Guide d'administration système : Services réseau

Référence : E22298
Août 2011

ORACLE

111013@25097

Table des matières

Liste des figures

Liste des tableaux

Liste des exemples

Préface

Guide d'administration système : Services réseau fait partie d'un jeu de plusieurs volumes couvrant une partie importante des informations d'administration du système d'exploitation Oracle Solaris. Ce manuel suppose que vous avez déjà installé le système d'exploitation Oracle Solaris 10 et configuré le logiciel réseau que vous envisagez d'utiliser.

Remarque – Cette version d'Oracle Solaris prend en charge les systèmes utilisant les architectures de processeur SPARC et x86. Les systèmes pris en charge sont répertoriés dans les listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*. Ce document présente les différences d'implémentation en fonction des divers types de plates-formes.

Dans ce document, les termes relatifs à x86 ont la signification suivante :

- x86 désigne la famille des produits compatibles x86 64 bits et 32 bits.
- x64 concerne spécifiquement les UC compatibles x86 64 bits.
- "x86 32 bits" désigne des informations 32 bits spécifiques relatives aux systèmes x86.

Pour connaître les systèmes pris en charge, reportez-vous aux listes de la page *Oracle Solaris OS: Hardware Compatibility Lists*.

Utilisateurs de ce manuel

Ce manuel s'adresse à ceux qui ont la charge d'administrer un ou plusieurs systèmes fonctionnant sous Solaris 10. Pour utiliser ce manuel, vous devez posséder d'un à deux ans d'expérience en administration de systèmes UNIX. Une formation en administration de systèmes UNIX peut se révéler utile.

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
Guide d'administration système : administration de base	Comptes utilisateur et groupes, prise en charge serveur et client, arrêt et démarrage d'un système, gestion des services et des logiciels (packages et patchs)
Guide d'administration système : Administration avancée	Terminaux et modems, ressources système (quotas d'utilisation de disque, comptabilisation et crontabs), processus système et dépannage du logiciel Oracle Solaris
System Administration Guide: Devices and File Systems	Médias amovibles, disques et périphériques, systèmes de fichiers, et sauvegarde et restauration des données
Guide d'administration système : services IP	Administration de réseau TCP/IP, administration d'adresses IPv4 et IPv6, DHCP, IPsec, IKE, filtre IP Solaris, IP mobile, multiacheminement sur réseau IP (IPMP) et IPQoS
Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)	Services d'annuaire et d'attribution de noms DNS, NIS et LDAP, et transition de NIS à LDAP et de NIS+ à LDAP
System Administration Guide: Naming and Directory Services (NIS+)	Services d'annuaire et d'attribution de noms NIS+
Guide d'administration système : Services réseau	Serveurs cache Web, services à facteur temps, systèmes de fichiers de réseau (NFS et Autofs), mail, SLP et PPP
System Administration Guide: Printing	Tâches et sections concernant l'impression, l'utilisation des services, les outils, protocoles et technologies permettant de configurer et de gérer les imprimantes et services d'impression
System Administration Guide: Security Services	Audit, gestion de périphérique, sécurité des fichiers, BART, services Kerberos, PAM, structure cryptographique Solaris, privilèges, RBAC, SASL et shell sécurisé Solaris
Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris	Gestion des ressources pour les projets et les tâches, comptabilisation étendue, contrôles de ressources, ordonnanceur FSS, contrôle de la mémoire physique à l'aide du démon d'allocation restrictive des ressources (rcapd) et pools de ressources ; virtualisation au moyen de la technologie de partitionnement du logiciel Solaris Zones et des zones marquées `lx`

Titre du manuel	Sujets
Guide d'administration Oracle Solaris ZFS	Création et gestion d'un système de fichiers et d'un pool de stockage ZFS, snapshots, clones, sauvegardes, utilisation de listes de contrôle d'accès (ACL) pour protéger les fichiers ZFS, utilisation de ZFS sur un système Oracle Solaris avec des zones installées, volumes émulés et dépannage et récupération de données
Procédures de l'administrateur Oracle Solaris Trusted Extensions	Administration système spécifique aux fonctionnalités d'extension sécurisée d'Oracle Solaris
Guide de configuration d'Oracle Solaris Trusted Extensions	À partir de la version Solaris 10 5/08, ce guide décrit la planification, l'activation et la configuration initiale de la fonction d'extension sécurisée d'Oracle Solaris.

Documentation connexe

Voici la liste de la documentation connexe à laquelle il est fait référence dans ce manuel.

- *Guide d'administration système : Administration avancée*
- *Guide d'administration système : administration de base*
- *Guide d'administration système : services IP*
- *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*
- *System Administration Guide: Naming and Directory Services (NIS+)*
- *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris*
- *System Administration Guide: Security Services*
- Anderson, Bart, Bryan Costales et Harry Henderson. *UNIX Communications*. Howard W. Sams & Company, 1987.
- Costales, Bryan. *sendmail, Third Edition*. O'Reilly & Associates, Inc., 2002.
- Frey, Donnalyn et Rick Adams. *!%@:: A Directory of Electronic Mail Addressing and Networks*. O'Reilly & Associates, Inc., 1993.
- Krol, Ed. *The Whole Internet User's Guide and Catalog*. O' Reilly & Associates, Inc., 1993.
- O'Reilly, Tim et Grace Todino. *Managing UUCP and Usenet* . O' Reilly & Associates, Inc., 1992.

Informations connexes

Pour plus d'informations sur les conditions d'octroi de licence PPPoE, reportez-vous aux documents disponibles dans les emplacements suivants :

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

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

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

Accès au support technique Oracle

Les clients Oracle ont accès au support électronique via My Oracle Support. Pour plus d'informations, rendez-vous sur le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou sur le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

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 `.login`. Utilisez `ls -a` pour afficher la liste de tous les fichiers. `nom_machine% Vous avez reçu du courrier.`
`AaBbCc123`	Ce que vous entrez, par opposition à ce qui s'affiche à l'écran.	`nom_machine%` **`su`** `Mot de passe :`
aabbcc123	Paramètre fictif : à remplacer par un nom ou une valeur réel(le).	La commande permettant de supprimer un fichier est `rm` *nom_fichier*.

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 *Guide de l'utilisateur*. Un *cache* est une copie des éléments stockés localement. *N'enregistrez pas* le fichier. **Remarque :** 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

Sujets relatifs aux services réseau

Cette section fournit un aperçu du manuel, ainsi que des informations de présentation, de tâche et de référence pour les services NCA et NTP.

◆ ◆ ◆ CHAPITRE 1

Service réseau (présentation)

Ce chapitre dresse la liste des principaux thèmes abordés dans ce manuel. En outre, il comporte une description du service PERL inclus dans cette version.

Rubriques d'Oracle Solaris version 10 mise à jour 10

Le présent manuel couvre les services et utilitaires suivants :

"Perl 5" à la page 46
: L'outil Perl (Practical Extraction and Report Language, extraction pratique et langage de rapport) permet de générer des scripts simplifiant les tâches de gestion de système.

Chapitre 2, "Gestion des serveurs cache Web"
: NCA permet d'améliorer les performances du serveur Web en mettant en mémoire cache les pages Web.

Chapitre 3, "Services d'horodatage"
: NTP et les utilitaires liés au temps peuvent être utilisés dans le cadre de la synchronisation temporelle de nombreux systèmes.

Chapitre 4, "Gestion des systèmes de fichiers NFS (présentation)"
: Le protocole NFS offre la possibilité d'accéder aux systèmes de fichiers à partir d'un hôte distant.

Chapitre 7, "SLP (présentation)"
: SLP est un protocole de découverte de service dynamique.

Chapitre 12, "Services de messagerie (présentation)"
: Les services de messagerie permettent l'acheminement d'un message à une ou plusieurs personnes par tous les réseaux nécessaires.

Chapitre 15, “Solaris PPP 4.0 (Présentation) ”
Le protocole PPP assure des liaisons point à point entre hôtes distants.

Chapitre 24, “UUCP (présentation)”
UUCP permet aux hôtes d'échanger des fichiers.

Chapitre 27, “Utilisation de systèmes distants (présentation)”
Ces commandes permettent d'accéder à des fichiers sur les systèmes distants. Il s'agit de `ftp`, `rlogin` et `rcp`.

Perl 5

Cette version de Solaris inclut Perl (Practical Extraction and Report Language) 5.8.4, un puissant langage de programmation à usage général, disponible sous forme de logiciel libre. Perl est devenu l'outil de développement standard pour les tâches complexes de gestion de système en raison de ses excellentes fonctionnalités de manipulation de texte, de fichier et de processus.

Perl 5 inclut une structure modulaire chargeable dynamiquement, qui permet d'ajouter de nouvelles capacités destinées à des tâches spécifiques. De nombreux modules sont disponibles gratuitement sur le site Web CPAN (Comprehensive Perl Archive Network), http://www.cpan.org. Si vous souhaitez créer et installer des modules complémentaires à partir du site CPAN à l'aide de `gcc`, utilisez le script `/usr/perl5/5.8.4/bin/perlgcc`. Pour plus d'informations, reportez-vous à la page de manuel `perlgcc`(1).

Accès à la documentation Perl

Plusieurs sources d'informations sur Perl sont incluses dans cette version de Solaris. Ces mêmes informations sont disponibles à l'aide des deux méthodes suivantes.

Vous pouvez accéder aux pages de manuel en ajoutant `/usr/perl5/man` à la variable d'environnement MANPATH. Cet exemple affiche la présentation Perl.

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

Vous pouvez accéder à la documentation supplémentaire à l'aide de l'utilitaire `perldoc`. Cet exemple affiche les mêmes informations de présentation.

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

La page de présentation `perl` répertorie toute la documentation incluse dans la version.

Problèmes de compatibilité avec Perl

En général, la version 5.8.4 de Perl est compatible avec la version précédente. Les scripts ne doivent pas nécessairement être recréés ou recompilés pour fonctionner. Cependant, tous les modules basés sur XSUB (.xs) doivent être recompilés et réinstallés.

Modifications apportées à la version Solaris de Perl

La version Solaris de Perl a été compilée pour inclure la prise en charge des fichiers volumineux, des entiers 64 bits et de l'allocation de mémoire. En outre, les correctifs appropriés ont été appliqués. Pour obtenir la liste complète des informations de configuration, passez en revue les résultats de cette commande.

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

Vous pouvez générer une liste plus courte à l'aide de `perl -V`.

◆ ◆ ◆ CHAPITRE 2

Gestion des serveurs cache Web

Ce chapitre présente Solaris Network Cache and Accelerator (NCA). Vous y trouverez les procédures d'utilisation de NCA et des documents de référence. Également pour Solaris 10 6/06, une introduction à l'utilisation du protocole SSL (Secure Sockets Layer) et les procédures d'utilisation du proxy SSL de noyau permettant d'améliorer les performances du traitement des paquets SSL ont été ajoutées.

NCA (Network Cache et Accelerator) (présentation)

Solaris Network Cache and Accelerator (NCA) accroît les performances du serveur Web en conservant un cache au niveau du noyau des pages Web visitées lors des demandes HTTP. Ce cache de noyau recourt à la mémoire système pour augmenter considérablement les performances des demandes HTTP, normalement gérées par les serveurs Web. L'utilisation de la mémoire système pour conserver des pages Web pour les demandes HTTP accroît les performances du serveur Web en réduisant le temps système entre le noyau et le serveur Web. NCA fournit une interface de sockets par l'intermédiaire de laquelle tous les serveurs Web peuvent communiquer avec NCA avec un minimum de modifications.

