents RFC (Request For Comments) sur la qualité de service

IPQoS se conforme aux spécifications décrites dans les RFC et les documents de travail Internet suivants :

- Le document [RFC 2474, Definition of the Differentiated Services Field \(DS Field\) in the IPv4 and IPv6 Headers](http://www.ietf.org/rfc/rfc2474.txt?number=2474) (<http://www.ietf.org/rfc/rfc2474.txt?number=2474>) (en anglais) décrit une amélioration du champ de type de service (ToS) ou champ DS des en-têtes de paquet IPv4 et IPv6 pour la prise en charge des services différenciés
- Le document [RFC 2475, An Architecture for Differentiated Services](http://www.ietf.org/rfc/rfc2475.txt?number=2475) (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>) (en anglais) décrit en détail l'organisation et les modules de l'architecture Diffserv
- Le document [RFC 2597, Assured Forwarding PHB Group](http://www.ietf.org/rfc/rfc2597.txt?number=2597) (<http://www.ietf.org/rfc/rfc2597.txt?number=2597>) (en anglais) décrit le fonctionnement du comportement AF (Assured Forwarding, transfert assuré) par saut
- Le document [RFC 2598, An Expedited Forwarding PHB](http://www.ietf.org/rfc/rfc2598.txt?number=2598) (<http://www.ietf.org/rfc/rfc2598.txt?number=2598>) (en anglais) décrit le fonctionnement du comportement EF (Expedited Forwarding, transfert accéléré) par saut
- Document de travail Internet, *An Informal Management Model for Diffserv Routers* : présente un modèle pour l'implémentation de l'architecture Diffserv sur les routeurs.

## Sites Web donnant des informations sur la qualité de service

Le groupe de travail Differentiated Services Working Group de l'IETF gère un site Web comportant des liens renvoyant vers des document de travail Internet à l'adresse <http://www.ietf.org/html.charters/diffserv-charter.html>.

Les fabricants de routeur tels que Cisco Systems et Juniper Networks fournissent des informations sur leur sites Web ; ces derniers décrivent la manière dont les services différenciés sont implémentés dans leurs produits.

## Pages de manuel IPQoS

Documentation IPQoS inclut les pages de manuel suivantes :

- [ipqosconf\(1M\)](#) : décrit la commande permettant de paramétrer le fichier de configuration IPQoS
- [ipqos\(7ipp\)](#) : décrit l'implémentation IPQoS du modèle d'architecture Diffserv
- [ipgpc\(7ipp\)](#) : décrit l'implémentation IPQoS d'un classificateur Diffserv
- [tokenmt\(7ipp\)](#) : décrit le module de mesure tokenmt d'IPQoS
- [tswtclmt\(7ipp\)](#) : décrit le module de mesure tswtclmt d'IPQoS
- [dscpmk\(7ipp\)](#) : décrit le module de marquage DSCP
- [dlcosmk\(7ipp\)](#) : décrit le module de marquage de priorité utilisateur IPQoS 802.1D

- `flowacct(7ipp)` : décrit le module de comptabilisation des flux IPQoS
- `acctadm(1M)` : décrit la commande permettant de configurer les fonctions de comptabilité étendues d'Oracle Solaris. La commande `acctadm` inclut des extensions IPQoS.

## Livraison d'une qualité de service avec IPQoS

Les fonctions IPQoS permettent aux fournisseurs d'accès Internet (FAI) ainsi qu'aux fournisseurs de services d'applications (ASP) d'offrir différents niveaux de service réseau à leurs clients. Ces fonctions permettent à des sociétés et à des organismes d'éducation ou de formation de hiérarchiser les services pour des organisations internes ou pour les applications principales.

### Implémentation des accords de niveau de service

Si votre organisation est un FAI ou un fournisseur de services d'applications, vous pouvez baser votre configuration IPQoS sur l'*accord de niveau de service* que votre entreprise propose à ses clients. Dans le cadre d'un accord de niveau de service, un fournisseur de service garantit à un client un certain niveau de service réseau basé sur une hiérarchie de prix. Par exemple, un accord de type premium implique que le client reçoive la plus haute priorité pour tous les types de trafic réseau 24 h/24h 7j/7. Inversement, un accord facturé à un prix moyen indique que le client bénéficie d'une haute priorité pour la transmission des messages électroniques uniquement pendant les heures d'ouverture de bureau. Tout autre trafic se voit appliquer une priorité moyenne 24 h/24h.

### Garantie d'une qualité de service pour une organisation

Si votre organisation est une entreprise ou une institution, vous pouvez également utiliser différentes fonctions liées à la qualité de service pour votre réseau. Ainsi, il est possible d'appliquer un degré de service plus ou moins élevé au trafic d'un groupe ou d'une application spécifique.

### Introduction à la stratégie de qualité de service

Vous implémentez la qualité de service en définissant une *stratégie de qualité de service (QoS)*. La stratégie de qualité de service spécifie plusieurs attributs de réseau comme la priorité des clients ou des applications et les actions pour le traitement de différentes catégories de trafic. Vous implémentez la stratégie de qualité de service de votre organisation dans un fichier de configuration IPQoS. Ce fichier configure les modules IPQoS se trouvant dans le noyau Oracle Solaris. Un hôte auquel une stratégie IPQoS est appliquée est considéré comme un *système IPQoS*.

Votre stratégie QoS définit les éléments suivants :

- Des groupes discrets de trafic réseau appelés *classes de service*.
- Des mesures de régulation du volume du trafic réseau de chaque classe. Elles régissent le processus de contrôle du trafic appelé *mesure*.
- Une action qu'un système IPQoS et un routeur Diffserv doivent appliquer à un flux de paquets. Ce type d'action est désigné comme le *PHB* (per-hop behavior ou comportement par pas).
- Toute collecte de statistiques dont votre organisation a besoin sur une classe de service. Citons par exemple, le trafic généré par un client ou une application spécifique.

Lorsque les paquets arrivent sur le réseau, le système IPQoS évalue les en-têtes de paquets. L'action que le système IPQoS réalise est déterminée par votre stratégie QoS.

Les tâches pour élaborer la conception de la stratégie QoS sont décrites dans la section [“Planification de la stratégie de qualité de service” à la page 431](#).

## Amélioration de l'efficacité du réseau dans IPQoS

IPQoS contient des fonctions qui contribuent à augmenter l'efficacité des performances réseau lors de l'implémentation de la qualité de service. Au fur et à mesure que le réseau d'ordinateurs s'étend, la nécessité de gérer le trafic réseau engendré par un nombre croissant d'utilisateurs et des processeurs plus puissants se fait plus grande. Un réseau surexploité peut manifester certains signes, par exemple, des pertes de données ou une congestion du trafic. Ces signes se traduisent par des délais de réponse très lents.

Par le passé, les administrateurs système géraient les problèmes de trafic réseau en augmentant la bande passante. Souvent, le niveau du trafic des liaisons variait considérablement. Grâce à IPQoS, il est possible de gérer le trafic sur le réseau existant et d'évaluer si une extension s'avère nécessaire et, le cas échéant, les zones visées.

Par exemple, dans le cadre d'une entreprise ou d'une institution, il est indispensable de maintenir un réseau performant afin d'éviter les goulets d'étranglement. Vous devez également veiller à ce qu'un groupe ou une application ne consomme pas plus de bande passante que le volume alloué. Pour un FAI ou un ASP, vous devez gérer les performances du réseau pour assurer que les clients reçoivent le service réseau correspondant à l'abonnement souscrit.

## Impact de la bande passante sur le trafic réseau

Vous pouvez utiliser IPQoS pour réguler la *bande passante* du réseau correspondant au volume maximal de données qu'une liaison réseau ou un périphérique intégralement exploité peut transférer. Votre stratégie QoS doit déterminer la priorité de l'utilisation de la bande passante

afin de fournir la qualité de service aux clients ou utilisateurs. Les modules de mesure IPQoS permettent de mesurer et de contrôler l'allocation de la bande passante aux classes de trafic sur un hôte IPQoS.

Avant de pouvoir gérer efficacement le trafic sur un réseau, vous devez répondre aux questions relatives à l'utilisation de la bande passante suivantes :

- Quelles sont les zones de votre réseau local associées à un problème de trafic ?
- Que devez vous faire pour atteindre l'utilisation optimale de la bande passante disponible ?
- Quelles sont les applications critiques de votre site auxquelles une priorité élevée doit être attribuée ?
- Quelles sont les applications sensibles à une éventuelle congestion ?
- Quelles sont, parmi vos applications, les applications les moins critiques compatibles avec une priorité la plus faible ?

## Utilisation des classes de service pour hiérarchiser le trafic

Pour implémenter la qualité de service, vous analysez le trafic du réseau afin de déterminer les groupes plus larges dans lesquels le trafic peut être réparti. Organisez ensuite les groupes en classes de service dotées de caractéristiques et de priorités spécifiques. Ces classes forment les catégories fondamentales sur lesquelles vous basez la stratégie QoS de votre organisation. Les classes de service représentent les groupes de trafic à contrôler.

Par exemple, un fournisseur peut offrir des accords de niveau de service platinum, gold, silver et bronze disponibles selon une échelle de prix. Un accord de niveau de service platinum accorde la priorité la plus haute au trafic entrant d'un site Web que le FAI héberge au nom du client. Ainsi, le trafic entrant du site Web du client peut correspondre à une classe de trafic.

Pour une entreprise, il est possible de créer des classes de service en fonction des besoins propres aux services. Une autre option consiste à créer des classes selon la prépondérance d'une application donnée dans le trafic réseau. Voici quelques exemples de classes de trafic pour une entreprise :

- Les applications courantes comme la messagerie électronique et le trafic FTP sortant vers un serveur particulier peuvent constituer l'un ou l'autre une classe. Puisque les employés font constamment appel à ces applications, votre stratégie QoS garantit aux courriers électroniques et au trafic FTP sortant une petite partie de la bande passante et une priorité plus faible.
- Une base de données d'entrées correspondant à des commandes devant fonctionner 24 h/24. Selon l'importance de l'application de la base de données pour l'entreprise, il est possible d'accorder à la base de données une grande partie de la bande passante et une priorité élevée.



- Un service qui réalise des tâches importantes ou confidentielle, comme le service de paie. L'importance du service pour l'organisation détermine la priorité et la largeur de bande passante accordée à un tel service.
- Les appels entrants du site Web externe d'une entreprise. Vous pouvez donner à cette classe une largeur de bande passante moyenne qui s'exécute à basse priorité.

## Modèle de services différenciés

IPQoS inclut les modules suivants qui font partie de l'architecture des *services différenciés* (*Diffserv*) définie dans le document RFC 2475 :

- Classifieur
- Compteur
- Marqueur

IPQoS apporte les améliorations suivantes au modèle Diffserv :

- Module de comptabilisation des flux
- Marqueur de datagramme 802.1D

Cette section présente les modules Diffserv tel qu'ils sont utilisés par IPQoS. Il est nécessaire de posséder des informations sur ces modules et de connaître notamment leur nom ainsi que leur utilisation en vue de la configuration de la stratégie QoS. Pour plus d'informations détaillées sur chaque module, reportez-vous à la section [“Architecture IPQoS et modèle Diffserv”](#) à la page 491.

## Présentation du classifieur (ipgpc)

Dans le modèle Diffserv, le *classificateur* sélectionne des paquets à partir d'un flux de trafic réseau. Un *flux de trafic* consiste en un groupe de paquets avec des informations identiques dans les champs d'en-tête IP suivants :

- Adresse source
- Adresse de destination
- Port source
- Port de destination
- numéro de protocole.

Dans IPQoS, ces champs sont désignés *5-uplet*.

Le module de classification IPQoS s'appelle *ipgpc*. Le classificateur *ipgpc* organise les flux de trafic en classes selon les caractéristiques configurées dans le fichier de configuration IPQoS.

Pour des informations détaillées sur *ipgpc*, reportez-vous à la section [“Module de classification”](#) à la page 491.

## Classes IPQoS

Une *classe* représente un groupe de flux de réseau qui partage des caractéristiques similaires. Par exemple, un FAI peut définir des classes visant à représenter des niveaux de service différents proposés aux clients. Un ASP peut définir des accords de niveau de service octroyant des niveaux de service différents à diverses applications. Dans le cadre de la stratégie QoS d'un ASP, une classe peut inclure le trafic FTP sortant associé à une adresse IP de destination spécifique. Le trafic sortant du site Web externe d'une entreprise peut également faire l'objet d'une classe.

L'organisation du trafic en classes constitue une partie primordiale de la planification de votre stratégie QoS. Lorsque vous créez des classes à l'aide de l'utilitaire `ipqosconf`, vous configurez de fait le module de classification `ipgpc`.

Pour obtenir des informations sur la définition des classes, reportez-vous à la section [“Définition des classes pour votre stratégie QoS”](#) à la page 434.

## Filtres IPQoS

Les *filtres* sont des jeux de règles qui contiennent des paramètres appelés *sélecteurs*. Chaque filtre doit désigner une classe. IPQoS fait correspondre aux paquets les sélecteurs de chaque filtre afin de déterminer si le paquet appartient à la classe du filtre. Toute une gamme de sélecteurs permet de filtrer un paquet, par exemple, l'uplet à 5 attributs d'IPQoS et d'autres paramètres courants :

- Adresses source et de destination
- Port source et port de destination
- Numéros de protocole
- ID utilisateur
- ID de projet
- Point de code de services différenciés (DSCP)
- Indice d'interface

Par exemple, un filtre simple peut comporter le port de destination avec la valeur 80. Le classificateur `ipgpc` sélectionne ensuite tous les paquets liés au port de destination 80 (HTTP) et traite les paquets comme indiqué dans la stratégie QoS.

Pour plus d'informations sur la création de filtres, reportez-vous à la section [“Définition de filtres dans la stratégie QoS”](#) à la page 437.

## Présentation des compteurs (tokenmt et tswtclmt)

Dans le modèle Diffserv, le *compteur* étudie le taux de transmission des flux de trafic par classe. Le compteur évalue dans quelle proportion le débit réel du flux se conforme aux débits configurés et définit le résultat qui convient. Selon le résultat obtenu par le flux du trafic, le compteur sélectionne l'action qui s'ensuit. Les actions suivantes peuvent être le transfert du paquet vers une autre action ou le retour du paquet vers le réseau sans traitement supplémentaire.

Les compteurs IPQoS déterminent si un flux de réseau est conforme au débit de transmission défini pour sa classe dans la stratégie QoS. IPQoS comporte deux modules de mesure :

- `tokenmt` : utilise un plan de mesure de seau à deux jetons.
- `tswtclmt` : utilise un plan de mesure se rapportant à une fenêtre (temporelle).

Les deux modules de mesure aboutissent aux trois résultats : rouge, orange et vert. Définissez les actions à réaliser en fonction de chaque résultat dans les paramètres `red_action_name`, `yellow_action_name` et `green_action_name`.

De plus, vous pouvez configurer `tokenmt` de sorte que ses résultats s'affiche sous forme d'un code en couleur. Une instance de mesure couleur utilise la taille du paquet, le DSCP, le débit du trafic et le paramètres configurés pour déterminer le résultat. Le compteur utilise le DSCP de manière à traduire le résultat du paquet en vert, orange ou rouge.

Pour plus d'informations sur la définition des paramètres pour les compteurs IPQoS, reportez-vous à la section [“Planification du contrôle de flux” à la page 438](#).

## Généralités des marqueurs (`dscpmk` et `dlcosmk`)

Dans le modèle Diffserv, le *marqueur* donne une valeur au paquet reflétant un comportement de transmission. Le *marquage* est le processus consistant à placer une valeur dans l'en-tête du paquet de façon à signaler le mode de transmission du paquet vers le réseau. IPQoS contient deux modules de marquage :

- `dscpmk` : attribue au champ DS de l'en-tête du paquet IP une valeur numérique appelée *point de code de services différenciés DSCP*. Un routeur Diffserv est alors en mesure d'utiliser le point de code DS pour appliquer le comportement de transmission au paquet.
- `dlcosmk` : spécifie l'étiquette du réseau local virtuel (VLAN) d'un entête de trame Ethernet. Pour cela, il lui attribue une valeur numérique appelée *priorité utilisateur*. La priorité utilisateur indique la *classe de service (CoS)*, définissant le comportement à appliquer au datagramme.

`dlcosmk` est une extension IPQoS qui ne fait pas partie du modèle Diffserv tel que ce dernier a été conçu par l'IETF.

Pour plus d'informations sur l'implémentation d'une approche utilisant un marqueur dans le cadre de la stratégie QoS, reportez-vous à la section [“Planification du comportement de transmission” à la page 441](#).

## Généralités sur la comptabilisation des flux (`flowacct`)

IPQoS ajoute le module de comptabilisation `flowacct` au modèle Diffserv. Vous pouvez utiliser `flowacct` pour collecter des statistiques sur les flux de trafic et facturer les clients en

conséquence conformément à l'accord de niveau de service souscrit. La comptabilisation des flux présente également un intérêt dans l'optique de la planification de la capacité et du contrôle du système.

Le module `flowacct` fonctionne avec la commande `acctadm` pour créer un fichier journal de comptabilisation. Un journal standard inclut l'uplet à 5 attributs d'IPQoS et deux attributs supplémentaires comme indiqué dans la liste suivante :

- Adresse source
- Port source
- Adresse de destination
- Port de destination
- Numéro du protocole
- Nombre de paquets
- Nombre d'octets

Vous pouvez recueillir les statistiques sur d'autres attributs, comme indiqué à la section [“Enregistrement des informations sur les flux de trafic” à la page 486](#) et dans les pages de manuel `flowacct(7ipp)` et `acctadm(1M)`.

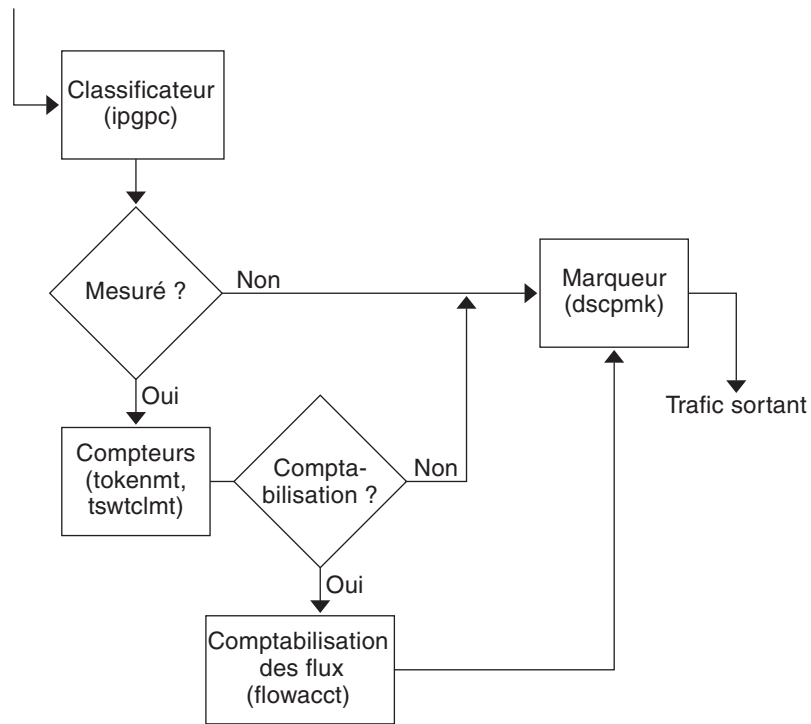
Pour plus d'informations sur la planification d'une stratégie de comptabilisation des flux, reportez-vous à la section [“Planification de la comptabilisation des flux” à la page 444](#).

## Transit du trafic par les modules IPQoS

La figure suivante présente un itinéraire que le trafic entrant peut suivre en passant par certains modules IPQoS.

FIGURE 27-1 Flux de trafic et implémentation IPQoS du modèle Diffserv

Trafic entrant



Cette figure illustre une séquence de flux courante sur un ordinateur compatible IPQoS :

1. Le classificateur sélectionne les paquets qui correspondent aux critères de filtre définis pour la stratégie QoS du système dans le flux de paquets.
2. Les paquets sélectionnés sont ensuite évalués en vue de l'action suivante à réaliser.
3. Le classificateur envoie au marqueur le trafic ne nécessitant aucun contrôle de flux.
4. Le trafic à contrôler est transmis au module de mesure.
5. Ce module applique le taux configuré. Il assigne ensuite une valeur de conformité du trafic aux paquets contrôlés.
6. Les paquets dont les flux ont été contrôlés sont ensuite analysés afin de déterminer si des paquets doivent être comptabilisés.
7. Le compteur transmet au marqueur le trafic qui n'exige pas de comptabilisation des flux.
8. Le flux de comptabilisation collecte les statistiques sur les paquets reçus. Le module transmet ensuite les paquets au marqueur.

9. Le marqueur introduit un point de code DS dans l'en-tête du paquet. Ce DSCP signale le traitement, ou PHB, qu'un système Diffserv doit appliquer au paquet.

## Trafic sur un réseau compatible IPQoS

Cette section présente les éléments impliqués dans la transmission des paquets sur un réseau IPQoS. Un système IPQoS traite les paquets du réseau en fonction de l'adresse IP du système faisant office de destination. Ce système applique ensuite la stratégie QoS aux paquets afin de fournir des services différenciés.

### Point de code DS

Le point de code DS (DSCP) définit, dans l'en-tête du paquet, l'action que le système Diffserv doit appliquer au paquet marqué. L'architecture Diffserv définit un ensemble de points de code DS pour le système IPQoS et le routeur Diffserv à utiliser. L'architecture Diffserv définit également un ensemble d'actions appelées *comportements de transmission* associés aux DSCP. Le système IPQoS marque, à l'aide du DSCP, les bits définissant le niveau de priorité du champ DS dans l'en-tête de paquet. Lorsqu'un routeur reçoit un paquet comportant une valeur DSCP, il applique le comportement associé à ce DSCP. Le paquet est ensuite libéré sur le réseau.

---

**Remarque** – Le marqueur `d\cosmk` ne fait pas appel aux valeurs DSCP. A la place, `d\cosmk` marque les en-têtes de trames Ethernet par une valeur CoS (classe de service). Si vous envisagez de configurer IPQoS sur un réseau utilisant des périphériques VLAN, reportez-vous à la section [“Module de marquage” à la page 497](#).

---

### PHB (Per-Hop Behaviors)

Dans la terminologie Diffserv, le comportement assigné à un DSCP est désigné comme le *PHB* (*per-hop behavior*). Le PHB définit le niveau de priorité dont bénéficie un paquet marqué par rapport à tout autre trafic sur le système Diffserv. C'est ce niveau de priorité qui détermine si le système IPQoS ou le routeur Diffserv transmet ou rejette le paquet marqué. Tous les routeurs Diffserv rencontrés par le paquet transmis lors de son trajet vers sa destination finale appliquent le même PHB. Une seule exception peut survenir : lorsqu'un autre système Diffserv modifie le DSCP. Pour plus d'informations sur les PHB, reportez-vous à la section [“Utilisation du marqueur `dscpmk` pour la transmission des paquets” à la page 497](#).

L'objectif d'un PHB consiste à fournir le volume de ressources réseau spécifié à une classe de trafic sur le réseau contigu. La stratégie QoS permet d'atteindre cet objectif. Définissez les DSCP chargés de signaler le niveau de priorité des classes de trafic lorsque les flux de trafic quittent le système IPQoS. Les niveaux de priorités varient entre une haute priorité/faible probabilité de rejet et une priorité faible/haute probabilité de rejet.

Votre stratégie QoS peut, par exemple, assigner à une classe de trafic un DSCP garantissant un PHB pour lequel la probabilité de perte des paquets est faible. Cette classe de trafic est donc traitée conformément à un PHB de faible probabilité de rejet par les routeurs Diffserv qui réservent une partie de la bande passante pour les paquets de cette classe. Vous pouvez associer d'autres DSCP à la stratégie QoS, assignant des niveaux variables de priorité à d'autres classes de trafic. La bande passante accordée aux paquets dont le niveau de priorité est le plus faible dépend des priorités spécifiées par les DSCP des paquets.

IPQoS prend en charge deux types de comportements, définis dans l'architecture Diffserv, le traitement accéléré (Expedited Forwarding) et le traitement garanti (Assured Forwarding).

## Expedited Forwarding

Le PHB *EF* (*Expedited forwarding*) garantie à toute classe de trafic de DSCP EF la priorité la plus élevée. Le trafic doté d'un DSCP EF n'est pas placé dans la file d'attente. EF assure des taux de perte, de délai et de gigue faibles. Le code DSCP recommandé pour EF est 101110. Un paquet ainsi marqué se voit garantir une faible probabilité de rejet alors qu'il transite par les réseaux Diffserv pour parvenir à sa destination. Utilisez le DSCP EF lorsque vous définissez la priorité des clients ou des applications bénéficiant d'un accord de niveau de service de type premium.

## Assured Forwarding

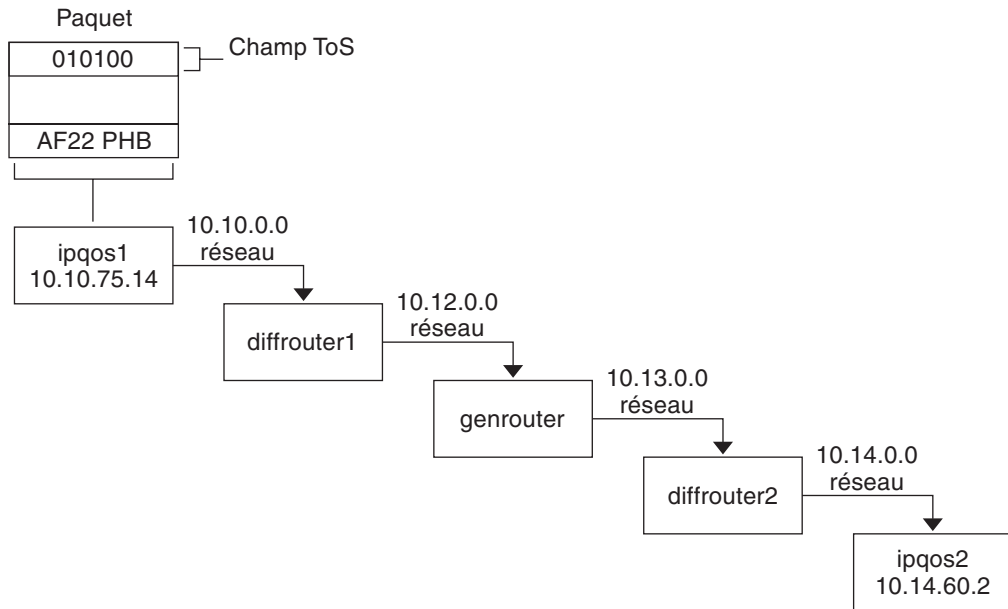
Le PHB *AF* (*assured forwarding*) comporte quatre classes de transmission différentes susceptibles d'être appliquées à un paquet. Chaque classe fournit, à son tour, trois niveaux de priorité comme indiqué dans le [Tableau 32-2](#).

Les points de codes AF offrent la possibilité d'assigner différents niveaux de service aux clients et aux applications. Dans la stratégie QoS, il est possible de hiérarchiser le trafic et les services de votre réseau lorsque vous planifiez la stratégie QoS. Vous pouvez ensuite assigner différents niveaux AF au trafic auquel la priorité est accordée.

## Transmission des paquets dans un environnement Diffserv

La figure suivante illustre une partie de l'intranet d'une entreprise dont l'environnement est partiellement soumis aux règles des services différenciés. Dans cet exemple, tous les hôtes des réseaux 10.10.0.0 et 10.14.0.0 sont compatibles IPQoS et les routeurs locaux sur les deux réseaux reconnaissent Diffserv. Cependant, des réseaux intermédiaires ne sont pas configurés pour prendre en charge les services du modèle Diffserv.

FIGURE 27-2 Transmission des paquets via les noeuds du réseau Diffserv



Les étapes suivantes montrent la progression du flux du paquet illustrée dans cette figure. Les étapes présentent le paquet provenant de l'hôte ipqos1. Elles se poursuivent par le passage par plusieurs noeuds afin d'atteindre l'hôte ipqos2.

1. L'utilisateur au niveau de l'hôte ipqos1 exécute la commande ftp pour accéder à l'hôte ipqos2, situé à trois sauts de là.
2. ipqos1 applique sa stratégie QoS au flux de paquet. ipqos1 établit la classification du trafic ftp.  
L'administrateur système a créé une classe pour tout le trafic ftp sortant issu du réseau local 10.10.0.0. Le trafic de la classe ftp est affecté au comportement AF22 : priorité de classe 2, niveau de perte moyen. Un débit de 2 Mbits/sec est défini pour la classe ftp.
3. ipqos -1 mesure le flux ftp pour déterminer si le flux dépasse le débit garanti de 2 Mbits/sec.
4. Le marqueur sur l'hôte ipqos1 définit les champs DS des paquets ftp sortant à l'aide du DSCP 010100, correspondant au PHB AF22.
5. Le routeur diffrouter1 reçoit les paquets ftp. diffrouter1 prend connaissance du DSCP. Si diffrouter1 est congestionné, les paquets marqués AF22 sont rejetés.
6. Le trafic ftp est transféré vers le noeud suivant conformément au PHB défini pour AF22 dans les fichiers de diffrouter1.
7. Le trafic ftp transite par le réseau 10.12.0.0 pour rejoindre le routeur genrouter qui ne reconnaît pas les services différenciés. Un traitement "au mieux" est alors appliqué au trafic.



8. `genrouter` transmet le trafic `ftp` au réseau `10.13.0.0` au sein duquel le trafic est reçu par le routeur `diffrouter2`.
9. `diffrouter2` reconnaît l'architecture Diffserv. Par conséquent, le routeur envoie les paquets `ftp` sur le réseau conformément au PHB défini dans la stratégie du routeur pour les paquets AF22.
10. `ipqos2` reçoit le trafic `ftp`. `ipqos2` demande à l'utilisateur au niveau de l'hôte `ipqos1` son nom d'utilisateur et son mot de passe.



## Planification d'un réseau IPQoS (tâches)

---

Vous pouvez configurer une architecture IPQoS sur un système qui exécute Oracle Solaris. Le système IPQoS fonctionne alors avec des routeurs Diffserv chargés de fournir des services différenciés et une gestion du trafic sur un intranet.

Ce chapitre décrit les tâches de planification visant à ajouter des systèmes IPQoS sur un réseau compatible avec Diffserv. Ce chapitre contient les sections suivantes.

- “Planification générale de la configuration IPQoS (liste des tâches)” à la page 427
- “Planification de la topologie de réseau Diffserv” à la page 428
- “Planification de la stratégie de qualité de service” à la page 431
- “Planification de la stratégie QoS (liste des tâches)” à la page 432
- “Présentation d'un exemple de configuration IPQoS” à la page 445

### Planification générale de la configuration IPQoS (liste des tâches)

Implémentation des services différenciés, et notamment IPQoS, sur un réseau nécessitant une planification étendue. Vous devez tenir compte de l'emplacement et de la fonction de chaque système IPQoS, mais également de la relation que chaque système entretient avec le routeur ou le réseau local. La liste des tâches suivante répertorie les principales tâches de planification pour l'implémentation d'une architecture IPQoS sur votre réseau et renvoie vers les procédures permettant d'effectuer ces tâches.

Tâche	Description	Voir
1. Planification d'une topologie de réseau Diffserv qui intègre les systèmes IPQoS.	Etudiez les différentes topologies de réseau Diffserv pour déterminer la solution la plus adaptée à votre site.	<a href="#">“Planification de la topologie de réseau Diffserv” à la page 428.</a>

Tâche	Description	Voir
2. Planification des différents types de service qui seront offerts par les systèmes IPQoS.	Organisez les types de service que le réseau fournit dans les accords de niveau de service.	<a href="#">“Planification de la stratégie de qualité de service” à la page 431.</a>
3. Planification de la stratégie QoS pour chaque système IPQoS.	Identifiez les classes, les fonctions de mesure et de comptabilité nécessaires à l'implémentation de chaque accord de niveau de service.	<a href="#">“Planification de la stratégie de qualité de service” à la page 431.</a>
4. Si nécessaire, planification de la stratégie du routeur Diffserv.	Elaborez d'éventuelles stratégies de programmation et de mise en file d'attente pour le routeur Diffserv utilisé avec les systèmes IPQoS.	Pour plus d'informations sur ces stratégies, reportez-vous à la documentation du routeur.

# Planification de la topologie de réseau Diffserv

Pour faire bénéficier votre réseau de services différenciés, vous devez disposer d'au moins un système IPQoS et d'un routeur compatible Diffserv. Vous pouvez intégrer ce scénario de base à une multitude de variantes, comme expliqué dans cette section.

## Stratégies matérielles pour le réseau Diffserv

En général, les clients exécutent IPQoS sur les serveurs et les consolidations de serveurs comme le serveur Sun Enterprise™ d'Oracle. Inversement, vous pouvez également exécuter IPQoS sur des ordinateurs de bureau tels que les systèmes UltraSPARC®, en fonction des besoins du réseau utilisé. La liste suivante décrit les systèmes possibles pour une configuration IPQoS :

- Systèmes Oracle Solaris offrant des services variés (serveurs Web et serveurs de base de données)
- Serveurs d'application proposant des applications de messagerie électronique, FTP ou d'autres applications réseau courantes
- Serveurs de cache Web ou serveurs proxy
- Réseau de batteries de serveurs IPQoS gérées par des équilibres de charge compatibles Diffserv
- Pare-feux gérant le trafic d'un seul réseau hétérogène
- Systèmes IPQoS faisant partie d'un réseau local virtuel

Vous pouvez insérer des systèmes IPQoS dans une topologie de réseau comportant des routeurs compatibles Diffserv. Si votre routeur n'inclut pas Diffserv, recherchez des solutions Diffserv auprès de Cisco Systems, Juniper Networks ou d'autres fabricants de routeurs. Si le routeur local n'implémente pas Diffserv, le routeur transmet les paquets marqués au noeud suivant sans analyser les marques.

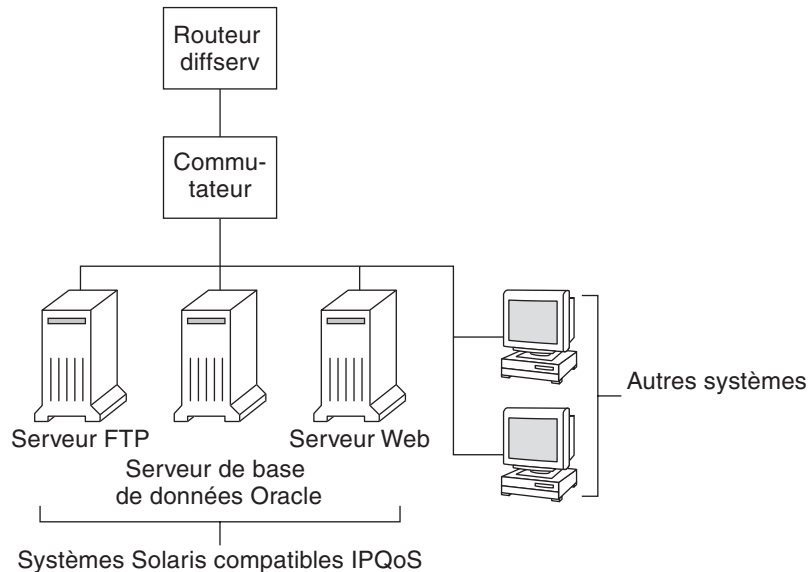
## Topologies de réseau IPQoS

Cette section illustre les stratégies IPQoS qui répondent à différentes exigences de réseau.