Lorsque la page demandée est récupérée du cache au niveau du noyau (succès du cache), les performances sont considérablement améliorées. Lorsque la page demandée ne se trouve pas dans le cache (échec du cache) et doit être récupérée à partir du serveur Web, les performances sont également améliorées de façon significative.

Ce produit est conçu pour être exécuté sur un serveur Web dédié. Si vous exécutez d'autres traitements importants sur un serveur qui exécute NCA, des problèmes risquent de se produire.

NCA prend en charge la journalisation des succès du cache. Ce journal est stocké au format binaire afin d'accroître les performances. La commande `ncab2clf` permet de convertir le journal du format binaire au format CLF (Common Log Format).

La version Solaris inclut les améliorations suivantes :

- Interface de sockets
- Prise en charge de sendfile vectorisé, permettant la gestion de AF_NCA. Pour plus d'informations, reportez-vous à la page de manuel `sendfilev(3EXT)`.
- Nouvelles options de la commande `ncab2clf` qui prennent en charge la possibilité d'ignorer les enregistrements avant une date sélectionnée (`-s`) et de traiter un nombre spécifié d'enregistrements (`-n`)
- L'entrée `logd_path_name` dans le fichier `ncalogd.conf` peut indiquer un périphérique brut, un fichier ou une combinaison des deux.
- Prise en charge d'un serveur Web pour ouvrir plusieurs sockets AF_NCA. Avec plusieurs sockets, différents serveurs Web peuvent s'exécuter sur un seul et même serveur.
- Nouveau fichier de configuration appelé `/etc/nca/ncaport.conf` . Ce fichier peut permettre de gérer les ports et adresses IP que NCA utilise. Il est possible que votre serveur Web ne fournisse pas la prise en charge native du socket AF_NCA. Si tel est le cas, utilisez ce fichier et la bibliothèque d'utilitaires de socket NCA pour convertir un socket AF_INET en socket AF_NCA.

Serveurs Web utilisant le protocole SSL (Secure Sockets Layer)

Dans le SE Solaris 10 6/06, vous pouvez configurer un serveur Web Apache 2.0 et Sun Java System pour utiliser le protocole SSL (Secure Sockets Layer). Ce protocole assure la confidentialité, l'intégrité des messages et l'authentification d'extrémité entre deux applications. Le noyau a été modifié afin d'accélérer le trafic SSL.

Le proxy SSL au niveau du noyau met en œuvre le côté serveur du protocole SSL. Il offre de meilleures performances SSL pour les applications serveur, telles que les serveurs Web, via des applications qui utilisent des bibliothèques SSL au niveau de l'utilisateur. L'amélioration des performances peut atteindre +35 % en fonction de la charge de travail de l'application.

Le proxy SSL au niveau du noyau prend en charge les protocoles SSL 3.0 et TLS 1.0, ainsi que la plupart des suites de chiffrement courantes. La page de manuel `ksslcfg(1M)` contient la liste complète. Le proxy peut être configuré pour remplacer le serveur SSL au niveau de l'utilisateur pour les suites de chiffrement qui ne sont pas prises en charge.

Les procédures suivantes indiquent comment configurer des serveurs dans le cadre d'une utilisation du proxy SSL au niveau du noyau.

- “Configuration d'un serveur Web Apache 2.0 pour utiliser le proxy SSL au niveau du noyau ” à la page 58
- “Configuration d'un serveur Web Sun Java System pour une utilisation du proxy SSL au niveau du noyau” à la page 60
- “Utilisation du proxy SSL au niveau du noyau dans les zones” à la page 62

Gestion des serveurs cache Web (liste des tâches)

Le tableau suivant décrit les procédures nécessaires à l'utilisation de NCA ou SSL.

Tâche	Description	Voir
Planification pour NCA	Liste de problèmes à résoudre avant d'activer l'utilisation de NCA	“Planification pour NCA” à la page 52
Activation de NCA	Étapes de l'activation de la mise en cache au niveau du noyau de pages Web sur un serveur Web	“Activation de la mise en cache de pages Web ” à la page 53
Désactivation de NCA	Étapes de la désactivation de la mise en cache au niveau du noyau de pages Web sur un serveur Web	“Désactivation de la mise en cache de pages Web ” à la page 56
Gestion de la journalisation NCA	Étapes de l'activation ou de la désactivation du processus de journalisation NCA	“Activation ou désactivation de la journalisation NCA” à la page 56
Chargement de la bibliothèque de sockets NCA	Étapes de l'utilisation de NCA si le socket AF_NCA n'est pas pris en charge	“Chargement de la bibliothèque d'utilitaires de socket NCA” à la page 57
Utilisation du proxy SSL de noyau avec un serveur Web Apache 2.0	Étapes de l'utilisation du proxy SSL au niveau du noyau avec un serveur Web afin d'améliorer le traitement des paquets SSL	“Configuration d'un serveur Web Apache 2.0 pour utiliser le proxy SSL au niveau du noyau ” à la page 58
Utilisation du proxy SSL de noyau avec un serveur Web Sun Java System	Étapes de l'utilisation du proxy SSL au niveau du noyau avec un serveur Web afin d'améliorer le traitement des paquets SSL	“Configuration d'un serveur Web Sun Java System pour une utilisation du proxy SSL au niveau du noyau” à la page 60
Utilisation du proxy SSL de noyau avec un serveur Web dans une zone locale	Étapes de l'utilisation du proxy SSL au niveau du noyau avec un serveur Web dans une zone locale	“Utilisation du proxy SSL au niveau du noyau dans les zones” à la page 62

Planification pour NCA

Les sections suivantes abordent les problèmes à résoudre avant de commencer le service NCA.

Configuration système requise pour NCA

Pour prendre en charge NCA, le système doit satisfaire les exigences suivantes :

- 256 Mo de RAM doivent être installés.
- La version Solaris 9 ou 10, ou l'une des mises à niveau de Solaris 8, doit être installé.
- Prise en charge d'un serveur Web offrant la gestion native de NCA ou bien d'un serveur Web dont le script de démarrage a été modifié de manière à utiliser la bibliothèque d'utilitaires de socket pour NCA :
  - Serveur Web Apache, fourni avec Solaris 10, Solaris 9 ou une mise à niveau de Solaris 8.
  - Serveur Web Sun Java System
  - Serveur Web Zeus, disponible auprès de Zeus Technology, `http://www.zeus.com`

Ce produit est conçu pour être exécuté sur un serveur Web dédié. Si vous exécutez d'autres traitements importants sur un serveur qui exécute NCA, des problèmes risquent de se produire.

Journalisation NCA

Le service NCA peut être configuré pour consigner l'activité Web. D'une manière générale, la journalisation NCA doit être activée si la journalisation du serveur Web l'est.

Bibliothèque d'interposition pour prise en charge démon du serveur de porte

De nombreux serveurs Web utilisent les sockets AF_INET. Par défaut, NCA utilise les sockets AF_NCA. Pour corriger cette situation, une bibliothèque d'interposition est fournie. La nouvelle bibliothèque est chargée devant la bibliothèque de sockets standard, `libsocket.so`. L'appel de bibliothèque `bind()` est interposé par la nouvelle bibliothèque, `ncad_addr.so`. Supposons que l'état est activé dans `/etc/nca/ncakmod.conf`. La version d'Apache incluse avec le SE Solaris 9 et Solaris 10 est déjà configurée pour appeler cette bibliothèque. Si vous utilisez des serveurs Netscape ou IWS, reportez-vous à la section “Chargement de la bibliothèque d'utilitaires de socket NCA” à la page 57 pour utiliser la nouvelle bibliothèque.

Prise en charge de plusieurs instances

Les systèmes sur lesquels NCA est installé doivent souvent exécuter plusieurs instances d'un serveur Web. Par exemple, un seul serveur doit peut-être prendre en charge un serveur Web pour l'accès extérieur, ainsi qu'un serveur d'administration Web. Pour séparer ces serveurs, vous devez les configurer de sorte qu'ils utilisent un port distinct.

Administration de la mise en cache de pages Web (tâches)

Les sections suivantes décrivent les procédures d'activation et de désactivation de certaines parties du service.

▼ Activation de la mise en cache de pages Web

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Inscrivez les interfaces.**

Entrez le nom de chaque interface physique dans le fichier `/etc/nca/nca.if`. Pour plus d'informations, reportez-vous à la page de manuel `nca.if(4)`.

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

Chaque interface doit être accompagnée d'un fichier `hostname.`*interface-name* et le fichier `/etc/hosts` doit inclure une entrée pour le contenu de `hostname.`*interface-name*. Pour démarrer la fonctionnalité NCA sur toutes les interfaces, placez un astérisque (*) dans le fichier `nca.si`.

3 **Activez le module de noyau `ncakmod`.**

Remplacez l'entrée `status` dans `/etc/nca/ncakmod.conf` par `enabled`.

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

Pour plus d'informations, reportez-vous à la page de manuel `ncakmod.conf(4)`.

4 (Facultatif) Activez la journalisation NCA.

Remplacez l'entrée `status` dans `/etc/nca/ncalogd.conf` par `enabled`.

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

Vous pouvez changer l'emplacement du fichier journal en modifiant le chemin d'accès indiqué par l'entrée `logd_path_name`. Le fichier journal peut être un périphérique brut ou un fichier. Reportez-vous aux exemples suivants pour obtenir des exemples de chemins d'accès au fichier journal NCA. Pour plus d'informations sur le fichier de configuration, reportez-vous à la page de manuel `ncalogd.conf(4)`.

5 (Facultatif) Définissez les ports pour la prise en charge de plusieurs instances.

Ajoutez le numéro des ports dans le fichier `/etc/nca/ncaport.conf` . Avec cette entrée, NCA contrôle le port 80 sur toutes les adresses IP configurées.

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

6 Pour x86 uniquement : augmentez la taille de la mémoire virtuelle.

Utilisez la commande `eeprom` pour définir l'entrée `kernelbase` du système.

```
# eeprom kernelbase=0x90000000
# eeprom kernelbase
kernelbase=0x90000000
```

La deuxième commande vérifie que le paramètre a été défini.

Remarque – Définir `kernelbase` permet de réduire la quantité de mémoire virtuelle que les processus utilisateurs peuvent utiliser à moins de 3 Go. Cette restriction signifie que le système n'est pas conforme à ABI. Lors de l'initialisation du système, la console affiche un message qui vous avertit de la non-conformité. La plupart de ces programmes n'ont pas réellement besoin de la totalité des 3 Go d'espace d'adressage virtuel. Si votre programme nécessite plus de 3 Go, vous devez l'exécuter sur un système sur lequel NCA n'est pas activé.

---

7 Redémarrez le serveur.

Exemple 2–1 Utilisation d'un périphérique brut comme fichier journal NCA

La chaîne `logd_path_name` dans le fichier `ncalogd.conf` peut définir un périphérique brut en tant qu'emplacement de stockage du fichier journal NCA. L'avantage de l'utilisation d'un périphérique brut est que le service peut s'exécuter plus rapidement, le temps système pour l'accès à un périphérique brut étant inférieur.

Le service NCA teste tous les périphériques bruts répertoriés dans le fichier afin de s'assurer qu'aucun système de fichiers n'est en place. Ce test garantit que vous n'écrivez pas sur les systèmes de fichiers actifs par mégarde.

Pour éviter que ce test ne trouve un système de fichiers, exécutez la commande suivante. Cette commande détruit en partie le système de fichiers sur les partitions de disque configurées en tant que système de fichiers. Dans cet exemple, `/dev/rdsk/c0t0d0s7` est le périphérique brut qui a un ancien système de fichiers en place.

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

Après l'exécution de `dd`, vous pouvez ajouter le périphérique brut dans le fichier `ncalogd.conf`.

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

Exemple 2–2 Utilisation de plusieurs fichiers pour la journalisation NCA

La chaîne `logd_path_name` dans le fichier `ncalogd.conf` peut définir plusieurs cibles en tant qu'emplacement de stockage du fichier journal NCA. Le deuxième fichier est utilisé lorsque le premier est saturé. L'exemple ci-dessous indique comment écrire dans le fichier `/var/nca/log` en premier, puis utiliser une partition brute.

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

▼ Désactivation de la mise en cache de pages Web

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le module de noyau `ncakmod`.**

Remplacez l'entrée `status` dans `/etc/nca/ncakmod.conf` par `disabled`.

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

Pour plus d'informations, reportez-vous à la page de manuel `ncakmod.conf(4)`.

3 **Désactivez la journalisation NCA.**

Remplacez l'entrée `status` dans `/etc/nca/ncalogd.conf` par `disabled`.

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

Pour plus d'informations, reportez-vous à la page de manuel `ncalogd.conf(4)`.

4 **Redémarrez le serveur.**

▼ Activation ou désactivation de la journalisation NCA

Une fois NCA activé, vous pouvez activer ou désactiver la journalisation NCA en fonction de vos besoins. Pour plus d'informations, reportez-vous à la section "Activation de la mise en cache de pages Web " à la page 53.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez la journalisation NCA.**

Pour désactiver l'enregistrement définitivement, vous devez remplacer le statut dans le fichier `/etc/nca/ncalogd.conf` par `disabled` et redémarrer le système. Pour plus d'informations, reportez-vous à la page de manuel `ncalogd.conf(4)`.

a. **Arrêtez la journalisation.**

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

b. **Démarrez la journalisation.**

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

Chargement de la bibliothèque d'utilitaires de socket NCA

Suivez cette procédure uniquement si votre serveur Web ne fournit pas la prise en charge native du socket AF_NCA.

Dans le script de démarrage du serveur Web, ajoutez une ligne qui déclenche le préchargement de la bibliothèque. La ligne doit ressembler à ceci :

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

▼ Ajout d'un port au service NCA

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez un port.**

Ajoutez une entrée de port à `/etc/nca/ncaport.conf`. Cet exemple ajoute le port `8888` sur l'adresse IP `192.168.84.71`. Pour plus d'informations, reportez-vous à `ncaport.conf(4)`.

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

3 **Démarrez une nouvelle instance.**

Une adresse doit figurer dans le fichier qui contient les configuration de port NCA avant qu'un serveur Web puisse l'utiliser pour NCA. Si le serveur Web est en cours d'exécution, vous devez le redémarrer avant de définir la nouvelle adresse.

▼ Configuration d'un serveur Web Apache 2.0 pour utiliser le proxy SSL au niveau du noyau

Cette procédure doit être utilisée pour améliorer les performances du traitement de paquets SSL sur un serveur Web Apache 2.0.

Avant de commencer

La procédure suivante exige qu'un serveur Web Apache 2.0 soit installé et configuré. Le serveur Web Apache 2.0 est inclus dans la version.

Pour utiliser le proxy SSL au niveau du noyau, la clé privée et le certificat du serveur doivent figurer dans un seul et même fichier. Si seul le paramètre `SSLCertificateFile` est précisé dans le fichier `ssl.conf`, le fichier spécifié peut être utilisé directement pour le protocole SSL au niveau du noyau. Si le paramètre `SSLCertificateKeyFile` est également spécifié, le fichier de certificat et le fichier de clé privée doivent être combinés. Pour combiner le fichier de certificat et le fichier de clé, vous pouvez exécuter la commande suivante :

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

1 **Connectez-vous en tant que superutilisateur ou prenez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*. La commande `ksslcfg` est incluse dans le profil `Network Security`.

2 **Arrêtez le serveur Web.**

Cette commande arrête le serveur Web sur un système dans lequel le serveur est configuré de manière à s'exécuter avec SMF.

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

Si le service n'a pas encore été converti, arrêtez-le à l'aide de cette syntaxe de commande : `/usr/apache2/bin/apachectl stop`

3 **Déterminez les paramètres à utiliser avec la commande `ksslcfg`.**

Toutes les options sont répertoriées dans la page de manuel ksslcfg(1M). Les paramètres pour lesquels vous devez disposer d'informations sont les suivants :

- `key-format` : utilisé avec l'option `-f` pour définir le format de clé et de certificat. Pour le proxy SSL au niveau du noyau, cette valeur doit être `pem` ou `pkcs12`.
- `key-and-certificate-file` : utilisé avec l'option `-i` pour définir l'emplacement du fichier de stockage du certificat et de la clé du serveur.
- `password-file` : utilisé avec l'option `-p` pour sélectionner l'emplacement du fichier contenant le mot de passe utilisé pour chiffrer la clé privée. Ce mot de passe est utilisé pour autoriser les redémarrages sans l'intervention d'un opérateur. Les autorisations du fichier doivent être `0400`.
- `proxy-port` : utilisé avec l'option `-x` pour définir le port proxy SSL. Sélectionnez un autre port que le port standard `80`. Le serveur Web est à l'écoute sur le port proxy SSL.
- `ssl-port` : sélectionne le port d'écoute du proxy SSL au niveau du noyau. Il s'agit généralement de la valeur `443`.

Remarque – Les valeurs `ssl-port` et `proxy-port` ne peuvent pas être configurées pour NCA, dans la mesure où ces ports sont utilisés exclusivement par le proxy SSL au niveau du noyau. Généralement, le port 80 est utilisé pour NCA, le port 8443 pour `proxy-port` et le port 443 pour `ssl-port`.

---

4 Créez l'instance de service.

La commande `ksslcfg` permet d'indiquer le port proxy SSL et les paramètres associés.

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

5 Vérifiez que l'instance a été créée correctement.

L'état du service signalé par la commande ci-dessous doit être "on line".

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

6 Configurez le serveur Web pour qu'il soit à l'écoute sur le port proxy SSL.

Modifiez le fichier `/etc/apache2/http.conf` et ajoutez une ligne pour définir le port proxy SSL. Si vous utilisez l'adresse IP des serveurs, le serveur Web écoute uniquement sur cette interface. La ligne doit ressembler à ce qui suit :

`Listen 0.0.0.0:`*proxy-port*

7 Définissez une dépendance SMF pour le serveur Web.

Le serveur Web doit uniquement être démarré après l'instance du proxy SSL au niveau du noyau. Les commandes suivantes établissent cette dépendance.

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

```
svc:/network/http:apache2> setprop kssl/restart_on = astring: refresh
svc:/network/http:apache2> setprop kssl/type = astring: service
svc:/network/http:apache2> end
```

8 Activez le serveur Web.

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

Si le service n'est pas démarré à l'aide de SMF, utilisez la commande suivante : `/usr/apache2/bin/apachectl startssl`

Exemple 2–3 Configuration d'un serveur Web Apache 2.0 pour une utilisation du proxy SSL au niveau du noyau

La commande suivante crée une instance avec le format de clé `pem`.

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

▼ Configuration d'un serveur Web Sun Java System pour une utilisation du proxy SSL au niveau du noyau

Cette procédure doit être utilisée pour améliorer les performances du traitement de paquets SSL sur un serveur Web Sun Java System. Pour plus d'informations sur ce serveur Web, reportez-vous au *Sun Java System Web Server 6.1 SP4 Administrator's Guide*.

Avant de commencer La procédure suivante exige qu'un serveur Web Sun Java System soit installé et configuré.

1 Connectez-vous en tant que superutilisateur ou prenez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*. La commande `ksslcfg` est incluse dans le profil `Network Security`.

2 Arrêtez le serveur Web.

Utilisez l'interface Web de l'administrateur pour arrêter le serveur. Pour plus d'informations, reportez-vous à la section *Starting and Stopping the Server* du *Sun Java System Web Server 6.1 SP4 Administrator's Guide*

3 Désactivez le metaslot de la structure de chiffrement.

Cette étape est nécessaire pour garantir la désactivation du metaslot lors de la création de l'instance de service SSL au niveau du noyau.

```
# cryptoadm disable metaslot
```

4 Déterminez les paramètres à utiliser avec la commande `ksslcfg`.

Toutes les options sont répertoriées dans la page de manuel `ksslcfg(1M)`. Les paramètres pour lesquels vous devez disposer d'informations sont les suivants :

- `key-format` : utilisé avec l'option `-f` pour définir le format de clé et de certificat.
- `token-label` : utilisé avec l'option `-T` pour spécifier le jeton PKCS#11.
- `certificate-label` : utilisé avec l'option `-C` pour sélectionner l'étiquette de l'objet de certificat dans le jeton PKCS#11.
- `password-file` : utilisé avec l'option `-p` pour sélectionner l'emplacement du fichier contenant le mot de passe pour la connexion de l'utilisateur au jeton PKCS#11 utilisé par le serveur Web. Ce mot de passe est utilisé pour autoriser les redémarrages sans l'intervention d'un opérateur. Les autorisations du fichier doivent être `0400`.
- `proxy-port` : utilisé avec l'option `-x` pour définir le port proxy SSL. Sélectionnez un autre port que le port standard `80`. Le serveur Web est à l'écoute sur le port proxy SSL.
- `ssl-port` : définit le port d'écoute du proxy SSL au niveau du noyau. Il s'agit généralement de la valeur `443`.

Remarque – Les valeurs `ssl-port` et `proxy-port` ne peuvent pas être configurées pour NCA, dans la mesure où ces ports sont utilisés exclusivement par le proxy SSL au niveau du noyau. Généralement, le port 80 est utilisé pour NCA, le port 8443 pour `proxy-port` et le port 443 pour `ssl-port`.

---

5 Créez l'instance de service.

La commande `ksslcfg` permet d'indiquer le port du proxy SSL et les paramètres associés.

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

6 Activez le metaslot de la structure de chiffrement.

```
# cryptoadm enable metaslot
```

7 Vérifiez que l'instance a été créée correctement.

L'état du service signalé par la commande ci-dessous doit être "on line".

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

8 Configurez le serveur Web pour qu'il soit à l'écoute sur le port du proxy SSL.

Pour plus d'informations, reportez-vous à la section *Adding and Editing Listen Sockets* du *Sun Java System Web Server 6.1 SP4 Administrator's Guide*.

9 Démarrez le serveur Web.

Exemple 2–4 Configuration d'un serveur Web Sun Java System pour une utilisation du proxy SSL au niveau du noyau

La commande suivante crée une instance avec le format de clé `pkcs11`.

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

Utilisation du proxy SSL au niveau du noyau dans les zones

Le proxy SSL au niveau du noyau fonctionne dans les zones avec les restrictions suivantes :

- L'ensemble de la gestion SSL au niveau du noyau doit être réalisé dans la zone globale. L'administrateur de la zone globale a besoin d'un accès aux fichiers de clé et de certificat de la zone locale. Le serveur Web de la zone locale peut être démarré une fois l'instance de service configurée à l'aide de la commande `ksslcfg` dans la zone globale.
- Un nom d'hôte ou une adresse IP spécifique doit être spécifié(e) lors de l'exécution de la commande `ksslcfg` pour configurer l'instance. En particulier, l'instance ne peut pas utiliser INADDR_ANY.