### IPQoS sur des hôtes indépendants

La figure suivante montre un réseau unique pour les systèmes compatibles IPQoS.

FIGURE 28-1 Systèmes IPQoS sur un segment de réseau

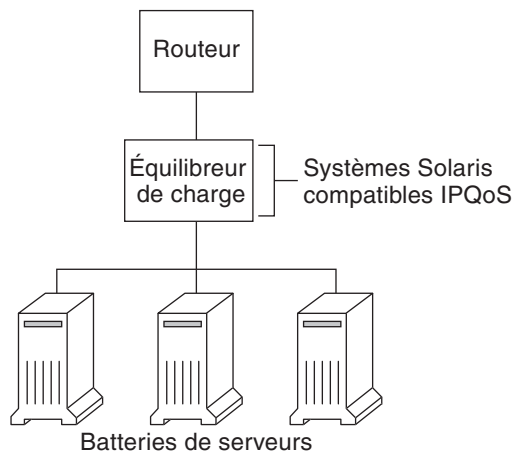


Ce réseau ne représente qu'un seul segment d'un intranet d'entreprise. En activant IPQoS sur les serveurs d'application et les serveurs Web, vous pouvez contrôler le débit auquel chaque système IPQoS libère le trafic sortant. Si le routeur Diffserv est compatible, vous pouvez contrôler davantage le trafic entrant et sortant.

Les exemples du présent guide font appel au scénario "IPQoS sur des hôtes indépendants". Pour en savoir plus sur la topologie utilisée en guise d'exemple tout au long du guide, reportez-vous à la [Figure 28-4](#).

### IPQoS sur une batterie de serveurs réseau

La figure suivante présente un réseau avec des batteries de serveurs hétérogènes.

**FIGURE 28-2** Réseau de batteries de serveurs compatibles IPQoS

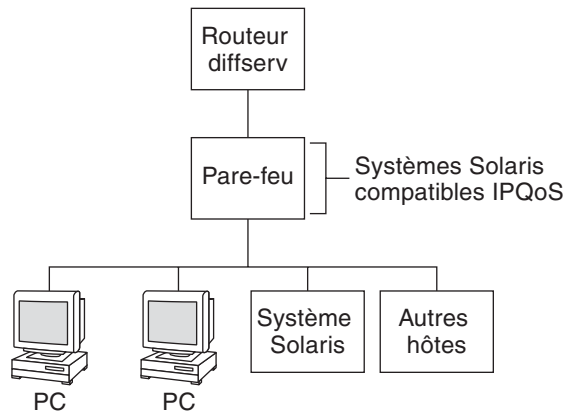
Dans une telle topologie, le routeur est compatible avec Diffserv et peut, à ce titre, mettre en attente et adapter le débit du trafic entrant et sortant. L'équilibreur de charge est également compatible avec Diffserv tandis que les batteries de serveurs reconnaissent le système IPQoS. L'équilibreur de charge peut fournir des fonctions de filtrage supplémentaires au-delà du routeur grâce à des sélecteurs de type ID utilisateur et ID projet. Ces sélecteurs sont inclus dans les données d'application.

Ce scénario illustre un contrôle des flux et un transfert du trafic en mesure de gérer une éventuelle congestion du réseau local. Il interdit également au trafic sortant des batteries des serveurs d'encombrer d'autres sections du réseau intranet.

## IPQoS sur un pare-feu

La figure suivante montre un segment d'un réseau d'entreprise sécurisé à partir d'autres segments au moyen d'un pare-feu.

FIGURE 28-3 Réseau protégé par un pare-feu compatible IPQoS



Dans l'exemple illustré, le trafic passe par le routeur compatible Diffserv où les paquets sont filtrés et mis en attente. Tout le trafic entrant, transféré par le routeur, transite alors par le pare-feu IPQoS. Pour utiliser IPQoS, le pare-feu ne doit pas passer outre la pile de transmission IP.

La stratégie de sécurité du pare-feu détermine si le trafic entrant est autorisé à entrer ou à sortir du réseau interne. La stratégie QoS contrôle les niveaux de service applicables au trafic entrant ayant traversé le pare-feu. Selon la stratégie QoS retenue, le trafic sortant peut également être associé à un comportement de transmission particulier.

## Planification de la stratégie de qualité de service

Lorsque vous planifiez une stratégie de qualité de service (QoS), vous devez examiner, classer les services que le réseau fournit, puis leur donner un ordre de priorité. Vous devez également évaluer la quantité de bande passante disponible de manière à déterminer le débit de chaque classe de trafic arrivant sur le réseau.

### Aides à la planification de la stratégie QoS

Rassemblez les informations pour la planification de la stratégie dans un format prenant en compte les informations nécessaires pour le fichier de configuration IPQoS. Par exemple, servez-vous du modèle suivant pour énumérer les catégories principales d'information à intégrer au fichier de configuration IPQoS.

TABLEAU 28-1    Modèle de planification QoS

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?	Comptabilisation ?
Classe 1	1	Filtre1	Sélecteur 1	Débits de l'indicateur selon le type de mesure	Niveau de priorité du marqueur	Requiert des statistiques de comptabilisation des flux
		Filtre 3	Sélecteur 2			
Classe 1	1	Filtre 2	Sélecteur 1	SO	SO	SO
			Sélecteur 2			
Classe 2	2	Filtre1	Sélecteur 1	Débits de l'indicateur selon le type de mesure	Niveau de priorité du marqueur	Requiert des statistiques de comptabilisation des flux
			Sélecteur 2			
Classe 2	2	Filtre 2	Sélecteur 1	SO	SO	SO
			Sélecteur 2			

Il est possible de diviser chaque catégorie principale pour définir encore plus précisément la stratégie QoS. Les sections suivantes indiquent comment obtenir des informations sur les catégories illustrées dans le modèle.

## Planification de la stratégie QoS (liste des tâches)

Cette liste de tâches répertorie les principales tâches de planification d'une stratégie QoS et renvoie vers les procédures permettant d'effectuer chaque tâche.

Tâche	Description	Voir
1. Etablissement de la topologie du réseau pour qu'il prenne en charge IPQoS.	Identifiez les hôtes et les routeurs du réseau de manière à fournir des services différenciés.	<a href="#">“Préparation d'un réseau pour IPQoS” à la page 433</a>
2. Définition des classes dans lesquelles les services du réseau doivent être répartis.	Examinez les types de service et les niveaux de service offerts par votre site et déterminez à quelles classes de trafic discret les services appartiennent.	<a href="#">“Définition des classes pour votre stratégie QoS” à la page 434</a>
3. Définition des filtres pour les classes.	Déterminez les méthodes les plus adaptées pour isoler le trafic d'une classe particulière par rapport au flux du trafic réseau.	<a href="#">“Définition de filtres dans la stratégie QoS” à la page 437</a>



Tâche	Description	Voir
4. Définition des débits de contrôle de flux visant à mesurer le trafic lorsque les paquets quittent le système IPQoS.	Déterminez les débits acceptables pour chaque classe de trafic.	<a href="#">“Planification du contrôle de flux” à la page 438</a>
5. Définition des valeurs DSCP ou les valeurs dont la priorité est définie par l'utilisateur à appliquer à la stratégie QoS.	Mettez en place un plan et déterminez le comportement de transmission assigné à un flux de trafic si le flux est géré par le routeur ou le commutateur.	<a href="#">“Planification du comportement de transmission” à la page 441</a>
6. Le cas échéant, définition d'un plan de contrôle statistique concernant les flux de trafic sur le réseau.	Analysez les classes de trafic pour identifier les flux à contrôler à des fins comptables ou statistiques.	<a href="#">“Planification de la comptabilisation des flux” à la page 444</a>

**Remarque** – La suite de la section décrit la planification de la stratégie QoS d'un système IPQoS. Pour planifier la stratégie QoS d'un routeur Diffserv, consultez la documentation du routeur ainsi que le site Web du fabricant.

## ▼ Préparation d'un réseau pour IPQoS

La procédure suivante dresse la liste des tâches générales de planification à effectuer avant de créer la stratégie QoS.

- 1 Examinez la topologie du réseau. Elaborez ensuite une stratégie associant les systèmes IPQoS et les routeurs Diffserv.**  
Pour consulter des exemples de topologie, reportez-vous à la section [“Planification de la topologie de réseau Diffserv” à la page 428](#).
- 2 Identifiez les hôtes de la topologie qui nécessitent IPQoS ou qui sont susceptibles d'être intéressés par le service IPQoS.**
- 3 Définissez parmi les systèmes compatibles IPQoS ceux qui peuvent recourir à la même stratégie QoS.**

Si, par exemple, vous envisagez d'activer IPQoS sur tous les hôtes du réseau, identifiez ceux qui peuvent utiliser une même stratégie QoS. Chaque système IPQoS doit posséder une stratégie QoS locale. Celle-ci est implémentée dans le fichier de configuration IPQoS associé. Cependant, il est possible de créer un fichier de configuration IPQoS exploitable par une large gamme de systèmes. Il suffit alors de copier le fichier de configuration dans chaque système partageant les mêmes exigences en matière de stratégie QoS.

- 4 Évaluez et effectuez toutes les tâches de planification requises par le routeur Diffserv sur votre réseau.**

Reportez-vous à la documentation du routeur et au site Web du fabricant pour plus de détails.

## ▼ Définition des classes pour votre stratégie QoS

La première étape de la définition de la stratégie QoS consiste à organiser les flux de trafic en plusieurs classes. Vous n'avez pas besoin de créer des classes pour chaque type de trafic sur un réseau Diffserv. De plus, selon la topologie du réseau, vous pouvez être amené à créer une stratégie QoS différente pour chaque système compatible IPQoS.

---

**Remarque** – Pour des informations générales sur les classes, reportez-vous à la section “Classes IPQoS” à la page 418.

---

La procédure suivante suppose que vous avez établi les systèmes de votre réseau qui sont compatibles IPQoS comme indiqué dans la section “Préparation d'un réseau pour IPQoS” à la page 433.

- 1 Créez un tableau de planification QoS pour organiser les informations de la stratégie QoS.**

Pour obtenir des suggestions, reportez-vous au [Tableau 28–1](#).

- 2 Effectuez les étapes restantes pour chaque stratégie QoS figurant sur le réseau.**

- 3 Définissez les classes à utiliser dans la stratégie QoS.**

Les questions suivantes contribuent à analyser le trafic réseau en vue de la définition de classes.

- **L'entreprise offre-t-elle des accords de niveau de service à ses clients ?**

Si oui, évaluez les niveaux de priorité relatifs définis pour les accords de niveau de service qu'offre l'entreprise. Les clients peuvent se voir proposer une même application assortie de niveaux de priorité différents.

Par exemple, l'entreprise peut offrir un hébergement de site Web à chacun de ses clients ce qui signifie qu'il est nécessaire de définir une classe pour chaque site Web client. Un accord de niveau de service peut fournir un site Web Premium au titre d'un niveau de service. Un autre accord de niveau de service peut consister en un site Web personnel utilisable "au mieux" à l'usage de clients bénéficiant de remises. Ce facteur signale non seulement différentes classes de sites Web, mais également des comportements (PHB) potentiellement différents, assignés aux classes de sites Web.

- **Le système IPQoS offre-t-il des applications courantes nécessitant éventuellement un contrôle des flux ?**

Vous pouvez améliorer les performances réseau en activant IPQoS sur les serveurs proposant des applications courantes qui génèrent un trafic important. Les exemples les plus courants sont les applications de messagerie électronique, de discussion réseau et FTP. Envisagez de créer des classes indépendantes pour le trafic entrant et sortant de chaque type de service, si besoin est. Par exemple, il est possible de créer une classe courrier entrant et une classe courrier sortant pour la stratégie QoS d'un serveur de courrier.

- **Le réseau exécute-t-il des applications qui impliquent une transmission en haute priorité ?**

Toute application critique nécessitant une transmission en priorité haute doit être prioritaire dans la file d'attente du routeur. C'est le cas, par exemple, des flux de données vidéo et audio.

Définissez les classes entrantes et sortantes pour ces applications à haute priorité. Ensuite, insérez les classes dans les stratégies QoS du routeur Diffserv et du système IPQoS fournissant les applications.

- **Le réseau fait-il l'objet de flux de trafic à contrôler en raison de la consommation importante de bande passante ?**

Exécutez `netstat`, `snoop` et d'autres utilitaires de contrôle réseau pour détecter les types de trafic à l'origine des problèmes survenant sur le réseau. Étudiez les classes que vous avez créées jusqu'ici, puis générez de nouvelles classes pour les catégories de problèmes de trafic non définis. Si vous avez déjà défini des classes pour une catégorie de problèmes, définissez les débits du compteur chargé de contrôler le trafic problématique.

Créez des classes pour le trafic posant problème dans chaque système IPQoS situé sur le réseau. Chaque système IPQoS peut alors gérer un trafic problématique en réduisant le débit du flux arrivant sur le réseau. Assurez-vous également de spécifier ces classes dans la stratégie QoS sur le routeur Diffserv. Le routeur peut ainsi mettre en attente et planifier les flux problématiques conformément à la configuration de la stratégie QoS.

- **Avez-vous besoin de connaître les statistiques sur certains types de trafic ?**

L'examen rapide d'un accord de niveau de service peut révéler les types des trafics client devant être comptabilisés. Si votre site offre des accords de niveau de service, vous avez sans doute déjà créé des classes relatives au trafic impliquant des données de comptabilisation. Vous pouvez également être amené à définir des classes en vue de la collecte de statistiques concernant les flux de trafic que vous contrôlez. Il est possible de définir des classes pour le trafic soumis à des restrictions d'accès pour des raisons de sécurité.

#### **4 Dressez la liste des classes que vous avez définies dans le tableau de planification QoS élaboré à l'étape 1.**

#### **5 Attribuez un niveau de priorité à chacune des classes.**

Par exemple, le niveau de priorité 1 représente la classe dotée de la priorité la plus élevée. Définissez les priorités suivantes en ordre décroissant pour les autres classes. Le niveau de priorité assigné est utilisé à des fins organisationnelles uniquement. Les niveaux de priorité

définis dans le modèle de stratégie QoS ne sont pas réellement utilisés par IPQoS. Par ailleurs, vous pouvez attribuer une même priorité à plusieurs classes si cela convient à la stratégie QoS.

- 6 Lorsque vous avez terminé la définition des classes, vous pouvez passer à la définition des filtres pour chaque classe, comme expliqué à la section [“Définition de filtres dans la stratégie QoS” à la page 437](#).

Informations  
supplémentaires

Définition de la priorité des classes

Au fur et à mesure que vous créez des classes, vous vous rendrez compte des classes devant bénéficier de la priorité la plus élevée, d'une priorité moyenne ou d'une priorité "au mieux". Un plan de hiérarchisation des classes s'avère particulièrement important lorsque vous assignez des comportements par pas au trafic sortant comme indiqué à la section [“Planification du comportement de transmission” à la page 441](#).

Outre l'attribution d'un tel comportement à une classe, il est également possible de définir, pour la classe, un sélecteur de priorité dans un filtre. Le sélecteur de priorité est actif sur l'hôte IPQoS seulement. Considérons plusieurs classes avec des débits et des valeurs DSCP (Differentiated Services Code Point) identiques qui se font concurrence au niveau de la bande passante lorsqu'ils sortent du système IPQoS. Le sélecteur de priorité de chaque classe permet de classer le niveau de service attribué aux classes dont les valeurs sont identiques.

Définition des filtres

Les filtres créés permettent d'identifier les flux de paquets appartenant à une classe particulière. Chaque filtre contient des sélecteurs définissant les critères qui contribuent à l'évaluation d'un flux de paquet. Le système IPQoS utilise ensuite les critères des sélecteurs pour extraire les paquets à partir d'un flux de trafic. Le système IPQoS associe ensuite les paquets à une classe. Pour obtenir une présentation des filtres, reportez-vous à la section [“Filtres IPQoS” à la page 418](#).

Le tableau suivant répertorie les sélecteurs les plus répandus. Les cinq premiers sélecteurs représentent l'uplet à 5 attributs IPQoS dont le système IPQoS se sert pour identifier les paquets sous forme de membres d'un flux. Pour obtenir la liste complète des sélecteurs, reportez-vous au [Tableau 32–1](#).

TABLEAU 28–2 Sélecteurs IPQoS communs

Nom	Définition
saddr	Adresse source.
daddr	Adresse de destination.
sport	Numéro de port source. Vous pouvez utiliser un numéro de port connu comme indiqué dans <code>/etc/services</code> ou un numéro de port défini par l'utilisateur.

TABLEAU 28-2 Sélecteurs IPQoS communs (Suite)

Nom	Définition
dport	Numéro de port de destination.
protocol	Numéro de protocole IP ou nom du protocole attribué au type de flux de trafic dans le fichier <code>/etc/protocols</code> .
ip_version	Style d'adresse à utiliser. Vous avez le choix entre IPv4 et IPv6. IPv4 est le style par défaut.
dsfield	Contenu du champ DS, c'est-à-dire la valeur DSCP. Servez-vous de ce sélecteur pour extraire les paquets entrants déjà signalés par une valeur DSCP.
priority	Niveau de priorité attribué à la classe. Pour plus d'informations, reportez-vous à la section <a href="#">“Définition des classes pour votre stratégie QoS” à la page 434</a> .
user	Identifiant utilisateur UNIX ou nom de l'utilisateur à l'exécution de l'application de niveau supérieur.
projid	ID de projet utilisé à l'exécution de l'application de niveau supérieur.
direction	Direction du flux de trafic. La valeurs est LOCAL_IN, LOCAL_OUT, FWD_IN ou FWD_OUT.

**Remarque** – Choisissez les sélecteurs avec discernement. Veillez à ne pas utiliser plus de sélecteurs que nécessaire pour extraire les paquets d'une classe. En effet plus le nombre de sélecteurs est important, plus cela aura d'impact sur les performances IPQoS.

## ▼ Définition de filtres dans la stratégie QoS

### Avant de commencer

Avant d'effectuer les étapes suivantes, vous devez avoir suivi la procédure [“Définition des classes pour votre stratégie QoS” à la page 434](#).

- 1 **Créez au moins un filtre pour chaque classe dans la planification QoS que vous avez mise sur pied à la section [“Définition des classes pour votre stratégie QoS” à la page 434](#).**

Envisagez de créer des filtres indépendants pour le trafic entrant et le trafic sortant de chaque classe, si besoin est. Par exemple, intégrez un filtre `ftp-in` et un filtre `ftp-out` à la stratégie QoS d'un serveur FTP compatible IPQoS. Vous pouvez ensuite définir le sélecteur `direction` qui convient en plus des sélecteurs de base.

- 2 **Définissez au moins un sélecteur pour chaque filtre au sein d'une classe.**

Utilisez le tableau de planification QoS, illustré par le [Tableau 28-1](#), pour remplir les filtres des classes définies.

### Exemple 28-1 Définition des filtres pour le trafic FTP

Le tableau suivant explique comment définir un filtre pour le trafic FTP sortant.

Classe	Priorité	Filtres	Sélecteurs
ftp-traffic	4	ftp-out	saddr 10.190.17.44 daddr 10.100.10.53 sport 21 direction LOCAL_OUT

- Voir aussi**
- Pour définir un plan de contrôle des flux, reportez-vous à la section [“Planification du contrôle de flux”](#) à la page 438.
  - Pour spécifier les comportements de transmission associés aux flux lorsqu'ils reviennent sur le réseau, reportez-vous à la section [“Planification du comportement de transmission”](#) à la page 441.
  - Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section [“Planification de la comptabilisation des flux”](#) à la page 444.
  - Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section [“Définition des classes pour votre stratégie QoS”](#) à la page 434.
  - Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section [“Définition de filtres dans la stratégie QoS”](#) à la page 437.

## ▼ Planification du contrôle de flux

Le contrôle de flux implique de mesurer les flux de trafic pour une classe, puis de libérer les paquets sur le réseau à un débit défini. Lorsque vous planifiez le contrôle de flux, vous définissez les paramètres à appliquer aux modules de mesure IPQoS. Les compteurs déterminent le débit auquel le trafic est diffusé sur le réseau. Pour une présentation des modules de mesure, reportez-vous à la section [“Présentation des compteurs \(tokenmt et tswtclmt\)”](#) à la page 418.

La procédure suivante suppose que vous ayez défini les filtres et les sélecteurs comme décrit dans la section [“Définition de filtres dans la stratégie QoS”](#) à la page 437.

- 1 **Déterminez la bande passante maximum pour votre réseau.**
- 2 **Vérifiez tous les accords de niveau de service gérés par le réseau. Identifiez les clients et le type de service assuré.**

Pour garantir un niveau de service donné, il peut être indispensable de contrôler certaines classes de trafic générées par le client.

### 3 Vérifiez la liste des classes créées à la section “Définition des classes pour votre stratégie QoS” à la page 434.

Déterminez si d'autres classes, outre celles qui sont associées aux accords de niveau de service, doivent faire l'objet de mesures.

Supposons que le système IPQoS exécute une application générant un niveau de trafic élevé. Après avoir établi une classification du trafic de l'application, évaluez les flux de manière à vérifier le débit auquel les paquets du flux arrivent sur le réseau.

---

**Remarque** – Il n'est pas utile de quantifier toutes les classes. Gardez à l'esprit cette consigne lorsque vous examinez la liste des classes.

---

### 4 Dans chaque classe, déterminez les filtres en rapport avec un trafic devant faire l'objet d'un contrôle de flux. Affinez ensuite la liste des classes nécessitant des opérations de mesure.

Lorsque les classes sont dotées de plusieurs filtres, il se peut que seul un filtre exige d'être contrôlé. Supposons que vous définissiez des filtres pour le trafic entrant et le trafic sortant d'une classe donnée. Vous pouvez établir que seul trafic d'une direction exige un contrôle de flux.

### 5 Choisissez un module de mesure pour chaque classe à traiter.

Ajoutez le nom du module à la colonne de mesure dans le tableau de planification QoS.

### 6 Ajoutez les débits des classes à mesurer dans la table organisationnelle.

Si vous utilisez le module `tokenmt`, définissez les débits en bits par seconde suivants :

- Débit garanti
- Débit de pointe

Si ces débits suffisent à mesurer une classe donnée, contentez-vous de spécifier le débit garanti et la taille de rafale garantie pour le module `tokenmt`.

Si nécessaire, vous pouvez également définir les débits suivants :

- Taille de rafale garantie
- Taille de rafale de pointe

Pour la définition complète des débits `tokenmt`, reportez-vous à la section “Configuration du `tokenmt` en tant que compteur à débit double” à la page 495. Vous trouverez également des informations plus détaillées dans la page de manuel `tokenmt` (7ipp).

Si vous recourez au module `tswtclmt`, il est nécessaire de définir les débits (en bits par seconde) suivants.

- Débit garanti
- Débit de pointe

Vous pouvez aussi paramétrer la taille de la fenêtre en millisecondes. Ces débits sont indiqués à la section “[Module de mesure tswtclmt](#)” à la page 496 et à la page de manuel [twstclmt\(7ipp\)](#).

7 **Ajoutez les résultats de conformité du trafic mesuré.**

Les résultats des deux modules de mesure s'affichent en vert, en rouge et en orange. Ajoutez à votre tableau organisationnel QoS, les résultats de la conformité du trafic concernant les débits que vous définissez. Les résultats des opérations de mesure sont expliqués en détail dans la section “[Module de mesure](#)” à la page 494.

Vous devez préciser l'action à entreprendre lorsque le trafic se conforme ou ne se conforme pas au débit garanti. La plupart du temps, cette action consiste à marquer l'en-tête du paquet par un comportement appelé PHB (per-hop behavior). Lorsque le trafic est vert, l'action autorisée peut être de continuer le traitement des flux de trafic tant que ces derniers ne dépassent pas le contrat de trafic. Une autre action possible peut être de rejeter les paquets de la classe si les flux sont supérieurs au débit de pointe.

**Exemple 28–2** Définition des compteurs

Le tableau suivant affiche les entrées d'une classe de trafic de messagerie électronique. Le réseau sur lequel se trouve le système IPQoS dispose d'une bande passante totale de 100 Mbits/sec, soit 10 millions de bits par seconde. La stratégie QoS assigne une priorité basse à la classe du courrier électronique. Cette classe obtient également le traitement "au mieux".

Classe	Priorité	Filtre	Sélecteur	Débit
email	8	mail_in	daddr10.50.50.5	
			dport imap	
			direction LOCAL_IN	
email	8	mail_out	saddr10.50.50.5	mesure=tokenmt
			sport imap	débit garanti=5000000
			direction	taille de rafale garantie =5000000
			LOCAL_OUT	débit de pointe =10000000
				taille de rafale de pointe=1000000
				niveau de priorité vert=poursuivre le traitement
				niveau de priorité orange=signaliser par un PHB orange
			niveau de priorité rouge=rejeter	



- Voir aussi**
- Pour spécifier les comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section “[Planification du comportement de transmission](#)” à la page 441.
  - Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section “[Planification de la comptabilisation des flux](#)” à la page 444.
  - Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section “[Définition des classes pour votre stratégie QoS](#)” à la page 434.
  - Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section “[Définition de filtres dans la stratégie QoS](#)” à la page 437.
  - Pour définir un autre plan de contrôle des flux, reportez-vous à la section “[Planification du contrôle de flux](#)” à la page 438.
  - Pour créer un fichier de configuration IPQoS, reportez-vous à la section “[Création du fichier de configuration IPQoS et définition des classes de trafic](#)” à la page 454.

## ▼ Planification du comportement de transmission

Le comportement de transmission détermine la priorité ainsi que le niveau de priorité des flux de trafic qui vont être transférés au réseau. Vous avez le choix entre deux comportements principaux : hiérarchiser les flux d'une classe par rapport à d'autres classes de trafic ou rejeter l'intégralité des flux.

Le modèle Diffserv utilise un marqueur pour assigner le comportement de transmission choisi aux flux de trafic. IPQoS comporte les deux modules de marquage suivants.

- `dscpmk` : permet de marquer le champ DS d'un paquet IP à l'aide d'un DSCP (Differentiated Service Code Point, point de code de services différenciés)
- `dlsosmk` : sert à marquer l'étiquette VLAN d'un datagramme par une valeur de classe de service (CoS)

---

**Remarque** – Les suggestions de cette section concernent les paquets IP uniquement. Si votre système IPQoS comprend un dispositif VLAN, vous pouvez utiliser le marqueur `dlsosmk` pour identifier certains comportements de transmission associés aux datagrammes. Pour plus d'informations, reportez-vous à la section “[Utilisation du marqueur `dlsosmk` avec les périphériques VLAN](#)” à la page 499.

---

Pour définir la priorité d'un trafic IP, vous devez attribuer un DSCP à chaque paquet. Le marqueur `dscpmk` code le champ DS du paquet à l'aide d'un DSCP. Vous choisissez le DSCP pour une classe dans un groupe de points de codes connus associés au type de comportement. Ces points de codes correspondent à 46 (101110) pour le PHB de classe EF et une plage de points de codes pour le PHB de classe AF. Pour des informations générales sur le DSCP et la transmission, reportez-vous à la section “[Trafic sur un réseau compatible IPQoS](#)” à la page 422.

**Avant de commencer** Les étapes suivantes supposent que vous ayez défini les classes et les filtres de la stratégie QoS. Même si vous combinez généralement les opérations de mesure et de marquage du trafic à contrôler, le marquage seul permet de définir un comportement de transmission.

**1 Vérifiez les classes créées jusqu'à présent, ainsi que les priorités assignées à chacune d'entre elles.**

Il n'est pas utile de marquer toutes les classes de trafic.

**2 Attribuez le PHB EF (expedited forwarding, traitement accéléré) à la classe avec la priorité la plus élevée.**

Le PHB EF garantit que les paquets marqués EF DSCP 46 (101110) sont diffusés sur le réseau avant les paquets de classe AF. Réservez le PHB EF pour le trafic prioritaire. Pour plus d'informations sur EF, reportez-vous à la section [“PHB Expedited Forwarding \(EF\) \(ou traitement accéléré\)”](#) à la page 498.

**3 Attribuez des comportements de routeurs aux classes dont le trafic doit être mesuré.**

**4 Définissez des points de codes DS pour les autres classes conformément aux priorités associées aux classes.**

**Exemple 28–3** Stratégie QoS pour une application de jeu

Le trafic est généralement mesuré pour les raisons suivantes :

- Un accord de niveau de service garantit aux paquets de cette classe un service supérieur ou inférieur lorsque le réseau est fortement sollicité.
- Une classe dotée d'une priorité moindre aura tendance à submerger le réseau.

Les fonctions de marquage et de mesure permettent de fournir à ces classes des services différenciés et une gestion de la bande passante. Le tableau suivant présente, à titre d'exemple, une partie d'une stratégie QoS. Cette stratégie définit une classe pour un jeu populaire générant un niveau important de trafic.

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?
games_app	9	games_in	sport 6080	SO	SO

Classe	Priorité	Filtre	Sélecteur	Débit	Transfert ?
games_app	9	games_out	dport 6081	mesure=tokenmt débit garanti=5000000 taille de rafale garantie =5000000 débit de pointe =10000000 taille de rafale de pointe=15 000 000 niveau de priorité vert=poursuivre le traitement niveau de priorité orange=signaliser par un PHB orange niveau de priorité rouge=rejeter	vert =AF31 orange=AF42 rouge=rejeter

Les comportements assignent des DSCP de priorité basse au trafic games\_app conforme au débit garanti ou inférieur au débit de pointe. Si le trafic games\_app dépasse le débit de pointe, la stratégie QoS indique que les paquets issus du trafic games\_app doivent être ignorés. Le [Tableau 32–2](#) dresse la liste de tous les points de codes AF.

- Voir aussi**
- Pour planifier la comptabilisation des flux pour certains types de trafic, reportez-vous à la section [“Planification de la comptabilisation des flux” à la page 444](#).
  - Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section [“Définition des classes pour votre stratégie QoS” à la page 434](#).
  - Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section [“Définition de filtres dans la stratégie QoS” à la page 437](#).
  - Pour définir un plan de contrôle des flux, reportez-vous à la section [“Planification du contrôle de flux” à la page 438](#).
  - Pour spécifier d'autres comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section [“Planification du comportement de transmission” à la page 441](#).
  - Pour créer un fichier de configuration IPQoS, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 454](#).

## ▼ Planification de la comptabilisation des flux

Faites appel au module `flowacct` IPQoS pour effectuer le suivi des flux de trafic à des fins de facturation et de gestion du réseau. Appliquez la procédure pour déterminer si votre stratégie QoS doit inclure une comptabilisation des flux.

### 1 Votre entreprise offre-t-elle des accords de niveaux de services à ses clients ?

Dans l'affirmative, recourez à la comptabilisation des flux. Examinez les accords de niveaux de services pour déterminer les types de trafic réseau que l'entreprise veut facturer à ces clients. Passez ensuite en revue votre stratégie QoS pour identifier les classes de trafic à facturer.

### 2 Existe-t-il des applications devant faire l'objet d'un contrôle ou d'un test pour pallier des éventuels problèmes liés au réseau ?

Dans l'affirmative, envisagez de faire appel à la comptabilisation des flux de manière à observer le comportement de ces applications. Examinez la stratégie QoS pour identifier les classes assignées au trafic et qui nécessitent un contrôle.

### 3 Signalez par la lettre O, dans la colonne de comptabilisation des flux, chaque classe nécessitant une comptabilisation dans la table de planification QoS.

- Voir aussi**
- Pour ajouter plusieurs classes à la stratégie QoS, reportez-vous à la section [“Définition des classes pour votre stratégie QoS” à la page 434.](#)
  - Pour ajouter plusieurs filtres à la stratégie QoS, reportez-vous à la section [“Définition de filtres dans la stratégie QoS” à la page 437.](#)
  - Pour définir un plan de contrôle des flux, reportez-vous à la section [“Planification du contrôle de flux” à la page 438.](#)
  - Pour spécifier les comportements de transmission associés aux flux lorsque les paquets arrivent dans le réseau, reportez-vous à la section [“Planification du comportement de transmission” à la page 441.](#)
  - Pour planifier d'autres comptabilisations des flux pour certains types de trafic, reportez-vous à la section [“Planification de la comptabilisation des flux” à la page 444.](#)
  - Pour créer le fichier de configuration IPQoS, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 454.](#)

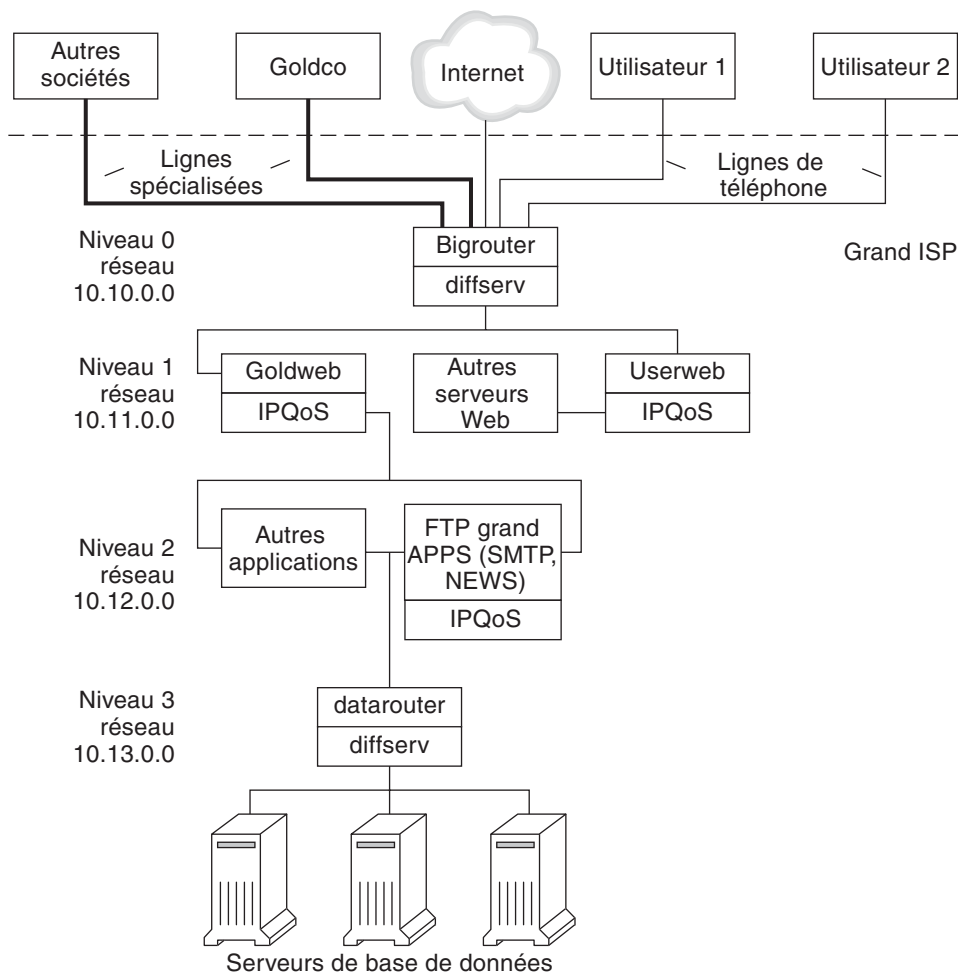
## Présentation d'un exemple de configuration IPQoS

Les tâches des autres chapitres de ce guide reprennent l'exemple de configuration IPQoS présenté dans cette section. L'exemple fait état d'une solution de services différenciés mise en place pour l'intranet public de BigISP, fournisseur de services fictif. BigISP offre des services à des grandes entreprises qui ont accès à BigISP par le biais de lignes spécialisées. Les utilisateurs qui se connectent via des modems peuvent également acheter des services auprès de BigISP.