EXEMPLE 2–5 Configuration d'un serveur Web Apache dans une zone locale pour une utilisation du proxy SSL au niveau du noyau

Dans la zone locale, arrêtez d'abord le serveur Web. Dans la zone globale, configurez le service, étape par étape. Pour créer une instance d'une zone locale appelée `apache-zone`, utilisez la commande suivante :

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

Dans la zone locale, exécutez la commande suivante pour activer l'instance de service :

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

Mise en cache des pages Web (référence)

Les sections suivantes traitent des fichiers et composants nécessaires à l'utilisation de NCA. Elles offrent également des précisions sur l'interaction entre NCA et le serveur Web.

Fichiers NCA

Plusieurs fichiers sont nécessaires à la prise en charge de la fonction NCA. La plupart sont au format ASCII, mais certains sont des fichiers binaires. Le tableau suivant répertorie tous les fichiers.

TABLEAU 2–1 Fichiers NCA

Nom de fichier	Fonction
`/dev/nca`	Nom de chemin d'accès au périphérique NCA
`/etc/hostname.*`	Fichier qui répertorie toutes les interfaces physiques configurées sur le serveur.
`/etc/hosts`	Fichier qui répertorie tous les noms d'hôtes associés au serveur. Les entrées de ce fichier doivent correspondre aux entrées des fichiers `/etc/hostname.*` pour que NCA fonctionne.
`/etc/init.d/ncakmod`	Script de démarrage du serveur NCA. Ce script est exécuté lorsqu'un serveur est démarré.
`/etc/init.d/ncalogd`	Script de démarrage de la journalisation NCA. Ce script est exécuté lorsqu'un serveur est démarré.
`/etc/nca/nca.if`	Fichier qui répertorie les interfaces sur lesquelles NCA est exécuté. Pour plus d'informations, reportez-vous à la page de manuel `nca.if(4)`.
`/etc/nca/ncakmod.conf`	Fichier qui répertorie les paramètres de configuration pour NCA. Pour plus d'informations, reportez-vous à la page de manuel `ncakmod.conf(4)`.
`/etc/nca/ncalogd.conf`	Fichier qui répertorie les paramètres de configuration pour la journalisation NCA. Pour plus d'informations, reportez-vous à la page de manuel `ncalogd.conf(4)`.
`/etc/nca/ncaport.conf`	Fichier qui répertorie les adresses IP et les ports pour NCA. Pour plus d'informations, reportez-vous à la page de manuel `ncaport.conf(4)`.
`/usr/bin/ncab2clf`	Commande qui convertit les données contenues dans le fichier journal au format CLF (Common Log Format). Pour plus d'informations, reportez-vous à la page de manuel `ncab2clf(1)`.
`/usr/lib/net/ncaconfd`	Commande qui configure NCA pour une exécution sur plusieurs interfaces lors de l'initialisation. Pour plus d'informations, reportez-vous à la page de manuel `ncaconfd(1M)`.
`/usr/lib/nca_addr.so`	Bibliothèque qui utilise les sockets AF_NCA au lieu des sockets AF_INET. Cette bibliothèque doit être utilisée sur les serveurs Web qui utilisent les sockets AF_INET. Pour plus d'informations, reportez-vous à la page de manuel `ncad_addr(4)`.

TABLEAU 2–1 Fichiers NCA *(Suite)*

Nom de fichier	Fonction
`/var/nca/log`	Fichier contenant les données de fichier journal. Le fichier est au format binaire, ne le modifiez pas.
`/var/run/nca_httpd_1.door`	Le nom du chemin d'accès à la porte.

Architecture NCA

La fonctionnalité NCA inclut les composants suivants :

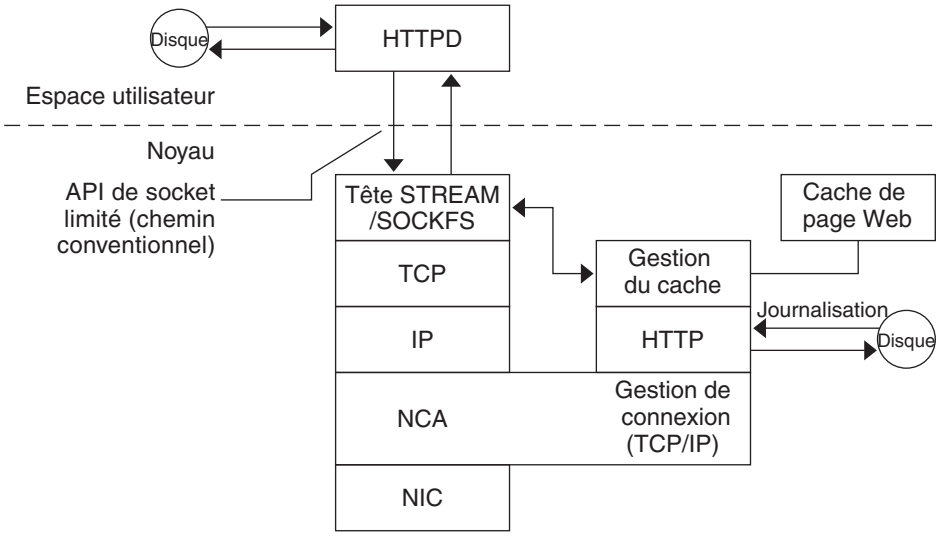
- Module de noyau, `ncakmod`
- Serveur Web, `httpd`

Le module de noyau `ncakmod` tient à jour le cache de pages Web dans la mémoire système. Le module communique avec un serveur Web, `httpd` , par l'intermédiaire d'une interface sockets. Le type de famille est PF_NCA.

Le module de noyau fournit également une fonction de journalisation qui enregistre tous les succès de cache HTTP. La journalisation NCA écrit les données HTTP au format binaire sur le disque. NCA fournit un utilitaire de conversion pour convertir les fichiers journaux binaires au format CLF (Common Log Format).

La figure suivante illustre le flux de données pour le chemin d'accès conventionnel et le chemin d'accès qui est utilisé lorsque NCA est activé.

FIGURE 2–1 Flux de données avec le service NCA



Flux d'une demande de NCA à HTTPD

La liste ci-dessous présente le flux des demandes entre le client et le serveur Web.

1. Une demande HTTP est effectuée du client vers le serveur Web.
2. Si la page figure dans le cache, la page Web du cache dans le noyau est renvoyée.
3. Si tel n'est pas le cas, la demande est transmise au serveur Web pour la récupération ou la mise à jour de la page.
4. En fonction de la sémantique du protocole HTTP utilisée dans la réponse, la page est mise en cache ou non. La page est ensuite renvoyée au client. Si l'en-tête Pragma: No-cache est inclus dans la demande HTTP, la page n'est pas mise en cache.

◆ ◆ ◆ CHAPITRE 3

Services d'horodatage

De nombreuses bases de données et services d'authentification nécessitent une bonne synchronisation des horloges système au sein d'un réseau. Ce chapitre comprend les sections suivantes :

Synchronisation de l'horloge (présentation)

Le logiciel NTP (Network Time Protocol), développé par l'University of Delaware et qui appartient au domaine public, est inclus dans le logiciel Solaris. Le démon `xntpd` définit et met à jour la date et l'heure du système. Le démon `xntpd` est une implémentation complète de la version 3, telle que définie par le RFC 1305.

Le démon `xntpd` lit le fichier `/etc/inet/ntp.conf` au démarrage du système. Pour plus d'informations sur les options de configuration, reportez-vous à la page de manuel `xntpd(1M)`.

N'oubliez pas les points suivants lorsque vous utilisez NTP sur votre réseau :

- Le démon `xntpd` utilise un minimum de ressources système.
- Un client NTP se synchronise automatiquement avec un serveur NTP lorsqu'il démarre. Si le client n'est plus synchronisé, il se synchronise de nouveau lorsque le client contacte un serveur d'horloge.

Un autre moyen de synchroniser les horloges consiste à exécuter la commande `rdate` lors de l'utilisation de `cron`.

Gestion du protocole NTP (tâches)

Les procédures ci-dessous décrivent la configuration et l'utilisation du service NTP.

▼ Configuration d'un serveur NTP

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez le fichier `ntp.conf`.**

   Afin de garantir l'exécution correcte du démon `xntpd`, le fichier `ntp.conf` doit tout d'abord être créé. Le fichier `ntp.server` peut être utilisé comme modèle.

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

3. **Démarrez le démon `xntpd`.**

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

▼ Configuration d'un client NTP

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez le fichier `ntp.conf`.**

   Pour activer le démon `xntpd`, le fichier `ntp.conf` doit d'abord être créé.

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

3. **Démarrez le démon `xntpd`.**

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

Utilisation d'autres commandes d'horodatage (tâches)

La procédure suivante peut être utilisée pour mettre à jour l'heure aussi souvent que nécessaire, sans avoir à configurer NTP.

▼ Synchronisation de la date et de l'heure à partir d'un autre système

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Réinitialisez la date et l'heure pour effectuer la synchronisation avec un autre système, à l'aide de la commande `rdate`.**

`# rdate` *another-system*

autre système Nom de l'autre système

3 **Vérifiez que vous avez réinitialisé votre système correctement à l'aide de la commande `date`.**

La sortie doit indiquer une date et une heure correspondant à celles de l'autre système.

Exemple 3–1 Synchronisation de la date et de l'heure à partir d'un autre système

L'exemple suivant présente l'utilisation de la commande `rdate` pour synchroniser la date et l'heure entre deux systèmes. Dans cet exemple, le système `earth`, qui retarde de plusieurs heures, est réinitialisé pour correspondre à la date et l'heure du serveur `starbug`.

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

Network Time Protocol (référence)

Les fichiers suivants sont nécessaires à l'exécution du service NTP.

TABLEAU 3–1 Fichiers NTP

Nom de fichier	Fonction
`/etc/inet/ntp.conf`	Répertorie les options de configuration pour le protocole NTP.
`/etc/inet/ntp.client`	Exemple de fichier de configuration pour les clients NTP.
`/etc/inet/ntp.server`	Exemple de fichier de configuration pour les serveurs NTP.
`/etc/inet/ntp.keys`	Contient les clés d'authentification NTP.
`/usr/lib/inet/xntpd`	Démon NTP. Pour plus d'informations, reportez-vous à la page de manuel `xntpd`(1M).
`/usr/sbin/ntpdate`	Utilitaire permettant de configurer la date et l'heure locales, basé sur le protocole NTP. Pour plus d'informations, reportez-vous à la page de manuel `ntpdate`(1M).
`/usr/sbin/ntpq`	Programme de requête NTP. Pour plus d'informations, reportez-vous à la page de manuel `ntpq`(1M).
`/usr/sbin/ntptrace`	Programme de suivi des hôtes NTP sur le serveur NTP maître. Pour plus d'informations, reportez-vous à la page de manuel `ntptrace`(1M).
`/usr/sbin/xntpdc`	Programme de requête NTP pour le démon `xntpd`. Pour plus d'informations, reportez-vous à la page de manuel `xntpdc`(1M).
`/var/ntp/ntpstats`	Répertoire contenant les statistiques NTP.
`/var/ntp/ntp.drift`	Définit la fréquence de décalage initiale sur les serveurs NTP.

PARTIE II

Accès aux systèmes de fichiers réseau

Cette section fournit une présentation, des listes de tâches et des informations de référence sur le service NFS.

◆ ◆ ◆ CHAPITRE 4

Gestion des systèmes de fichiers NFS (présentation)

Ce chapitre fournit un aperçu du service NFS, qui peut être utilisé pour accéder aux systèmes de fichiers sur le réseau. Il décrit les concepts nécessaires pour comprendre le service NFS ainsi que les fonctions les plus récentes dans NFS et autofs.