### Topologie IPQoS

La figure suivante illustre la topologie du réseau exploitée par l'intranet public de BigISP.

FIGURE 28-4 Exemple de topologie IPQoS



BigISP a mis en place les quatre niveaux suivants dans son intranet public :

- **Niveau 0 :** le réseau 10.10.0.0 inclut un routeur Diffserv étendu appelé Bigrouter possédant des interfaces externes et internes. Plusieurs sociétés, notamment une grande organisation dénommée Goldco, a loué des services à lignes spécialisées aboutissant au Bigrouter. Le niveau 0 gère également des particuliers qui communiquent via les lignes téléphoniques ou le réseau RNIS.
- **Niveau 1 :** le réseau 10.11.0.0 fournit des services Web. Le serveur Goldweb héberge le site Web de Goldco que ce dernier a acquis auprès de BigISP dans le cadre du service premium. Le serveur Userweb héberge des sites Web de taille réduite achetés par des particuliers. Les sites Goldweb et Userweb sont compatibles IPQoS.

- **Niveau 2** : le réseau 10.12.0.0 met des applications à la disposition de l'ensemble de ses clients. Le serveur d'applications BigAPPS est compatible IPQoS. BigAPPS fournit des services de type SMTP, actualités et FTP.
- **Niveau 3** : le réseau 10.13.0.0 héberge des serveurs de bases de données de grande taille. L'accès au niveau 3 est contrôlé par datarouter (routeur Diffserv).





## Création du fichier de configuration IPQoS (tâches)

---

Ce chapitre décrit la procédure de création de fichiers de configuration IPQoS. Ce chapitre aborde les points suivants :

- [“Définition d'une stratégie QoS dans le fichier de configuration IPQoS \(liste des tâches\)” à la page 449](#)
- [“Outils de création d'une stratégie QoS” à la page 451](#)
- [“Création de fichiers de configuration IPQoS pour les serveurs Web” à la page 452](#)
- [“Création d'un fichier de configuration pour un serveur d'application” à la page 465](#)
- [“Fourniture de services différenciés sur un routeur” à la page 475](#)

Ce chapitre suppose que vous ayez préalablement défini une stratégie QoS complète et que vous soyez prêt à l'appliquer comme base du fichier de configuration IPQoS. Pour obtenir des instructions sur la planification de la stratégie QoS, reportez-vous à la section [“Planification de la stratégie de qualité de service” à la page 431](#).

### Définition d'une stratégie QoS dans le fichier de configuration IPQoS (liste des tâches)

Cette liste répertorie les tâches IPQoS d'ordre général nécessaires à la création d'un fichier de configuration et les liens vers les sections décrivant les étapes à suivre pour effectuer ces tâches.

Tâche	Description	Voir
1. Planification de la configuration de votre réseau IPQoS.	Déterminez les systèmes sur le réseau local qui doivent être activés pour IPQoS.	<a href="#">“Préparation d'un réseau pour IPQoS” à la page 433</a>

Tâche	Description	Voir
2. Planification de la stratégie QoS pour les systèmes IPQoS sur votre réseau.	Déterminez les différentes classes de service pour les flux de trafic. Déterminez ensuite les flux nécessitant une gestion du trafic.	“Planification de la stratégie de qualité de service” à la page 431
3. Création du fichier de configuration IPQoS et définition son action initiale.	Créez le fichier IPQoS, appelez le classificateur IP et définissez une classe de traitement.	“Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 454
4. Création des filtres d'une classe.	Ajoutez les filtres qui définissent le trafic sélectionné et organisé en une classe.	“Définition des filtres dans le fichier de configuration IPQoS” à la page 456
5. Ajout de plusieurs classes et de filtres au fichier de configuration IPQoS.	Créez des classes et des filtres supplémentaires pour le traitement par le classificateur IP.	“Création d'un fichier de configuration IPQoS pour un serveur Web au mieux” à la page 462
6. Ajout d'une instruction action avec des paramètres visant à configurer les modules de mesure.	Si la stratégie QoS fait appel au contrôle de flux, spécifiez les débits de contrôle de flux ainsi que les niveaux de conformité par rapport au compteur.	“Configuration du contrôle de flux dans le fichier de configuration IPQoS” à la page 472
7. Ajout d'une instruction d'action avec des paramètres visant à configurer le marqueur.	Si la stratégie QoS fait intervenir des comportements différenciés, définissez le mode de transmission des différentes classes de service.	“Définition de la transmission du trafic dans le fichier de configuration IPQoS” à la page 458
8. Ajout d'une instruction action aux paramètres visant à configurer les modules de mesure.	Si la stratégie QoS implique la collecte de statistiques relatives aux flux de trafic, définissez la manière dont les données sont rassemblées.	“Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS” à la page 461
9. Application du fichier de configuration IPQoS.	Ajoutez le contenu d'un fichier de configuration IPQoS spécifié dans le module du noyau qui convient.	“Application d'une nouvelle configuration aux modules de noyau IPQoS” à la page 478
10. Configuration des comportements dans les fichiers du routeur.	Si les fichiers de configuration IPQoS du réseau définissent les comportements de transmission, ajoutez les DSCP obtenus dans les fichiers d'ordonnancement appropriés sur le routeur.	“Configuration d'un routeur dans un réseau compatible IPQoS” à la page 475

## Outils de création d'une stratégie QoS

La stratégie QoS de votre réseau se trouve dans le fichier de configuration IPQoS. Vous créez ce fichier de configuration dans un éditeur de texte. Définissez ensuite ce fichier comme argument de l'utilitaire de configuration IPQoS, `ipqosconf`. Lorsque vous donnez pour instruction à `ipqosconf` d'appliquer la stratégie définie dans le fichier de configuration, la stratégie est consignée dans le noyau du système IPQoS. Pour des informations détaillées sur la commande `ipqosconf`, reportez-vous à la page de manuel `ipqosconf(1M)`. Pour obtenir des instructions sur l'utilisation d'`ipqosconf`, reportez-vous à la section “[Application d'une nouvelle configuration aux modules de noyau IPQoS](#)” à la page 478.

## Fichier de configuration IPQoS standard

Un fichier de configuration IPQoS consiste en l'arborescence d'une instruction d'action chargée d'implémenter la stratégie QoS, définie à la section “[Planification de la stratégie de qualité de service](#)” à la page 431. Le fichier de configuration IPQoS permet de configurer les modules IPQoS. Chaque instruction d'action contient un jeu de *classes*, de *filtres* ou de *paramètres* à traiter par le module appelé dans l'instruction d'action.

Pour connaître la syntaxe complète du fichier de configuration IPQoS, reportez-vous à l'[Exemple 32–3](#) et à la page de manuel `ipqosconf(1M)`.

## Configuration de la topologie d'un exemple IPQoS

Les tâches décrites dans ce chapitre indiquent comment créer un fichier de configuration IPQoS pour trois systèmes compatibles IPQoS. Ces systèmes font partie de la topologie du réseau de l'entreprise BigISP, présentée dans la [Figure 28–4](#).

- Goldweb : serveur Web hébergeant les sites Web de clients ayant acquis des accords de niveau de service de type premium
- Userweb : serveur Web moins puissant hébergeant des sites web personnels pour des usagers domestiques qui ont souscrit à des accords de niveau de service "au mieux"
- BigAPPS : serveur d'application délivrant des messages électroniques, des actualités sur le réseau et un service FTP aux clients des services Premium et au mieux

Ces trois fichiers de configuration illustrent les configurations IPQoS les plus courantes. Il est possible d'utiliser les fichiers d'exemple présentés à la section suivante comme modèle de votre propre implémentation IPQoS.

## Création de fichiers de configuration IPQoS pour les serveurs Web

Cette section présente le fichier de configuration IPQoS et la procédure destinée à créer un fichier de configuration pour un serveur Web de type premium. Cette section explique comment configurer un niveau de service complètement différent dans un autre fichier de configuration pour un serveur hébergeant des sites Web personnels. Les deux serveurs appartiennent au réseau illustré dans la [Figure 28-4](#).

Le fichier de configuration suivant définit les activités IPQoS du serveur Goldweb. Ce serveur héberge le site Web de Goldco, l'entreprise qui a acquis un accord de niveau de service de niveau premium.

### EXEMPLE 29-1 Fichier de configuration IPQoS pour un serveur Web premium

```
fmt_version 1.0

action {
  module ipgpc
  name ipgpc.classify
  params {
    global_stats TRUE
  }
  class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
  }
  class {
    name video
    next_action markEF
    enable_stats FALSE
  }
  filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
  }
  filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
  }
}
action {
  module dscpmk
  name markAF11
  params {
    global_stats FALSE
    dscp_map{0-63:10}
    next_action continue
  }
}
```

**EXEMPLE 29-1** Fichier de configuration IPQoS pour un serveur Web premium (Suite)

```

}
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
action {
    module flowacct
    name acct
    params {
        enable_stats TRUE
        timer 10000
        timeout 10000
        max_limit 2048
    }
}

```

Le fichier de configuration suivant définit les activités IPQoS sur Userweb. Ce serveur héberge des sites Web pour les accords de niveau de service à bas prix ou *au mieux*. Ce niveau de service garantit le meilleur service susceptible d'être fourni après la gestion, par le système IPQoS, du trafic correspondant aux clients bénéficiant d'accords de niveau de service plus onéreux.

**EXEMPLE 29-2** Exemple de configuration pour un serveur Web "au mieux"

```

fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name Userweb
        next_action markAF12
        enable_stats FALSE
    }
    filter {
        name webout
        sport 80
        direction LOCAL_OUT
        class Userweb
    }
}
action {
    module dscpmk
    name markAF12
    params {
        global_stats FALSE
    }
}

```

**EXEMPLE 29-2** Exemple de configuration pour un serveur Web "au mieux" (Suite)

```

    dscp_map{0-63:12}
    next_action continue
  }
}

```

## ▼ Création du fichier de configuration IPQoS et définition des classes de trafic

Vous créez le fichier de configuration IPQoS initial dans le répertoire que vous jugez le plus facile à gérer. Les tâches ce chapitre font appel au répertoire `/var/ipqos` pour enregistrer les fichiers de configuration IPQoS. La procédure suivante génère le segment initial du fichier de configuration IPQoS présenté dans l'[Exemple 29-1](#).

---

**Remarque** – Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque instruction `action` et chaque clause par des accolades (`{ }`). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'[Exemple 29-1](#).

---

### 1 Connectez-vous au serveur Web premium et générez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.

La première ligne non commentée de chaque fichier de configuration IPQoS doit commencer par le numéro de version `fmt_version 1.0`.

### 2 Faites suivre le paramètre d'ouverture par l'instruction `action` initiale chargée de configurer le classificateur d'IP générique `ipgpc`.

L'action initiale marque le début de l'arborescence des instructions `action` composant le fichier de configuration IPQoS. Par exemple, le fichier `/var/ipqos/Goldweb.qos` commence par l'instruction initiale `action` destinée à appeler le classificateur `ipgpc`.

```
fmt_version 1.0
```

```
action {
    module ipgpc
    name ipgpc.classify

```

`fmt_version 1.0` Marque le début du fichier de configuration IPQoS.

`action {` Marque le début de l'instruction d'action.

`module ipgpc` Configure le classificateur `ipgpc` en tant qu'action initiale du fichier de configuration.

`name ipgpc.classify` Définit le nom de l'instruction `action` du classifieur qui doit toujours correspondre à `ipgpc.classify`.

Pour plus d'informations sur les détails de la syntaxe des instructions `action`, reportez-vous à la section “[Instruction action](#)” à la page 505 et à la page de manuel `ipqosconf(1M)`.

### 3 Ajoutez une clause `params` au paramètre de statistiques `global_stats`.

```
params {
    global_stats TRUE
}
```

Le paramètre `global_stats TRUE` dans l'instruction `ipgpc.classify` permet de collecter les statistiques liées à cette action. `global_stats TRUE` permet de recueillir des statistiques par classe dès qu'une définition de clause de classe a la valeur `enable_stats TRUE`.

L'activation des statistiques a un effet sur les performances. Il est possible de recueillir des statistiques sur un nouveau fichier de configuration IPQoS pour vérifier qu'IPQoS fonctionne correctement. Par la suite, vous pouvez désactiver la collecte de statistiques en attribuant à l'argument `global_stats` la valeur `FALSE`.

Les statistiques générales ne représentent qu'un seul type de paramètre que vous pouvez définir dans une clause `params`. Pour plus d'informations sur la syntaxe et sur d'autres détails relatifs aux clauses `params`, reportez-vous à la section “[Clause params](#)” à la page 508 et à la page de manuel `ipqosconf(1M)`.

### 4 Définissez une classe destinée à identifier le trafic lié au serveur premium.

```
class {
    name goldweb
    next_action markAF11
    enable_stats FALSE
}
```

Cette instruction appelée une *clause de classe*. Le contenu de la clause `class` est le suivant.

<code>name goldweb</code>	Crée la classe <code>goldweb</code> pour identifier le trafic rattaché au serveur <code>Goldweb</code> .
<code>next_action markAF11</code>	Donne l'instruction au module <code>ipgpc</code> de transmettre les paquets de la classe <code>goldweb</code> à l'instruction d'action <code>markAF11</code> . Cette instruction <code>markAF11</code> appelle le marqueur <code>ds_cpmk</code> .
<code>enable_stats FALSE</code>	Active le recueil de statistiques pour la classe <code>goldweb</code> . Cependant, étant donné que la valeur <code>FALSE</code> est définie pour le paramètre <code>enable_stats</code> , les statistiques de cette classe ne sont pas recueillies.

Pour des informations détaillées sur la syntaxe de la clause `class`, reportez-vous à la section “[Clause class](#)” à la page 507 et à la page de manuel `ipqosconf(1M)`.

### 5 Définissez une classe identifiant une application devant bénéficier de la priorité de transmission la plus haute.

```
class {
    name video
```

<pre>        next_action marKEF         enable_stats FALSE     }</pre>	
name video	Crée la classe vidéo destinée à identifier le trafic du flux vidéo sortant du serveur Goldweb.
next_action marKEF	Donne l'instruction au module ipgpc de transmettre les paquets de la classe video à l'instruction marKEF après traitement par ipgpc. L'instruction marKEF appelle le marqueur dscpmk.
enable_stats FALSE	Active le recueil de statistiques pour la classe video. Néanmoins, étant donné que la valeur FALSE est définie pour le paramètre enable_stats, la collecte de statistiques n'est pas activée pour la classe.

- Voir aussi**
- Pour définir les filtres de la classe que vous venez de créer, reportez-vous à la section [“Définition des filtres dans le fichier de configuration IPQoS”](#) à la page 456.
  - Pour créer une clause de classe supplémentaire pour le fichier de configuration, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic”](#) à la page 454.

## ▼ Définition des filtres dans le fichier de configuration IPQoS

La procédure suivante précise comment définir les filtres d'une classe dans le fichier de configuration IPQoS.

### Avant de commencer

La procédure suppose que vous ayez déjà lancé la création du fichier et défini des classes. Les étapes poursuivent la génération du fichier /var/ipqos/Goldweb.qos créé à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic”](#) à la page 454.

---

**Remarque** – Lors de la création du fichier de configuration IPQoS, veillez à commencer et à terminer chaque clause `class` et chaque clause `filter` par des accolades (`{ }`). Pour plus de détails sur l'utilisation des accolades, reportez-vous à l'[Exemple 29–1](#).

---

### 1 Ouvrez le fichier de configuration IPQoS et recherchez la fin de la dernière classe définie.

Par exemple, sur le serveur IPQoS Goldweb, vous devez débiter après la clause `class` suivante dans le fichier /var/ipqos/Goldweb.qos :

```
class {
    name video
    next_action marKEF
```



```

    enable_stats FALSE
}

```

## 2 Définissez une clause `filter` afin de sélectionner le trafic sortant du système IPQoS.

```

filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class goldweb
}

```

`name webout`                      Attribue le nom `webout` au filtre.

`sport 80`                              Sélectionne le trafic par le port source 80, port réservé au trafic (Web) HTTP.

`direction LOCAL_OUT`              Affine la sélection du trafic sortant provenant du système local.

`class goldweb`                      Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `goldweb`.

Pour des informations sur la syntaxe et d'autres détails sur la clause `filter` figurant dans le fichier de configuration IPQoS, reportez-vous à la section “[Clause `filter`](#)” à la page 507.

## 3 Définissez une clause `filter` pour sélectionner le trafic de flux vidéo dans le système IPQoS.

```

filter {
    name videoout
    sport videosrv
    direction LOCAL_OUT
    class video
}

```

`name videoout`                      Attribue le nom `videoout` au filtre.

`sport videosrv`                      Sélectionne le trafic par le port source `videosrv`, port précédemment défini pour les applications de flux vidéo du système.

`direction LOCAL_OUT`              Affine la sélection du trafic sortant provenant du système local.

`class video`                              Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `video`.

- Voir aussi**
- Pour définir les comportements au niveau des modules de marquage, reportez-vous à la section “[Définition de la transmission du trafic dans le fichier de configuration IPQoS](#)” à la page 458.
  - Pour définir les paramètres de contrôle des flux au niveau des modules de mesure, reportez-vous à la section “[Configuration du contrôle de flux dans le fichier de configuration IPQoS](#)” à la page 472.
  - Pour activer le fichier de configuration IPQoS, reportez-vous à la section “[Application d'une nouvelle configuration aux modules de noyau IPQoS](#)” à la page 478.

- Pour définir des filtres supplémentaires, reportez-vous à la section “[Définition des filtres dans le fichier de configuration IPQoS](#)” à la page 456.
- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section “[Configuration d'un fichier de configuration IPQoS pour un serveur d'application](#)” à la page 467.

## ▼ Définition de la transmission du trafic dans le fichier de configuration IPQoS

La procédure suivante indique comment définir la transmission du trafic en ajoutant des comportements par pas à une classe dans le fichier de configuration IPQoS.

### Avant de commencer

Cette procédure suppose que vous disposiez d'un fichier de configuration IPQoS assorti de classes et de filtres déjà définis. Les étapes poursuivent la génération du fichier `/var/ipqos/Goldweb.qos` de l'[Exemple 29-1](#).

---

**Remarque** – La procédure montre comment configurer la transmission du trafic à l'aide du module de marquage `dscpmk`. Pour plus d'informations sur la transmission du trafic sur des systèmes VLAN à l'aide du marqueur `dlcosmk`, reportez-vous à la section “[Utilisation du marqueur `dlcosmk` avec les périphériques VLAN](#)” à la page 499.

---

### 1 Ouvrez le fichier de configuration IPQoS et recherchez la fin du dernier filtre défini.

Par exemple, sur le serveur IPQoS Goldweb, vous devez débiter après la clause `filter` suivante dans le fichier `/var/ipqos/Goldweb.qos` :

```
filter {  
    name videoout  
    sport videosrv  
    direction LOCAL_OUT  
    class video  
}
```

La clause `filter` se trouve à la fin de l'instruction `action` du classificateur `ipgpc`. Par conséquent, vous devez insérer deux accolades : la première signale la fin du filtre et la deuxième la fin de l'instruction `action`.

### 2 Appelez le marqueur à l'aide de l'instruction `action` suivante.

```
action {  
    module dscpmk  
    name markAF11
```

`module dscpmk`      Sollicite le module de marquage `dscpmk`.

`name markAF11` Attribue le nom `markAF11` à l'instruction `action`.

La classe précédemment définie `goldweb` inclut une instruction `next_action markAF11`. Cette instruction envoie les flux de trafic vers l'instruction d'action `markAF11` à l'issue du traitement par le classificateur.

### 3 Définissez les actions que le marqueur doit appliquer au flux de trafic.

```
params {
    global_stats FALSE
    dscp_map{0-63:10}
    next_action continue
}
```

`global_stats FALSE` Active la collecte de statistiques pour l'instruction `action markAF11` du marqueur. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

`dscp_map{0-63:10}` Attribue un DSCP égal à 10 aux en-têtes de paquets de la classe de trafic `goldweb` actuellement traitée par le marqueur.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic `goldweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP 10 donne pour instruction au marqueur d'attribuer la valeur décimale 10 (binaire 001010) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `goldweb` sont soumis au comportement AF11. AF11 garantit à tous les paquets de DSCP 10 un service haute priorité avec un taux de perte faible. Ainsi, le trafic sortant des client premium sur `Goldweb` bénéficie de la priorité la plus haute disponible pour le PHB Assured Forwarding (AF). Pour consulter le tableau des DSCP possibles pour AF, reportez-vous au [Tableau 32-2](#).

### 4 Lancez une autre instruction action du marqueur.

```
action {
    module dscpmk
    name markEF
```

`module dscpmk` Sollicite le module de marquage `dscpmk`.

`name markEF` Attribue le nom `markEF` à l'instruction `action`.

### 5 Définissez les actions que le marqueur doit appliquer au flux de trafic.

```
params {
    global_stats TRUE
    dscp_map{0-63:46}
    next_action acct
}
```

<code>global_stats TRUE</code>	Active la collecte des statistiques sur une classe video, chargée de sélectionner les paquets de flux vidéo.
<code>dscp_map{0-63:46}</code>	Attribue un DSCP égal à 46 aux en-têtes de paquets de la classe de trafic video actuellement traitée par le marqueur.
<code>next_action acct</code>	Donne l'instruction au module dscpmk de transmettre les paquets de la classe video à l'instruction action acct après traitement par dscpmk. L'instruction acct action appelle le module flowacct.

Le DSCP 46 demande au module dscpmk d'attribuer la valeur décimale 46 (binaire 101110) à toutes les entrées de structure dscp, dans le champ DS. Ce point de code signale que les paquets de la classe de trafic video sont soumis au comportement EF.

---

**Remarque** – Le point de code recommandé est 46 (binaire 101110). D'autres DSCP assignent des PHB AF à un paquet.

---

Le PHB EF garantit aux paquets de DSCP 46 un traitement prioritaire par les systèmes compatibles IPQoS et Diffserv. Définir des flux pour les applications nécessite un service de priorité élevée conduisant logiquement à l'attribution de PHB de type EF dans la stratégie QoS. Pour plus de détails sur le PHB EF, reportez-vous à la section [“PHB Expedited Forwarding \(EF\) \(ou traitement accéléré\)”](#) à la page 498.

- 6 Ajoutez les DSCP que vous venez de créer dans les fichiers appropriés sur le routeur Diffserv.**  
Pour plus d'informations, reportez-vous à la section [“Configuration d'un routeur dans un réseau compatible IPQoS”](#) à la page 475.

- Voir aussi**
- Pour lancer la collecte de statistiques de comptabilisation des flux de trafic, reportez-vous à la section [“Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS”](#) à la page 461.
  - Pour définir les comportements au niveau des modules de marquage, reportez-vous à la section [“Définition de la transmission du trafic dans le fichier de configuration IPQoS”](#) à la page 458.
  - Pour définir les paramètres de contrôle des flux au niveau des modules de mesure, reportez-vous à la section [“Configuration du contrôle de flux dans le fichier de configuration IPQoS”](#) à la page 472.
  - Pour activer le fichier de configuration IPQoS, reportez-vous à la section [“Application d'une nouvelle configuration aux modules de noyau IPQoS”](#) à la page 478.
  - Pour définir des filtres supplémentaires, reportez-vous à la section [“Définition des filtres dans le fichier de configuration IPQoS”](#) à la page 456.

- Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section “[Configuration d'un fichier de configuration IPQoS pour un serveur d'application](#)” à la page 467.

## ▼ Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS

La procédure suivante indique la manière d'activer la comptabilisation pour une classe de trafic dans le fichier de configuration IPQoS. La procédure précise comment définir la comptabilisation des flux pour la classe video, présentée à la section “[Création du fichier de configuration IPQoS et définition des classes de trafic](#)” à la page 454. Cette classe sélectionne le trafic vidéo qui doit être facturé au client premium au titre de l'accord de niveau de service contracté.

### Avant de commencer

La procédure suppose que vous possédiez un fichier de configuration IPQoS comportant des classes, des filtres, des actions de mesure, le cas échéant, et d'éventuelles actions de marquage. Les étapes poursuivent la génération du fichier `/var/ipqos/Goldweb.qos` de l'[Exemple 29-1](#).

#### 1 Ouvrez le fichier de configuration IPQoS et recherchez la fin de la dernière instruction action définie.

Par exemple, sur le serveur IPQoS Goldweb, vous devez débiter après l'instruction action markEF suivante dans le fichier `/var/ipqos/Goldweb.qos`.

```
action {
    module dscpmk
    name markEF
    params {
        global_stats TRUE
        dscp_map{0-63:46}
        next_action acct
    }
}
```

#### 2 Spécifiez une instruction action qui déclenche la comptabilisation des flux.

```
action {
    module flowacct
    name acct
```

module flowacct      Invoque le module de comptabilisation des flux flowacct.

name acct              Attribue le nom acct à l'instruction action.

#### 3 Définissez une clause params pour contrôler la comptabilisation de la classe de trafic.

```
params {
    global_stats TRUE
    timer 10000
```

```

        timeout 10000
        max_limit 2048
        next_action continue
    }
}

```

<code>global_stats TRUE</code>	Active la collecte des statistiques sur la classe video, chargée de sélectionner les paquets de flux vidéo.
<code>timer 10000</code>	Spécifie la durée de l'intervalle, exprimé en millisecondes, lors de l'analyse de la table de flux afin de vérifier les flux dont le délai d'attente a expiré. Pour ce paramètre, l'intervalle correspond à 10 000 millisecondes.
<code>timeout 10000</code>	Spécifie la valeur minimale de l'intervalle du délai d'expiration. Un flux arrive à expiration lorsque les paquets du flux n'apparaissent pas à l'issue de l'intervalle défini. Pour ce paramètre, les paquets parviennent à expiration au bout de 10 000 millisecondes.
<code>max_limit 2048</code>	Définit le nombre maximum d'enregistrements de flux actifs dans la table de flux pour cette instance d'action.
<code>next_action continue</code>	Indique qu'aucun traitement supplémentaire n'est requis sur les paquets de la classe de trafic video et que ces paquets peuvent revenir dans le flux réseau.

Le module `flowacct` collecte les informations statistiques sur les flux de paquet d'une classe particulière tant que la valeur `timeout` spécifiée n'est pas atteinte.

- Voir aussi**
- Pour configurer les comportements par pas sur un routeur, reportez-vous à la section [“Configuration d'un routeur dans un réseau compatible IPQoS”](#) à la page 475.
  - Pour activer le fichier de configuration IPQoS, reportez-vous à la section [“Application d'une nouvelle configuration aux modules de noyau IPQoS”](#) à la page 478.
  - Pour créer des classes pour les flux de trafic provenant d'applications, reportez-vous à la section [“Configuration d'un fichier de configuration IPQoS pour un serveur d'application”](#) à la page 467.

## ▼ Création d'un fichier de configuration IPQoS pour un serveur Web au mieux

Le fichier de configuration IPQoS d'un serveur Web au mieux diffère légèrement du fichier de configuration IPQoS utilisé par un serveur Web de niveau premium. La procédure utilise le fichier de configuration illustré à l'[Exemple 29-2](#).

### 1 Connectez-vous au serveur Web au mieux.

**2 Produisez un nouveau fichier de configuration IPQoS suivi de l'extension .qos.**

```

fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}

```

Le fichier `/var/ipqos/userweb.qos` doit commencer par l'instruction partielle `action` visant à appeler le classificateur `ipgpc`. En outre, l'instruction `action` possède une clause `params` en mesure d'activer le recueil de statistiques. Pour obtenir une explication de l'instruction `action`, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic”](#) à la page 454.

**3 Définissez une classe identifiant le trafic lié au serveur Web au mieux.**

```

class {
    name userweb
    next_action markAF12
    enable_stats FALSE
}

```

`name userweb`                      Crée une classe appelée `userweb` pour la transmission du trafic Web émanant des utilisateurs.

`next_action markAF1`              Demande au module `ipgpc` de transmettre les paquets de la classe `userweb` à l'instruction `action markAF12` après traitement par `ipgpc`. L'instruction `action markAF12` appelle le module `dscpmk`.

`enable_stats FALSE`              Active le recueil de statistiques pour la classe `userweb`. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques ne se produit pas.

Pour obtenir une explication de la tâche de la clause `class`, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic”](#) à la page 454.

**4 Définissez une clause `filter` pour sélectionner les flux de trafic pour la classe `userweb`.**

```

filter {
    name webout
    sport 80
    direction LOCAL_OUT
    class userweb
}
}

```

`name webout`                      Attribue le nom `webout` au filtre.

`sport 80`                              Sélectionne le trafic par le port source 80, port réservé au trafic (Web) HTTP.

`direction LOCAL_OUT`              Affine la sélection du trafic sortant provenant du système local.

`class userweb` Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe `userweb`.

Pour obtenir une explication de la tâche liée à la clause `filter`, reportez-vous à la section [“Définition des filtres dans le fichier de configuration IPQoS”](#) à la page 456.

## 5 Commencez l'instruction `action` en appelant le marqueur `dscpmk`.

```
action {
    module dscpmk
    name markAF12
```

`module dscpmk` Sollicite le module de marquage `dscpmk`.

`name markAF12` Attribue le nom `markAF12` à l'instruction `action`.

La classe précédemment définie `userweb` inclut une instruction `next_action markAF12`. Cette instruction envoie les flux de trafic vers l'instruction `action markAF12` à l'issue du traitement par le classificateur.

## 6 Définissez les paramètres pour le marqueur à utiliser pour traitement du flux de trafic.

```
params {
    global_stats FALSE
    dscp_map{0-63:12}
    next_action continue
}
```

`global_stats FALSE` Active la collecte de statistiques pour l'instruction `action markAF12` du marqueur. Néanmoins, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, la collecte de statistiques n'a pas lieu.

`dscp_map{0-63:12}` Attribue un DSCP égal à 12 aux en-têtes de paquets de la classe de trafic `userweb` actuellement traitée par le marqueur.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `userweb` et que ces paquets peuvent revenir dans le flux réseau.

Un DSCP 12 donne pour instruction au marqueur d'attribuer la valeur décimale 12 (binaire 001100) à toutes les entrées de la structure `dscp`. Ce point de code signale que les paquets de la classe de trafic `userweb` sont soumis au comportement AF12. AF12 garantit à tous les paquets de DSCP 12 un service haute priorité avec un taux de perte moyen.

## 7 Lorsque vous terminez le fichier de configuration IPQoS, appliquez la configuration.

- Voir aussi**
- Pour ajouter des classes et d'autres configurations aux flux de trafic provenant d'applications, reportez-vous à la section [“Configuration d'un fichier de configuration IPQoS pour un serveur d'application”](#) à la page 467.



- Pour configurer les comportements par pas sur un routeur, reportez-vous à la section “[Configuration d'un routeur dans un réseau compatible IPQoS](#)” à la page 475.
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section “[Application d'une nouvelle configuration aux modules de noyau IPQoS](#)” à la page 478.

## Création d'un fichier de configuration pour un serveur d'application

Cette section décrit comment créer un fichier de configuration pour un serveur d'application délivrant des applications importantes aux clients. La procédure utilise le serveur BigAPPS de la [Figure 28–4](#) en guise d'exemple.

Le fichier de configuration suivant définit les activités IPQoS du serveur BigAPPS. Ce serveur héberge, à l'usage des clients, des données FTP, des messages électroniques (SMTP) ainsi que des informations sur le réseau (NNTP).

### EXEMPLE 29–3 Exemple de fichier de configuration pour un serveur d'application

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
    class {
        name smtp
        enable_stats FALSE
        next_action markAF13
    }
    class {
        name news
        next_action markAF21
    }
    class {
        name ftp
        next_action meterftp
    }
    filter {
        name smtpout
        sport smtp
        class smtp
    }
    filter {
        name newsout
        sport nntp
        class news
    }
    filter {
```

**EXEMPLE 29-3** Exemple de fichier de configuration pour un serveur d'application (Suite)

```
        name ftpout
        sport ftp
        class ftp
    }
    filter {
        name ftpdata
        sport ftp-data
        class ftp
    }
}
action {
    module dscpmk
    name markAF13
    params {
        global_stats FALSE
        dscp_map{0-63:14}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
action {
    module tokenmt
    name meterftp
    params {
        committed_rate 50000000
        committed_burst 50000000
        red_action_name AF31
        green_action_name markAF22
        global_stats TRUE
    }
}
action {
    module dscpmk
    name markAF31
    params {
        global_stats TRUE
        dscp_map{0-63:26}
        next_action continue
    }
}
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

## EXEMPLE 29-3 Exemple de fichier de configuration pour un serveur d'application (Suite)

```
    }
}
```

## ▼ Configuration d'un fichier de configuration IPQoS pour un serveur d'application

- 1 Connectez-vous au serveur IPQoS et générez un nouveau fichier de configuration IPQoS suivi de l'extension `.qos`.

Par exemple, créez le fichier `/var/ipqos/BigAPPS.qos` pour le serveur d'application. Commencez par les phrases suivantes pour lancer l'instruction `action` visant à appeler le classificateur `ipgpc` :

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
    params {
        global_stats TRUE
    }
}
```

Pour obtenir une explication de l'instruction `action` d'ouverture, reportez-vous à la section “Création du fichier de configuration IPQoS et définition des classes de trafic” à la page 454.

- 2 Créez des classes pour sélectionner le trafic de trois applications situées sur le serveur BigAPPS.

Ajoutez les définitions de classe après l'instruction `action` de départ.

```
class {
    name smtp
    enable_stats FALSE
    next_action markAF13
}
class {
    name news
    next_action markAF21
}
class {
    name ftp
    enable_stats TRUE
    next_action meterftp
}
```

`name smtp`

Crée une classe appelée `smtp` qui intègre les flux de trafic de messagerie électronique à gérer par l'application SMTP.

<code>enable_stats FALSE</code>	Active le recueil de statistiques pour la classe <code>smtp</code> . Cependant, étant donné que la valeur <code>FALSE</code> est définie pour le paramètre <code>enable_stats</code> , les statistiques de cette classe ne sont pas recueillies.
<code>next_action markAF13</code>	Demande au module <code>ipgpc</code> de transmettre les paquets de la classe <code>smtp</code> à l'instruction <code>action markAF13</code> après traitement par <code>ipgpc</code> .
<code>name news</code>	Crée une classe appelée <code>news</code> qui intègre les flux d'informations sur le réseau à gérer par l'application <code>NNTP</code> .
<code>next_action markAF21</code>	Donne l'instruction au module <code>ipgpc</code> de transmettre les paquets de la classe <code>news</code> à l'instruction <code>markAF21</code> après traitement par <code>ipgpc</code> .
<code>name ftp</code>	Crée une classe appelée <code>ftp</code> qui traite le trafic sortant géré par l'application <code>FTP</code> .
<code>enable_stats TRUE</code>	Active le recueil de statistiques pour la classe <code>ftp</code> .
<code>next_action meterftp</code>	Demande au module <code>ipgpc</code> de transmettre les paquets de la classe <code>ftp</code> à l'instruction <code>action meterftp</code> après traitement par <code>ipgpc</code> .

Pour plus d'informations sur la définition des classes, reportez-vous à la section [“Création du fichier de configuration IPQoS et définition des classes de trafic”](#) à la page 454.

### 3 Définissez des clauses `filter` afin de sélectionner le trafic des classes définies à l'étape 2.

```
filter {  
    name smtpout  
    sport smtp  
    class smtp  
}  
filter {  
    name newsout  
    sport nntp  
    class news  
}  
    filter {  
        name ftpout  
        sport ftp  
        class ftp  
    }  
    filter {  
        name ftpdata  
        sport ftp-data  
        class ftp  
    }  
}
```

<code>name smtpout</code>	Attribue le nom <code>smtpout</code> au filtre.
<code>sport smtp</code>	Sélectionne le trafic transitant par le port source 25 représentant le port consacré à l'application <code>sendmail</code> (SMTP).

<code>class smtp</code>	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe <code>smtp</code> .
<code>name newsout</code>	Attribue le nom <code>newsout</code> au filtre.
<code>sport nntp</code>	Sélectionne le trafic transitant par le port source <code>nntp</code> , couramment utilisé pour l'application d'informations réseau (NNTP).
<code>class news</code>	Identifie la classe à laquelle le filtre appartient, dans cette instance, il s'agit de la classe <code>news</code> .
<code>name ftpout</code>	Attribue le nom <code>ftpout</code> au filtre.
<code>sport ftp</code>	Sélectionne les données de contrôle passant par le port source 21, port réservé au trafic FTP.
<code>name ftpdata</code>	Attribue le nom <code>ftpdata</code> au filtre.
<code>sport ftp-data</code>	Sélectionne les données de contrôle passant par le port source 20, port réservé aux données de trafic FTP.
<code>class ftp</code>	Identifie la classe à laquelle les filtres <code>ftpout</code> et <code>ftpdata</code> appartiennent. Dans cet exemple, il s'agit de <code>ftp</code> .

- Voir aussi**
- Pour définir des filtres, reportez-vous à la section “[Définition des filtres dans le fichier de configuration IPQoS](#)” à la page 456.
  - Pour définir les comportements pour le trafic de l'application, reportez-vous à la section “[Configuration de la transmission du trafic d'une application dans le fichier de Configuration IPQoS](#)” à la page 469.
  - Pour configurer le contrôle des flux à l'aide des modules de mesure, reportez-vous à la section “[Configuration du contrôle de flux dans le fichier de configuration IPQoS](#)” à la page 472.
  - Pour configurer la comptabilisation des flux, reportez-vous à la section “[Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS](#)” à la page 461.

## ▼ Configuration de la transmission du trafic d'une application dans le fichier de Configuration IPQoS

La procédure suivante indique comment configurer le transfert du trafic d'une application. Dans la procédure, vous définissez les comportements par pas pour les classes de trafic de l'application qui sont susceptibles d'avoir des niveaux de priorité inférieurs à ceux d'autres flux de trafic sur un réseau. Les étapes poursuivent la génération du fichier `/var/ipqos/BigAPPS.qos` de l'[Exemple 29-3](#).

**Avant de commencer**

Cette procédure suppose que vous disposiez d'un fichier de configuration IPSQoS assorti de classes et de filtres déjà définis pour les applications à marquer.

**1 Ouvrez le fichier de configuration IPQoS créé pour le serveur d'application et localisez la fin de la dernière clause `filter`.**

Dans le fichier `/var/ipqos/BigAPPS.qos`, le filtre final est le suivant :

```
filter {
    name ftpdata
    sport ftp-data
    class ftp
}
```

**2 Appelez le marqueur de la manière suivante :**

```
action {
    module dscpmk
    name markAF13
```

`module dscpmk`      Sollicite le module de marquage `dscpmk`.

`name markAF13`      Attribue le nom `markAF13` à l'instruction `action`.

**3 Définissez le comportement par pas à signaler au niveau des flux de trafic de courriers électroniques.**

```
params {
    global_stats FALSE
    dscp_map{0-63:14}
    next_action continue
}
```

`global_stats FALSE`      Active la collecte de statistiques pour l'instruction `action markAF13` du marqueur. Cependant, étant donné que la valeur `FALSE` est définie pour le paramètre `enable_stats`, les statistiques ne sont pas recueillies.

`dscp_map{0-63:14}`      Attribue un DSCP égal à 14 aux en-têtes de paquets de la classe de trafic `smtp` actuellement traitée par le marqueur.

`next_action continue`      Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic `smtp`. Ces paquets peuvent alors revenir dans le flux du réseau.

Un DSCP 14 donne pour instruction au marqueur d'attribuer la valeur décimale 14 (binaire 001110) à toutes les entrées de la structure `ds cp`. Le DSCP 14 définit le comportement AF13. Le marqueur signale les paquets de la classe de trafic `smtp` par le DSCP 14 dans le champ DS.

AF13 assigne à l'ensemble des paquets marqués d'un DSCP 14 un niveau de priorité élevé. Cependant, étant donné que AF13 garantit une priorité de classe 1, le routeur garantit une

priorité élevée au trafic sortant des courriers électroniques dans la file d'attente. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au [Tableau 32-2](#).

#### 4 Ajoutez une instruction **action** de marqueur pour définir un comportement pour le trafic des informations réseau :

```
action {
  module dscpmk
  name markAF21
  params {
    global_stats FALSE
    dscp_map{0-63:18}
    next_action continue
  }
}
```

`name markAF21`      Attribut le nom `markAF21` à l'instruction `action`.

`dscp_map{0-63:18}`      Attribue un DSCP égal à 18 aux en-têtes de paquets de la classe de trafic `nntp` actuellement traitée par le marqueur.

Le DSCP 18 donne pour instruction au marqueur d'attribuer la valeur décimale 18 (binaire 010010) à toutes les entrées de la structure `dscp`. Le DSCP 18 définit le comportement AF21. Le marqueur signale les paquets de la classe de trafic `news` par le DSCP 18 dans le champ `DS`.

AF21 garantit que tous les paquets avec un DSCP égal à 18 se voient attribuer un niveau de perte faible assorti d'une priorité de classe 2. Ainsi, les probabilités de perdre les données de trafic d'informations sur le réseau sont faibles.

- Voir aussi**
- Pour ajouter des informations de configuration pour les serveurs Web, reportez-vous à la section “[Création du fichier de configuration IPQoS et définition des classes de trafic](#)” à la page 454.
  - Pour configurer le contrôle des flux à l'aide des modules de mesure, reportez-vous à la section “[Configuration du contrôle de flux dans le fichier de configuration IPQoS](#)” à la page 472.
  - Pour configurer la comptabilisation des flux, reportez-vous à la section “[Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS](#)” à la page 461.
  - Pour configurer les comportements sur un routeur, reportez-vous à la section “[Configuration d'un routeur dans un réseau compatible IPQoS](#)” à la page 475.
  - Pour activer le fichier de configuration IPQoS, reportez-vous à la section “[Application d'une nouvelle configuration aux modules de noyau IPQoS](#)” à la page 478.

## ▼ Configuration du contrôle de flux dans le fichier de configuration IPQoS

Pour contrôler le débit selon lequel un flux de trafic est libéré sur le réseau, vous devez définir des paramètres de mesure. Vous pouvez utiliser un des deux modules de mesure, `tokenmt` ou `tswtc_lmt`, dans le fichier de configuration IPQoS.

La procédure suivante poursuit l'élaboration du fichier de configuration IPQoS pour le serveur d'application de l'[Exemple 29-3](#). Dans la procédure, vous pouvez configurer les actions de mesure, mais aussi les actions de deux modules de marquage appelées par l'instruction `action` du module de mesure.

### Avant de commencer

Les étapes supposent que vous ayez déjà défini une classe et un filtre pour l'application dont vous voulez contrôler le flux.

#### 1 Ouvrez le fichier de configuration IPQoS que vous avez créé pour le serveur d'applications.

Dans le fichier `/var/ipqos/BigAPPS.qos`, vous commencez après l'action du marqueur suivante :

```
action {
    module dscpmk
    name markAF21
    params {
        global_stats FALSE
        dscp_map{0-63:18}
        next_action continue
    }
}
```

#### 2 Créez une instruction `action` pour le module de mesure afin de contrôler le trafic d'une classe ftp.

```
action {
    module tokenmt
    name meterftp
```

`module tokenmt`      Sollicite le module de mesure `tokenmt`.

`name meterftp`      Attribut le nom `meterftp` à l'instruction `action`.

#### 3 Ajoutez les paramètres à configurer le débit du module de mesure.

```
params {
    committed_rate 50000000
    committed_burst 50000000
```

`committed_rate 50000000`      Assigne une vitesse de transmission de 50 000 000 bps au trafic de la classe ftp.



`committed_burst 50000000` Valide une taille de rafale de 50 000 000 bits pour le trafic de la classe ftp.

Pour une explication des paramètres `tokenmt`, reportez-vous à la section “[Configuration du tokenmt en tant que compteur à débit double](#)” à la page 495.

#### 4 Ajoutez des paramètres pour configurer les niveaux de priorité de conformité de trafic :

```
red_action markAF31
green_action_name markAF22
global_stats TRUE
}
```

`red_action_name markAF31` Indique que le flux de trafic de la classe ftp dépasse le débit garanti, les paquets sont envoyés vers l'instruction de marquage `action markAF31`.

`green_action_name markAF22` Indique que le flux de trafic de la classe ftp est conforme au débit garanti, les paquets sont envoyés à l'instruction de l'action `markAF22`.

`global_stats TRUE` Active le recueil de statistiques pour la classe ftp.

Pour plus d'informations sur la conformité du trafic, reportez-vous à la section “[Module de mesure](#)” à la page 494.

#### 5 Ajoutez une instruction action du marqueur pour assigner un comportement par pas aux flux de trafic non conformes d'une classe ftp.

```
action {
  module dscpmk
  name markAF31
  params {
    global_stats TRUE
    dscp_map{0-63:26}
    next_action continue
  }
}
```

`module dscpmk` Sollicite le module de marquage `dscpmk`.

`name markAF31` Attribue le nom `markAF31` à l'instruction `action`.

`global_stats TRUE` Active le recueil de statistiques pour la classe ftp.

`dscp_map{0-63:26}` Assigne un DSCP 26 aux en-têtes de paquets de la classe de trafic ftp lorsque ce trafic dépasse le taux garanti.

`next_action continue` Indique qu'aucun traitement supplémentaire n'est requis pour les paquets de la classe de trafic ftp. Ces paquets peuvent alors revenir dans le flux du réseau.

Un DSCP 26 donne pour instruction au marqueur d'attribuer la valeur décimale 26 (binaire 011010) à toutes les entrées de la structure `dscp`. Le DSCP 26 définit le comportement AF31. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP 26 dans le champ DS.

AF31 garantit que tous les paquets avec un DSCP égal à 26 se voient attribuer un niveau de perte faible assorti d'une priorité de classe 3. En d'autres termes, la probabilité de rejeter un trafic FTP non conforme est faible. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au [Tableau 32-2](#).

**6 Ajoutez une instruction `action` du module de marquage pour assigner un PHB aux flux de trafic `ftp` qui se conforment au débit contractuel.**

```
action {
    module dscpmk
    name markAF22
    params {
        global_stats TRUE
        dscp_map{0-63:20}
        next_action continue
    }
}
```

`name markAF22`            Attribut le nom `markAF22` à l'instruction `action`.

`dscp_map{0-63:20}`        Assigne un DSCP 20 aux en-têtes de paquets de la classe de trafic `ftp` lorsque le trafic `ftp` dépasse le débit configuré.

Un DSCP égal à 20 donne pour instruction au marqueur d'attribuer la valeur décimale 20 (binaire 010100) à toutes les entrées de la structure `dscp`. Le DSCP 20 définit le comportement AF22. Le marqueur signale les paquets de la classe de trafic `ftp` par le DSCP 20 dans le champ DS.

AF22 garantit que tous les paquets avec un DSCP égal à 20 se voient attribuer un niveau de perte moyen assorti d'une priorité de classe 2. En conséquence, le trafic FTP respectant ces conditions peut compter sur un niveau de priorité moyen parmi les flux libérés simultanément par le système IPQoS. Toutefois, le routeur assigne une plus grande priorité aux classes de trafic dotées d'un niveau de priorité identique de classe 1 ou supérieur. Pour consulter le tableau de l'ensemble des points de code AF, reportez-vous au [Tableau 32-2](#).

**7 Insérez les DSCP créés pour le serveur d'application dans les fichiers correspondants sur le routeur Diffserv.**

- Voir aussi**
- Pour activer le fichier de configuration IPQoS, reportez-vous à la section “[Application d'une nouvelle configuration aux modules de noyau IPQoS](#)” à la page 478.
  - Pour ajouter des informations de configuration pour les serveurs Web, reportez-vous à la section “[Création du fichier de configuration IPQoS et définition des classes de trafic](#)” à la page 454.

- Pour configurer la comptabilisation des flux, reportez-vous à la section “[Activation de la comptabilisation d’une classe dans le fichier de configuration IPQoS](#)” à la page 461.
- Pour configurer les comportements sur un routeur, reportez-vous à la section “[Configuration d’un routeur dans un réseau compatible IPQoS](#)” à la page 475.

## Fourniture de services différenciés sur un routeur

Pour fournir des services réellement différenciés, vous devez inclure un routeur Diffserv dans la topologie de votre réseau comme décrit dans la section “[Stratégies matérielles pour le réseau Diffserv](#)” à la page 428. Les étapes véritables de la configuration Diffserv sur un routeur ainsi que la mise à jour des fichiers du routeur dépassent le cadre de ce guide.

Cette section donne des indications générales sur la procédure de coordination des informations de transmission entre les différents systèmes IPQoS sur le réseau et le routeur Diffserv.

### ▼ Configuration d'un routeur dans un réseau compatible IPQoS

La procédure suivante prend pour exemple la topologie illustrée dans la [Figure 28–4](#).

#### Avant de commencer

Elle suppose que vous ayez déjà configuré les systèmes IPQoS sur votre réseau en effectuant les tâches précédemment décrites dans ce chapitre.

- 1 Examinez les fichiers de configuration pour tous les systèmes IPQoS de votre réseau.
- 2 Identifiez chaque point de code utilisé dans les stratégies QoS.

Dressez la liste des points de code ainsi que celle des systèmes et des classes auxquels font référence les points de code. Le tableau suivant indique les zones pour lesquelles vous pouvez avoir fait appel à un même point de code. Cette pratique est autorisée. Cependant, veillez à fournir d’autres critères dans le fichier de configuration IPQoS (un sélecteur de priorité, par exemple) pour déterminer la priorité de deux classes marquées de manière identique.

Par exemple, dans le cadre du réseau illustré dans les procédures de ce chapitre, il est possible d’élaborer le tableau de points de codes suivants.

Système	Classe	PHB	Point de code DS
Goldweb	video	EF	46 (101110)

Système	Classe	PHB	Point de code DS
Goldweb	goldweb	AF11	10 (001010)
Userweb	webout	AF12	12 ( 001100)
BigAPPS	smtp	AF13	14 ( 001110)
BigAPPS	news	AF18	18 ( 010010)
BigAPPS	Trafic ftp conforme	AF22	20 ( 010100)
BigAPPS	Trafic ftp non conforme	AF31	26 ( 011010)

**3 Ajoutez les points de code provenant des fichiers de configuration IPQoS de votre réseau au fichiers qui conviennent sur le routeur Diffserv.**

Les points de code fournis contribuent à configurer le mécanisme d'ordonnancement Diffserv du routeur. Reportez-vous à la documentation du fabricant du routeur ainsi qu'à son site Web pour obtenir des instructions.

## Démarrage et maintenance d'IPQoS (tâches)

Ce chapitre inclut les tâches destinées à activer un fichier de configuration IPQoS et à consigner les événements en rapport avec IPQoS. Il aborde les sujets suivants :

- [“Administration d'IPQoS \(liste des tâches\)” à la page 477](#)
- [“Application d'une configuration IPQoS” à la page 478](#)
- [“Activation de la journalisation des messages IPQoS syslog” à la page 479](#)
- [“Dépannage à l'aide des messages d'erreur IPQoS” à la page 480](#)

### Administration d'IPQoS (liste des tâches)

Cette section répertorie l'ensemble des tâches visant à démarrer et à gérer IPQoS sur un système Oracle Solaris. Avant d'utiliser ces tâches, vous devez disposer d'un fichier de configuration IPQoS complet comme décrit dans la section [“Définition d'une stratégie QoS dans le fichier de configuration IPQoS \(liste des tâches\)” à la page 449](#).

Le tableau suivant répertorie et décrit ces tâches et contient des liens vers les sections expliquant en détails comment effectuer ces tâches.

Tâche	Description	Voir
1. Configuration d'IPQoS sur un système.	Exécutez la commande <code>ipqosconf</code> pour activer le fichier de configuration IPQoS sur un système.	<a href="#">“Application d'une nouvelle configuration aux modules de noyau IPQoS” à la page 478</a>
2. Vérification que les scripts de démarrage Oracle Solaris sont appliqués au fichier de configuration IPQoS débogué après chaque initialisation du système.	Veillez à ce que le fichier de configuration IPQoS soit appliqué chaque fois que le système redémarre.	<a href="#">“Vérification de l'application de la configuration IPQoS après chaque redémarrage” à la page 479</a> .

Tâche	Description	Voir
3. Activation de la journalisation de syslog pour IPQoS.	Ajoutez une entrée pour activer la journalisation par syslog des messages IPQoS.	<a href="#">“Activation de la journalisation des messages IPQoS au cours de l’amorce” à la page 479.</a>
4. Résolution de tout problème éventuel lié à IPQoS.	Examinez les messages d'erreur pour résoudre les problèmes relatifs à IPQoS.	Reportez-vous aux messages d'erreur figurant dans le <a href="#">Tableau 30–1</a> .

# Application d'une configuration IPQoS

Vous activez ou effectuez toute autre opération pour le fichier de configuration IPQoS à l'aide de la commande `ipqosconf`.

## ▼ Application d'une nouvelle configuration aux modules de noyau IPQoS

Vous exécutez la commande `ipqosconf` pour lire le fichier de configuration IPQoS et pour configurer les modules IPQoS dans le noyau UNIX. La procédure suivante présente le fichier `/var/ipqos/Goldweb.qos`, en guise d'exemple, créé dans la section [“Création de fichiers de configuration IPQoS pour les serveurs Web” à la page 452](#). Pour obtenir des informations détaillées, reportez-vous à la page de manuel `ipqosconf(1M)`.

### 1 Appliquez la nouvelle configuration.

```
# /usr/sbin/ipqosconf -a/var/ipqos/Goldweb.qos
```

La commande `ipqosconf` consigne les informations du fichier de configuration IPQoS spécifié dans les modules IPQoS du noyau Oracle Solaris. Dans cet exemple, les informations du fichier `/var/ipqos/Goldweb.qos` sont appliquées au noyau Oracle Solaris actuel.

**Remarque** – Lorsque vous appliquez un fichier de configuration IPQoS avec l'option `-a`, les actions dans le fichier sont actives seulement pour la session en cours.

### 2 Testez et déboguez la nouvelle configuration IPQoS.

Les utilitaires UNIX permettent d'effectuer le suivi du comportement d'IPQoS et de recueillir des statistiques sur votre mise en oeuvre IPQoS. Ces informations vous aident à déterminer si la configuration fonctionne comme prévu.

- Voir aussi**
- Pour étudier les statistiques concernant le fonctionnement des modules IPQoS, reportez-vous à la section [“Collecte des informations statistiques” à la page 488](#).
  - Pour consigner les messages `ipqosconf`, reportez-vous à la section [“Activation de la journalisation des messages IPQoS syslog” à la page 479](#).

- Pour veiller à ce que la configuration IPQoS soit appliquée après chaque amorce, reportez-vous à la section [“Vérification de l'application de la configuration IPQoS après chaque redémarrage”](#) à la page 479.

## ▼ Vérification de l'application de la configuration IPQoS après chaque redémarrage

Vous devez rendre explicite la persistance de la configuration IPQoS d'un redémarrage à l'autre. Sinon, la configuration actuelle n'a d'effet que jusqu'au redémarrage système suivant. Lorsque IPQoS fonctionne convenablement sur un système, procédez comme suit pour définir la configuration de manière permanente.

### 1 Testez l'existence d'une configuration IPQoS dans des modules de noyau.

```
# ipqosconf -l
```

Si une configuration existe déjà, `ipqosconf` affiche la configuration à l'écran. En l'absence de sortie, appliquez la configuration comme indiqué à la section [“Application d'une nouvelle configuration aux modules de noyau IPQoS”](#) à la page 478.

### 2 Assurez-vous que la configuration IPQoS existante est appliquée chaque fois que le système IPQoS redémarre.

```
# /usr/sbin/ipqosconf -c
```

L'option `-c` a pour effet d'inclure la configuration IPQoS actuelle dans le fichier de configuration à l'amorce `/etc/inet/ipqosinit.conf`.

## Activation de la journalisation des messages IPQoS syslog

Pour enregistrer des messages IPQoS lors de l'initialisation, vous devez modifier le fichier `/etc/syslog.conf` comme indiqué dans la procédure suivante.

## ▼ Activation de la journalisation des messages IPQoS au cours de l'amorce

### 1 Ouvrez le fichier `/etc/syslog.conf`.

### 2 Ajoutez le texte suivant comme ultime entrée du fichier.

```
user.info /var/adm/messages
```

Insérez des tabulations plutôt que des espaces entre les colonnes.

L'entrée permet de journaliser tous les messages générés par IPQoS dans le fichier `/var/adm/messages`, lors de l'initialisation.

3 Réinitialisez le système pour appliquer les messages.

Exemple 30–1 Sortie d'IPQoS du fichier `/var/adm/messages`

Lorsque vous affichez `/var/adm/messages` après le redémarrage système, la sortie peut contenir des messages de journalisation IPQoS similaires aux suivants.

```
May 14 10:44:33 ipqos-14 ipqosconf: [ID 815575 user.info]
New configuration applied.
May 14 10:44:46 ipqos-14 ipqosconf: [ID 469457 user.info]
Current configuration saved to init file.
May 14 10:44:55 ipqos-14 ipqosconf: [ID 435810 user.info]
Configuration flushed.
```

Des messages d'erreur IPQoS, identiques aux suivants, peuvent éventuellement apparaître dans le fichier `/var/adm/messages` du système IPQoS.

```
May 14 10:56:47 ipqos-14 ipqosconf: [ID 123217 user.error]
Missing/Invalid config file fmt_version.
May 14 10:58:19 ipqos-14 ipqosconf: [ID 671991 user.error]
No ipgpc action defined.
```

Pour obtenir la description de ces messages d'erreur, reportez-vous au [Tableau 30–1](#).

# Dépannage à l'aide des messages d'erreur IPQoS

Cette section contient le tableau des messages d'erreur qui sont générés par IPQoS ainsi que leurs solutions possibles.

TABLEAU 30–1 Messages d'erreur IPQoS

Message d'erreur	Description	Solution
Undefined action in parameter <i>nom du paramètre</i> action <i>nom de l'action</i>	Dans le fichier de configuration IPQoS, le nom de l'action spécifiée pour <i>nom du paramètre</i> n'existe pas dans le fichier de configuration.	Créez l'action. Ou faites appel à une action différente existante dans le paramètre.
action <i>nom de l'action</i> involved in cycle	Dans le fichier de configuration IPQoS, <i>nom de l'action</i> fait partie du cycle d'actions, ce qui n'est pas autorisé par IPQoS.	Déterminez le cycle d'actions. Supprimez ensuite une des références cycliques du fichier de configuration IPQoS.



TABLEAU 30-1 Messages d'erreur IPQoS (Suite)

Message d'erreur	Description	Solution
action <i>nom de l'action</i> isn't referenced by any other actions	Une définition d'action non <code>ipgpc</code> n'est pas référencée par d'autres actions définies dans le fichier de configuration IPQoS, ce qui n'est pas autorisé par IPQoS.	Supprimez l'action non référencée. Vous pouvez aussi faire en sorte qu'une action fasse référence à l'action actuellement sans référence.
Missing/Invalid config file <i>fmt_version</i>	Le format du fichier de configuration n'est pas spécifié en tant que première entrée du fichier, ce qui est requis par IPQoS.	Ajoutez la version du format comme indiqué dans la section <a href="#">“Création du fichier de configuration IPQoS et définition des classes de trafic”</a> à la page 454.
Unsupported config file format version	La version de format spécifiée dans le fichier de configuration n'est pas prise en charge par IPQoS.	Remplacez la version du format par <code>fmt_version 1.0</code> , nécessaire pour utiliser la version Solaris 9 9/02 d'IPQoS.
No <code>ipgpc</code> action defined.	Vous n'avez pas défini une action pour la classification <code>ipgpc</code> dans le fichier de configuration alors que cela est une exigence d'IPQoS.	Définissez une action pour <code>ipgpc</code> comme indiqué dans la section <a href="#">“Création du fichier de configuration IPQoS et définition des classes de trafic”</a> à la page 454.
Can't commit a null configuration	Lorsque vous avez exécuté <code>ipqosconf -c</code> pour valider une configuration, cette configuration était vide. Or, ce n'est pas autorisé par IPQoS.	Assurez-vous d'avoir appliqué un fichier de configuration avant de valider une configuration. Pour obtenir plus d'instructions, reportez-vous à la section <a href="#">“Application d'une nouvelle configuration aux modules de noyau IPQoS”</a> à la page 478.
Invalid CIDR mask on line <i>numéro de la ligne</i>	Dans le fichier de configuration, vous avez utilisé un masque CIDR en tant que partie de l'adresse IP qui se trouve hors de la plage des adresses IP valides.	Changez la valeur du masque pour qu'elle soit comprise dans la page 1–32 pour IPv4 et 1–128 pour IPv6.
Address masks aren't allowed for host names line <i>numéro de la ligne</i>	Dans le fichier de configuration, vous avez défini un masque CIDR en guise de nom d'hôte ce qui n'est pas autorisé dans IPQoS.	Supprimez le masque ou remplacez le nom d'hôte par une adresse IP.
Invalid module name line <i>numéro de la ligne</i>	Le nom du module spécifié dans une instruction d'action au sein du fichier de configuration est incorrect.	Vérifiez l'orthographe du nom de module. Pour obtenir la liste des modules IPQoS, reportez-vous au <a href="#">Tableau 32-5</a> .
<code>ipgpc</code> action has incorrect name line <i>numéro de la ligne</i>	Le nom assigné à l'action <code>ipgpc</code> dans le fichier de configuration ne correspond pas à l'action <code>ipgpc.classify</code> demandée.	Renommez l'action <code>ipgpc.classify</code> .
Second parameter clause not supported line <i>numéro de la ligne</i>	Dans le fichier de configuration, vous avez spécifié deux clauses de paramètres pour une seule action ce que IPQoS n'autorise pas.	Combinez tous les paramètres faisant référence à l'action en une seule clause de paramètres.
Duplicate named action	Dans le fichier de configuration, vous avez attribué le même nom à deux actions.	Renommez ou supprimez une des actions.

TABLEAU 30-1 Messages d'erreur IPQoS (Suite)

Message d'erreur	Description	Solution
Duplicate named filter/class in action <i>nom de l'action</i>	Vous avez donné le même nom à deux filtres ou à deux classes de la même action, ce qui n'est pas autorisé dans le fichier de configuration IPQoS.	Renommez ou supprimez une des classes.
Undefined class in filter <i>nom du filtre</i> in action <i>nom de l'action</i>	Dans le fichier de configuration, le filtre fait référence à une classe qui n'est pas définie dans l'action.	Créez la classe ou remplacez la référence de filtre par une classe déjà existante.
Undefined action in class <i>nom de la classe</i> action <i>nom de l'action</i>	Le classe fait référence à une action non définie dans le fichier de configuration.	Créez l'action ou remplacez la référence par une action déjà existante.
Invalid parameters for action <i>nom de l'action</i>	Dans le fichier de configuration, un des paramètres est incorrect.	Pour le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section “ <a href="#">Architecture IPQoS et modèle Diffserv</a> ” à la page 491. Vous avez également la possibilité de consulter la page du manuel <code>ipqosconf(1M)</code> .
Mandatory parameter missing for action <i>nom de l'action</i>	Vous n'avez pas défini un paramètre requis pour une action dans le fichier de configuration.	Pour le module appelé par l'action nommée, reportez-vous à l'entrée du module figurant dans la section “ <a href="#">Architecture IPQoS et modèle Diffserv</a> ” à la page 491. Vous avez également la possibilité de consulter la page du manuel <code>ipqosconf(1M)</code> .
Max number of classes reached in <code>ipgpc</code>	Vous avez spécifié plus de classes qu'il n'est permis de le faire dans l'action <code>ipgpc</code> du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les classes inutiles. Une autre solution consiste à atteindre le nombre maximum de classes en ajoutant l'entrée <code>ipgpc_max_classes nom de la classe</code> au fichier <code>/etc/system</code> .
Max number of filters reached in action <code>ipgpc</code>	Vous avez spécifié plus de filtres qu'il n'est permis de le faire dans l'action <code>ipgpc</code> du fichier de configuration IPQoS. Le nombre maximum est 10007.	Vérifiez le fichier de configuration et supprimez les filtres inutiles. Vous pouvez aussi élever le nombre maximum de filtres en ajoutant l'entrée <code>ipgpc_max_filters nombre de filtres</code> au fichier <code>/etc/system</code> .
Invalid/missing parameters for filter <i>nom du filtre</i> in action <code>ipgpc</code>	Dans le fichier de configuration, le filtre <i>nom du filtre</i> comporte un paramètre non valide ou un paramètre est manquant.	Reportez-vous à la page de manuel <code>ipqosconf(1M)</code> pour obtenir la liste des paramètres corrects.
Name not allowed to start with '!', line <i>numéro de la ligne</i>	Un nom d'action, de filtre ou de classe doit commencer par un point d'exclamation mark (!), ce qui n'est pas autorisé dans le fichier IPQoS.	Supprimez le point d'exclamation ou changez le nom de l'action, de la classe ou du filtre.

TABLEAU 30-1 Messages d'erreur IPQoS (Suite)

Message d'erreur	Description	Solution
Name exceeds the maximum name length line <i>numéro de la ligne</i>	Vous avez donné un nom à une action, une classe ou un filtre dans le fichier de configuration qui dépasse la longueur maximum de 23 caractères.	Choisissez un nom d'action, de classe ou de filtre plus court.
Array declaration line <i>numéro de la ligne</i> is invalid	Dans le fichier de configuration, la déclaration de tableau pour le paramètre sur la ligne <i>numéro de la ligne</i> n'est pas valide.	Pour définir correctement la syntaxe de déclaration de tableau appelée par l'instruction <code>action</code> avec le tableau non valide, reportez-vous à la section <a href="#">“Architecture IPQoS et modèle Diffserv” à la page 491</a> . Vous pouvez aussi consulter la page du manuel <code>ipqosconf(1M)</code> .
Quoted string exceeds line, <i>numéro de la ligne</i>	La chaîne n'inclut pas les guillemets de fermeture sur la même ligne, ce qui est obligatoire dans le fichier de configuration.	Assurez-vous que la chaîne comprise entre les guillemets commence et finit sur la même ligne dans le fichier de configuration.
Invalid value, line <i>numéro de la ligne</i>	La valeur attribuée à la ligne <i>numéro de la ligne</i> du fichier de configuration n'est pas prise en charge par le paramètre.	Pour connaître les valeurs autorisées pour le module appelé par l'instruction <code>action</code> , reportez-vous à la description du module dans la section <a href="#">“Architecture IPQoS et modèle Diffserv” à la page 491</a> . Vous avez également la possibilité de consulter la page du manuel <code>ipqosconf(1M)</code> .
Unrecognized value, line <i>numéro de la ligne</i>	La valeur du <i>numéro de la ligne</i> du fichier de configuration n'est pas une valeur d'énumération prise en charge par le paramètre.	Vérifiez la validité de la valeur d'énumération choisie pour le paramètre. Pour obtenir une description du module appelé par l'instruction <code>action</code> avec le numéro de ligne non reconnu, reportez-vous à la section <a href="#">“Architecture IPQoS et modèle Diffserv” à la page 491</a> . Vous avez également la possibilité de consulter la page du manuel <code>ipqosconf(1M)</code> .
Malformed value list line <i>numéro de la ligne</i>	L'énumération spécifiée à la ligne <i>numéro de la ligne</i> du fichier de configuration n'est pas conforme à la syntaxe de spécification.	Pour en savoir plus sur la syntaxe correcte du module appelé par l'instruction <code>action</code> avec la liste de valeurs non conforme, reportez-vous à la description du module figurant à la section <a href="#">“Architecture IPQoS et modèle Diffserv” à la page 491</a> . Vous avez également la possibilité de consulter la page du manuel <code>ipqosconf(1M)</code> .
Duplicate parameter line <i>numéro de la ligne</i>	Un paramètre en double a été spécifié à la ligne <i>numéro de la ligne</i> qui n'est pas autorisé dans le fichier de configuration.	Supprimez les paramètres en double.
Invalid action name line <i>numéro de la ligne</i>	Vous avez attribué à l'action, ligne <i>numéro de la ligne</i> du fichier de configuration un nom correspondant à un des noms prédéfinis ("continue" ou "drop").	Renommez l'action de sorte que son nom diffère des noms prédéfinis.

TABLEAU 30-1 Messages d'erreur IPQoS (Suite)

Message d'erreur	Description	Solution
Failed to resolve src/dst host name for filter at line <i>numéro de la ligne</i> , ignoring filter	ipqosconf n'a pas pu résoudre l'adresse d'origine ou de destination définie pour le filtre concerné dans le fichier de configuration. En conséquence, le filtre n'est pas pris en compte.	Si le filtre est important, réessayez d'appliquer la configuration plus tard.
Incompatible address version line <i>numéro de la ligne</i>	La version IP de l'adresse à la ligne <i>numéro de la ligne</i> est incompatible avec la version d'une adresse IP ou d'un paramètre <i>version_ip</i> déjà spécifié.	Modifiez les deux entrées en conflit de manière à ce qu'elles soient compatibles.
Action at line <i>numéro de la ligne</i> has the same name as currently installed action, but is for a different module	Vous avez essayé de modifier le module d'une action qui existe déjà dans la configuration IPQoS du système, mais ce n'est pas autorisé.	Videz la configuration actuelle avant d'appliquer la nouvelle configuration.

## Utilisation de la comptabilisation des flux et de la collecte statistique (tâches)

---

Ce chapitre décrit comment obtenir des informations comptables et statistiques sur le trafic géré par un système IPQoS. Il aborde les sujets suivants :

- “Configuration de la comptabilisation des flux (liste des tâches)” à la page 485
- “Enregistrement des informations sur les flux de trafic” à la page 486
- “Collecte des informations statistiques” à la page 488

### Configuration de la comptabilisation des flux (liste des tâches)

La liste de tâches suivante répertorie les tâches générales dont le but est d'obtenir des informations sur les flux de trafic à l'aide du module `flowacct`. La liste renvoie également aux procédures permettant d'effectuer ces tâches.

Tâche	Description	Voir
1. Création d'un fichier destiné à contenir les informations comptables sur les flux de trafic.	Exécutez la commande <code>acctadm</code> pour produire un fichier répertoriant les résultats issus du traitement de <code>flowacct</code> .	“Création d'un fichier contenant les données de comptabilisation des flux” à la page 486
2. Définition des paramètres de <code>flowacct</code> dans le fichier de configuration IPQoS.	Définissez les valeurs des paramètres <code>timer</code> , <code>timeout</code> et <code>max_limit</code> .	“Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS” à la page 461

## Enregistrement des informations sur les flux de trafic

Collectez les informations sur les flux à l'aide du module `flowacct` IPQoS. Il est possible, par exemple, de recueillir les adresses source et de destination, le nombre de paquets d'un flux et d'autres données similaires. Le processus consistant à accumuler et à enregistrer des informations relatifs aux flux s'appelle la *comptabilisation de flux*.

Les résultats de la comptabilisation de flux sur le trafic d'une classe donnée sont enregistrés dans la table des *enregistrements de flux*. Chaque enregistrement de flux se décompose en une série d'attributs. Ces attributs contiennent des données sur les flux de trafic de la classe en question sur une période de temps. Pour connaître la liste des attributs de `flowacct`, reportez-vous au [Tableau 32–4](#).

La comptabilisation des flux est un outil pratique pour la facturation des clients telle qu'elle est définie dans leur accord de niveau de service. Vous pouvez également faire appel à la comptabilisation des flux pour obtenir des statistiques sur les flux en rapport avec des applications critiques. Cette section récapitule les tâches au cours desquelles le module `flowacct` est associé à l'utilitaire de comptabilité étendue Oracle Solaris afin d'obtenir les données des flux de trafic.

Les informations suivantes se trouvent dans des ressources hors de ce chapitre :

- Pour connaître la procédure permettant de créer une instruction `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section “[Configuration du contrôle de flux dans le fichier de configuration IPQoS](#)” à la page 472.
- Pour en savoir plus sur le fonctionnement de `flowacct`, reportez-vous à la section “[Module de classification](#)” à la page 491.
- Pour obtenir des informations techniques, reportez-vous à la page de manuel `flowacct(7ipp)`.

### ▼ Création d'un fichier contenant les données de comptabilisation des flux

Avant d'ajouter une action `flowacct` dans le fichier de configuration IPQoS, vous devez créer un fichier pour les enregistrements de flux provenant du module `flowacct`. A cet effet, exécutez la commande `acctadm`. La commande `acctadm` enregistre les attributs de base ou les attributs étendus dans le fichier. Tous les attributs `flowacct` sont répertoriés dans le [Tableau 32–4](#). Pour plus d'informations sur `acctadm`, reportez-vous à la page de manuel `acctadm(1M)`.

#### 1 Créez un fichier standard de comptabilisation de flux.

Voici comment créer un fichier standard de comptabilisation de flux pour le serveur Web Premium tel qu'il est configuré dans l'[Exemple 29–1](#).