Remarque – Si votre système comporte des zones activées et que vous souhaitez utiliser cette fonction dans une zone non globale, reportez-vous à la section *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris* pour plus d'informations.

Nouveautés du service NFS

Cette section fournit des informations sur les nouvelles fonctionnalités des versions du système d'exploitation Solaris.

Modifications apportées dans la version Solaris 10 11/06

La version Solaris 10 11/06 fournit la prise en charge d'un outil de contrôle de système de fichiers. Reportez-vous aux rubriques suivantes :

- "Commande `fsstat`" à la page 159 pour une description et des exemples
- Page de manuel `fsstat(1M)` pour plus d'informations

En outre, ce guide propose une description plus détaillée du démon `nfsmapid`. Pour plus d'informations sur la commande `nfsmapid`, reportez-vous aux éléments suivants :

- "Démon `nfsmapid`" à la page 148
- Page de manuel `nfsmapid`(1M)

Pour obtenir la liste complète des nouvelles fonctionnalités, reportez-vous à la section *Nouveautés apportées à Oracle Solaris 10 8/11*.

Modifications apportées dans la version Solaris 10

À partir de la version Solaris 10, la version 4 de NFS est la valeur par défaut. Pour plus d'informations sur les fonctions de la version 4 de NFS et toute autre modification, reportez-vous aux rubriques suivantes :

- "Protocole de la version 4 de NFS" à la page 78
- "Fichier `/etc/default/autofs`" à la page 141
- "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142
- "Démon `lockd`" à la page 146
- "Démon `nfs4cbd`" à la page 147
- "Démon `nfsmapid`" à la page 148
- "Options `mount` pour les systèmes de fichiers NFS" à la page 160
- "NFS sur RDMA" à la page 181
- "Négociation de version dans NFS" à la page 182
- "Fonctionnalités de la version 4 de NFS" à la page 183
- "Méthode de sélection par autofs des fichiers en lecture seule les plus proches pour les clients (plusieurs emplacements) " à la page 217

Reportez-vous également aux sections suivantes :

- "Configuration des services NFS" à la page 96 pour plus d'informations sur les tâches
- *Nouveautés apportées à Oracle Solaris 10 8/11* pour obtenir la liste complète des nouvelles fonctionnalités

En outre, le service NFS est géré par l'utilitaire de gestion des services. Les actions administratives sur ce service, telles que l'activation, la désactivation ou le redémarrage, peuvent être effectuées à l'aide de la commande `svcadm`. Servez-vous de la commande `svcs` pour connaître l'état du service. Pour plus d'informations sur l'utilitaire de gestion des services, reportez-vous à la page de manuel `smf`(5) et au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*.

Terminologie NFS

Cette section présente quelques termes de base que vous devez maîtriser afin de pouvoir de travailler avec le service NFS. Le service NFS est abordé de façon détaillée dans le Chapitre 6, "Accès aux systèmes de fichiers réseau (référence) ".

Serveurs et clients NFS

Les termes *client* et *serveur* sont utilisés pour décrire les rôles que remplit un ordinateur en cas de partage de systèmes de fichiers. Les ordinateurs qui partagent leurs systèmes de fichiers sur un réseau agissent en tant que serveurs. Les ordinateurs qui accèdent au système de fichiers sont considérés comme des clients. Le service NFS permet à un ordinateur d'accéder aux systèmes de fichiers de n'importe quel autre ordinateur. Dans le même temps, il fournit l'accès à ses propres systèmes de fichiers. Un ordinateur peut jouer le rôle de client et/ou de serveur à tout moment sur un réseau.

Les clients accèdent aux fichiers sur le serveur en montant les systèmes de fichiers partagés du serveur. Lorsqu'un client monte un système de fichiers distant, il n'effectue aucune copie du système de fichiers. Au lieu de cela, le processus de montage utilise une série d'appels de procédure distants qui permettent au client d'accéder au système de fichiers en toute transparence sur le disque du serveur. Le montage ressemble à un montage local. Les utilisateurs entrent les commandes comme si les systèmes de fichiers étaient en local. Reportez-vous à la section "Montage de systèmes de fichiers" à la page 90 pour plus d'informations sur les tâches qui montent les systèmes de fichiers.

Une fois qu'un système de fichiers a été partagé sur un serveur NFS par l'intermédiaire d'une opération NFS, le système de fichiers peut être accessible à partir d'un client. Vous pouvez monter automatiquement un système de fichiers NFS avec autofs. Reportez-vous aux sections "Partage automatique des systèmes de fichiers" à la page 86 et "Présentation des tâches d'administration Autofs" à la page 106 pour obtenir des informations sur les tâches utilisant la commande `share` et autofs.

Systèmes de fichiers NFS

Les objets qui peuvent être partagés avec le service NFS incluent tout ou partie d'une arborescence de répertoires ou une hiérarchie de fichiers qui comporte un fichier unique. Un ordinateur ne peut pas partager une hiérarchie de fichiers qui chevauche une hiérarchie de fichiers qui est déjà partagée. Les périphériques tels que les modems et imprimantes ne peuvent pas être partagés.

Dans la plupart des environnements du système UNIX, une hiérarchie de fichiers pouvant être partagée correspond à tout ou partie d'un système de fichiers. Cependant, la prise en charge de NFS fonctionne sur divers systèmes d'exploitation, et le concept de système de fichiers peut être

dénué de sens dans d'autres environnements non UNIX. Par conséquent, le terme *système* de *fichiers* fait référence à un fichier ou à une hiérarchie de fichiers pouvant être partagé et monté avec NFS.

A propos du service NFS

Le service NFS permet à des ordinateurs à architectures diverses, qui exécutent différents systèmes d'exploitation, de partager des fichiers via un réseau. La prise en charge NFS a été implémentée sur de nombreuses plates-formes, de MS-DOS au système d'exploitation VMS.

L'environnement NFS peut être implémenté sur différents systèmes d'exploitation car NFS définit un modèle abstrait de système de fichiers, et non une spécification architecturale. Chaque système d'exploitation applique le modèle NFS à sa sémantique. Ce modèle signifie que les opérations du système de fichiers telles que la lecture et l'écriture fonctionnent comme si elles accédaient à un fichier local.

Le service NFS présente les avantages suivants :

- possibilité donnée à plusieurs ordinateurs d'utiliser les mêmes fichiers de sorte que toute personne sur le réseau est à même d'accéder aux mêmes données ;
- réduction des coûts de stockage grâce au partage des applications plutôt qu'à l'allocation d'espace disque local pour chaque application utilisateur ;
- cohérence des données et fiabilité car tous les utilisateurs peuvent lire le même ensemble de fichiers ;
- montage de systèmes de fichiers transparent pour les utilisateurs ;
- accès aux fichiers distants transparent pour les utilisateurs ;
- prise en charge d'environnements hétérogènes ;
- frais d'administration système réduits.

Avec le service NFS, l'emplacement physique d'un système de fichiers n'a pas d'importance pour l'utilisateur. Vous pouvez utiliser l'implémentation de NFS pour permettre aux utilisateurs de voir tous les fichiers pertinents quel que soit l'emplacement. Au lieu de placer des copies des fichiers couramment utilisés sur chaque système, le service NFS vous permet de placer une copie sur un disque. Tous les autres systèmes accèdent aux fichiers sur le réseau. Sous fonctionnement NFS, les systèmes de fichiers distants sont pratiquement semblables aux systèmes de fichiers locaux.

À propos d'Autofs

Les systèmes de fichiers partagés par l'intermédiaire du service NFS peuvent être montés à l'aide du montage automatique. Autofs, service côté client, est une structure de système de fichiers qui offre ce montage automatique. Le système de fichiers autofs est initialisé par `automount`, qui s'exécute automatiquement lorsqu'un système est amorcé. Le démon de montage automatique, `automountd`, s'exécute en continu, montant et démontant les répertoires distants selon les besoins.

Lorsqu'un ordinateur client qui exécute `automountd` tente d'accéder à un fichier distant ou à un répertoire distant, le démon monte le système de fichiers distant. Ce système de fichiers distant reste monté aussi longtemps que nécessaire. S'il n'est pas accédé pendant un certain temps, le système de fichiers est automatiquement démonté.

Il n'est pas nécessaire d'effectuer le montage à l'initialisation et l'utilisateur n'a plus besoin de connaître le mot de passe superutilisateur pour monter un répertoire. Les utilisateurs n'ont pas besoin d'utiliser les commandes `mount` et `umount`. Le service autofs monte et démonte les systèmes de fichiers en fonction des besoins sans intervention de l'utilisateur.

Le montage de certaines hiérarchies de fichiers avec la commande `automountd` n'exclut pas la possibilité de monter d'autres hiérarchies avec `mount`. Un ordinateur sans disque *doit* monter `/` (root), `/usr`, et `/usr/kvm` via la commande `mount` et le fichier `/etc/vfstab`.

Les sections "Présentation des tâches d'administration Autofs" à la page 106 et "Fonctionnement d'autofs" à la page 212 donnent des informations plus détaillées sur le service autofs.

Fonctions du service NFS

Cette section décrit les principales fonctions incluses dans le service NFS.

Protocole de la version 2 de NFS

La version 2 a été la première version du protocole NFS à être largement utilisée. Elle continue d'être disponible sur une grande variété de plates-formes. Toutes les versions de Solaris prennent en charge la version 2 du protocole NFS, mais les versions antérieures à Solaris 2.5 ne prennent en charge que la version 2.

Protocole de la version 3 de NFS

L'implémentation du protocole de la version 3 de NFS a été introduite dans la version Solaris 2.5. Plusieurs modifications ont été apportées pour améliorer l'interopérabilité et les performances. Afin d'en optimiser l'utilisation, le protocole de la version 3 doit être en cours d'exécution sur les serveurs et clients NFS.

A la différence du protocole de la version 2 de NFS, le protocole de la version 3 de NFS peut gérer des fichiers de plus de 2 Go. La limitation précédente n'est plus de mise. Reportez-vous à la section "Prise en charge des fichiers NFS volumineux" à la page 81.

Le protocole de la version 3 de NFS permet les écritures asynchrones en toute sécurité sur le serveur, ce qui améliore les performances en permettant au serveur de mettre les demandes d'écriture du client en cache dans la mémoire. Le client n'a pas besoin d'attendre que le serveur valide les modifications sur le disque ; le temps de réponse est donc plus rapide. De plus, le serveur peut mettre les demandes en lot, ce qui améliore le temps de réponse sur le serveur.

De nombreuses opérations de la version 3 de Solaris NFS renvoient les attributs de fichiers, lesquels sont stockés dans le cache local. Etant donné que le cache est mis à jour plus régulièrement, il est moins souvent nécessaire de faire une opération distincte pour mettre à jour ces données. Par conséquent, le nombre des appels RPC vers le serveur est réduit, ce qui améliore les performances.

Le processus de vérification des autorisations de fichiers a été amélioré. La version 2 générait un message d'erreur d'écriture ou d'erreur de lecture si les utilisateurs tentaient de copier un fichier distant sans disposer des autorisations appropriées. Dans la version 3, les autorisations sont vérifiées avant l'ouverture du fichier, ce pourquoi l'erreur est signalée comme étant une erreur d'ouverture.

Le protocole de la version 3 de NFS supprime la limite de taille de transfert de 8 Ko. Les clients et les serveurs peuvent négocier n'importe quelle taille de transfert qu'ils prennent en charge, et non se conformer à la limite de 8 Ko imposée par la version 2. Notez que dans l'implémentation de la version Solaris 2.5, la taille par défaut du protocole de transfert est de 32 Ko. À partir de la version Solaris 10, les restrictions concernant les tailles des transferts par câble sont modérées. La taille du transfert dépend des possibilités de transport sous-jacent.