```
# /usr/sbin/acctadm -e basic -f /var/ipqos/goldweb/account.info flow
```

<code>acctadm -e</code>	Appelle la commande <code>acctadm</code> assortie de l'option <code>-e</code> . L'option <code>-e</code> active les arguments qui suivent.
<code>basic</code>	Déclare que seules les données des huit attributs <code>flowacct</code> standard doivent être enregistrées dans le fichier.
<code>/var/ipqos/goldweb/account.info</code>	Spécifie le nom du chemin complet du fichier contenant les enregistrements de flux émanant de <code>flowacct</code> .
<code>flow</code>	Demande à <code>acctadm</code> d'activer la comptabilisation des flux.

## 2 Examinez les information sur la comptabilisation des flux concernant le système IPQoS en tapant `acctadm` sans arguments.

`acctadm` génère la sortie suivante :

```
Task accounting: inactive
  Task accounting file: none
  Tracked task resources: none
  Untracked task resources: extended
    Process accounting: inactive
    Process accounting file: none
  Tracked process resources: none
  Untracked process resources: extended,host,mstate
    Flow accounting: active
    Flow accounting file: /var/ipqos/goldweb/account.info
  Tracked flow resources: basic
  Untracked flow resources: dsfield,ctime,lseen,projid,uid
```

Toutes les entrées hormis les quatre dernières sont destinées à la fonction du gestionnaire de ressources (Resource Manager) d'Oracle Solaris. Le tableau suivant décrit les entrées spécifiques à IPQoS.

Entrée	Description
Flow accounting: active	Indique que la comptabilisation est activée.
Flow accounting file: /var/ipqos/goldweb/account.info	Indique le nom du fichier de comptabilisation des flux actuel.
Tracked flow resources: basic	Spécifie que seuls les attributs de flux standard sont suivis.
Untracked flow resources: dsfield,ctime,lseen,projid,uid	Dresse la liste des attributs de <code>flowacct</code> pour lequel aucun suivi n'est effectué dans le fichier.

## 3 (Facultatif) Ajoutez des attributs étendus au fichier de comptabilisation.

```
# acctadm -e extended -f /var/ipqos/goldweb/account.info flow
```

**4 (Facultatif) Revenez au seul enregistrement des attributs standard dans le fichier de comptabilisation.**

```
# acctadm -d extended -e basic -f /var/ipqos/goldweb/account.info
```

L'option -d désactive la comptabilité étendue.

**5 Affichez le contenu du fichier de comptabilisation des flux.**

Pour des instructions sur l'affichage du contenu d'un fichier de comptabilisation des flux, reportez-vous à la section “[Interface Perl pour libexacct](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

- Voir aussi**
- Pour plus d'informations sur la fonction de comptabilisation étendue, reportez-vous au [Chapitre 4, “Comptabilisation étendue \(présentation\)”](#) du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.
  - Pour définir les paramètres de flowacct dans le fichier de configuration IPQoS, reportez-vous à la section “[Activation de la comptabilisation d'une classe dans le fichier de configuration IPQoS](#)” à la page 461.
  - Pour imprimer les données du fichier créé avec la commande acctadm, reportez-vous à la section “[Interface Perl pour libexacct](#)” du manuel *Administration Oracle Solaris : Oracle Solaris Zones, Oracle Solaris 10 Zones et gestion des ressources*.

## Collecte des informations statistiques

Vous pouvez utiliser la commande `kstat` pour produire des informations statistiques grâce aux modules IPQoS. Utilisez la syntaxe suivante :

```
/bin/kstat -m ipqos-module-name
```

Spécifiez un nom de module IPQoS valide comme illustré dans le [Tableau 32–5](#). Ainsi, pour afficher les statistiques générées par le marqueur `dscpmk`, utilisez le format suivant de la commande `kstat` :

```
/bin/kstat -m dscpmk
```

Pour obtenir des informations techniques, reportez-vous à la page de manuel `kstat(1M)`.

**EXEMPLE 31–1** Statistiques `kstat` pour IPQoS

Voici les résultats qu'il est possible d'obtenir suite à l'exécution de la commande `kstat` afin d'obtenir des statistiques sur le module `flowacct`.

```
# kstat -m flowacct
module: flowacct           instance: 3
name:   Flowacct statistics class:   flacct
```



EXEMPLE 31-1    Statistiques kstat pour IPQoS    (Suite)

bytes_in_tbl	84
crtime	345728.504106363
epackets	0
flows_in_tbl	1
nbytes	84
npackets	1
snaptime	345774.031843301
usedmem	256
class: flacct	Désigne la classe par le nom de la classe à laquelle les flux de trafic appartiennent. Dans l'exemple illustré, il s'agit de flacct.
bytes_in_tbl	Nombre total d'octets dans la table des flux. Le nombre total d'octets constitue la somme, exprimée en octets, de tous les enregistrements de flux actuellement consignés dans la table de flux. Le nombre total d'octets de cette table de flux est 84. Si aucun flux ne se trouve dans la table, la valeur de bytes_in_tbl est 0.
crtime	Heure à laquelle la sortie kstat a été générée.
epackets	Nombre de paquets ayant entraîné une erreur au cours du traitement. Dans l'exemple, cette valeur est nulle.
flows_in_tbl	Nombre d'enregistrements de flux dans la table de flux qui, dans cet exemple, est 1. Si aucun enregistrement ne se trouve dans la table, la valeur de flows_in_tbl est 0.
nbytes	Nombre total d'octets visibles par cette instance d'action flowacct. Il est de 84 dans l'exemple. La valeur inclut les octets qui se trouvent actuellement dans la table des flux. La valeur inclut également des octets dont le délai est dépassé et qui ne figurent plus dans la table des flux.
npackets	Nombre total de paquets visibles par cette instance d'action flowacct. Il est de 1 dans l'exemple. npackets inclut les paquets qui se trouvent actuellement dans la table de flux. npackets inclut les paquets dont le délai est dépassé et ne figurant plus dans la table des flux.
usedmem	Mémoire, exprimée en nombre d'octets, utilisée par la table de flux qui est gérée par cette instance de flowacct. La valeur usedmem est de 256 dans l'exemple. La valeur de usedmem est de 0 si la table des flux n'affiche aucun enregistrement de flux.



## IPQoS en détails (référence)

---

Ce chapitre contient du matériel de référence fournissant des informations approfondies sur les sujets IPQoS suivants :

- “Architecture IPQoS et modèle Diffserv” à la page 491
- “Fichier de configuration IPQoS” à la page 504
- “Utilitaire de configuration `ipqosconf`” à la page 508

Pour obtenir une présentation générale, reportez-vous au [Chapitre 27, “Présentation d'IPQoS \(généralités\)”](#). Pour obtenir des informations sur la planification, reportez-vous au [Chapitre 28, “Planification d'un réseau IPQoS \(tâches\)”](#). Pour consulter les procédures de configuration d'IPQoS, reportez-vous au [Chapitre 29, “Création du fichier de configuration IPQoS \(tâches\)”](#).

## Architecture IPQoS et modèle Diffserv

Cette section décrit l'architecture IPQoS et la manière dont IPQoS implémente le modèle de services différenciés (Diffserv) défini par le document [RFC 2475, An Architecture for Differentiated Services](http://www.ietf.org/rfc/rfc2475.txt?number=2475) (<http://www.ietf.org/rfc/rfc2475.txt?number=2475>) (en anglais). Les éléments suivants du modèle Diffserv sont inclus dans IPQoS :

- Classifieur
- Compteur
- Marqueur

Par ailleurs, IPQoS inclut le module de comptabilisation des flux et le marqueur `lcosmk` utilisé avec les périphériques VLAN (réseau local virtuel).

## Module de classification

Dans le modèle Diffserv, le *classifieur* est chargé d'organiser les flux de trafic sélectionnés en groupes auxquels s'appliquent différents niveaux de service. Les classificateurs définis dans le document RFC 2475 ont été initialement conçus pour les routeurs de bordure. En revanche, le

classificateur IPQoS `ipgpc` est destiné à traiter les flux de trafic pour les hôtes internes au réseau local. En conséquence, un réseau doté de systèmes IPQoS et d'un routeur Diffserv peut fournir un niveau supérieur de services différenciés. Pour obtenir une description technique du classificateur `ipgpc`, reportez-vous à la page de manuel `ipgpc` (7ipp).

Le classificateur `ipgpc` effectue les opérations suivantes :

1. Sélection des flux de trafic répondant aux critères spécifiés dans le fichier de configuration IPQoS sur le système IPQoS  
La stratégie QoS définit les différents critères obligatoirement présents dans les en-têtes de paquets. Ces critères sont appelés *sélecteurs*. Le classificateur `ipgpc` compare ces sélecteurs aux en-têtes de paquets reçus par le système IPQoS. `ipgpc` sélectionne ensuite tous les paquets correspondants.
2. Séparation des flux de paquets en *classes* : trafic réseau dont les caractéristiques sont identiques comme indiqué dans le fichier de configuration IPQoS
3. Examen de la valeur du champ de services différenciés (DS) du paquet grâce à la présence d'un point de code de services différenciés ou DSCP  
La présence du DSCP indique si l'expéditeur a prévu un comportement de transmission pour le trafic entrant.
4. Définition de l'action supplémentaire spécifiée dans le fichier de configuration IPQoS pour les paquets d'une classe particulière
5. Transmission des paquets au module IPQoS suivant indiqué dans le fichier de configuration IPQoS ou renvoi des paquets dans le trafic réseau

Pour obtenir des informations générales sur le classificateur, reportez-vous à la section [“Présentation du classifieur \(ipgpc\)” à la page 417](#). Pour plus d'informations sur l'appel du classificateur dans le fichier de configuration IPQoS, reportez-vous à la section [“Fichier de configuration IPQoS” à la page 504](#).

### Sélecteurs IPQoS

Le classificateur `ipgpc` prend en charge un grand nombre de sélecteurs que vous pouvez utiliser dans la clause `filter` du fichier de configuration IPQoS. Lorsque vous définissez un filtre, veillez à n'utiliser que le minimum de sélecteurs nécessaire à la récupération du trafic d'une classe particulière. Le nombre de filtres défini peut avoir des conséquences sur les performances du protocole IPQoS.

Le tableau suivant dresse la liste des sélecteurs disponibles pour `ipgpc`.

TABLEAU 32-1 Sélecteurs de filtre pour le classificateur IPQoS

Sélecteur	Argument	Informations sélectionnées
<code>saddr</code>	Numéro d'adresse IP.	Adresse source.

TABLEAU 32-1 Sélecteurs de filtre pour le classificateur IPQoS (Suite)

Sélecteur	Argument	Informations sélectionnées
daddr	Numéro d'adresse IP.	Adresse de destination.
sport	Numéro du port ou nom du service comme indiqué dans le fichier <code>/etc/services</code> .	Port source à partir duquel provient une classe de trafic.
dport	Numéro du port ou nom du service comme indiqué dans le fichier <code>/etc/services</code> .	Port de destination auquel une classe de trafic est liée.
protocol	Numéro ou nom de protocole comme indiqué dans le fichier <code>/etc/services</code> .	Protocole à utiliser par cette classe de trafic.
dsfield	Point de code DS (DSCP) d'une valeur comprise dans l'intervalle 0-63.	DSCP définissant un comportement de transmission à appliquer au paquet. Si ce paramètre est spécifié, le paramètre <code>dsfield_mask</code> doit également être spécifié.
dsfield_mask	Masque de bits d'une valeur comprise entre 0 et 255.	Utilisé conjointement avec le sélecteur <code>dsfield</code> . <code>dsfield_mask</code> est appliqué au sélecteur <code>dsfield</code> pour déterminer les bits qu'il faut faire correspondre.
if_name	Nom de l'interface.	Interface à utiliser pour le trafic entrant et le trafic sortant d'une classe particulière.
user	Numéro de l'identifiant utilisateur UNIX ou nom d'utilisateur à sélectionner. Si aucun identifiant utilisateur ou nom d'utilisateur ne se trouve dans le paquet, le paramètre par défaut -1 est appliqué.	ID utilisateur fourni à une application.
projid	Numéro de l'ID du projet à sélectionner.	ID du projet fourni à une application.
priority	Numéro de la priorité. La priorité la plus basse est de 0.	Priorité attribuée aux paquets de cette classe. La priorité sert à classer les filtres selon leur importance dans une même classe.
direction	Cet argument correspond à l'un des éléments suivants :	Direction du flux du paquet de la machine IPQoS.
	LOCAL_IN	Trafic local d'entrée au système IPQoS.
	LOCAL_OUT	Trafic local de sortie au système IPQoS.
	FWD_IN	Trafic d'entrée à transférer.
	FWD_OUT	Trafic de sortie à transférer.
precedence	Valeur du niveau de priorité. Le niveau de priorité le plus élevé est de 0.	Le niveau de priorité sert à classer les filtres de même priorité.

TABLEAU 32-1    Sélecteurs de filtre pour le classificateur IPQoS    (Suite)

Sélecteur	Argument	Informations sélectionnées
ip_version	V4 ou V6	Schéma d'adressage utilisé par les paquets. Il s'agit d'IPv4 ou d'IPv6.

## Module de mesure

Le *compteur* permet de suivre le taux de transmission des flux exprimé en nombre de paquets. Le compteur détermine si le paquet est conforme aux paramètres configurés. Le module de mesure détermine l'action suivante à entreprendre pour un paquet provenant d'un jeu d'actions en fonction de la taille du paquet, des paramètres configurés et du débit du flux.

Le compteur comprend deux modules de mesure, *tokenmt* et *tswtclmt*, que vous définissez dans le fichier de configuration IPQoS. Vous pouvez configurer l'un des deux modules ou les deux modules pour une classe donnée.

Lorsque vous configurez un module de mesure, vous pouvez définir deux paramètres pour une même vitesse de transfert :

- *committed-rate* : définit le taux de transmission acceptable en bits par seconde pour les paquets d'une classe particulière.
- *peak-rate* : définit le taux de transmission maximal en bits par seconde autorisé pour les paquets d'une classe particulière.

Une action de mesure d'un paquet peut aboutir à l'un des trois résultats suivants :

- *green* : le paquet contraint le flux à rester dans les limites du débit garanti.
- *yellow* : le paquet contraint le flux à dépasser le débit garanti, mais pas le débit de pointe.
- *red* : le paquet contraint le flux à dépasser le débit de pointe.

Vous pouvez associer chaque résultat à différentes actions dans le fichier de configuration IPQoS. Le débit garanti et le débit de pointe sont traités à la section suivante.

### Module de mesure tokenmt

Le module *tokenmt* utilise des *seaux de jetons* pour mesurer le taux de transmission d'un flux. Vous pouvez configurer *tokenmt* pour fonctionner comme un compteur à débit simple ou à débit double. Une instance d'action *tokenmt* gère deux seaux de jetons qui déterminent si le flux de trafic est conforme aux paramètres configurés.

La page de manuel [tokenmt\(7ipp\)](#) explique comment IPQoS implémente le paradigme du contrôle de jetons. Pour obtenir des informations générales sur les seaux de jetons, reportez-vous à la documentation *Services différenciés pour Internet* de Kalevi Kilkki et à différents sites Web.

Les paramètres de configuration pour tokenmt sont les suivants :

- `committed_rate` : spécifie le taux garanti du flux en bits par seconde.
- `committed_burst` : spécifie la taille maximale de rafale garantie en bits. Le paramètre `committed_burst` définit le nombre de paquets sortants d'une classe spécifique pouvant arriver sur le réseau à un débit garanti.
- `peak_rate` : spécifie le débit de pointe en bits par seconde.
- `peak_burst` : spécifie la taille maximale de rafale ou de pointe en bits. Le paramètre `peak_burst` accorde à une classe de trafic une taille peak-burst qui dépasse le débit garanti.
- `color_aware` : active le mode de compatibilité pour tokenmt.
- `color_map` : définit un tableau d'entiers faisant correspondre les valeurs DSCP au vert, à l'orange et au rouge.

## Configuration du tokenmt en tant que compteur à débit simple

Pour configurer tokenmt en tant que compteur à débit simple, ne spécifiez pas le paramètre `peak_rate` pour tokenmt dans le fichier de configuration IPQoS. Pour configurer une instance tokenmt à débit simple afin d'obtenir un résultat rouge, vert ou orange, vous devez spécifier le paramètre `peak_burst`. Si vous n'utilisez pas le paramètre `peak_burst`, vous pouvez configurer tokenmt de sorte qu'il aboutisse seulement à un résultat rouge ou vert. Pour consulter un exemple de tokenmt à débit simple donnant lieu à deux résultats, reportez-vous à l'[Exemple 29-3](#).

Lorsque tokenmt fonctionne comme un compteur à débit simple, le paramètre `peak_burst` définit, en fait, la taille de rafale excessive. Les paramètres `committed_rate` et `committed_burst` ou `peak_burst` doivent désigner des entiers positifs non nuls.

## Configuration du tokenmt en tant que compteur à débit double

Pour configurer tokenmt en tant que compteur à débit double, spécifiez le paramètre `peak_rate` pour l'action tokenmt dans le fichier de configuration IPQoS. Un module tokenmt à débit double a toujours trois résultats : vert, rouge et orange. Les paramètres `committed_rate`, `committed_burst` et `peak_burst` doivent désigner des entiers positifs non nuls.

## Configuration du module tokenmt en mode de reconnaissance des couleurs

Pour configurer un module tokenmt à débit double en mode de reconnaissance des couleurs, vous devez prévoir des paramètres supplémentaires pour ajouter la fonction d'interprétation des couleurs.” L'instruction suivante montre comment configurer le mode de reconnaissance des couleurs pour tokenmt.

**EXEMPLE 32-1** Action tokenmt de prise en compte des couleurs dans le fichier de configuration IPQoS

```
action {
    module tokenmt
    name meter1
```

**EXEMPLE 32-1** Action tokenmt de prise en compte des couleurs dans le fichier de configuration IPQoS  
(Suite)

```
params {
    committed_rate 4000000
    peak_rate 8000000
    committed_burst 4000000
    peak_burst 8000000
    global_stats true
    red_action_name continue
    yellow_action_name continue
    green_action_name continue
    color_aware true
    color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
}
}
```

Vous pouvez activer la fonction de reconnaissance des couleurs en définissant le paramètre `color_aware` sur `true`. En tant que module d'interprétation des couleurs, `tokenmt` suppose que le paquet est déjà marqué en rouge, orange ou vert par une action `tokenmt` précédente. Le module d'interprétation des couleurs `tokenmt` évalue un paquet à l'aide du DSCP figurant dans l'en-tête du paquet en plus des paramètres de compteur à débit double.

Le paramètre `color_map` contient un tableau auquel le DSCP de l'en-tête du paquet est lié. Considérez le tableau `color_map` suivant :

```
color_map {0-20,22:GREEN;21,23-42:RED;43-63:YELLOW}
```

Les paquets avec un DSCP compris entre 0 et 20 ou équivalent à 22 correspondent au vert. Les paquets avec un DSCP équivalent à 21 ou compris entre 23 et 42 correspondent au rouge. Les paquets avec un DSCP compris entre 43 et 63 sont associés à l'orange. Par défaut, `tokenmt` conserve une table de correspondance de couleurs. Cependant, il est possible de modifier au besoin les valeurs par défaut à l'aide des paramètres `color_map`.

Pour les paramètres *couleur\_action\_name*, vous pouvez spécifier `continue` de manière à terminer le traitement du paquet. Vous pouvez aussi ajouter un argument pour soumettre le paquet à une action de marquage, par exemple, `yellow_action_name mark22`.

## Module de mesure `tswtclmt`

Le module `tswtclmt` évalue la bande passante moyenne pour une classe de trafic en procédant à l'estimation du débit en fonction du temps. `tswtclmt` fonctionne toujours comme un contrôle à trois résultats. La fonction d'estimation du débit fournit une indication du taux d'arrivée du flux. Ce taux doit correspondre à la bande passante moyenne applicable à un flux de trafic sur une période de temps donnée appelée *fenêtre*. L'algorithme d'estimation du débit provient de la spécification RFC 2859 *A Time Sliding Window Three Colour Marker*.

Servez-vous des paramètres suivants pour configurer `tswtclmt` :

- `committed_rate` : spécifie le taux garanti en bits par seconde.



- `peak_rate` : spécifie le débit de pointe en bits par seconde.
- `window` : définit la fenêtre de temps, exprimée en millisecondes pendant laquelle la bande passante moyenne est maintenue.

Pour des détails techniques sur `tswtclmt`, reportez-vous à la page de manuel [tswtclmt\(7ipp\)](#). Pour obtenir des informations générales sur les lisseurs de débits semblables à `tswtclmt`, reportez-vous au document [RFC 2963, A Rate Adaptive Shaper for Differentiated Services](http://www.ietf.org/rfc/rfc2963.txt?number=2963) (<http://www.ietf.org/rfc/rfc2963.txt?number=2963>) (en anglais).

## Module de marquage

IPQoS inclut deux modules de marquage, `dscpmk` et `dlcosmk`. Cette section contient des informations sur l'utilisation des deux marqueurs. En théorie, vous devez utiliser `dscpmk`, car `dlcosmk` n'est disponible que pour les systèmes IPQoS et les périphériques VLAN.

Pour obtenir des informations techniques sur `dscpmk`, reportez-vous à la page de manuel `dscpmk(7ipp)`. Pour obtenir des informations techniques sur `dlcosmk`, reportez-vous à la page de manuel `dlcosmk(7ipp)`.

## Utilisation du marqueur `dscpmk` pour la transmission des paquets

Le marqueur reçoit les flux de trafic après traitements successifs par les modules de classification ou de mesure. Le marqueur associe un comportement de transmission au trafic. Ce comportement indique l'action à appliquer aux flux lorsque ces flux quittent le système IPQoS. Le comportement de transmission d'une classe de trafic est défini par le *comportement par pas ou PHB*. Le PHB affecte une priorité à une classe de trafic précisant les flux prioritaires de cette classe par rapport aux autres classes de trafic. Les PHB régissent uniquement les comportements de transmission sur le réseau contigu du système IPQoS. Pour plus d'informations sur les PHB, reportez-vous à la section [“PHB \(Per-Hop Behaviors\)” à la page 422](#).

La *transmission de paquet* est le processus consistant à envoyer le trafic d'une classe particulière vers sa prochaine destination sur un réseau. Pour un hôte tel qu'un système IPQoS, un paquet est transmis de l'hôte vers le flux de réseau local. Lorsqu'il s'agit d'un routeur Diffserv, un paquet est transmis du réseau local vers le pas suivant du routeur.

Le marqueur signale dans le champ DS de l'en-tête du paquet un comportement défini dans le fichier de configuration IPQoS. Par la suite, le système IPQoS et les systèmes Diffserv suivants transmettent le trafic comme indiqué dans le champ DS jusqu'à ce que le marquage change. Pour attribuer un PHB, le système IPQoS inscrit une valeur dans le champ DS de l'en-tête du paquet. Cette valeur est appelée le point de code de services différenciés (DSCP). L'architecture Diffserv définit deux types de comportement de transmission, EF et AF, utilisant des DSCP différents. Pour plus d'informations sur les DSCP, reportez-vous à la section [“Point de code DS” à la page 422](#).

Le système IPQoS lit le DSCP et évalue le niveau de priorité par rapport à d'autres flux de trafic sortants. Le système IPQoS établit la priorité des flux de trafic simultanés et libère chaque flux sur le réseau en fonction de sa priorité.

Le routeur Diffserv reçoit les flux de trafic sortants et lit le champ DS dans les en-têtes de paquets. Le DSCP permet au routeur de classer et d'ordonner les flux de trafic simultanés. Le routeur transmet chaque flux en fonction de la priorité indiquée par le PHB. Notez que le PHB ne peut pas être appliqué au-delà de la limite du routeur du réseau à moins que les systèmes Diffserv des pas suivants reconnaissent le même PHB.

**PHB Expedited Forwarding (EF) (ou traitement accéléré)**

*Expedited forwarding* (EF) garantit que les paquets dotés du point de code recommandé 46 EF (101110) bénéficient du meilleur traitement disponible sur le réseau. Le service Expedited forwarding est souvent comparé à une ligne spécialisée. Les routeurs Diffserv garantissent un traitement préférentiel aux paquets accompagnés du point de code 46 (101110) pour l'acheminement vers leur destination. Pour obtenir des informations techniques sur le service EF, reportez-vous au document RFC 2598, *An Expedited Forwarding PHB*.

**PHB Assured Forwarding (AF) (traitement assuré)**

*Assured forwarding* (AF) offre quatre classes de comportements de transmission applicables au marqueur. Le tableau suivant présente les classes, les trois "drop precedences" (niveaux de priorité) de chaque classe et les DSCP recommandés associés à chaque priorité. Chaque DSCP est représenté par sa valeur AF, sa valeur en notation décimale et en notation binaire.

TABLEAU 32-2 Points de code Assured Forwarding

	Classe 1	Classe 2	Classe 3	Classe 4
Faible niveau de priorité	AF11 =	AF21 =	AF31 =	AF41 =
	10 (001010)	18 (010010)	26 (011010)	34 (100010)
Niveau de priorité intermédiaire	AF12 =	AF22 =	AF32 =	AF42 =
	12 (001100)	20 (010100)	28 (011100)	36 (100100)
Niveau de priorité élevé	AF13 =	AF23 =	AF33 =	AF43 =
	14 (001110)	22 (010110)	30 (011110)	38 (100110)

Tout système Diffserv peut faire appel au point de code AF afin de l'utiliser en tant que guide lors de la fourniture de services différenciés à différentes classes de trafic.

Lorsque ces paquets atteignent un routeur Diffserv, le routeur évalue les points de code des paquets ainsi que les DSCP d'autres flux de trafic placés dans la file d'attente. Le routeur transmet ou rejette les paquets, selon la bande passante disponible et les priorités définies par les

DSCP des paquets. Notez que l'accès à la bande passante est garanti en priorité aux paquets marqués par un PHB EF par rapport aux paquets marqués par un PHB AF (quelle que soit leur classe).

Coordonnez le marquage des paquets entre les différents systèmes IPQoS de votre réseau et le routeur Diffserv pour veiller à ce que les paquets soient transférés comme prévu. Par exemple, supposons que les systèmes IPQoS de votre réseau marquent les paquets à l'aide des points de code AF21 (010010), AF13 (001110), AF43 (100110) et EF (101110). Vous devez ensuite ajouter les DSCP AF21, AF13, AF43 et EF au fichier approprié sur le routeur Diffserv.

Vous trouverez des informations techniques sur le tableau de points de code AF dans le document RFC 2597. Vous trouverez des informations détaillées concernant la configuration du PHB AF sur le site Web des fabricants de routeurs Cisco Systems et Juniper Networks. Servez-vous de ces informations pour définir les PHB AF des systèmes IPQoS ainsi que les routeurs. Par ailleurs, la documentation des fabricants de routeurs contient des instructions pour la définition des points de code DS sur leur matériel.

## Fourniture d'un DSCP au marqueur

Le DSCP occupe 6 bits. Le champ DS a une longueur d'1 octet. Lorsque vous définissez un DSCP, le marqueur marque les 6 premiers bits significatifs de l'en-tête du paquet avec le code de point DS. Les deux bits restants (les moins significatifs) ne sont pas utilisés.

Pour définir un DSCP, servez-vous du paramètre suivant au sein d'une instruction d'action du marqueur :

```
dscp_map{0-63:DS_codepoint}
```

Le paramètre `dscp_map` est un tableau à 64 éléments que vous remplissez à l'aide de la valeur (DSCP). Le paramètre `dscp_map` sert à faire correspondre les DSCP entrants aux DSCP sortants appliqués par le marqueur `dscpmk`.

Vous devez spécifier la valeur DSCP pour le paramètre `dscp_map` en notation décimale. Par exemple, vous devez traduire le point de code EF de 101110 en valeur décimale 46 ce qui équivaut à `dscp_map{0-63:46}`. Pour les points de code AF, vous devez exprimer les différents points de code présentés dans le [Tableau 32-2](#) en notation décimale spécialement pour le paramètre `dscp_map`.

## Utilisation du marqueur `dlcosmk` avec les périphériques VLAN

Le module de marquage `dlcosmk` spécifie le comportement dans l'en-tête MAC d'un datagramme. Vous ne pouvez utiliser le paramètre `dlcosmk` que dans un système IPQoS avec une interface VLAN.

`dlcosmk` ajoute quatre octets, désignés sous l'appellation d'*étiquette VLAN*, à l'en-tête MAC. L'étiquette VLAN inclut une valeur de priorité utilisateur de 3 bits, définie par la norme IEEE

801.D. Les commutateurs Diffserv en mesure de reconnaître VLAN peuvent lire le champ de priorité utilisateur dans un datagramme. Les valeurs de priorité utilisateur 801.D implémentent les marques de classe de service (CoS), connues et comprises par les commutateurs du marché.

Vous pouvez utiliser les valeurs de priorité utilisateur dans l'action du marqueur `dlcosmk` en définissant les indices de classes de service répertoriés dans le tableau suivant.

**TABLEAU 32-3** Valeurs de priorité utilisateur 801.D

Classe de service	Définition
0	Au mieux (Best effort)
1	Arrière-plan (Background)
2	Secours (Spare)
3	Effort excellent (Excellent effort)
4	Charge contrôlée (Controlled load)
5	Vidéo inférieure à une latence de 100ms (Video less than 100ms latency)
6	Vidéo inférieure à une latence de 10ms (Video less than 10ms latency)
7	Contrôle du réseau (Network control)

Pour plus d'informations sur `dlcosmk`, reportez-vous à la page de manuel [dlcosmk\(7ipp\)](#).

### Configuration IPQoS pour les systèmes comportant des périphériques VLAN

Cette section illustre un scénario de réseau simple montrant comment implémenter IPQoS sur les systèmes avec des périphériques VLAN. Le scénario prend en compte deux systèmes IPQoS, `ordinateur1` et `ordinateur2`, reliés par un commutateur. Le périphérique VLAN sur `ordinateur1` a l'adresse IP `10.10.8.1`. Le périphérique VLAN sur l'`ordinateur2` a l'adresse IP `10.10.8.3`.

Le fichier de configuration IPQoS suivant de l'`ordinateur1` décrit une solution simple pour marquer le trafic allant du commutateur à l'`ordinateur2`.

**EXEMPLE 32-2** Fichier de configuration IPQoS pour un système avec un périphérique VLAN

```
fmt_version 1.0
action {
    module ipgpc
    name ipgpc.classify

    filter {
        name myfilter2
```

**EXEMPLE 32-2** Fichier de configuration IPQoS pour un système avec un périphérique VLAN (Suite)

```

        daddr 10.10.8.3
        class myclass
    }

    class {
        name myclass
        next_action mark4
    }
}

action {
    name mark4
    module dlcsmk
    params {
        cos 4
        next_action continue
    }
    global_stats true
}

```

Dans cette configuration, tout le trafic de l'ordinateur1 destiné au périphérique VLAN sur l'ordinateur2 est transféré sur le marqueur dlcsmk. L'action de marqueur marque4 indique à dlcsmk d'ajouter une marque VLAN aux datagrammes de la classe maclasse possédant une classe de service de 4. La valeur de priorité utilisateur 4 indique que le commutateur reliant les deux machines doit donner le transfert de charge contrôlé aux flux de trafic maclasse de machine1.

## Module flowacct

Le module flowacct d'IPQoS enregistre les informations sur les flux de trafic, un processus connu sous le nom de *comptabilisation des flux*. La comptabilisation des flux produit des données qui peuvent servir à la facturation des clients ou à l'évaluation du trafic d'une classe particulière.

La comptabilisation des flux est facultative. Le module flowacct est généralement le dernier module par lequel passent les flux de trafic mesurés ou marqués avant d'être libérés sur le réseau. Pour voir la position de flowacct dans le modèle Diffserv, reportez-vous à la [Figure 27-1](#). Pour obtenir des informations techniques sur flowacct, reportez-vous à la page de manuel flowacct(7ipp).

Pour activer la comptabilisation des flux, vous devez utiliser la fonction de comptabilisation Oracle Solaris exacct et la commande acctadm, ainsi que flowacct. Pour connaître les étapes générales de la configuration de la comptabilisation, reportez-vous à la section “[Configuration de la comptabilisation des flux \(liste des tâches\)](#)” à la page 485.

## Paramètres flowacct

Le module `flowacct` rassemble les informations sur les flux dans une *table de flux* composée d'*enregistrements de flux*. Chaque entrée de la table contient un enregistrement de flux. Vous ne pouvez pas afficher une table de flux.

Dans le fichier de configuration IPQoS, vous définissez les paramètres `flowacct` suivants pour mesurer les enregistrements de flux et consigner les enregistrements dans la table :

- `timer` : définit un intervalle, en millisecondes, lorsque les flux dont le délai a expiré sont supprimés de la table de flux et consignés dans le fichier créé par `acctadm`.
- `timeout` : définit un intervalle, en millisecondes, spécifiant la durée d'inactivité d'un flux de paquet avant que ce dernier ne soit considéré comme ayant expiré.

---

**Remarque** – Vous pouvez configurer `timer` et `timeout` de sorte qu'ils aient des valeurs différentes.

---

- `max_limit` : définit la limite supérieure du nombre d'enregistrements de flux pouvant être stockés dans la table de flux.

Pour obtenir un exemple d'utilisation des paramètres `flowacct` dans le fichier de configuration IPQoS, reportez-vous à la section [“Configuration du contrôle de flux dans le fichier de configuration IPQoS”](#) à la page 472.

## Table de flux

Le module `flowacct` gère une table visant à enregistrer tous les flux de paquets rencontrés par une instance de `flowacct`. Un flux est identifié par les paramètres suivants qui incluent l'uplet à 8 attributs de `flowacct` :

- Adresse source
- Adresse de destination
- Port source
- Port de destination
- DSCP
- ID d'utilisateur
- ID du projet
- Numéro du protocole

Si tous les paramètres de l'uplet à 8 attributs concernant un même flux sont identiques, la table de flux ne contient qu'une seule entrée. Le paramètre `max_limit` détermine le nombre d'entrées que peut inclure une table de flux.

La table de flux est numérisée à l'intervalle spécifié dans le fichier de configuration IPQoS grâce au paramètre `timer`. Le paramètre par défaut est de 15 secondes. Un flux "arrive à expiration" lorsque ses paquets ne sont pas visibles par le système IPQoS à la fin du délai d'attente (au

moins) indiqué dans le fichier de configuration IPQoS. Le délai d'attente par défaut est de 60 secondes. Les entrées dont le délai d'attente a été dépassé sont ensuite enregistrées dans le fichier de comptabilisation créé par la commande `acctadm`.

## Enregistrements `flowacct`

Un enregistrement `flowacct` inclut les attributs décrits dans le tableau suivant.

TABLEAU 32-4 Attributs d'un enregistrement `flowacct`

Nom d'attribut	Contenu des attributs	Type
<code>src-addr-type-adresse</code>	Adresse source de l'expéditeur. <i>type-adresse</i> équivaut à v4 pour IPv4 ou v6 pour IPv6, comme indiqué dans le fichier de configuration IPQoS.	De base
<code>dest-addr-type-adresse</code>	Adresse de destination des paquets. <i>type-adresse</i> équivaut à v4 pour IPv4 ou v6 pour IPv6, comme indiqué dans le fichier de configuration IPQoS.	De base
<code>src-port</code>	Port source d'où provient le flux.	De base
<code>dest-port</code>	Numéro du port de destination vers lequel le flux est dirigé.	De base
<code>protocol</code>	Numéro du protocole du flux.	De base
<code>total-packets</code>	Nombre de paquets dans le flux.	De base
<code>total-bytes</code>	Nombre d'octets dans le flux.	De base
<code>nom-action</code>	Nom de l'action <code>flowacct</code> ayant enregistré le flux.	De base
<code>creation-time</code>	Première fois qu'un paquet est vu par <code>flowacct</code> .	Étendu uniquement
<code>last-seen</code>	Dernière fois qu'un paquet du flux a été vu.	Étendu uniquement
<code>diffserv-field</code>	DSCP dans les en-têtes de paquets sortants du flux.	Étendu uniquement
<code>user</code>	ID utilisateur ou nom d'utilisateur UNIX obtenu par l'application.	Étendu uniquement
<code>projid</code>	ID du projet obtenu par l'application.	Étendu uniquement

## Utilisation d'`acctadm` avec le module `flowacct`

Vous utilisez la commande `acctadm` pour créer un fichier réservé aux enregistrements de flux générés par `flowacct`. `acctadm` s'utilise en parallèle avec la fonction de comptabilisation étendue. Pour plus d'informations techniques sur `acctadm`, reportez-vous à la page de manuel [acctadm\(1M\)](#).

Le module `flowacct` observe les flux et inscrit les enregistrements de flux dans la table de flux. `flowacct` évalue ensuite ses paramètres et attributs dans l'intervalle spécifié par `timer`. Un paquet expire s'il n'est pas visible pendant la durée équivalent aux valeurs `last_seen` et `timeout`. Toutes les entrées ayant dépassé le délai d'expiration sont supprimées de la table de flux. Elles sont alors consignées dans le fichier de comptabilisation à l'issue de l'intervalle spécifié par le paramètre `timer`.

Pour appliquer `acctadm` au module `flowacct`, respectez la syntaxe suivante :

```
acctadm -e file-type -f filename flow
```

`acctadm -e` Appelle la commande `acctadm` assortie de l'option `-e`. La valeur `-e` indique la présence d'une liste de ressources.

*file-type* Spécifie les attributs à collecter. *file-type* doit être remplacé par la valeur `basic` ou `extended`. Pour connaître la liste des attributs de chaque type de fichier, reportez-vous au [Tableau 32–4](#).

`-f file-name` Crée le fichier *file-name* dans lequel sont consignés les enregistrements de flux.

`flow` Implique l'exécution de la commande `acctadm` avec IPQoS.

## Fichier de configuration IPQoS

Cette section décrit en détail les différentes parties du fichier de configuration IPQoS. La stratégie activée au démarrage d'IPQoS est stockée dans le fichier `/etc/inet/ipqosinit.conf`. Bien qu'il soit possible de modifier ce fichier, dans le cas d'un nouveau système IPQoS, il est préférable de créer un fichier de configuration sous un autre nom. Les tâches à réaliser pour appliquer et déboguer une configuration IPQoS sont présentées dans le [Chapitre 29, "Création du fichier de configuration IPQoS \(tâches\)"](#).

La syntaxe du fichier de configuration IPQoS est présentée dans l'[Exemple 32–3](#). Cet exemple utilise les conventions suivantes :

- **caractères machine** : informations d'ordre syntaxique décrivant les différentes parties du fichier de configuration. Comme ce style correspond à des explications, vous n'avez pas à saisir de texte.
- **caractères gras** : texte littéral qu'il est nécessaire de saisir dans le fichier de configuration IPQoS. Vous devez toujours commencer, par exemple, le fichier de configuration IPQoS par l'instruction **`fmt_version`**.
- *caractères en italique* : variable que vous devez remplacer par des données descriptives de votre configuration. Vous devez toujours remplacer, par exemple, la variable *nom-action* ou *nom-module* par les informations relatives à votre configuration.



**EXEMPLE 32-3** Syntaxe du fichier de configuration IPQoS

```

file_format_version ::= fmt_version version

action_clause ::= action {
    name action-name
    module module-name
    params-clause | ""
    cf-clauses
}
action_name ::= string
module_name ::= ipgpc | dlcosmk | dscpmk | tswtclmt | tokenmt | flowacct

params_clause ::= params {
    parameters
    params-stats | ""
}
parameters ::= prm-name-value parameters | ""
prm_name_value ::= param-name param-value

params_stats ::= global-stats boolean

cf_clauses ::= class-clause cf-clauses |
              filter-clause cf-clauses | ""

class_clause ::= class {
    name class-name
    next_action next-action-name
    class-stats | ""
}
class_name ::= string
next_action_name ::= string
class_stats ::= enable_stats boolean
boolean ::= TRUE | FALSE

filter_clause ::= filter {
    name filter-name
    class class-name
    parameters
}
filter_name ::= string

```

Le texte restant décrit chacune des principales parties du fichier de configuration IPQoS.

## Instruction action

Les instructions action servent à appeler les différents modules IPQoS décrits à la section [“Architecture IPQoS et modèle Diffserv”](#) à la page 491.

Lorsque vous créez le fichier de configuration IPQoS, vous devez toujours commencer par indiquer le numéro de version. Vous devez ensuite ajouter l’instruction action suivante pour appeler le classificateur :

```
fmt_version 1.0

action {
    module ipgpc
    name ipgpc.classify
}
```

Faites suivre l'instruction action du classificateur par une clause params ou une clause class.

Respectez la syntaxe suivante pour toutes les autres instructions action :

```
action {
name action-name
module module-name
params-clause | ""
cf-clauses
}
```

- name *action\_name* Attribue un nom à l'action.
- module *module\_name* Identifie le module IPQoS à appeler (il doit s'agir de l'un des modules présentés dans le [Tableau 32-5](#)).
- params\_clause* Il peut s'agir des paramètres à traiter par le classificateur (statistiques globales ou prochaine action à effectuer, par exemple).
- cf\_clauses* Ensemble constitué d'aucune ou de plusieurs clauses class ou filter

## Définitions des modules

La définition du module désigne le module chargé de traiter les paramètres dans l'instruction action. Le fichier de configuration IPQoS peut inclure les modules suivants.

TABLEAU 32-5 Modules IPQoS

Nom du module	Définition
ipgpc	Classifieur IP
dscpmk	Marqueur servant à créer des DSCP dans des paquets IP
dlcosmk	Marqueur à utiliser avec les périphériques VLAN
tokenmt	Compteur de seuil à jetons
tswtclmt	Compteur de fenêtre de temps

TABLEAU 32-5 Modules IPQoS (Suite)

Nom du module	Définition
flowacct	Module de comptabilisation des flux

## Clause class

Vous définissez une clause `class` pour chaque classe de trafic.

Respectez la syntaxe suivante pour définir les classes restantes dans la configuration IPQoS :

```
class {  
    name class-name  
    next_action next-action-name  
}
```

Pour collecter des statistiques au sujet d'une classe particulière, vous devez d'abord activer les statistiques globales dans l'instruction `ipgpc.classify action`. Pour plus d'informations, reportez-vous à la section “[Instruction action](#)” à la page 505.

Utilisez l'instruction `enable_stats TRUE` chaque fois que vous souhaitez établir des statistiques pour une classe. Si vous n'avez pas besoin de connaître les statistiques d'une classe, il suffit de spécifier `enable_stats FALSE` ou de supprimer l'instruction `enable_stats`.

Le trafic sur un réseau IPQoS non défini de façon explicite est relégué vers la *classe par défaut*.

## Clause filter

Les *filtres* sont constitués de sélecteurs qui regroupent les flux de trafic en classes. Ces sélecteurs définissent plus précisément les critères à appliquer au trafic de la classe créée dans la clause `class`. Si un paquet répond à tous les critères des sélecteurs du filtre de priorité supérieur, il est considéré comme un membre de la classe du filtre. Pour obtenir la liste complète des sélecteurs applicables au classificateur `ipgpc`, reportez-vous au [Tableau 32-1](#).

Vous définissez les filtres dans le fichier de configuration IPQoS à l'aide d'une *clause filter* correspondant à la syntaxe suivante :

```
filter {  
    name filter-name  
    class class-name  
    parameters (selectors)  
}
```

## Clause params

La clause `params` contient les instructions de traitement pour le module défini dans l'instruction `action`. Respectez la syntaxe suivante pour la clause `params` :