Protocole de la version 4 de NFS

La version 4 de NFS offre des fonctions qui ne sont pas disponibles dans les versions précédentes.

Le protocole de la version 4 de NFS représente l'ID d'utilisateur et l'ID de groupe sous forme de chaînes. `nfsmapid` est utilisé par le client et le serveur pour effectuer les opérations suivantes :

- mapper les chaînes d'ID de version 4 avec un identifiant numérique local ;
- mapper les ID numériques locaux avec des chaînes d'ID de la version 4.

Pour plus d'informations, reportez-vous à la section "Démon `nfsmapid`" à la page 148.

Notez que dans la version 4 de NFS, le mappeur d'ID, `nfsmapid`, est utilisé pour mettre en correspondance des ID d'utilisateur ou de groupe dans les entrées d'ACL sur un serveur avec des ID d'utilisateur ou de groupe dans les entrées d'ACL sur un client. L'inverse est également vrai. Pour plus d'informations, reportez-vous à la section "Listes de contrôle d'accès (ACL) et `nfsmapid` dans la version 4 de NFS" à la page 192.

Dans la version 4 de NFS, lorsque vous annulez le partage d'un système de fichiers, tous les états des fichiers ouverts ou verrous de fichiers dans ce système de fichiers sont détruits. Dans la version 3 de NFS, le serveur assurait la gestion des verrous que les clients avaient obtenu avant l'annulation du partage du système de fichiers. Pour plus d'informations, reportez-vous à la section "Annulation et rétablissement du partage d'un système de fichiers dans la version 4 de NFS" à la page 184.

Les serveurs de la version 4 de NFS utilisent un pseudo système de fichiers pour permettre aux clients d'accéder aux objets exportés sur le serveur. Ce pseudo système de fichiers n'existait pas dans les versions antérieures. Pour plus d'informations, reportez-vous à la section "Espace de noms du système de fichiers dans la version 4 de NFS" à la page 184.

Dans les versions 2 et 3 de NFS, le serveur renvoyait des identificateurs de fichier persistants. La version 4 de NFS prend en charge des identificateurs de fichier volatiles. Pour plus d'informations, reportez-vous à la section "Identificateurs de fichiers volatile de la version 4 de NFS" à la page 186.

La délégation, qui désigne une technique par laquelle le serveur délègue la gestion d'un fichier au client, est prise en charge à la fois sur le client et le serveur. Par exemple, le serveur peut attribuer une délégation de lecture ou d'écriture à un client. Pour plus d'informations, reportez-vous à la section "Délégation dans la version 4 de NFS" à la page 190.

À partir de la version Solaris 10, la version 4 de NFS ne prend pas en charge la variante de sécurité LIPKEY/SPKM.

En outre, la version 4 de NFS n'utilise pas les démons suivants :

- `mountd`
- `nfslogd`
- `statd`

Pour obtenir la liste complète des fonctions de la version 4 de NFS, reportez-vous à la section "Fonctionnalités de la version 4 de NFS" à la page 183.

Pour plus d'informations sur les procédures relatives à l'utilisation de la version 4 de NFS, reportez-vous à la section "Configuration des services NFS" à la page 96.

Contrôle des versions NFS

Le fichier `/etc/default/nfs` est doté de mots-clés pour contrôler les protocoles NFS qui sont utilisés à la fois par le client et le serveur. Par exemple, vous pouvez utiliser des mots-clés pour gérer la négociation de version. Pour plus d'informations, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142 ou à la page de manuel `nfs(4)`.

Prise en charge des ACL de NFS

La prise en charge des listes de contrôle d'accès (ACL) a été ajoutée dans la version Solaris 2.5. Les ACL fournissent un mécanisme de plus fine granularité pour définir les autorisations d'accès de fichier disponibles par le biais des autorisations de fichiers UNIX standard. La prise en charge des ACL NFS fournit une méthode de modification et d'affichage des entrées d'ACL à partir d'un client NFS Solaris vers un serveur NFS Solaris.

Les protocoles des versions 2 et 3 de NFS prennent en charge les anciennes ACL POSIX-draft. Les ACL POSIX-draft sont prises en charge par UFS en mode natif. Reportez-vous à la section "Using Access Control Lists to Protect UFS Files" du *System Administration Guide: Security Services* pour plus d'informations sur les ACL UFS.

Le protocole de la version 4 de NFS prend en charge les nouvelles ACL de style NFSv4. Les ACL NFSv4 sont prises en charge par ZFS en mode natif. Pour être doté de toutes les fonctionnalités ACL NFSv4, ZFS doit être utilisé en tant que système de fichiers sous-jacent sur le serveur NFSv4. Les ACL NFSv4 disposent d'un riche ensemble de propriétés d'héritage et d'un ensemble de bits d'autorisation s'étendant au-delà des autorisations standard en lecture, écriture et exécution. Reportez-vous à la section Chapitre 8, "Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS" du *Guide d'administration Oracle Solaris ZFS* pour une présentation des nouvelles ACL. Pour plus d'informations sur la prise en charge des ACL dans la version 4 de NFS, reportez-vous à la section "Listes de contrôle d'accès (ACL) et `nfsmapid` dans la version 4 de NFS" à la page 192.

NFS via TCP

Le protocole de transport par défaut du protocole NFS a été modifié en TCP (Transport Control Protocol) dans la version Solaris 2.5. TCP améliore les performances sur les réseaux lents et étendus. TCP fournit également un contrôle sur l'encombrement et la reprise sur erreur. NFS via TCP fonctionne avec les versions 2, 3 et 4. Dans les versions antérieures à Solaris 2.5, le protocole NFS par défaut était UDP (User Datagram Protocol).

NFS via UDP

À partir de la version Solaris 10, le client NFS n'utilise plus un nombre excessif de ports UDP. Auparavant, les transferts NFS via UDP utilisaient un port UDP séparé pour chaque demande à traiter. Désormais, par défaut, le client NFS utilise seulement un port UDP réservé. Cependant, cette prise en charge est configurable. Si l'utilisation simultanée de davantage de ports augmente les performances du système par une capacité d'évolution accrue, alors le système peut être configuré pour utiliser plusieurs ports. Cette possibilité reflète, par ailleurs, la prise en charge NFS via TCP qui est dotée de ce type de configurabilité dès sa prise d'effet. Pour plus d'informations, reportez-vous au manuel *Oracle Solaris Tunable Parameters Reference Manual*.

Remarque – La version 4 de NFS n'utilise pas UDP. Si vous montez un système de fichiers avec l'option `proto=udp`, la version 3 de NFS est utilisée à la place de la version 4.

Présentation de NFS via RDMA

La version Solaris 10 inclut le protocole RDMA (Remote Direct Memory Access), technologie de transfert de données mémoire-à-mémoire sur les réseaux haut débit. Plus précisément, RDMA fournit un transfert de données distantes directement vers et depuis la mémoire sans intervention de CPU. Pour ce faire, RDMA combine la technologie d'interconnexion d'E/S des plates-formes Infiniband sur SPARC au système d'exploitation Solaris. Pour plus d'informations, reportez-vous à la section "NFS sur RDMA" à la page 181.

Gestionnaire de verrous réseau et NFS

La version Solaris 2.5 comporte également une version améliorée du gestionnaire de verrous réseau. Le gestionnaire de verrous réseau fournit à UNIX le verrouillage d'enregistrements et le partage de fichiers PC pour les fichiers NFS. Le mécanisme de verrouillage est désormais plus fiable pour les fichiers NFS ; les commandes qui utilisent le verrouillage sont donc moins susceptibles de se bloquer.

Remarque – Le gestionnaire de verrous réseau est utilisé uniquement pour les montages des versions 2 et 3 de NFS. Le verrouillage de fichier est intégré au protocole de la version 4 de NFS.

Prise en charge des fichiers NFS volumineux

L'implémentation Solaris 2.6 du protocole de la version 3 de NFS a été modifiée pour une meilleure manipulation des fichiers de plus de 2 Go. Le protocole de la version 2 de NFS et l'implémentation Solaris 2.5 du protocole de la version 3 ne pouvaient pas traiter les fichiers de plus de 2 Go.

Basculement du client NFS

Le basculement dynamique de systèmes de fichiers en lecture seule a été ajouté à la version Solaris 2.6. Le basculement offre un haut niveau de disponibilité pour les ressources en lecture seule qui sont déjà répliquées, telles que les pages de manuel, les autres documents et les fichiers binaires partagés. Il peut se produire à tout moment après montage du système de fichiers. Les montages manuels peuvent désormais répertorier plusieurs répliques, tout comme l'agent de montage automatique dans les versions précédentes. L'agent de montage automatique reste

inchangé, exception faite du basculement immédiat sans plus attendre le remontage du système de fichiers. Reportez-vous aux sections "Utilisation du basculement côté client" à la page 94 et "Basculement côté client" à la page 196 pour plus d'informations.

Prise en charge de Kerberos pour le service NFS

La prise en charge des clients Kerberos V4 a été incluse dans la version Solaris 2.0. Dans la version 2.6, les commandes `mount` et `share` ont été modifiées pour prendre en charge les montages de la version 3 de NFS qui utilisent l'authentification Kerberos V5. En outre, la commande `share` a été modifiée pour permettre de multiples variantes d'authentification pour différents clients. Reportez-vous à la section "Variante de sécurité RPCSEC_GSS" à la page 82 pour plus d'informations sur les modifications qui impliquent les variantes de sécurité. Reportez-vous à la section "Configuring Kerberos NFS Servers" du *System Administration Guide: Security Services* pour plus d'informations sur l'authentification Kerberos V5.

Prise en charge de WebNFS

La version Solaris 2.6 permet également de rendre un système de fichiers sur Internet accessible via les pare-feux. Cette capacité a été possible grâce à une extension du protocole NFS. Le protocole WebNFS pour l'accès Internet offre l'avantage d'être fiable. Le service est conçu comme une extension des protocoles des versions 2 et 3 de NFS. En outre, l'implémentation WebNFS offre la possibilité de partager ces fichiers sans les frais d'administration d'un site `ftp` anonyme. Reportez-vous à la section "Négociation de sécurité pour le service WebNFS" à la page 83 pour une description des autres modifications liées au service WebNFS. Reportez-vous à la section "Tâches d'administration WebNFS" à la page 104 pour plus d'informations sur la tâche.

Remarque – Le protocole de la version 4 de NFS est préféré au service WebNFS. La version 4 de NFS intègre pleinement toutes les négociations de sécurité ajoutées au protocole MOUNT et au service WebNFS.

Variante de sécurité RPCSEC_GSS

Une variante de sécurité appelée RPCSEC_GSS est prise en charge dans la version Solaris 7. Cette variante utilise les interfaces standard GSS-API pour assurer l'authentification, l'intégrité et la confidentialité, ainsi que l'activation de la prise en charge de divers mécanismes de sécurité. Reportez-vous à la section "Prise en charge de Kerberos pour le service NFS" à la page 82 pour plus d'informations sur la prise en charge de l'authentification Kerberos V5. Reportez-vous au *Developer's Guide to Oracle Solaris Security* pour plus d'informations sur GSS-API.

Extensions Solaris 7 pour le montage NFS

La version Solaris 7 comporte des extensions pour les commandes `mount` et `automountd`. Les extensions activent la demande de montage afin d'utiliser l'identificateur de fichier public à la place du protocole MOUNT. Le protocole MOUNT désigne la même méthode d'accès que celle utilisée par le service WebNFS. En contournant le protocole MOUNT, le montage peuvent s'effectuer par le biais d'un pare-feu. En outre, le montage devrait s'effectuer plus rapidement car un nombre moins important de transactions entre le serveur et le client est nécessaire.