```
params {  
    parameters  
    params-stats | ""  
}
```

Dans la clause `params`, vous utilisez les paramètres qui se rapportent au module.

La valeur *params-stats* définie dans la clause `params` est soit `global_stats TRUE`, soit `global_stats FALSE`. L'instruction `global_stats TRUE` a pour effet d'activer les statistiques de type UNIX pour l'instruction `action` à partir de laquelle les statistiques globales sont demandées. Pour afficher les statistiques, exécutez la commande `ksstat`. Vous devez activer les statistiques de l'instruction `action` avant d'activer les statistiques par classe.

## Utilitaire de configuration ipqosconf

L'utilitaire `ipqosconf` sert à lire le fichier de configuration IPQoS et à configurer les modules IPQoS dans le noyau UNIX. `ipqosconf` effectue les actions suivantes :

- Il applique le fichier de configuration aux modules du noyau IPQoS (`ipqosconf -a nom-fichier`).
- Il affiche le fichier de configuration IPQoS résidant actuellement dans le noyau (`ipqosconf -l`).
- Il s'assure que la configuration IPQoS en cours est lue et appliquée à chaque redémarrage de la machine (`ipqosconf -c`).
- Il vide les modules du noyau IPQoS actuels (`ipqosconf -f`).

Pour des détails techniques, reportez-vous à la page de manuel [ipqosconf\(1M\)](#).

# Glossaire

---

<b>3DES</b>	Voir <a href="#">Triple-DES</a> .
<b>adresse à usage local</b>	Adresse unicast dont la portée du routage est exclusivement locale (au sein du masque de sous-réseau ou d'un réseau d'abonnés). Cette adresse peut également avoir un caractère local ou global.
<b>adresse anycast</b>	Adresse IPv6 attribuée à un groupe d'interfaces (appartenant généralement à des noeuds différents). Un paquet envoyé à une adresse anycast est acheminé vers l'interface <i>la plus proche</i> possédant cette adresse. La route suivie par le paquet est conforme à la mesure de distance du protocole de routage.
<b>adresse CIDR</b>	Classless Inter-Domain Routing, routage interdomaine sans classe. Format d'adresse IPv4 non basé sur les classes de réseau (classe A, B et C). Les adresses CIDR ont une longueur de 32 bits. Elles utilisent le format de notation décimal avec points IPv4 standard en plus d'un préfixe réseau. Ce préfixe définit le numéro de réseau et le masque de réseau.
<b>adresse de diffusion</b>	Adresses réseau IPv4 avec la partie hôte de l'adresse ne comportant que des zéros (10.50.0.0) ou des valeurs à un bit (10.50.255.255). Un paquet envoyé à une adresse de diffusion à partir d'un ordinateur situé sur le réseau local est transmis à tous les ordinateurs reliés au réseau.
<b>adresse de multidiffusion</b>	Adresse IPv6 identifiant un groupe d'interfaces d'une manière particulière. Un paquet envoyé à une adresse de multidiffusion est diffusé à toutes les interfaces du groupe. La fonctionnalité de l'adresse de multidiffusion IPv6 est similaire à celle de l'adresse de diffusion IPv4.
<b>adresse de site local (site-local-use)</b>	Désignation utilisée pour l'adressage sur un site unique.
<b>adresse lien-local</b>	Dans IPv6, désignation utilisée en guise d'adresse d'une liaison simple lors d'une configuration d'adresse automatique, par exemple. Par défaut, l'adresse lien-local est créée à partir de l'adresse MAC du système.
<b>adresse privée</b>	Adresse IP impossible à acheminer via le réseau Internet. Les adresses privées peuvent être utilisées par des réseaux internes sur des hôtes n'ayant pas besoin d'établir une connexion Internet. Ces adresses sont définies dans <a href="#">Allocation d'adresses aux Internets privés</a> ( <a href="http://www.ietf.org/rfc/rfc1918.txt?number=1918">http://www.ietf.org/rfc/rfc1918.txt?number=1918</a> ) et souvent appelées adresses "1918".
<b>adresse unicast</b>	Adresse IPv6 identifiant une interface unique sur un noeud IPv6. Le préfixe de site, l'ID du sous-réseau et l'ID de l'interface sont les trois composantes de l'adresse unicast.
<b>AES</b>	Standard de chiffrement avancé (Advanced Encryption Standard). Technique de chiffrement de données symétrique par blocs de 128 bits. Le gouvernement des Etats-Unis a adopté la variante Rijndael de l'algorithme comme norme de chiffrement en octobre 2000. AES remplace le chiffrement <a href="#">DES</a> comme norme administrative.

<b>algorithme Diffie-Hellman</b>	Egalement appelé cryptographie par clé publique. Protocole d'accord de clés cryptographique asymétrique mis au point par Diffie et Hellman en 1976. Ce protocole permet à deux utilisateurs d'échanger une clé secrète via un moyen non sécurisé sans secrets préalables. Diffie-Hellman est utilisé par le protocole IKE.
<b>association de sécurité</b>	SA, Security Association. Association définissant les propriétés en matière de sécurité entre un premier hôte et un deuxième hôte.
<b>attaque par réflexion</b>	Attaque consistant à envoyer à distance des paquets ICMP requête d'écho à une <a href="#">adresse de diffusion IP</a> ou à plusieurs adresses de diffusion dans le but de congestionner le réseau ou de provoquer de graves interruptions de service.
<b>attaque par rejeu</b>	Dans IPsec, attaque impliquant la capture d'un paquet par un intrus. Le paquet stocké remplace ou réplique l'original par la suite. Pour se protéger contre ce type d'attaque, il suffit que le paquet contienne un champ qui s'incrémente pendant la durée de vie de la clé secrète assurant la sécurité du paquet.
<b>autorité de certification (CA)</b>	Organisation ou société « tiers de confiance » publiant des certificats numériques utilisés pour créer des signatures numériques et des bclés. La CA garantit l'identité d'une personne ayant reçu un certificat unique.
<b>base de données des stratégies de sécurité</b>	SPD, Security Policy Database. Base de données définissant le niveau de protection à appliquer à un paquet. La base de données SPD filtre le trafic IP afin de déterminer s'il est nécessaire de rejeter un paquet, de le transmettre en clair ou de le protéger avec IPsec.
<b>Blowfish</b>	Algorithme de chiffrement par bloc symétrique de longueur de clé variable (entre 32 et 448 bits). Son créateur, Bruce Schneier, affirme que Blowfish est optimisé pour les applications pour lesquelles la clé n'a pas besoin d'être régulièrement modifiée.
<b>CA</b>	Voir <a href="#">autorité de certification (CA)</a> .
<b>charge utile</b>	Données transportées dans un paquet. La charge utile n'inclut pas les informations d'en-tête nécessaires pour amener le paquet à destination.
<b>classe</b>	Dans IPQoS, groupe de flux de réseau dotés de caractéristiques identiques. Vous définissez les classes dans le fichier de configuration IPQoS.
<b>comptabilisation des flux</b>	Dans IPQoS, processus visant à collecter et à enregistrer les informations sur les flux de trafic. Pour ce faire, il convient de définir les paramètres du module <code>flowacct</code> dans le fichier de configuration IPQoS.
<b>compteur</b>	Module de l'architecture Diffserv mesurant le débit du trafic d'une classe particulière. L'implémentation IPQoS inclut deux compteurs, <code>tokenmt</code> et <code>tswtclmt</code> .
<b>configuration automatique</b>	Processus selon lequel un hôte configure automatiquement son adresse IPv6 à partir du préfixe de site et des adresses MAX locales.
<b>configuration automatique sans état</b>	Processus par lequel un hôte génère ses propres adresses IPv6 en combinant son adresse MAC et un préfixe IPv6 publié par un routeur IPv6 local.
<b>couche liaison</b>	Couche située immédiatement sous <a href="#">IPv4/IPv6</a> .

<b>cryptographie par clé asymétrique</b>	Système de chiffrement dans lequel l'expéditeur et le destinataire du message utilisent différentes clés pour chiffrer et déchiffrer le message. Les clés asymétriques servent à établir un canal sécurisé pour le chiffrement par clé symétrique. L' <a href="#">algorithme Diffie-Hellman</a> est un exemple de protocole de clé asymétrique. Voir aussi <a href="#">cryptographie par clé symétrique</a> .
<b>cryptographie par clé publique</b>	Système cryptographique utilisant deux clés différentes : une clé publique connue de tous et une clé privée présentée exclusivement au destinataire du message. IKE fournit des clés publiques à IPsec.
<b>cryptographie par clé symétrique</b>	Système de chiffrement dans lequel l'expéditeur et le destinataire d'un message partagent une clé unique commune. Cette clé commune sert au chiffrement et au déchiffrement du message. Les clés symétriques permettent de chiffrer l'ensemble de la transmission de données dans IPsec. <a href="#">DES</a> est un exemple de système de cryptographie par clé symétrique.
<b>datagramme</b>	Voir <a href="#">datagramme IP</a> .
<b>datagramme IP</b>	Paquet d'informations transporté par IP. Un datagramme IP contient un en-tête et des données. L'en-tête inclut les adresses de la source et de la destination du datagramme. Les autres champs de l'en-tête permettent d'identifier et de recombinaer les données avec les datagrammes associés lorsqu'ils arrivent à destination.
<b>DES</b>	Standard de chiffrement de données (Data Encryption Standard). Méthode de chiffrement à clé symétrique développée en 1975 et standardisée par l'ANSI en 1981 comme ANSI X.3.92. Le DES utilise une clé de 56 bits.
<b>détection de réparation</b>	Processus permettant de déterminer à quel moment une NIC ou le chemin de la carte vers un périphérique de couche 3 est de nouveau fonctionnel après un échec.
<b>détection de routeur</b>	Processus selon lequel les hôtes localisent des routeurs résidant sur une liaison directe.
<b>détection des voisins</b>	Mécanisme IP permettant à des hôtes de localiser d'autres hôtes résidant sur une liaison directe.
<b>DOI</b>	Un DOI (Domain of Interpretation, domaine d'interprétation) définit les formats de données, les types d'échange du trafic réseau ainsi que les conventions d'appellation des informations liées à la sécurité. Les stratégies de sécurité, les algorithmes et les modes cryptographiques sont toutes des informations ayant trait à la sécurité.
<b>double pile</b>	Protocole TCP/IP intégrant IPv4 et IPv6 au niveau de la couche réseau, le reste de la pile étant identique. Lorsque vous activez le protocole IPv6 lors de l'installation d'Oracle Solaris, l'hôte reçoit la version double pile du protocole TCP/IP.
<b>DSA</b>	algorithme de signature numérique (Digital Signature Algorithm) Algorithme de clé publique dont la longueur de clé varie de 512 à 4 096 bits. La norme du gouvernement américain, DSS, atteint 1 024 bits. L'algorithme DSA repose sur l'algorithme <a href="#">SHA-1</a> en entrée.
<b>DSCP</b>	DS Codepoint, point de code DS. Valeur de 6 bits qui, si elle figure dans le champ DS d'un en-tête IP, indique le mode de transfert d'un paquet.
<b>en-tête</b>	Voir <a href="#">en-tête IP</a> .

<b>en-tête d'authentification</b>	En-tête d'extension assurant l'authentification et l'intégrité des datagrammes IP, mais pas leur confidentialité.
<b>en-tête de paquet</b>	Voir <a href="#">en-tête IP</a> .
<b>en-tête IP</b>	Vingt octets de données identifiant de manière unique un paquet Internet. L'en-tête inclut l'adresse source et l'adresse de destination du paquet. Une partie facultative de l'en-tête permet d'insérer des octets supplémentaires.
<b>encapsulation</b>	Processus selon lequel un en-tête et une charge utile sont placés dans le premier paquet, puis insérés dans la charge utile du deuxième paquet.
<b>encapsulation IP-in-IP</b>	Mécanisme de mise en tunnel des paquets IP au sein de paquets IP.
<b>encapsulation minimal</b>	Forme facultative IPv4 de la mise en tunnel IPv4 prise en charge par les agents locaux, les agents étrangers et les noeuds mobiles. L'encapsulation permet d'économiser 8 ou 12 octets de surcharge par rapport à l'encapsulation IP-in-IP.
<b>filtrage de paquets</b>	Fonction de pare-feu pouvant être configurée pour autoriser ou interdire le transit de paquets particuliers via un pare-feu.
<b>filtre</b>	Ensemble de règles définissant les caractéristiques d'une classe dans le fichier de configuration IPQoS. Le système IPQoS sélectionne les flux de trafic conformes aux filtres du fichier de configuration IPQoS en vue de leur traitement. Voir <a href="#">filtrage de paquets</a> .
<b>filtre de paquets dynamique</b>	Voir <a href="#">filtre de paquets sans état</a> .
<b>filtre de paquets sans état</b>	<a href="#">filtrage de paquets</a> permettant de contrôler l'état des connexions actives et d'identifier, à l'aide des informations obtenues, les paquets du réseau autorisés à franchir le <a href="#">pare-feu</a> . En assurant le suivi et la coordination des requêtes et des réponses, un filtre de paquets sans état a la possibilité d'écarter une réponse non satisfaisante.
<b>gestion des clés</b>	La façon dont vous gérez les associations de sécurité.
<b>groupe anycast</b>	Groupe d'interfaces dotées de la même adresse anycast IPv6. L'implémentation du protocole IPv6 dans Oracle Solaris n'est pas compatible avec la création de groupes et d'adresses anycast. Cependant, les noeuds IPv6 Oracle Solaris peuvent assurer le transport du trafic vers des groupes anycast.
<b>HMAC</b>	Méthode de hachage à clé pour l'authentification de messages. HMAC est un algorithme d'authentification à clé secrète. HMAC est utilisé avec une fonction de repère cryptographique répétitive, telle que MD5 ou SHA-1, combinée avec une clé secrète partagée. La puissance cryptographique de HMAC dépend des propriétés de la fonction de repère sous-jacente.
<b>hôte</b>	Système qui n'effectue pas le transfert des paquets. Lors de l'installation d'Oracle Solaris, un système est désigné comme hôte par défaut et ne peut plus transmettre de paquets. Un hôte possède généralement une seule interface physique, mais peut également en avoir plusieurs.
<b>hôte multiréseau</b>	Système doté de plusieurs interfaces physiques et qui ne traite pas les paquets. Un hôte multiréseau peut exécuter des protocoles de routage.



<b>ICMP</b>	Internet Control Message Protocol, protocole Internet des messages de contrôle. Ce protocole sert à gérer les messages d'erreur ainsi que les messages de contrôle des échanges.
<b>ICMP requête d'écho</b>	Paquet transmis à une machine sur Internet en vue de solliciter une réponse. De tels paquets sont communément appelés paquets "ping".
<b>IKE</b>	Internet Key Exchange, échange de clé Internet. IKE automatise la mise en service de matériel d'identification authentifié pour les associations de sécurité IPsec.
<b>index du paramètre de sécurité</b>	SPI, Security Parameter Index. Nombre entier indiquant la rangée de la SADB qui permettra au récepteur de décrypter un paquet reçu.
<b>interface de réserve</b>	Interface physique prévue pour gérer le trafic des données uniquement en cas de défaillance d'une autre interface physique.
<b>interface physique</b>	Mode de raccordement d'un système à une liaison. Ce mode de raccordement est souvent mis en oeuvre sous la forme d'un pilote de périphérique et d'une NIC. Certaines cartes d'interface réseau (igb, par exemple) peuvent disposer de plusieurs points de connexion.
<b>interface réseau virtuelle (VNIC)</b>	Pseudo-interface offrant une connectivité réseau virtuelle qu'elle soit ou non configurée sur une interface réseau physique. Des conteneurs, tels que des zones IP exclusives, sont configurés sur des VNIC afin de former un réseau virtuel.
<b>IP</b>	Internet Protocol, protocole Internet. Méthode ou protocole utilisé pour envoyer les données d'un ordinateur à l'autre via Internet.
<b>IP</b>	Voir <a href="#">IP</a> , <a href="#">IPv4</a> , <a href="#">IPv6</a> .
<b>IPQoS</b>	Fonction logicielle qui permet l'implémentation du <a href="#">modèle Diffserv</a> standard en plus de la comptabilisation des flux et du marquage 802.1 D des réseaux locaux virtuels. A l'aide d'IPQoS, il est possible de fournir différents niveaux de services réseau aux clients et applications, comme indiqué dans le fichier de configuration IPQoS.
<b>IPsec</b>	Sécurité IP. Architecture de sécurité assurant la protection des datagrammes IP.
<b>IPv4</b>	Protocole Internet, version 4. IPv4 est parfois appelé IP. Cette version prend en charge un espace d'adressage à 32 bits.
<b>IPv6</b>	Protocole Internet, version 6. IPv6 prend en charge un espace d'adressage à 128 bits.
<b>liaison IP</b>	Utilitaire ou moyen de communication à l'aide duquel les noeuds peuvent communiquer dans la couche liaison. La couche liaison se trouve immédiatement sous IPv4/IPv6. Les réseaux Ethernet (simple ou reliés par un pont) ou les réseaux ATM sont des exemples de liaisons IP. Une liaison IP est définie par un ou plusieurs numéros ou préfixes de masque de sous-réseau IPv4. Un même numéro ou préfixe de masque de sous-réseau ne peut pas être attribué à plusieurs liaisons IP. Dans le système ATM LANE, une liaison IP est un LAN à émulation simple. Lorsque vous utilisez le système ARP, la portée du protocole ARP correspond à une liaison IP simple.
<b>liste de visiteurs</b>	Liste des noeuds mobiles qui visitent actuellement un agent étranger.

<b>liste des certificats révoqués (CRL)</b>	Liste des certificats de clés publiques ayant fait l'objet d'une révocation par une CA. Les CRL sont stockées dans la base de données des CRL, gérée par IKE.
<b>MAC</b>	MAC garantit l'intégrité des données et authentifie leur origine. MAC ne protège aucunement contre l'écoute frauduleuse des informations échangées.
<b>marqueur</b>	<p>1. Module de l'architecture diffserv et IPQoS attribuant une valeur au champ DS d'un paquet IP. Cette valeur indique la manière dont est traité le paquet. Dans l'implémentation IPQoS, le module du marqueur est ds cpmk.</p> <p>2. Module dans l'implémentation IPQoS qui marque l'indicateur de réseau local virtuel d'un datagramme Ethernet par une valeur de priorité utilisateur. La valeur de priorité utilisateur indique comment les datagrammes sont transmis sur un réseau comportant des périphériques VLAN. Ce module est appelé dl cosmk.</p>
<b>MD5</b>	Fonction de hachage cryptographique répétitive utilisée pour authentifier les messages, y compris les signatures numériques. Elle a été développée en 1991 par Rivest.
<b>modèle Diffserv</b>	Norme d'architecture du groupe IETF (Internet Engineering Task Force, groupe d'étude d'ingénierie Internet) destinée à l'implémentation de services différenciés sur les réseaux IP. Les modules principaux comprennent la classification, la mesure, le marquage, l'ordonnancement et le rejet. IPQoS implémente les modules de classification, de mesure et de marquage. Le modèle Diffserv est décrit dans le document RFC 2475, <i>An Architecture for Differentiated Services</i> .
<b>MTU</b>	Maximum Transmission Unit, unité de transmission maximale. Taille, exprimée en octets, des données pouvant être transmises via une liaison. Ainsi, la MTU d'une liaison Ethernet est de 1 500 octets.
<b>NAT</b>	Voir <a href="#">traduction d'adresses réseau</a> .
<b>NIC</b>	Network Interface Card, carte d'interface réseau. Carte réseau jouant le rôle d'interface d'un réseau. Certaines NIC ont plusieurs interfaces physiques. C'est le cas des cartes igb.
<b>noeud</b>	Dans IPv6, tout système IPv6, qu'il s'agisse d'un hôte ou d'un routeur.
<b>nom du keystore</b>	Nom qu'un administrateur attribue à une zone de stockage, ou keystore, sur une <a href="#">NIC</a> . Le nom du keystore est également appelé jeton ou ID de jeton.
<b>paquet</b>	Groupe d'informations transmis sous forme d'une unité sur les lignes de communications. Un paquet contient un <a href="#">en-tête IP</a> et une <a href="#">charge utile</a> .
<b>pare-feu</b>	Dispositif ou logiciel prévu pour isoler le réseau privé ou le réseau intranet d'une organisation d'Internet, afin de le protéger contre d'éventuelles intrusions. Un pare-feu peut inclure le filtrage de paquets, des serveurs proxy et les valeurs NAT (Network Address Translation, translation d'adresse réseau).
<b>périphérique VLAN</b>	Interface réseau permettant de renvoyer le trafic vers le niveau Ethernet (liaison de données) de la pile de protocole IP.
<b>PFS</b>	Perfect Forward Secrecy, secret rigoureux des transmission .Avec la fonction PFS, la clé visant à protéger la transmission des données n'est pas utilisée pour dériver d'autres clés. Il en est de même pour la source de la clé.

	PFS s'applique à l'échange de clés authentifiées uniquement. Voir aussi <a href="#">algorithme Diffie-Hellman</a> .
<b>PHB</b>	Per-Hop Behavior, comportement par saut. Priorité accordée à une classe de trafic. Le comportement par saut indique la priorité des flux de cette classe par rapport aux autres classes de trafic.
<b>pile</b>	Voir <a href="#">pile IP</a> .
<b>pile de protocole</b>	Voir <a href="#">pile IP</a> .
<b>pile IP</b>	TCP/IP est souvent appelé une "pile". Ce terme fait référence aux couches (TCP, IP et parfois d'autres) par lesquelles transitent toutes les données aux extrémités client et serveur d'un échange de données.
<b>PKI</b>	Public Key Infrastructure, infrastructure de clé publique. Système de certificats numériques, d'autorités de certification et d'autres autorités d'enregistrement prévu pour vérifier et authentifier la validité de chaque partie impliquée dans une transaction Internet.
<b>priorité utilisateur</b>	Valeur de 3 bits ayant pour effet de mettre en oeuvre des marqueurs de classe de services, qui définissent la façon dont les datagrammes Ethernet sont transférés sur un réseau de périphériques VLAN.
<b>protocole de transport de contrôle de flux</b>	SCTP, Stream Control Transport Protocol. Protocole de la couche transport assurant des communications orientées connexion sous une forme similaire au protocole TCP. De plus, SCTP gère les multiréseaux (une des extrémités de la connexion peut être associée à plusieurs adresses IP).
<b>protocole ESP</b>	Encapsulating Security Payload, association de sécurité. Extension de l'en-tête assurant l'intégrité et la confidentialité des datagrammes. ESP est l'un des cinq composants de l'architecture de sécurité IP (IPsec).
<b>publication des voisins</b>	Réponse à un message de sollicitation de voisinage ou processus selon lequel un noeud envoie des publications de voisinage non sollicitées pour signaler une modification de l'adresse de couche liaison.
<b>publication du routeur</b>	Processus selon lequel les routeurs annoncent leur présence (avec divers paramètres de connexion et paramètres Internet) de façon périodique ou en réponse à un message de sollicitation d'un routeur.
<b>reconfiguration dynamique</b>	Fonction permettant de reconfigurer un système en cours d'exécution sans incidence ou presque sur les opérations en cours. La reconfiguration dynamique n'est pas prise en charge par toutes les plates-formes Sun d'Oracle. Certaines plates-formes Sun d'Oracle ne prennent en charge que la reconfiguration dynamique de certains types de matériel comme les NIC.
<b>redirection</b>	Dans un routeur, technique permettant de signaler à un hôte le meilleur noeud (prochain saut) en vue d'atteindre une destination particulière.
<b>reniflage</b>	Action d'espionner les communications des réseaux informatiques. Cette technique est fréquemment employée avec des programmes automatisés pour extirper hors ligne des informations telles que des mots de passe en clair.
<b>répartition de charge</b>	Processus consistant à distribuer le trafic entrant et sortant au sein d'un groupe d'interfaces. La répartition de charge permet d'augmenter le rendement. Elle ne se produit que lorsque le trafic réseau se dirige vers plusieurs destinations utilisant plusieurs connexions. Il existe deux types de répartition de charge : la répartition de charge entrante pour le trafic entrant et la répartition de charge sortante pour le trafic sortant.

<b>réseau virtuel</b>	Regroupement de ressources et fonctionnalités réseau logicielles et matérielles gérées en tant qu'entité logicielle unique. Un réseau virtuel <i>interne</i> regroupe les ressources réseau sur un seul système, parfois appelé "réseau en boîte".
<b>réseau visité</b>	Réseau autre que le réseau domestique du noeud mobile auquel le noeud mobile est actuellement connecté.
<b>résultat</b>	Action à réaliser à l'issue de la mesure du trafic. Les compteurs IPQoS aboutissent à trois résultats signalés par la couleur rouge, jaune et verte. Vous définissez ces codes couleur dans le fichier de configuration IPQoS.
<b>routeur</b>	Système généralement composé de plusieurs interfaces ayant pour fonction d'exécuter des protocoles de routage et de transférer des paquets. Vous pouvez configurer un système à une seule interface en guise de routeur à condition que le système se trouve à l'extrémité d'une liaison PPP.
<b>RSA</b>	Méthode permettant d'obtenir des signatures numériques et des systèmes de cryptographie par clé publique. Cette méthode qui date de 1978 a été décrite par trois développeurs (Rivest, Shamir et Adleman).
<b>SA</b>	Voir <a href="#">association de sécurité</a> .
<b>SADB</b>	Security Associations Database, base de données des associations de sécurité. Table définissant les clés cryptographiques et les algorithmes cryptographiques. Les clés et les algorithmes ont pour intérêt de sécuriser la transmission des données.
<b>saut</b>	Mesure permettant l'identification du nombre de routeurs séparant deux hôtes. Si trois routeurs séparent une source et une destination, les hôtes se trouvent à quatre sauts l'un de l'autre.
<b>SCTP</b>	Voir protocole de transport de contrôle de flux.
<b>sélecteur</b>	Élément définissant de façon spécifique les critères à appliquer aux paquets d'une classe particulière en vue de sélectionner ce trafic dans le flux du réseau. Vous définissez les sélecteurs dans la clause de filtrage du fichier de configuration IPQoS.
<b>serveur proxy</b>	Serveur faisant l'interface entre une application client (telle qu'un navigateur Web) et un autre serveur. Ce type de serveur permet de filtrer les requêtes afin d'interdire l'accès à certains sites Web, par exemple.
<b>SHA-1</b>	Algorithme de hachage sécurisé (Secure Hashing Algorithm) L'algorithme s'applique à toute longueur d'entrée inférieure à $2^{64}$ afin d'obtenir une synthèse des messages. L'algorithme SHA-1 sert d'entrée à l'algorithme DSA.
<b>signature numérique</b>	Code numérique associé à un message électronique qui identifie l'expéditeur de manière unique.
<b>sollicitation des voisins</b>	Sollicitation envoyée par un noeud afin de déterminer l'adresse de couche liaison d'un voisin. Une telle sollicitation consiste à vérifier qu'un voisin est toujours accessible par une adresse de couche liaison mise en cache.
<b>sollicitation du routeur</b>	Processus selon lequel les hôtes demandent à des routeurs de générer immédiatement des publications du routeur, et non pas lors de la prochaine exécution programmée.
<b>SPD</b>	Voir <a href="#">base de données des stratégies de sécurité</a> .

---

<b>SPI</b>	Voir <a href="#">index du paramètre de sécurité</a> .
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol, protocole de contrôle de la transmission/protocole Internet. TCP/IP est le langage de communication ou protocole de base sur Internet. Il peut également servir de protocole de communication sur un réseau privé (intranet ou extranet).
<b>traduction d'adresses réseau</b>	NAT, Network Address Translation. Traduction d'une adresse IP utilisée au sein d'un réseau sous une adresse IP différente connue au sein d'un autre réseau. Cette technique sert à limiter le nombre d'adresses IP globales nécessaires.
<b>Triple-DES</b>	Triple-Data Encryption, triple chiffrement des données. Méthode de chiffrement par clé symétrique. Elle nécessite une clé de 168 bits. L'abréviation de Triple-DES est 3DES.
<b>tunnel</b>	Chemin suivi par un <a href="#">datagramme</a> pendant son encapsulation. Voir <a href="#">encapsulation</a> .
<b>tunnel bidirectionnel</b>	Tunnel pouvant transmettre des datagrammes dans les deux directions.
<b>tunnel inverse</b>	Tunnel débutant à l'adresse d'hébergement du noeud mobile et se terminant au niveau de l'agent local.
<b>usurpation</b>	Action d'accéder par intrusion à un ordinateur en envoyant un message avec une adresse IP provenant prétendument d'un hôte de confiance. Pour ce faire, un pirate doit d'abord utiliser différentes techniques pour identifier l'adresse IP d'un hôte fiable, puis modifier les en-têtes de paquets pour donner l'impression que les paquets proviennent de cet hôte.
<b>valeur de hachage</b>	Nombre généré à partir d'une chaîne de texte. Les fonctions de hachage garantissent que les messages transmis n'ont pas été sabotés. <a href="#">MD5</a> et <a href="#">SHA-1</a> sont des exemples de fonctions de hachage unidirectionnel.
<b>VPN</b>	Virtual Private Network, réseau privé virtuel. Réseau logique sécurisé utilisant des tunnels dans un réseau public tel qu'Internet.



# Index

---

## Nombres et symboles

- , répertoire, Clé privée (IKE), 305
- 6to4, routeur relais
  - Problème de sécurité, 122–124
  - Tâche de configuration de tunnel, 133, 134
  - Tunnel 6to4, 157
- 6to4relay, commande, 133
  - Définition, 157
  - Exemple, 158
  - Syntaxe, 157
  - Tâche de configuration d'un tunnel, 133

## A

- A, option
  - ikecert, commande, 305
  - ikecert certlocal, commande, 275
- a, option
  - ikecert, commande, 285
  - ikecert certdb, commande, 276, 281
  - ikecert certrldb, commande, 290
- Abandon ou perte de paquet, 102
- Accélération, Calculs IKE, 298
- Accès aux CRL via http, use\_http, mot-clé, 290
- Accord de niveau de service
  - Classes de services, 418
  - Différentes classes de service, 416
  - Facturation des clients basée sur la comptabilisation des flux, 486
- Accords de niveau de service, 414

- acctadm, commande pour la comptabilisation de flux, 420
- acctadm, commande, comptabilisation des flux, 487
- acctadm, commande pour la comptabilisation de flux, 503
- action, instruction, 505
- Actualisation, Clés prépartagées (IKE), 270–271
- Administration du réseau, Conception du réseau, 25
- Administration réseau, Noms d'hôtes, 30
- Adresse
  - Sélection des adresses par défaut, 114–116
  - Temporaire, dans IPv6, 83–86
- Adresse IPv6, Unicité, 166
- Adresse lien-local
  - Configuration manuelle, avec un jeton, 88
  - IPv6, 166, 169
- Adresse MAC, 189
- Adresse multicast, IPv6, Comparaison aux adresses de diffusion, 169
- Adresse temporaire, dans IPv6
  - Configuration, 84–86
  - Définition, 83–86
- Adresses IP
  - Classes de réseau
    - Administration des numéros de réseau, 27
    - Conception d'un schéma d'adressage, 27
    - Notation CIDR, 27
- Affichage
  - Configuration IPsec, 252–254
  - Stratégie IPsec, 235
- Affichage des statistiques de protocole, 95
- AH, Voir En-tête d'authentification (AH)

AH (Authentication Header, en-tête d'authentification)  
  Mécanisme de protection IPsec, 218–221  
  Protection des datagrammes IP, 218  
  Sécurité, 219

Ajout  
  Certificats autosignés (IKE), 275  
  Certificats de clés publiques (IKE), 279–285  
  Certificats émanant de CA (IKE), 279–285  
  Clés prépartagées (IKE), 271–272  
  manuellement, clés (IPsec), 243–245  
  SA IPsec, 232, 243–245

Algorithme d'authentification DSS, 305

Algorithme de chiffrement  
  IPsec  
    3DES, 221  
    AES, 221  
    Blowfish, 221  
    DES, 221

Algorithme de chiffrement 3DES, IPsec, 221

Algorithme de chiffrement AES, IPsec, 221

Algorithme de chiffrement Blowfish, IPsec, 221

Algorithme de chiffrement DES, IPsec, 221

Algorithme de chiffrement RSA, 306

Algorithme de chiffrement Triple-DES, IPsec, 221

Algorithmes d'authentification  
  Certificats IKE, 305  
  Clés prépartagées IKE, 265–267

Algorithmes de chiffrement, Clés prépartagées  
  IKE, 265–267

anycast, adresse, 133

anycast, groupe, Routeur relais 6to4, 133

Architecture IPsec, *Voir* IPsec

ARP (Address Resolution Protocol, protocole de  
  résolution d'adresse), Comparaison avec le protocole  
  de détection des voisins, 168–170

AS (Autonomous System, Système autonome), *Voir*  
  Topologie réseau

Association d'identité, 190

Association de sécurité (SA), Création  
  manuelle, 243–245

Association de sécurité (SA, Security Association),  
  IPsec, 217–218

Associations de sécurité (SA)  
  Ajout d'IPsec, 232, 240

Associations de sécurité (SA) (*Suite*)  
  Base de données IPsec, 255  
  Définition, 212  
  Génération de nombres aléatoires, 261  
  IKE, 302  
  IPsec, 232, 240  
  ISAKMP, 260

assured forwarding (AF), 423

Assured forwarding (AF), 498

Assured Forwarding (AF), Pour une instruction action  
  d'un marqueur, 459

Assured forwarding (AF), Table de points de code  
  AF, 498

ATM, prise en charge, IPv6, 172

## B

Base de données  
  Base de données des associations de sécurité  
    (SADB), 255  
  IKE, 304–307  
  ike/crls, base de données, 306, 307  
  ike.privatekeys, base de données, 305  
  ike/publickeys, base de données, 306  
  SPD (Security Policy Database, base de données de  
    stratégie de sécurité), 212

Base de données des associations de sécurité  
  (SADB), 255

IPsec, 212

Base de données réseau  
  ethers, base de données  
    Vérification des entrées, 140  
  name-service/switch, service SMF, 145

Bases de données  
  ike.privatekeys, base de données, 307  
  ike/publickeys, base de données, 307

Bases de données de réseau  
  hosts, base de données  
    Vérification des entrées, 140

Bases de données réseau  
  name-service/switch, service SMF, 145  
  Services de noms, 147

Bibliothèque PKCS #11, ike/config, fichier, 304

Brouillons Internet, SCTP avec IPsec, 213



## C

- c, option
  - in.iked, démon, 270
  - ipseckey, commande, 255
- Calculs, Accélération matérielle d'IKE, 298–299
- cert\_root, mot-clé, Fichier de configuration IKE, 282
- cert\_root, mot de passe, Fichier de configuration IKE, 287
- cert\_trust, mot-clé
  - Fichier de configuration IKE, 278
  - ikecert, commande, 305
- cert\_trust, mot de passe, Fichier de configuration IKE, 287
- Certificat
  - Stockage
    - IKE, 306
- Certificats
  - Ajout à une base de données, 281
  - Autosignés, création (IKE), 275
  - De CA, 281
  - Demande
    - Auprès d'une CA, 280
    - Sur le matériel, 286
  - Description, 281
  - Emanant d'une CA sur le matériel, 288
  - Ignorer les CRL, 283
  - IKE, 262
  - ike/config, fichier, 287
  - Liste, 276
  - Stockage
    - Matériel, 298
    - Sur un ordinateur, 274
- Certificats de clés publiques, *Voir* Certificats
- Chiffre, *Voir* Algorithme de chiffrement
- class, clause, dans le fichier de configuration IPQoS, 455
- class, clause du fichier de configuration IPQoS, 507
- Classes, 418
  - Définition dans le fichier de configuration IPQoS, 463, 467
  - Liste de sélecteurs, 492
  - Syntaxe de la clause class, 507
- Classes de service, *Voir* Classes
- Clause params, Pour une action de mesure, 472
- Clé
  - Création pour les SA IPsec, 243–245
  - Gestion IPsec, 217–218
  - ike/publickeys, base de données, 307
  - Stockage (IKE)
    - Certificat, 306
    - Clé publique, 306
    - Privée, 305
  - Clé prépartagée (IKE), Stockage, 304
  - Clé prépartagée (IPsec), Création, 243–245
  - Clé privée, Stockage (IKE), 305
  - Clé publique, Stockage (IKE), 306
- Clés
  - Gestion automatique, 260
  - Gestion manuelle, 255–256
  - ike.privatekeys, base de données, 307
  - Prépartage (IKE), 262
- Clés prépartagées (IKE)
  - Liste des tâches, 268
  - Remplacement, 270–271
- Client DHCP
  - Abandon de l'adresse IP, 198
  - Activation, 195–196
  - Administration, 197
  - Annulation de la configuration, 196–197
  - Arrêt, 195
  - Définition, 181
  - Démarrage, 192, 197
  - Désactivation, 196–197
  - Exécution de programmes, 203–204
  - Extension de bail, 197
  - Informations réseau sans bail, 197
  - Interfaces logiques, 199–200
  - Interfaces réseau multiples, 199–200
  - Libération de l'adresse IP, 198
  - Nom d'hôte
    - Spécification, 200–201
  - Paramètres, 198–199
  - Scripts d'événement, 203–204
- Client DHCPv4, Gestion de l'interface réseau, 193
- Client DHCPv6, Gestion de l'interface réseau, 194
- Commande
  - IKE, 304–307
  - ikeadm, commande, 302, 303–304

Commande, IKE (*Suite*)

- ikecert, commande, 302, 304
- in.iked, démon, 302

## IPsec

- ipsecalgs, commande, 220
- ipseconf, commande, 227
- snoop, commande, 257

## Commandes

## IKE

- ikeadm, commande, 263
- ikecert, commande, 263

## IPsec

- in.iked, commande, 218
- ipsecalgs, commande, 254
- ipseconf, commande, 252
- ipseckey, commande, 227, 255–256
- Liste, 227–228
- Questions de sécurité, 256

## Comportement par pas (PHB), Définition dans le fichier de configuration IPQoS, 474

## Comptabilisation des flux, 486, 501

- Table des enregistrements de flux, 502

## Conception du réseau

- Nommage des hôtes, 30
- Présentation, 25
- Schéma d'adressage IP, 27
- Sélection du nom de domaine, 31

## Confidentialité de transmission parfaite (PFS)

- Description, 260
- IKE, 260

## Configuration

- Client DHCP, 187
- Fichiers de configuration TCP/IP, 143
- IKE, 267
- IKE avec certificats de clés publiques, 273
- IKE avec des certificats autosignés, 274–279
- IKE avec des certificats de clés publiques, 274–279
- IKE avec des certificats émanant de CA, 279–285
- IKE avec des certificats sur le matériel, 285–288
- IKE avec des systèmes portables, 291–298
- ike/config, fichier, 302
- IPsec, 252
- ipseconf, fichier, 252–254
- Manuelle, interfaces pour IPv6, 78–79

Configuration (*Suite*)

- Pools d'adresses, 319–320
  - Règles de filtrage de paquets, 314–317
  - Règles NAT, 317–319
  - Réseau TCP/IP
    - Service TCP/IP standard, 70
  - Réseaux TCP/IP
    - name-service/switch, service SMF, 145
  - Routeur, 147
  - Routeurs, 56
    - Présentation, 57
  - Routeurs IPv6, 80
  - Tunnels
    - Voir Tunnels
  - VPN en mode Tunnel avec IPsec, 239–242
  - VPN protégé par IPsec, 239–242
- Configuration automatique d'adresse, IPv6, 164
- Configuration automatique d'adresse sans état, 165
- Configuration d'adresse automatique, IPv6, 160
- Configuration de liaison persistante, Création, 50
- Configuration de réseau, Activation d'IPv6 sur un hôte, 82–89
- Configuration de routeur, Routeur IPv4, 56
- Configuration du client, 189
- Configuration du protocole IKE (liste des tâches), 267
- Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches), 273
- Configuration du protocole IKE avec des clés prépartagées (liste des tâches), 268
- Configuration du protocole IKE pour les systèmes portables (liste des tâches), 291
- Configuration du réseau, Configuration de la sécurité, 209
- Configuration IPQoS, fichiers d'exemple, Serveur Web au mieux, 453
- Configuration IPsec, Configuration, 221
- Configuration réseau
- Configuration
    - Service, 70
  - Configuration du serveur de configuration réseau, 55
  - Hôtes multiréseau IPv6, 78–79
  - Routeur, 57
  - Routeur IPv6, 80

- Configuration réseau (*Suite*)
    - Tâches de configuration réseau IPv4, 45
  - Conformité du trafic
    - Définition, 472
    - Paramètres de débit, 494, 495
    - Planification
      - Débits dans la stratégie QoS, 439
      - Résultats dans la stratégie QoS, 440
    - Résultats, 419, 494
  - Considérations de sécurité
    - Configuration
      - IPsec, 231
    - Problèmes liés au routeur relais 6to4, 142
  - Contournement
    - IPsec sur LAN, 240
    - Stratégie IPsec, 221
  - Contrôle des flux, Via les modules de mesure, 419
  - Couche transport
    - Obtention du statut des protocoles de transport, 96–97
    - TCP/IP
      - SCTP, protocole, 71–74
  - Couleurs, 419, 495
  - Création
    - Certificats autosignés (IKE), 275
    - Demandes de certificats, 280
    - `ipsecinit.conf`, fichier, 232
    - Rôle lié à la sécurité, 245–246
    - SA IPsec, 232, 243–245
  - CRL
    - Accès depuis un point central, 289
    - Ignorer, 283
    - `ikecert certrl.db`, commande, 306
    - Liste, 289
  - Crochet de filtre de paquets, 320
- D**
- D, option
    - `ikecert`, commande, 305
    - `ikecert certlocal`, commande, 275
  - Datagramme IP, 211
  - Datagramme IP, Protection avec IPsec, 211
  - Découverte de routeur sur IPv6, 160
  - `defaultrouter`, fichier, Configuration du mode
    - Fichiers locaux, 53
  - Demande de certificat, Utilisation, 306
  - Demandes d'options, 191
  - Demandes de certificats
    - Àuprès d'une CA, 280
    - Sur le matériel, 286
  - Démon
    - `in.iked`, démon, 302
    - `in.ndpd`, 160
    - `in.ripngd`, démon, 80
    - `inetd`, services Internet, 145
  - Démons
    - `in.iked`, démon, 260, 263
    - `in.ripngd`, démon, 161
  - Dépannage
    - ?Réseaux TCP/IP
      - Perte de paquets, 103
    - Charge IKE, 284
    - IPv6, 140–142
    - Problèmes avec IPv6, 141
    - Réseau TCP/IP
      - Affichage du statut des routes connues, 100–101
      - Contrôle du statut du réseau à l'aide de la commande `netstat`, 95
      - Contrôle du transfert des paquets à l'aide de la commande `snoop`, 107
      - Observation des transmissions des interfaces, 98
      - Obtention des statistiques par protocole, 95–96
      - Obtention du statut des protocoles de transport, 96–97
      - Perte de paquet, 102
      - Sondage des hôtes distants à l'aide de la commande `ping`, 102
      - Suivi de l'activité de `in.ndpd`, 105
      - Suivi de l'activité de `in.routed`, 104–105
      - `traceroute`, commande, 106–107
      - Vérification des paquets transmis entre un client et un serveur, 110
  - Réseaux TCP/IP
    - Contrôle de transfert de paquets sur la couche IP, 110–114
    - Méthodes générales, 139
    - `ping`, commande, 103

Dépannage, Réseaux TCP/IP (*Suite*)

- Programmes de diagnostic tiers, 139
- TCP/IP, réseau
  - Méthode générale, 139
  - Vérification logicielle, 139
  - Vérification des liaisons PPP
    - Flux de paquets, 107
- Désactivation d'IP Filter, 328–329
- Détection d'adresse dupliquée, Algorithme, 167
- Détection d'inaccessibilité de voisin
  - IPv6, 166, 169
- Détection de routeur, dans IPv6, 165, 168
- dhcpageant, commande, Description, 206
- dhcpageant, démon, 192
- dhcpageant, démon, Fichier de paramètres, 207
- dhcpageant, fichier, Description, 207
- dhcpcfg, commande, Description, 206
- dhcpcd, démon, Description, 205
- dhcpcd4.conf, fichier, Description, 207
- dhcpcd6.conf, fichier, Description, 207
- dhcpcinfo, commande, Description, 206
- dhcpcmgr, commande, Description, 206
- dhcpsvc.conf, fichier, 207
- dhcptab, table, Description, 207
- DHCPv4, comparaison avec DHCPv6, 188
- DHCPv6, Nom du client, 189
- DHCPv6, comparaison avec DHCPv4, 188
- DHCPv6, modèle administratif, 189
- dhcrelay, commande, Description, 205
- dhtadm, commande, Description, 206
- dladm, commande
  - Affichage des informations de tunnel, 136–137
  - Création de tunnels, 127–131
  - Modification de configuration de tunnel, 135–136
  - Suppression de tunnels IP, 138
- dlcosmk, marqueur, 419
  - Étiquettes VLAN, 499
  - Planification de la transmission du
    - datagramme, 441
  - Tableau des valeurs de priorité utilisateur, 500
- DNS, Préparation à la prise en charge d'IPv6, 40–41
- DNS (Domain Name System), Sélection d'un service de noms, 31

## DNS (Domain Name System, système de nom de domaine)

- Fichier de zone, 89
- Fichier de zone inversé, 89
- DNS (domain name system, système de noms de domaine), Extensions IPv6, 172
- Document RFC (Request for Comments)
  - IKE, 213
  - IPsec, 213
- Domaine logique, IPsec, 226
- DSCP (point de code DS), 422
  - Configuration des couleurs, 496
  - Configuration sur un routeur diffserv, 475, 498
  - Définition dans le fichier de configuration
    - IPQoS, 459
  - Paramètre dscp\_map, 499
  - PHB et DSCP, 422
  - Point de code de traitement assuré, 423
  - Point de code de traitement assuré (AF), 498
  - Point de code de traitement EF, 423, 498
- dscpmk, marqueur, 419
  - Appel dans une instruction action du
    - marqueur, 458, 464, 470, 473
  - PHB pour la transmission des marqueurs, 497
  - Planification de la transmission des paquets, 441

**E**

- En-tête d'authentification (AH), Protection de paquets IP, 211
- Enregistrement, Réseau, 29
- Enregistrement AAAA, 90, 172
- Ensemble de règles