Les extensions permettent également d'utiliser les URL NFS à la place du chemin d'accès standard. Par ailleurs, vous pouvez utiliser l'option `public` avec la commande `mount` et le montage automatique effectue un mappage pour forcer l'utilisation de l'indicateur de fichier public. Reportez-vous à la section "Prise en charge de WebNFS" à la page 82 pour plus d'informations sur les modifications du service WebNFS.

Négociation de sécurité pour le service WebNFS

Un nouveau protocole a été ajouté pour permettre à un client WebNFS de négocier un mécanisme de sécurité avec un serveur NFS dans la version Solaris 8. Ce protocole permet d'utiliser des transactions sécurisées lors de l'utilisation du service WebNFS. Reportez-vous à la section "Fonctionnement de la négociation de sécurité WebNFS" à la page 201 pour plus d'informations.

Connexion au serveur NFS

Dans la version Solaris 8, la connexion au serveur NFS permet à un serveur NFS de fournir un enregistrement d'opérations de fichier qui ont été effectuées sur ses systèmes de fichiers. L'enregistrement inclut des informations sur le fichier ayant été consulté, la date à laquelle il a été accédé et le nom de la personne qui l'a consulté. Vous pouvez spécifier l'emplacement des journaux contenant ce type d'informations par le biais d'un ensemble d'options de configuration. Vous pouvez également utiliser ces options pour sélectionner les opérations devant être consignées. Cette fonction est particulièrement utile pour les sites qui rendent les archives FTP anonymes accessibles aux clients NFS et WebNFS. Reportez-vous à la section "Activation de la journalisation de serveur NFS" à la page 89 pour plus d'informations.

Remarque – La version 4 de NFS ne prend pas en charge la consignation du serveur.

Fonctions Autofs

Autofs utilise des systèmes de fichiers spécifiés dans l'espace de noms local. Ces informations peuvent être conservées dans NIS, NIS+ ou des fichiers locaux.

Une version multithread de la commande `automountd` a été incluse dans la version Solaris 2.6. Cette amélioration rend autofs plus fiable et permet plusieurs montages simultanés, ce qui évite le blocage du service en cas d'indisponibilité d'un serveur.

La nouvelle commande `automountd` fournit également un meilleur montage à la demande. Les versions précédentes montaient un ensemble complet de systèmes de fichiers si ces systèmes de fichiers étaient hiérarchiquement liés. Désormais, seul le premier système de fichiers est monté. Les autres systèmes de fichiers liés à ce point de montage sont montés au besoin.

Le service autofs prend en charge la navigabilité des mappages indirects. Cette prise en charge permet à l'utilisateur de voir les répertoires pouvant être montés, sans avoir à monter réellement chaque système de fichiers. Une option `-nobrowse` a été ajoutée aux mappages autofs pour que les systèmes de fichiers volumineux tels que `/net` et `/home` ne soient pas automatiquement navigables. En outre, vous pouvez désactiver la navigabilité autofs sur chaque client en utilisant l'option `-n` avec `automount`. Reportez-vous à la section "Désactivation de la navigabilité Autofs" à la page 121 pour plus d'informations.

◆ ◆ ◆ CHAPITRE 5

Administration de système de fichiers réseau (tâches)

Ce chapitre fournit des informations sur la manière d'effectuer des tâches d'administration NFS telles que la mise en place des services NFS, l'ajout de nouveaux systèmes de fichiers à partager et le montage de systèmes de fichiers. En outre, ce chapitre couvre l'utilisation du système Secure NFS et de la fonctionnalité WebNFS. La dernière partie de ce chapitre inclut des procédures de dépannage et une liste de plusieurs messages d'erreur NFS et leur signification.

Vos responsabilités en tant qu'administrateur NFS dépendent des besoins spécifiques de votre site et du rôle de votre ordinateur sur le réseau. Vous pouvez être responsable de tous les ordinateurs de votre réseau local, auquel cas vous pouvez être chargé de déterminer les éléments de configuration suivants :

- ordinateurs devant être des serveurs dédiés ;
- ordinateurs devant servir à la fois comme serveurs et clients ;
- ordinateurs devant être clients uniquement.

Une fois un serveur configuré, sa gestion inclut les tâches suivantes :

- partage et annulation du partage de systèmes de fichiers, le cas échéant ;
- modification des fichiers administratifs pour mettre à jour les listes de systèmes de fichiers que votre ordinateur partage ou monte automatiquement ;
- vérification de l'état du réseau ;
- diagnostic et résolution des problèmes liés à NFS lorsqu'ils surviennent ;

- configuration des mappages pour autofs.

N'oubliez pas qu'un ordinateur peut être à la fois un serveur et un client. Un ordinateur peut donc être utilisé pour le partage des systèmes de fichiers locaux avec des ordinateurs distants et le montage des systèmes de fichiers à distance.

Remarque – Si des zones sont activées pour votre système et que vous souhaitez utiliser cette fonction dans une zone non globale, reportez-vous au *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris* pour plus d'informations.

Partage automatique des systèmes de fichiers

Les serveurs permettent d'accéder à leurs systèmes de fichiers en partageant ceux-ci par le biais de l'environnement NFS. Vous pouvez spécifier les systèmes de fichiers à partager à l'aide de la commande `share` ou du fichier `/etc/dfs/dfstab`.

Les entrées du fichier `/etc/dfs/dfstab` sont partagées automatiquement chaque fois que vous démarrez le serveur NFS. Vous devez configurer le partage automatique si vous avez besoin de partager le même ensemble de systèmes de fichiers de façon régulière. Par exemple, si votre ordinateur est un serveur qui prend en charge les répertoires personnels, vous devez rendre les répertoires personnels disponibles à tout moment. Le partage des systèmes de fichiers doit être effectué principalement de manière automatique. Le partage doit être effectué de manière manuelle au cours des tests et du dépannage uniquement.

Le fichier `dfstab` répertorie tous les systèmes de fichiers que votre serveur partage avec ses clients. Ce fichier détermine également les clients qui peuvent monter un système de fichiers. Vous pouvez modifier `dfstab` pour ajouter ou supprimer un système de fichiers ou modifier la façon dont le partage se produit. Éditez le fichier à l'aide d'un éditeur de texte pris en charge quelconque (`vi`, par exemple). La prochaine fois que l'ordinateur passe au niveau d'exécution 3, le système lit le fichier `dfstab` mis à jour pour déterminer les systèmes de fichiers qui doivent être partagés automatiquement.

Chaque ligne du fichier `dfstab` contient une commande `share`, la même commande que vous tapez à l'invite de ligne de commande afin de partager le système de fichiers. La commande `share` se trouve dans `/usr/sbin`.

TABLEAU 5–1 Liste des tâches de partage de système de fichiers

Tâche	Description	Voir
Configuration du partage automatique des systèmes de fichiers	Étapes de la configuration d'un serveur de façon à ce que les systèmes de fichiers soient automatiquement partagés lorsque le serveur est redémarré	"Configuration du partage automatique des systèmes de fichiers" à la page 87

TABLEAU 5–1 Liste des tâches de partage de système de fichiers *(Suite)*

Tâche	Description	Voir
Activation de WebNFS	Procédure de configuration d'un serveur de façon à ce que les utilisateurs puissent accéder à des fichiers en utilisant WebNFS	"Activation de l'accès WebNFS" à la page 88
Activation de la journalisation de serveur NFS	Procédure de configuration d'un serveur de sorte que la journalisation NFS soit exécutée sur les systèmes de fichiers sélectionnés	"Activation de la journalisation de serveur NFS" à la page 89

▼ Configuration du partage automatique des systèmes de fichiers

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez des entrées pour chaque système de fichiers à partager.

Modifiez `/etc/dfs/dfstab`. Ajoutez une entrée au fichier pour chaque système de fichiers qui doit être automatiquement partagé. Chaque entrée doit figurer seule sur une ligne dans le fichier et présenter la syntaxe suivante :

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

Reportez-vous à la page de manuel `dfstab(4)` pour une description du fichier `/etc/dfs/dfstab` et à la page `share_nfs(1M)` pour une liste exhaustive des options.

3 Partagez le système de fichiers.

Une fois l'entrée ajoutée à `/etc/dfs/dfstab`, vous pouvez partager le système de fichiers en redémarrant le système ou à l'aide de la commande `shareall`.

```
# shareall
```

4 Vérifiez que les informations sont correctes.

Exécutez la commande `share` pour vérifier que les options correctes sont répertoriées :

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

Voir aussi L'étape suivante consiste à configurer vos mappages autofs afin que les clients puissent accéder aux systèmes de fichiers que vous avez partagés sur le serveur. Reportez-vous à la section "Présentation des tâches d'administration Autofs" à la page 106.

▼ Activation de l'accès WebNFS

À partir de Solaris 2.6, tous les systèmes de fichiers disponibles pour le montage NFS sont par défaut automatiquement disponibles pour l'accès WebNFS. Cette procédure doit être utilisée uniquement dans l'un des cas suivants :

- pour permettre le montage NFS sur un serveur qui n'autorise pas le montage NFS ;
- pour réinitialiser l'identificateur de fichier public afin de raccourcir les URL NFS en utilisant l'option `public` ;
- pour forcer le chargement d'un fichier HTML spécifique à l'aide de l'option `index`.

Reportez-vous à la section "Planification de l'accès WebNFS" à la page 104 pour obtenir une liste des problèmes à prendre en compte avant de démarrer le service WebNFS.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez des entrées pour chaque système de fichiers à partager en utilisant le service WebNFS.

Modifiez `/etc/dfs/dfstab`. Ajoutez une entrée au fichier pour chaque système de fichiers. Les balises `public` et `index` qui sont présentées dans l'exemple suivant sont facultatives.

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

Reportez-vous à la page de manuel `dfstab(4)` pour une description du fichier `/etc/dfs/dfstab` et à la page `share_nfs(1M)` pour une liste exhaustive des options.

3 Partagez le système de fichiers.

Une fois l'entrée ajoutée à `/etc/dfs/dfstab`, vous pouvez partager le système de fichiers en réinitialisant le système ou à l'aide de la commande `shareall`.

```
# shareall
```

4 Vérifiez que les informations sont correctes.

Exécutez la commande `share` pour vérifier que les options correctes sont répertoriées :

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

▼ Activation de la journalisation de serveur NFS

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **(Facultatif) Modifiez les paramètres de configuration des systèmes de fichiers.**

   Dans `/etc/nfs/nfslog.conf`, vous pouvez modifier les paramètres de l'une des deux façons suivantes. Vous pouvez modifier les paramètres par défaut pour tous les systèmes de fichiers en modifiant les données associées à la balise `global` . Sinon, vous pouvez ajouter une nouvelle balise pour ce système de fichiers. Si ces modifications ne sont pas nécessaires, vous n'avez pas besoin de modifier ce fichier. Le format de `/etc/nfs/nfslog.conf` est décrit dans `nfslog.conf(4)`.

3. **Ajoutez des entrées pour chaque système de fichiers devant être partagé à l'aide de la journalisation de serveur NFS.**

   Modifiez `/etc/dfs/dfstab`. Ajoutez une entrée au fichier pour le système de fichiers sur lequel vous activez la journalisation de serveur NFS. La balise utilisée avec l'option `log=`*tag* doit être saisie dans `/etc/nfs/nfslog.conf`. Cet exemple utilise les paramètres par défaut de la balise `global`.