  - Voir Voir IP Filter*
  - Filtrage de paquets, 314–320
  - Inactif
    - Voir aussi IP Filter*
- Ensemble de règles actif, *Voir IP Filter*
- Ensemble de règles inactif, *Voir IP Filter*
- Ensembles de règles, NAT, 317–319
- Équilibrage de charge
  - Réseau compatible IPQoS, 429
  - Sur un réseau activé IPv6, 167
- Équilibrage de charge entrante, 167

- ESP, *Voir* ESP (Encapsulating Security Payload, association de sécurité)
- ESP (Encapsulating Security Payload, association de sécurité)
  - Description, 219–220
  - Mécanisme de protection IPsec, 218–221
  - Protection de paquets IP, 211
  - Sécurité, 219
- /etc/bootparams, fichier, Description, 143
- /etc/default/dhcpagent, fichier, 198–199
- /etc/default/dhcpagent, fichier, Description, 207
- /etc/default/inet\_type, fichier, 103–104
  - Valeur de DEFAULT\_IP, 158
- /etc/defaultrouter, fichier
  - Configuration du mode Fichiers locaux, 53
  - Description, 143
- /etc/dhcp/dhcptags, fichier, Description, 208
- /etc/dhcp/eventhook, fichier, 204
  - Description, 207
- /etc/dhcp/inittab, fichier, Description, 208
- /etc/dhcp/interface.dh\*, fichier, Description, 207
- /etc/ethers, fichier, Description, 143
- /etc/inet/dhcd4.conf, fichier, Description, 207
- /etc/inet/dhcd6.conf, fichier, Description, 207
- /etc/inet/dhcsvc.conf, fichier, Description, 207
- /etc/inet/hosts, fichier, 231
  - Configuration du mode Fichiers locaux, 53
  - Configuration en mode Client réseau, 54
  - Description, 143
- /etc/inet/ike/config, fichier
  - cert\_root, mot-clé, 282, 287
  - cert\_trust, mot-clé, 278
  - cert\_trust, mot de passe, 287
  - Certificats autosignés, 278
  - Certificats de clés publiques, 282, 287
  - Clés prépartagées, 269
  - Considérations en matière de sécurité, 303
  - Description, 261, 302
  - Entrée de bibliothèque PKCS #11, 304
  - Exemple, 269
  - ignore\_crls, mot-clé, 283
  - ikecert, commande, 305
  - ldap-list, mot-clé, 290
  - pkcs11\_path, mot-clé, 285, 304
  - /etc/inet/ike/config, fichier (*Suite*)
    - proxy, mot-clé, 290
    - Récapitulatif, 263
    - Stockage des certificats sur le matériel, 287
    - use\_http, mot-clé, 290
  - /etc/inet/ike/crls, répertoire, 307
  - /etc/inet/ike/publickeys, répertoire, 307
  - /etc/inet/ipaddrsel.conf, fichier, 115, 155
  - /etc/inet/ipsecinit.conf, fichier, 252–254
  - /etc/inet/ndpd.conf, fichier, 81, 160
    - Configuration d'adresse temporaire, 84
    - Création, 81
    - Mot-clé, 152–155, 161
    - Publication de routeur 6to4, 132
    - Variables de configuration d'interface, 152
    - Variables de configuration de préfixes, 154
  - /etc/inet/secret/ike.privatekeys, répertoire, 307
  - /etc/ipf/ipf.conf, fichier, *Voir* IP Filter
  - /etc/ipf/ipnat.conf, fichier, *Voir* IP Filter
  - /etc/ipf/ippool.conf, fichier, *Voir* IP Filter
  - /etc/netmasks, fichier, Description, 143
  - /etc/networks, fichier, Description, 143
  - /etc/protocols, fichier, Description, 143
  - /etc/services, fichier, Description, 143
  - ethers, base de données, Vérification des entrées, 140
  - Événements DHCP, 203–204
  - eventhook, fichier, 204
  - Exemple de fichier de configuration IPQoS, Mode de reconnaissance des couleurs, 495
  - Exemple de réseau pour IPQoS, 451
  - Expedited Forwarding (EF), 423
  - Expedited forwarding (EF), 498
  - Expedited Forwarding (EF), Définition dans le fichier de configuration IPQoS, 460
  - Extension de bail DHCP, 197

**F**

  - F, option, ikecert certlocal, commande, 275
  - f, option, in.iked, démon, 270
  - Fichier
    - IKE
      - crls, répertoire, 264, 307
      - ike/config, fichier, 261

Fichier, IKE (*Suite*)

- `ike.preshared`, fichier, 263, 304
- `ike.privatekeys`, répertoire, 263
- `publickeys`, répertoire, 263, 307

## IPsec

- `ipsecinit.conf`, fichier, 227

## Fichier de configuration

## IPv6

- `/etc/inet/ipaddrsel.conf`, fichier, 155
- `/etc/inet/ndpd.conf`, fichier, 152–155

## Fichier de zone, 89

## Fichier de zone inversé, 89

## Fichier journal

- Affichage pour IP Filter, 345–346
- Vidage dans IP Filter, 346–347

## Fichier keystore de clés softtoken

- Stockage de clés avec metaslot, 299, 304

## Fichiers

## IKE

- `ike/config`, fichier, 228, 263, 302
- `ike.privatekeys`, répertoire, 307

## IPsec

- `ipsecinit.conf`, fichier, 252–254
- `ipseckeys`, fichier, 228

## Fichiers de configuration

- Création pour IP Filter, 348–349

- Exemples IP Filter, 314

## IPv6

- `/etc/inet/ndpd.conf`, fichier, 152, 154

## Fichiers de configuration IPQoS, exemple,

- Configuration du périphérique VLAN, 500

## Fichiers de configuration IPQoS (exemples)

- Serveur d'application, 465
- Serveur Web premium, 452

## Fichiers de stratégie

- `ike/config`, fichier, 228, 263, 302
- `ipsecinit.conf`, fichier, 252–254
- Questions de sécurité, 253–254

## Fichiers journaux, Création pour IP Filter, 344–345

## Fichiers locaux, Sélection d'un service de noms, 31

`filter`, clause, dans le fichier de configuration

- IPQoS, 457

`filter`, clause du fichier de configuration IPQoS, 507

## Filtrage de paquets

- Activation d'un nouvel ensemble de règles, 331–333

## Ajout de règles

- Ensemble actif, 333–334
- Ensemble inactif, 334–335

## Basculement entre les ensembles de règles, 335–336

## Configuration, 314–317

## Désactivation, 327–328

## Gestion des ensembles de règles, 330–336

## Rechargement après la mise à jour de l'ensemble de règles actuel, 331–333

## Suppression

- Ensemble de règles actif, 333

## Filtrage par paquet

## Suppression

- Ensemble de règles inactif, 336

## Filtre, Planification de la stratégie QoS, 436

## Filtres, 418

## Création dans le fichier de configuration

- IPQoS, 463, 468

## Liste de sélecteurs, 492

Syntaxe de la clause `filter`, 507`flowacct`, module, 419, 501

## Attributs des enregistrements de flux, 503

Commande `acctadm` pour le fichier de comptabilisation de flux, 503

## Enregistrements de flux, 486

Instruction `action` pour `flowacct`, 461

## Paramètres, 502

## Table des enregistrements de flux, 502

## Flux de paquets

## Routeur relais, 123

## Tunnel, 121

## Flux de paquets, IPv6, Tunnel 6to4, 121

## Flux de paquets vers IPv6, 6to4 et IPv6 natif, 123

**G**

## Gestion de clés, Manuel, 255–256

## Gestion de trafic, Contrôle du flux, 418

## Gestion des clés

## Automatique, 260

## IKE, 260

`ike`, service, 218

**Gestion des clés (*Suite*)**

- IPsec, 217–218
- manual-key, service, 218
- Zone, 229

**Gestion du trafic**

- Hiérarchisation des flux de trafic, 416
- Planification de topologies de réseau, 429
- Régulation de la bande passante, 415
- Transfert du trafic, 422, 423, 424

**Groupes Diffie-Hellman, Clés prépartagées**

- IKE, 265–267

**H**

hosts, base de données, Vérification des entrées, 140

hosts, fichier, 231

**Hôte**

- Adresse IPv6 temporaire, 83–86
- Configuration pour IPv6, 82–89

**Hôte Base de données**

- /etc/inet/hosts, fichier
- Configuration du mode Fichiers locaux, 53

**Hôtes**

- Dépannage de problèmes généraux, 139
- Multiréseau
  - Configuration, 62
- Nom d'hôte
  - Administration, 30
- Vérification de la connectivité des hôtes à l'aide de la commande ping, 102
- Vérification de la connectivité IP, 103

**Hôtes multiréseau**

- Activation pour IPv6, 78–79
- Définition, 62

**I****ICMP, protocole**

- Affichage des statistiques, 95
- Appel via la commande ping, 102

**ID d'interface, Utilisation d'un jeton configuré**

- manuellement, 88

**ID de client, 189**

ID de jeton, Matériel, 307

Identificateur universel de ressources (URI), Accès aux CRL, 289

ignore\_crls, mot-clé, Fichier de configuration

IKE, 283

**IKE****Affichage**

Affichage des algorithmes et groupes de la phase 1, 265–267

Affichage des algorithmes disponibles, 265–267

Affichage des algorithmes et groupes de la phase 1, 265–267

Ajout de certificats autosignés, 275

Associations de sécurité, 302

Base de données, 304–307

Certificats, 262

Clés prépartagées, 262

Affichage des algorithmes et groupes de la phase 1, 265–267

Confidentialité de transmission parfaite (PFS), 260

**Configuration**

Avec des certificats de clés publiques, 273

avec des certificats émanant de CA, 279–285

Avec des clés prépartagées, 268

Systèmes portables, 291–298

Création de certificats autosignés, 275

crls, base de données, 307

Démon, 302

Description des commandes, 263–264

Description du service SMF, 263–264

Document RFC, 213

Emplacements de stockage des clés, 263–264

Fichiers de configuration, 263–264

Génération de demandes de certificats, 280

Gestion avec SMF, 246–248

Gestion des clés, 260

ike.preshared, fichier, 304

ike.privatekeys, base de données, 307

ikeadm, commande, 303–304

ikecert, commande, 304

ikecert certdb, commande, 281

ikecert certrldb, commande, 290

ikecert tokens, commande, 299

Implémentation, 267



**IKE (Suite)**

- `in.iked`, démon, 302
- Modification
  - Niveau de privilège, 304
- NAT et, 294–295, 296–297
- Niveau de privilège
  - Description, 303
  - Modification, 304
- Phase 1, 260
- Phase 2, 261
- Présentation, 259
- `publickeys`, base de données, 307
- Référence, 301
- SA ISAKMP, 260, 261
- Service de SMF, 301–302
- Systèmes portables, 291–298
- Utilisation avec une carte Sun Crypto
  - Accelerator, 307
- Utilisation d'une carte Sun Crypto Accelerator, 305
- Utilisation de la carte Sun Crypto Accelerator 6000, 298–299
- Vérification de la validité de la configuration, 270
- `ike`, service
  - Description, 218, 251
  - Utilisation, 232
- `ike/config`, fichier, *Voir /etc/inet/ike/config*, fichier
- `ike.preshared`, fichier, 270, 304
  - Exemple, 272
- `ike.privatekeys`, base de données, 307
- `ikeadm`, commande
  - Description, 302, 303–304
  - dump, sous-commande, 265–267
- `ikecert`, commande
  - A, option, 305
  - a, option, 285
  - Description, 302, 304
  - T, option, 285
  - t, option, 305
- `ikecert certdb`, commande
  - a, option, 276, 281
- `ikecert certlocal`, commande
  - kc, option, 280
  - ks, option, 275
- `ikecert certrldb`, commande, -a, option, 290
- `ikecert tokens`, commande, 299
- `in.dhcpd`, démon, Description, 205
- `in.iked`, démon
  - Activation, 302
  - c, option, 270
  - Description, 260
  - f, option, 270
- `in.ndpd`, démon
  - Création d'un journal, 105
  - Option, 160
- `in.ndpd` (démon), Vérification du statut, 140
- `in.rdisc`, programme, Description, 148
- `in.ripngd`, démon, 80, 161
- `in.routed`, démon
  - Création d'un journal, 104–105
  - Description, 147
  - Mode d'économie d'espace, 148
- `in.tftpd`, démon, 55
- `in.tftpd`, démon, Activation, 55
- Index de paramètre de sécurité (SPI, Security Parameter Index), Description, 217–218
- `inet_type`, fichier, 103–104
- `inetd`, démon
  - Services d'administration, 145
  - Services IPv6, 161–163
- `inetd`, démon, Vérification du statut, 140
- `inetd` (démon), Service démarré, 70
- Interface, Vérification des paquets, 108
- Interface logique, 190
- Interface socket PF\_KEY, IPsec, 217
- Interfaces
  - Configuration
    - Adresse temporaire, 83–86
    - Manuelle, pour IPv6, 78–79
    - Sur une liaison de données, 48
  - Création d'une configuration persistante, 50
- Interfaces IP
  - Configuration sur les tunnels, 125, 129, 131
- Interfaces logiques, Systèmes clients DHCP, 199–200
- Interfaces réseau multiples, Systèmes clients DHCP, 199–200
- Internet Security Association and Key Management Protocol (ISAKMP), Description, 261



Internet Security Association and Key Management Protocol (ISAKMP) SA, Emplacement de stockage, 304

IP, protocole

- Affichage des statistiques, 95
- Vérification de la connectivité des hôtes, 102

IP Filter

- Affichage
  - Fichier journal, 345–346
  - Statistiques d'état, 342–343
  - Statistiques de pool d'adresses, 343–344
  - Statistiques NAT, 343
  - Table d'état, 341–342
- Création
  - Fichiers journaux, 344–345
- Création de fichiers de configuration, 348–349
- Crochet de filtre de paquets, 320, 324–325
- Désactivation, 328–329
  - NAT, 328
- Enregistrement dans un fichier des paquets consignés, 347–348
- Ensemble de règles, 314–320
  - Actif, 330–331
    - Activation d'un nouvel ensemble, 331–333
    - Ajout de règles à l'ensemble actif, 333–334
    - Ajout de règles à l'ensemble inactif, 334–335
    - Basculement de l'un à l'autre, 335–336
  - Inactif, 331
  - Suppression, 333
  - Suppression de l'ensemble inactif, 336
- /etc/ipf/ipf.conf, fichier, 348–349
- /etc/ipf/ipf6.conf, fichier, 320–321
- /etc/ipf/ipnat.conf, fichier, 348–349
- /etc/ipf/ippool.conf, fichier, 348–349
- Exemples de fichier de configuration, 314
- Filtrage de loopback, 326–327
- Gestion des ensembles de règles de filtrage de paquets, 330–336
- ipadm, commande, 313
- ipf, commande, 325–326
  - 6, option, 320–321
- ipf.conf, fichier, 314–317
- ipf6.conf, fichier, 320–321

IP Filter (*Suite*)

- ipfstat, commande
  - 6, option, 320–321
- ipmon, commande
  - IPv6, 320–321
- IPMP, 313
- ipnat, commande, 325–326
- ipnat.conf, fichier, 317–319
- ippool, commande, 339
  - IPv6, 320–321
- ippool.conf, fichier, 319–320
- IPv6, 320–321
- NAT, 317–319
- Open Source, 310
- Pool d'adresses
  - Affichage, 339
  - Ajout, 340
  - Suppression, 339–340
- Pools d'adresses, 319–320
- Présentation, 309–310
- Présentation du filtrage de paquets, 314–317
- Réactivation, 325–326
- Recommandations relatives à l'utilisation, 313
- Règles NAT
  - Affichage, 337
  - Ajout, 338
  - Suppression
    - Règles NAT, 337–338
  - Vidage de fichier journal, 346–347
- ipaddrsel, commande, 115, 156–157
- ipaddrsel.conf, fichier, 115, 155
- ipadm, commande, 313
  - Contrôle du client DHCP, 197
  - hostmodel, paramètre, 240
  - Hôtes multiréseau, 63
  - Montage d'une interface, 48
  - Multiréseau strict, 240
  - Outil de dépannage, 139
- ipdam, commande, DHCP, 206
- ipf, commande
  - Voir aussi* IP Filter
  - 6, option, 320–321
  - a, option, 331–333
  - Ajout de règles via la ligne de commande, 333–334

- ipf, commande (*Suite*)
    - D, option, 328–329
    - E, option, 325–326
    - F, option, 327–328, 331–333, 333, 336
    - f, option, 325–326, 331–333, 333–334, 334–335
    - I, option, 336
    - l, option, 334–335
    - s, option, 335–336
  - ipf.conf, fichier, 314–317
    - Voir* IP Filter
  - ipfstat, commande, 341–342
    - Voir aussi* IP Filter
    - 6, option, 320–321
    - I, option, 331
    - i, option, 330–331, 331
    - o, option, 330–331, 331
    - s, option, 342–343
    - t, option, 341–342
  - ipgpc (classificateur), *Voir* Module de classification
  - ipmon, commande
    - Voir aussi* IP Filter
    - a, option, 345–346
    - F, option, 346–347
    - IPv6, 320–321
    - o, option, 345–346
  - IPMP, Activation du filtrage de paquets, 313
  - ipnat, commande
    - Voir aussi* IP Filter
    - Ajout de règles via la ligne de commande, 338
    - C, option, 328
    - F, option, 328, 337–338
    - f, option, 325–326, 338
    - l, option, 337
    - s, option, 343
  - ipnat.conf, fichier, 317–319
    - Voir* IP Filter
  - ippool, commande
    - Voir aussi* IP Filter
    - Ajout de règles via la ligne de commande, 340
    - F, option, 339–340
    - f, option, 340
    - IPv6, 320–321
    - l, option, 339
    - s, option, 343–344
  - ippool.conf, fichier, 319–320
    - Voir* IP Filter
  - IPQoS, 411
    - Exemple de configuration, 445–447
    - Exemple de réseau, 451
    - Fichier de configuration, 451, 504
      - Clause class, 455
      - Clause filter, 457
    - Instruction action du marqueur, 458
    - Instruction action initiale, 505
    - Instruction d'action initiale, 454
    - Liste des modules IPQoS, 506
    - Syntaxe, 504
      - Syntaxe de l'instruction action, 506
  - Fonctionnalités de gestion du trafic, 415
  - Fonctions, 412
  - Fonctions de gestion du trafic, 417
  - Génération statistique, 488
  - Implémentation du modèle Diffserv, 417
  - Journalisation des messages, 479
  - Messages d'erreur, 480
  - Pages de manuel, 413
  - Planification de la configuration, 427
  - Planification de la stratégie QoS, 431
  - Prise en charge du périphérique VLAN, 499
  - RFC, 413
  - Routeurs dans un réseau IPQoS, 475
  - stratégie pour réseaux compatibles IPv6, 40
  - Topologies de réseau pris en charge, 428
  - Topologies de réseau prises en charge, 429, 430
  - Topologies de réseaux pris en charge, 429
- ipqosconf, 451
- ipqosconf, commande
  - Affichage de la configuration, 479
  - Application d'une configuration, 478, 479
  - Options, 508
- IPsec
  - Activation, 227
  - Affichage des stratégies, 235
  - Ajout d'associations de sécurité (SA), 232, 240
  - Algorithme d'authentification, 220
  - Algorithme de chiffrement, 221
  - Association de sécurité (SA, Security Association), 217–218

*IPsec (Suite)*

- Associations de sécurité (SA), 212
- Base de données des associations de sécurité (SADB), 212, 255
- Commande de stratégie
  - `ipseccconf`, 252
- Commandes, liste, 227–228
- Composants, 212
- Configuration, 252
- Contournement, 221, 234
- Création manuelle de SA, 243–245
- Définition de la stratégie
  - Temporairement, 252
- Définition de stratégie
  - Permanent, 252–254
- Domaine logique, 226
- Encapsulation de données, 219
- ESP (Encapsulating Security Payload, association de sécurité), 218–221
- `/etc/hosts`, fichier, 231
- Extension d'utilitaire
  - `snoop`, commande, 257
- Fichiers de configuration, 227–228
- Fichiers de stratégie, 252–254
- Gestion avec SMF, 246–248
- Gestion des clés, 217–218
- Implémentation, 230
- `in.iked`, démon, 218
- Index de paramètre de sécurité (SPI, Security Parameter Index), 217–218
- `ipsecalgs`, commande, 220, 254
- `ipseccconf`, commande, 221, 252
- `ipsecinit.conf`, fichier
  - Configuration, 232
  - Contournement de LAN, 240
  - Description, 252–254
  - Fichier de stratégie, 221
  - Protection du serveur Web, 234
- `ipseckey`, commande, 218, 255–256
- Mécanisme de sécurité, 212
- Mécanismes de protection, 218–221
- Mode Transport, 222–224
- Mode Tunnel, 222–224
- NAT, 225

*IPsec (Suite)*

- Paquets étiquetés, 230
- Présentation, 211
- Processus de paquet entrant, 214
- Processus de paquet sortant, 214
- Protection
  - Paquet, 211
  - Serveur Web, 233–235
  - Systèmes portables, 291–298
  - VPN, 239–242
- Protection d'un VPN, 236–242
- Protocole de sécurité, 212, 217–218
- Protocole SCTP, 226
- RBAC, 229
- Réseaux privés virtuels (VPN), 224
- RFC, 213
- Rôles de sécurité, 245–246
- `route`, commande, 242
- SCTP, protocole, 230
- Sécurisation des connexions à distance, 231
- Sécurisation du trafic, 231–233
- Services
  - `ipsecalgs`, 228
  - `manual-key`, 228
  - Stratégie, 227
- Services, liste, 227–228
- Services de SMF, 251–252
- `snoop`, commande, 257
- Source d'algorithme, 254
- SPD (Security Policy Database, base de données de stratégie de sécurité), 212, 214, 252
- Stratégie de protection, 221
- Structure cryptographique, 254
- Terminologie, 213–214
- Trusted Extensions, étiquettes, 230
- Tunnels, 224
- Utilisation de `ssh` pour la connexion à distance sécurisée, 233
- Utilitaires de génération de clés
  - IKE, 260
  - `ipseckey`, commande, 255–256
- Vérification de la protection des paquets, 248–249
- VPN (Virtual Private Network), 239–242
- VPN IPv4, 239–242

**IPsec (Suite)**

- Zone, 226, 229
- `ipsecalgs`, service, Description, 251
- `ipseccconf`, commande
  - Affichage de la stratégie IPsec, 235, 252–254
  - Affichage de stratégie IPsec, 233–235
  - Configuration de la stratégie IPsec, 252
  - Configuration de tunnels, 222
  - Description, 227
  - Objectif, 221
  - Questions de sécurité, 253–254
- `ipseccinit.conf`, fichier
  - Contournement de LAN, 240
  - Description, 227
  - Emplacement et étendue, 226
  - Exemple, 253
  - Objectif, 221
  - Protection du serveur Web, 234
  - Questions de sécurité, 253–254
  - Vérification de la syntaxe, 232
  - Vérification de syntaxe, 241
- `ipseckey`, commande
  - Description, 227, 255–256
  - Fonction, 218
  - Questions de sécurité, 256
- `ipseckeykeys`, fichier
  - Stockage de clés IPsec, 228
  - Vérification de syntaxe, 244
- IPv6
  - Activation, sur un serveur, 88–89
  - Adresse, configuration automatique, 164
  - Adresse lien-local, 166, 169
  - Adresse multicast, 169
  - Adresse temporaire, configuration, 83–86
  - Ajout
    - Prise en charge DNS, 89
  - ATM, prise en charge, 172
  - Comparaison avec IPv4, 168–170
  - Configuration automatique d'adresse sans état, 165
  - Configuration automatique d'adresses sans état, 166
  - Configuration d'adresse automatique, 160
  - Contrôle du trafic, 110
  - Découverte de routeur, 160
  - Dépannage de problèmes IPv6 courants, 140–142

**IPv6 (Suite)**

- Détection d'inaccessibilité de voisin, 169
- Détection de routeur, 168
- Enregistrement DNS AAAA, 90
- `in.ndpd`, démon, 160
- `in.ripngd`, démon, 161
- IP Filter, 320–321
- ND, protocole de détection des voisins, 163–170
- `nslookup`, commande, 91
- Plan d'adressage, 37–38
- Préparation de prise en charge DNS, 40–41
- Présentation du protocole, 164
- Publication de routeur, 164, 165, 168, 171
- Redirection, 164, 169
- Routage, 170
- Sécurité, 42
- Sollicitation de routeur, 164, 165
- Sollicitation de voisin, 164
- Sollicitation de voisin et inaccessibilité, 166
- Tableau de stratégie de sélection d'adresse par défaut, 156
- Vérification du statut de `in.ndpd`, 140

**K**

- `-kc`, option
  - `ikecert certlocal`, commande, 280, 305
- `-ks`, option
  - `ikecert certlocal`, commande, 275, 305
- `kstat`, commande, utilisation avec IPQoS, 488

**L**

- `-L`, option, `ipseccconf`, commande, 235
- `-l`, option
  - `ikecert certdb`, commande, 276
  - `ipseccconf`, commande, 235
- `ldap-list`, mot-clé, Fichier de configuration IKE, 290
- Liaisons de données, Configuration d'une interface IP sur une liaison, 48
- Liste
  - Algorithmes (IPsec), 220
  - Certificats (IPsec), 276, 289

Liste (*Suite*)

- CRL (IPsec), 289
- ID de jeton (IPsec), 299
- ID de jetons de metaslot, 299
- Matériel (IPsec), 299
- Liste des certificats révoqués, *Voir* CRL
- Liste des tâches
  - Configuration du protocole IKE (liste des tâches), 267
  - Configuration du protocole IKE avec des certificats de clés publiques (liste des tâches), 273
  - Configuration du protocole IKE avec des clés prépartagées (liste des tâches), 268
  - Configuration du protocole IKE pour les systèmes portables (liste des tâches), 291
- IPQoS
  - Configuration de la comptabilisation des flux, 485
  - Création d'un fichier de configuration, 449
  - Planification de la configuration, 427
  - Planification de stratégies QoS, 432
- IPv6
  - Planification, 33–34
  - Protection du trafic à l'aide d'IPsec (liste des tâches), 230
  - Tâche d'administration réseau, 94
- Logements, Matériel, 307
- LRC, ike/cr1s, base de données, 307

**M**

- m, option, ikecert certlocal, commande, 275
- Machine, Protection des communications, 231–233
- manual -key, service
  - Description, 218, 251
  - Utilisation, 245
- Marque de classe de service (CoS), 419
- Matériel
  - Accélération des calculs IKE, 298
  - Recherche de matériel connecté, 298
  - Stockage de clés IKE, 298–299
- Matériel pour les réseaux IPQoS, 428
- Mécanismes de protection, IPsec, 218–221
- Messages, Publication de routeur, 171

- Messages d'erreur pour IPQoS, 480
- Metaslot, Stockage de clés, 299
- Mode d'économie d'espace, Option du démon
  - in.routed, 148
- Mode Transport
  - Données protégées avec ESP, 223
  - IPsec, 222–224
  - Protection de données avec AH, 223
- Mode Tunnel
  - IPsec, 222–224
  - Protection de l'intégralité du paquet IP interne, 223
- Modèle administratif, 189
- Modèle Diffserv
  - Exemple de suivre, 420
  - Implémentation IPQoS, 417, 418, 419, 420
  - Module de classification, 417
  - Modules de marquage, 419
  - Modules de mesure, 418
- Modification d'adresse lien-local, 168
- Module de classification, 417
  - Fonction du classificateur, 492
- Module du classificateur, action (instruction), 454
- Modules de marquage, 419
  - Voir aussi* dlcosmk, marqueur
  - Voir aussi* dscpmk, marqueur
  - PHB en vue de la transmission des marqueurs IP, 422
  - Prise en charge des périphériques VLAN, 499
  - Spécification d'un point de code DS, 499
- Modules de mesure
  - Voir aussi* tokenmt, compteur
  - Voir aussi* tswtclmt, compteur
  - Appel dans le fichier de configuration IPQoS, 472
  - Introduction, 418
  - Résultats de la mesure, 419, 494
- MTU (maximum transmission unit, unité de transmission maximale ), 168

**N**

- name-service/switch, service SMF, 145
- NAT
  - Affichage des statistiques, 343
  - Configuration des règles, 317–319

NAT (*Suite*)

- Désactivation, 328
- IPsec et IKE, 294–295, 296–297
- Limitations d'IPsec, 225
- Présentation, 317–319
- Règles NAT
  - Affichage, 337
  - Ajout, 338
  - Suppression des règles NAT, 337–338
- ND, protocole de détection de voisin
  - Algorithme de détection d'adresse dupliquée, 167
  - Détection de routeur, 165
  - Sollicitation de voisin, 166
- ND, protocole de détection des voisins
  - Adresse, configuration automatique, 164
  - Comparaison ARP, 168–170
  - Détection de préfixe, 165
  - Fonctionnalités principales, 163–170
- `ndpd.conf`, fichier
  - Configuration d'adresse temporaire, 84
  - Création sur un routeur IPv6, 81
- `ndpd.conf`, fichier
  - Liste de mots-clés, 152–155
- `ndpd.conf`, fichier
  - Publication 6to4, 132
- `ndpd.conf`, fichier
  - Variables de configuration d'interface, 152
  - Variables de configuration de préfixes, 154
- netmasks, base de données, Ajout de sous-réseaux, 54
- netstat, commande
  - a, option, 98
  - Affichage des statistiques par protocole, 95
  - Affichage du statut des routes connues, 100–101
  - Description, 95
  - Extension IPv6, 158
  - f, option, 98
  - inet, option, 98
  - inet6, option, 98
  - r, option, 100–101
  - Syntaxe, 95
  - Vérification logicielle, 140
- /network/dhcp/relay, services SMF, Description, 208
- /network/dhcp-server, service SMF, Description, 208

- /network/dhcp/server, services SMF,
  - Description, 208
- /network/dns/client, service SMF, Utilisation par DHCP, 208
- Network Management, profil de droits, 245
- NIS, Sélection d'un service de noms, 31
- nis/tdomain, service SMF, Configuration de mode de fichiers locaux, 53
- Nom d'hôte, Activation d'une requête client, 200–201
- Nom de keystore, *Voir* ID de jeton
- Nom de répertoire (DN), Accès aux CRL, 289
- Noms/attribution de noms
  - Nom de noeud
    - Hôte local, 54
- Noms de domaine
  - nis/domain, service SMF, 55
  - Sélection, 31
- Noms de domaines, nis/domain, service SMF, 53
- Notation CIDR, 27
- Nouvelle fonctionnalité
  - Configuration manuelle d'une adresse
    - lien-local, 86–88
  - Sélection des adresses par défaut, 114–116
- Nouvelles caractéristiques, DHCP sur les interfaces logiques, 199–200
- Nouvelles fonctionnalités
  - Adresses temporaires dans IPv6, 83–86
  - inetconv, commande, 56
  - routeadm, commande, 80
- Nouvelles fonctions
  - Scripts d'événement DHCP, 203–204
  - SCTP, protocole, 71–74
  - SMF (Service Management Facility), 56
- nslookup, commande, 172
  - IPv6, 91
- Numéros de réseau de classe A, B ou C, 27

**O**

- omshell, commande, Description, 206
- /opt/SUNWconn/lib/libpkcs11.so, entrée,
  - ike/config, fichier, 304

**P****Paquet**

- Abandon ou perte, 102
- Affichage du contenu, 108
- Protection
  - Avec IPsec, 214
  - IPsec, 218–221
  - Paquet sortant, 214
- Vérification de la protection, 248–249
- Vérification du flux, 107

**Paquet consigné, Enregistrement dans un fichier, 347–348****Paquets**

- Observation sur la couche IP, 110–114
- Protection
  - A l'aide d'IKE, 260
- Paquets entrants, 214

**params, clause**

- actionflowacct, 461
- Définition de statistiques générales, 455
- Définition des statistiques globales, 508
- Pour une action du marqueur, 459
- Syntaxe, 508

**Passerelle, dans une topologie de réseau, 59****Périphériques LAN (VLAN) virtuels sur un réseau IPQoS, 499****Perte ou abandon de paquet, 102****PF\_KEY, interface socket, IPsec, 227****PFS, Voir Confidentialité de transmission parfaite (PFS)****PHB, 422**

- Traitement EF, 423
- Transmission AF, 423
- Utilisation avec le marqueur dscpmk, 497

**ping, commande, 103**

- Description, 102
- Exécution, 103
- Extension pour IPv6, 159
- s, option, 102
- Syntaxe, 102

**pkcs11\_path, mot-clé**

- Description, 304
- Utilisation, 285

**Planification de réseau, Enregistrement d'un réseau, 29****Planification du réseau, Décisions de conception, 25****Planification réseau, Schéma d'adressage IP, 27****pnatadm, commande, Description, 206****Point de code DS (DSCP), 419**

- Planification dans la stratégie QoS, 442

**policy, service**

- Description, 251
- Utilisation, 232, 241

**Pool d'adresses**

- Affichage, 339
- Affichage des statistiques, 343–344
- Ajout, 340
- Suppression, 339–340

**Pools d'adresses**

- Configuration, 319–320
- Présentation, 319–320

**PPP, liaison**

- Dépannage
- Flux de paquets, 107

**Préfixe**

- Publication de routeur, 165, 168, 171

**Préfixe de site, IPv6**

- Procédure d'obtention, 37
- Publication sur le routeur, 81

**Prépartage, clés (IKE)**

- Affichage des algorithmes et groupes de la phase 1, 265–267
- Description, 262

**Profil de droits Network IPsec Management, 245****Profils de droits**

- Network IPsec Management, 245
- Network Management, 245

**Profils de droits de sécurité réseau, 245–246****Protection**

- Paquet entre deux systèmes, 231–233
- Serveur Web, à l'aide d'IPsec, 233–235
- Systèmes portables avec IPsec, 291–298
- Trafic IPsec, 211
- VPN avec un tunnel IPsec en mode Tunnel, 239–242

**Protection du trafic à l'aide d'IPsec (liste des tâches), 230****Protocole BOOTP, DHCP, 175****Protocole de routage**

- Démon de routage associé, 148–149



**Protocole de routage (*Suite*)**

Description, 147, 148

**RDISC**

Description, 148

**RIP**

Description, 147

**Protocole de sécurité**

AH (Authentication Header, en-tête d'authentification), 218

ESP (Encapsulating Security Payload, association de sécurité), 219–220

Présentation, 212

Sécurité, 219

**Protocole DHCP**

Avantages de l'implémentation d'Oracle Solaris, 176

Présentation, 175

Séquence des événements, 177

**Protocole ICMP, Messages, pour le protocole ND, 164****Protocole IP, Vérification de la connectivité de l'hôte, 103****Protocole SCTP, Restrictions avec IPsec, 226****Protocoles de sécurité, Mécanismes de protection IPsec, 218**

proxy, mot-clé, Fichier de configuration IKE, 290

Publication 6to4, 132

**Publication de routeur**

IPv6, 164, 165, 168, 170–171

Préfixe, 165

Publications du routeur, 193

publickeys, base de données, 307

**Q**

-q, option, in.routed, démon, 148

**Qualité de service (QoS)**

Stratégie QoS, 414

Tâches, 411

**Questions de sécurité**

ipseccnf, commande, 253–254

ipseccinit.conf, fichier, 253–254

ipseckey, commande, 256

Sockets verrouillés, 253

**R**

RARP, protocole, Vérification des adresses

Ethernet, 140

RBAC, IPsec, 229

RDISC, Description, 148

RDISC (ICMP Router Discovery), protocole, 148

**Redirection**

IPv6, 164, 169

Régulation de la bande passante, 415

Planification de la stratégie QoS, 435

Remarques de sécurité, clé prépartagée, 262

Remplacement, Clés prépartagées (IKE), 270–271

**Répertoire**

Certificat (IKE), 306

Clé prépartagée (IKE), 304

Clé publique (IKE), 306

/etc/inet/ike, 263

/etc/inet/publickeys, 306

/etc/inet/secret, 263

/etc/inet/secret/ike.privatekeys, 305

Répertoires, /etc/inet, 263

**Réseau TCP/IP****Configuration**

Service TCP/IP standard, 70

**Dépannage, 110**

Affichage du contenu des paquets, 108

netstat, commande, 95

Perte de paquet, 102

ping, commande, 102

Protection à l'aide d'ESP, 219

Réseaux IPv4, Fichiers de configuration, 143

**Réseaux privés virtuels (VPN)**

Configuration routeadm, commande, 239

Création avec IPsec, 224

**Réseaux TCP/IP****Configuration**

name-service/switch, service SME, 145

**Dépannage**

Méthodes générales, 139

Perte de paquets, 103

ping, commande, 103

Programmes de diagnostic tiers, 139

RFC, IPQoS, 413

RIP (Routing Information Protocol), Description, 147



Rôle de configuration, Sécurité réseau à l'aide d'un rôle, 245–246

Rôles, Création d'un rôle pour la sécurité réseau, 245–246

## Routage

- Configuration statique, 65
- Hôtes à interface unique, 65
- IPv6, 170
- Passerelle, 59
- Routage dynamique, 59
- Routage statique, 59

Routage dynamique, Utilisation privilégiée, 60

## Routage statique

- Ajout d'une route statique, 61–62
- Configuration manuelle sur un hôte, 65
- Exemple de configuration, 61–62
- Utilisation privilégiée, 60

## route, commande

- IPsec, 242
- Option inet6, 159

## routeadm, commande

- Configuration de routeur IPv6, 80
- Transmission IP, 239

## Routeur

- Configuration, 147
- Configuration du mode Fichiers locaux, 53
- Définition, 147
- Problème de mise à niveau vers IPv6, 141
- Protocole de routage
  - Description, 147, 148
- Rôle, topologie 6to4, 120

## Routeur de bordure, 46

## Routeur de bordure, site 6to4, 121

## Routeur de transfert de paquet, 47

## Routeur Diffserv

- Evaluation de points de code DS, 498
- Planification, 433

## Routeur par défaut, Définition, 47

## Routeur relais, configuration d'un tunnel 6to4, 133

## Routeur relais, configuration de tunnel 6to4, 134

## Routeur relais 6to4

- Problèmes de sécurité, 142
- Topologie du tunnel, 123

## Routeurs

- Configuration
  - IPv6, 80
- Définition, 57
- Routeur de transfert de paquet, 47

## S

- S, option
  - ikecert certlocal, commande, 275
  - in.routed, démon, 148

- s, option, ping, commande, 103

## Saut suivant, 169

## SCTP, protocole

- Affichage des statistiques, 95
- Affichage du statut, 97
- Ajout de services SCTP, 71–74
- IPsec, 230

## Sécurité

- AH (Authentication Header, en-tête d'authentification), 219
- ESP (Encapsulating Security Payload, association de sécurité), 219
- IKE, 302
  - ike/config, fichier, 302
- IPsec, 211
  - ipseckey, fichier, 244
- Protocole de sécurité, 219
- Réseau compatible IPv6, 42

## Sécurité du réseau, Configuration, 209

## Sélecteurs, 418

- Liste de sélecteurs, 492
- Planification de la stratégie QoS, 436
- Uplet à 5 attributs IPQoS, 417

## Sélection d'adresse par défaut, 156–157

## Sélection des adresses par défaut

- Définition, 114–116
- Table des règles de sélection des adresses
  - IPv6, 114–116

## Serveur, DHCPv6, 188

## Serveur, IPv6, Activation d'IPv6, 88–89

## Serveur d'application, configuration pour IPQoS, 465

## Serveur Web, Protection à l'aide d'IPsec, 233–235

## Serveurs de configuration réseau, Configuration, 55

- Serveurs IPv6, Planification de tâches, 37
- Serveurs Web
  - Configuration IPQoS, 462
  - Configuration pour IPQoS, 452, 453, 464
- Service Base de données, Mise à jour, pour SCTP, 72
- Service de noms, fichiers locaux, /etc/inet/hosts, fichier, 231
- Services de noms
  - Bases de données, 147
  - Sélection d'un service, 31
  - Spécification d'ordre de recherche de base de données, 145
- Services différenciés, 411
  - Différentes classes de service, 416
  - Modèle de services différenciés, 417
  - Topologies de réseau, 428
- Services SMF, Utilisation par DHCP, 208
- Signature numérique, RSA, 306
- Signatures numériques, DSA, 305
- SMF (Service Management Facility)
  - Service IKE
    - Activation, 232, 294, 302
    - Actualisation, 245
    - Description, 301–302
    - ike, service, 218, 263
    - Propriétés configurables, 301
    - Redémarrage, 232
  - Service IPsec
    - manual-key, description, 218
- Services IPsec, 251–252
  - ipsecalgs, service, 254
  - Liste, 227–228
  - manual-key, service, 255
  - manual-key, utilisation, 245
  - policy, service, 227
  - Utilisation pour la gestion d'IKE, 246–248
  - Utilisation pour la gestion d'IPsec, 246–248
- snoop, commande
  - Affichage des paquets protégés, 257
  - Affichage du contenu des paquets, 108
  - Contrôle du trafic IPv6, 110
  - DHCP, 206
  - Extension pour IPv6, 159
  - Mot-clé de protocole ip6, 159
  - snoop, commande (*Suite*)
    - Vérification de la protection des paquets, 248–249
    - Vérification de paquets sur la couche IP, 110–114
    - Vérification des paquets transmis entre un serveur et un client, 109–110
    - Vérification du flux de paquets, 107
- Socket, Affichage du statut des sockets à l'aide de netstat, 98
- Sockets, Sécurité IPsec, 253
- Sollicitation de routeur
  - IPv6, 164, 165
- Sollicitation de voisin, IPv6, 164
- Sous-réseau
  - IPv6
    - Suggestion de numérotation, 38–39
- Sous-réseaux, 32
  - Ajout à un réseau IPv4, 68–70
  - IPv4
    - Configuration de masque de réseau, 54
  - IPv6
    - Topologie 6to4, 121
- SPD (Security Policy Database, base de données de stratégie de sécurité)
  - Configuration, 252
  - IPsec, 212, 214
- Statistiques
  - Par protocole (netstat), 95
  - Transmission de paquet (ping), 102
  - Transmission de paquets (ping), 103
- Statistiques d'état, Affichage, 342–343
- Statistiques pour IPQoS
  - Activation des statistiques générales, 455
  - Activation des statistiques globales, 507
  - Activation des statistiques relatives aux classes, 507
  - Génération, via la commande kstat, 488
- Stockage
  - Clé IKE sur disque, 307
  - Clés IKE sur disque, 281, 306
  - Clés IKE sur du matériel, 298–299
- Stockage de clés
  - Fichier keystore de clés softtoken, 299
  - ID de jetons de metaslot, 299
  - SA IPsec, 228

- Stockage des clés
    - SA ISAKMP, 304
    - Softtoken, 304
  - Stratégie, IPsec, 221
  - Stratégie de protection, IPsec, 221
  - Stratégie de sécurité
    - ike/config, fichier (IKE), 228
    - ipsecinit.conf, fichier (IPsec), 252–254
  - Stratégie IPsec, Exemple de syntaxe de tunnel, 236–237
  - Stratégie oS, Création de filtre, 436
  - Stratégie QoS, 415
    - Implémentation, dans le fichier de configuration IPQoS, 449
    - Liste des tâches de planification, 432
    - Modèle d'organisation de la stratégie, 431
  - Structure cryptographique, IPsec, 254
  - Suite de protocoles TCP/IP, Service standard, 70
  - Sun Crypto Accelerator 6000, carte, Utilisation avec IKE, 298–299
  - syslog.conf (journalisation pour IPQoS), 479
  - /system/name-service/switch, service SMF,
    - Utilisation par DHCP, 208
  - Système, Protection des communications, 231–233
  - Systèmes multiréseau, Définition, 47
- T**
- T, option
    - ikecert, commande, 285, 306
    - ikecert certlocal, commande, 275
  - t, option
    - ikecert, commande, 305
    - ikecert certlocal, commande, 275
  - t (option), inetd (démon), 70
  - Table d'état, Affichage, 341–342
  - Table de réseau DHCP, Description, 207
  - Table de routage, 59
    - in.routed, création, 147
    - Mode d'économie d'espace, 148
    - Suivi de toutes les routes, 107
  - Tables de routage
    - Affichage, 139
    - Configuration manuelle, 61
  - TCP, protocole, Affichage des statistiques, 95
  - TCP, wrapper, 74
  - TCP/IP, réseau
    - Dépannage
      - Méthode générale, 139
      - Vérification logicielle, 139
  - TCP/IP, suite de protocoles, Affichage des statistiques, 95
  - /tftpboot, création de répertoire, 55
  - tokenmt, compteur, 419
    - Compteur à débit double, 495
    - Compteur à débit simple, 495
    - Configuration des couleurs, 419, 495
    - Paramètres de débit, 495
  - tokenmt, mesure, Débits de mesure, 494
  - tokens, argument, ikecert, commande, 305
  - Topologie réseau, Système autonome, 45
  - Topologies de réseau pour IPQoS, 428
    - Réseau local avec batteries de serveurs compatibles IPQoS, 429
    - Réseau local avec hôtes IPQoS, 429
    - Réseau local avec le pare-feu IPQoS, 430
  - Topologies des réseaux pour IPQoS, Exemple de configuration, 445
  - traceroute, commande
    - Définition, 106–107
    - Extension pour IPv6, 159
    - Suivi des routes, 106–107
  - Transfert du trafic
    - Effet des PHB sur la transmission du paquet, 497
    - Flux du trafic par les réseaux Diffserv, 423
    - Transmission du datagramme, 499
    - Transmission du paquet IP avec DSCP, 422
  - Transfert IP, VPN (Virtual Private Network, réseau virtuel privé), 224
  - Translation d'adresse réseau, Voir NAT
  - Transmission du trafic, Planification de la stratégie QoS, 435
  - Transmission IP, VPN IPv4, 239
  - Trusted Extensions, IPsec, 230
  - tswtclmt, compteur, 419, 496
    - Mesure des débits, 496
  - Tunnel
    - , mode dans IPsec, 222–224

Tunnel (*Suite*)

- Configuration IPv6
  - Routeur relais 6to4, 133
- Mode Transport, 222
- Planification, pour IPv6, 41
- tunnel, mot-clé
  - Stratégie IPsec, 222, 237, 240
- Tunnel 6to4, Routeur relais 6to4, 133
- Tunnels, 117–138
  - Adresse de destination du tunnel
    - Voir* Tunnels, *tdst*
  - Adresse source du tunnel
    - Voir* Tunnels, *tsrc*
  - Adresses locales et distantes, 135
  - Affichage des informations de tunnel, 136–137
  - Configuration d'IPv4 sur des tunnels IPv4, 130
  - Configuration d'IPv6 sur des tunnels IPv4, 130
  - Configuration d'IPv6 sur des tunnels IPv6, 130
  - Configuration de tunnels 6to4, 132
  - Configuration d'*ladm*, commandes, 126–138
  - Création et configuration de tunnels, 127–131
  - Déploiement, 124–125
  - dladm*, commandes
    - create-iptun*, 127–131
    - delete-iptun*, 138
    - modify-iptun*, 135–136
    - show-iptun*, 136–137
  - Sous-commandes de configuration des tunnels, 126
- encaplimit, 128
- Encapsulation de paquet, 118
- Exigences en matière de création, 124–125
- hoplimit, 128
- Interfaces IP requises, 125
- IPsec, 224
- IPv4, 118–119
- IPv6, 118–119
- Mécanismes de mise en tunnels IPv6, 118
- Mode Tunnel, 222
- Modification de configuration de tunnel, 135–136
- Protection de paquets, 224
- Suppression de tunnels IP, 138
- Topologie, vers le routeur relais 6to4, 123
- Tunnels 6to4, 119

Tunnels, Tunnels 6to4 (*Suite*)

- Flux de paquets, 121, 123
- Topologie, 120
- Types, 118
  - 6to4, 118
  - IPv4, 118
  - IPv4 sur IPv4, 118
  - IPv4 sur IPv6, 118
  - IPv6, 118
  - IPv6 sur IPv4, 118
  - IPv6 sur IPv6, 118
- VPN
  - Voir* VPN (réseaux privés virtuels, virtual private networks)
- Tunnels 6to4
  - Voir aussi* Tunnels, types
  - Exemple de topologie, 120
  - Flux de paquets, 121, 123
- Tunnels IP, *Voir* Tunnels
- Tunnels IPv4, *Voir* Tunnels, types
- Tunnels IPv6, *Voir* Tunnels, types

## U

- UDP, protocole, Affichage des statistiques, 95
- use\_http*, mot-clé, Fichier de configuration IKE, 290
- /usr/lib/inet/dhcpd*, démon, Description, 205
- /usr/lib/inet/dhcrelay*, commande,
  - Description, 205
- /usr/lib/inet/in.dhcpd*, démon, Description, 205
- /usr/sadm/admin/bin/dhcppmgr*, commande,
  - Description, 206
- /usr/sbin/6to4relay*, commande, 133
- /usr/sbin/dhcpagent*, commande, Description, 206
- /usr/sbin/dhcpconfig*, commande, Description, 206
- /usr/sbin/dhcpinfo*, commande, Description, 206
- /usr/sbin/dhtadm*, commande, Description, 206
- /usr/sbin/in.rdisc*, programme, Description, 148
- /usr/sbin/in.routed*, démon, Mode d'économie d'espace, 148
- /usr/sbin/in.routed* Démon, Description, 147
- /usr/sbin/inetd*, démon, Vérification du statut de *inetd*, 140
- /usr/sbin/inetd* (démon), Service démarré, 70

---

/usr/sbin/ipdam, commande, DHCP, 206  
 /usr/sbin/omshell, commande, Description, 206  
 /usr/sbin/ping, commande, 103  
     Description, 102  
     Exécution, 103  
     Syntaxe, 102  
 /usr/sbin/pntadm, commande, Description, 206  
 /usr/sbin/snoop, commande, DHCP, 206  
 Utilitaire de génération de clés  
     ipseckey, commande, 218  
     manual-key, service, 218  
 Utilitaire de génération des clés, ike, service, 218  
 Utilitaires de gestion de clés, Protocole IKE, 259  
 Utilitaires de ligne de commande DHCP,  
     Privilèges, 183

## V

-V, option, snoop, commande, 257  
 Valeur de priorité utilisateur, 419  
 /var/inet/ndpd\_state.interface, fichier, 160  
 Vérification  
     ipseccinit.conf, fichier  
         Syntaxe, 232, 241  
     ipseckey, fichier  
         Syntaxe, 244  
     Protection des paquets, 248–249  
 Vidage, *Voir* Suppression  
 VPN, *Voir* Réseau privé virtuel (VPN)  
 VPN (Virtual Private Network)  
     IPv4, exemple, 239–242  
     Protection à l'aide d'IPsec, 239–242

## W

Wrapper TCP, activation, 74

## Z

Zone  
     Gestion des clés, 229