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

   Reportez-vous à la page de manuel `dfstab(4)` pour une description du fichier `/etc/dfs/dfstab` et à la page `share_nfs(1M)` pour une liste exhaustive des options.

4. **Partagez le système de fichiers.**

   Une fois l'entrée ajoutée à `/etc/dfs/dfstab`, vous pouvez partager le système de fichiers en réinitialisant l'ordinateur ou à l'aide de la commande `shareall`.

   ```
   # shareall
   ```

5. **Vérifiez que les informations sont correctes.**

   Exécutez la commande `share` pour vérifier que les options correctes sont répertoriées :

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

6. **Vérifiez si `nfslogd`, le démon de journalisation NFS, est en cours d'exécution.**

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

7 **(Facultatif) Démarrez `nfslogd`, s'il n'est pas déjà en cours d'exécution.**

- **(Facultatif) Si `/etc/nfs/nfslogtab` est présent, démarrez le démon de journalisation NFS en tapant la commande suivante :**

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

- **(Facultatif) Si `/etc/nfs/nfslogtab` n'est pas présent, exécutez l'une des commandes `share` suivantes pour créer le fichier, puis lancez le démon.**

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

Montage de systèmes de fichiers

Vous pouvez monter les systèmes de fichiers de plusieurs façons. Les systèmes de fichiers peuvent être montés automatiquement lorsque le système est démarré, à la demande à partir de la ligne de commande ou via l'agent de montage automatique. L'agent de montage automatique offre de nombreux avantages pour le montage au moment de l'initialisation ou à partir de la ligne de commande. Toutefois, de nombreuses situations nécessitent une combinaison de ces trois méthodes. En outre, il existe plusieurs façons d'activer ou de désactiver les processus, selon les options que vous utilisez lors du montage du système de fichiers. Reportez-vous au tableau ci-après pour obtenir la liste complète des tâches qui sont associées au montage de système de fichiers.

TABLEAU 5–2 Liste des tâches de montage des systèmes de fichiers

Tâche	Description	Voir
Montage d'un système de fichiers à l'initialisation	Procédure à suivre afin qu'un système de fichiers soit monté à chaque réinitialisation d'un système.	“Montage d'un système de fichiers à l'initialisation” à la page 91.
Montage d'un système de fichiers à l'aide d'une commande	Procédure de montage d'un système de fichiers lorsqu'un système est en cours d'exécution. Cette procédure est utile lors des tests.	“Montage d'un système de fichiers à partir de la ligne de commande ” à la page 92.
Montage avec l'agent de montage automatique	Procédure d'accès à un système de fichiers à la demande, sans l'utilisation de la ligne de commande.	“Montage à l'aide de l'agent de montage automatique ” à la page 92.
Désactivation de la création de fichiers volumineux	Procédure de désactivation de la création de fichiers volumineux sur un système de fichiers.	“Désactivation des fichiers volumineux sur un serveur NFS” à la page 93.
Activation du basculement côté client	Procédure d'activation du basculement automatique sur un système de fichiers fonctionnel si un serveur tombe en panne.	“Utilisation du basculement côté client” à la page 94.
Désactivation de l'accès à distance pour un client	Procédures de désactivation de la capacité d'un client à accéder à un système de fichiers à distance.	“Désactivation de l'accès par montage pour un client” à la page 94.

TABLEAU 5–2 Liste des tâches de montage des systèmes de fichiers *(Suite)*

Tâche	Description	Voir
Autorisation de l'accès à un système de fichiers par le biais d'un pare-feu	Procédure d'autorisation de l'accès à un système de fichiers par le biais d'un pare-feu à l'aide du protocole WebNFS.	"Montage d'un système de fichiers NFS via un pare-feu" à la page 95.
Montage d'un système de fichiers à l'aide d'un URL NFS	Procédure d'autorisation de l'accès à un système de fichiers à l'aide d'un URL NFS. Ce processus permet d'accéder à un système de fichiers sans utiliser le protocole MOUNT.	"Montage d'un système de fichiers NFS à l'aide d'un URL NFS " à la page 95.

▼ Montage d'un système de fichiers à l'initialisation

Si vous souhaitez monter des systèmes de fichiers au moment de l'initialisation au lieu d'utiliser les mappages autofs, suivez la procédure ci-après. Cette procédure doit être effectuée sur tous les clients qui doivent avoir accès à des systèmes de fichiers à distance.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez une entrée pour le système de fichiers à `/etc/vfstab` .**

Les entrées du fichier `/etc/vfstab` présentent la syntaxe suivante :

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

Pour plus d'informations, reportez-vous à la page de manuel `vfstab(4)`.

Attention – Les serveurs NFS qui contiennent également des entrées `vfstab` de client NFS doivent toujours spécifier l'option `bg` afin d'éviter le blocage du système pendant la réinitialisation. Pour plus d'informations, reportez-vous à la section "Options `mount` pour les systèmes de fichiers NFS" à la page 160.

Exemple 5–1 Entrée du fichier `vfstab` du client

Vous voulez un ordinateur client pour monter le répertoire `/var/mail` à partir du serveur `wasp`. Vous souhaitez que le système de fichiers soit monté en tant que `/var/mail` sur le client et que ce dernier dispose d'un accès en lecture-écriture. Ajoutez l'entrée suivante au fichier `vfstab` du client.

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

▼ Montage d'un système de fichiers à partir de la ligne de commande

Le montage d'un système de fichiers à partir de la ligne de commande est souvent effectué pour tester un nouveau point de montage. Ce type de montage permet d'accéder de manière temporaire à un système de fichiers qui n'est pas disponible par le biais de l'agent de montage automatique.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Montez le système de fichiers.**

Tapez la commande suivante :

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

Dans cette instance, le système de fichiers `/export/share/local` du serveur `bee` est monté sur `/mnt` en lecture seule sur le système local. Le montage à partir de la ligne de commande permet l'affichage temporaire du système de fichiers. Vous pouvez démonter le système de fichiers avec `umount` ou en redémarrant l'hôte local.

Attention – Aucune version de la commande `mount` n'avertit l'utilisateur en cas d'options non valides. La commande ignore de manière silencieuse toutes les options qui ne peuvent pas être interprétées. Afin d'éviter tout comportement inattendu, vous devez vérifier toutes les options qui ont été utilisées.

Montage à l'aide de l'agent de montage automatique

"Présentation des tâches d'administration Autofs" à la page 106 inclut les instructions spécifiques pour la réalisation et la prise en charge des montages avec l'agent de montage automatique. Sans aucune modification du système générique, les clients doivent être en mesure d'accéder aux systèmes de fichiers à distance par l'intermédiaire du point de montage `/net`. Pour monter le système de fichiers `/export/share/local` de l'exemple précédent, saisissez la commande suivante :

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

Dans la mesure où l'agent de montage automatique permet à tous les utilisateurs de monter des systèmes de fichiers, un accès `root` n'est pas nécessaire. L'agent de montage automatique permet également le démontage automatique des systèmes de fichiers, de sorte qu'il n'est pas nécessaire de démonter les systèmes de fichiers une fois que vous avez terminé.

▼ Désactivation des fichiers volumineux sur un serveur NFS

Pour les serveurs qui prennent en charge des clients qui ne peuvent gérer un fichier d'une taille supérieure à 2 Go, vous pouvez être amené à désactiver la possibilité de créer des fichiers volumineux.

Remarque – Les versions antérieures à la version 2.6 de Solaris ne peuvent pas utiliser des fichiers volumineux. Si les clients ont besoin d'accéder à des fichiers volumineux, vérifiez que les clients du serveur NFS exécutent, au minimum, la version 2.6.

---

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Assurez-vous qu'aucun fichier volumineux n'existe sur le système de fichiers.

Exemple :

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

Si des fichiers volumineux se trouvent sur le système de fichiers, vous devez supprimer ou déplacer ces fichiers sur un autre système de fichiers.

3 Démontez le système de fichiers.

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

4 Réinitialisez l'état du système de fichiers si le système de fichiers a été monté à l'aide de l'option `largefiles`.

`fsck` réinitialise l'état du système de fichiers s'il n'existe aucun fichier volumineux sur le système de fichiers :

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

5 Montez le système de fichiers à l'aide de l'option `nolargefiles`.

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

Vous pouvez effectuer le montage à partir de la ligne de commande. Toutefois, afin que l'option soit plus permanente, ajoutez une entrée comme suit à `/etc/vfstab` :

```
/dev/dsk/c0t3d0s1 /dev/rdsk/c0t3d0s1 /export/home1  ufs  2  yes  nolargefiles
```

▼ Utilisation du basculement côté client

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Sur le client NFS, montez le système de fichiers à l'aide de l'option `ro`.**

Vous pouvez effectuer le montage à partir de la ligne de commande, par le biais de l'agent de montage automatique, ou en ajoutant une entrée à `/etc/vfstab` comme suit :

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

Cette syntaxe a été autorisée par l'agent de montage automatique. Cependant, le basculement n'était pas disponible lorsque les systèmes de fichiers étaient montés, mais uniquement lorsqu'un serveur était sélectionné.

Remarque – Les serveurs qui exécutent plusieurs versions du protocole NFS ne peuvent pas être combinés à l'aide d'une ligne de commande ou dans une entrée `vfstab`. Seul autofs permet de combiner des serveurs prenant en charge les protocoles des versions 2, 3 et 4 de NFS. Dans autofs, le meilleur sous-ensemble de serveurs de version 2, 3 ou 4 est utilisé.

▼ Désactivation de l'accès par montage pour un client

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez une entrée dans `/etc/dfs/dfstab`.**

Le premier exemple permet l'accès par montage à tous les clients du groupe réseau `eng`, à l'exception de l'hôte nommé `rose`. Le deuxième exemple permet l'accès par montage à tous les clients du domaine DNS `eng.example.com`, à l'exception de `rose`.

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

Pour plus d'informations sur les listes d'accès, reportez-vous à la section "Définition des listes d'accès avec la commande `share`" à la page 170. Pour obtenir une description de `/etc/dfs/dfstab`, reportez-vous à `dfstab`(4).

3 **Partagez le système de fichiers.**

Le serveur NFS n'utilise pas les modifications apportées à `/etc/dfs/dfstab` jusqu'à ce que les systèmes de fichiers soient à nouveau partagés ou jusqu'à ce que le serveur ait redémarré.

```
# shareall
```

▼ Montage d'un système de fichiers NFS via un pare-feu

Pour accéder à des systèmes de fichiers par le biais d'un pare-feu, utilisez la procédure suivante.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Montez manuellement le système de fichiers à l'aide d'une commande telle que la suivante :**

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

Dans cet exemple, le système de fichiers `/export/share/local` est monté sur le client local à l'aide de l'identificateur de fichier public. Un URL NFS peut être utilisé à la place du chemin d'accès standard. Si l'identificateur de fichier public n'est pas pris en charge par le serveur `bee`, l'opération de montage échoue.

Remarque – Cette procédure nécessite que le système de fichiers sur le serveur NFS soit partagé à l'aide de l'option `public`. En outre, tous les pare-feu situés entre le client et le serveur doivent autoriser les connexions TCP sur le port `2049`. Tous les systèmes de fichiers qui sont partagés permettent l'accès à l'identificateur de fichier public, de sorte que l'option `public` est appliquée par défaut.

▼ Montage d'un système de fichiers NFS à l'aide d'un URL NFS

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **(Facultatif) Si vous utilisez la version 2 ou la version 3 de NFS, montez manuellement le système de fichiers à l'aide d'une commande telle que la suivante :**

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

Dans cet exemple, le système de fichiers `/export/share/local` est en cours de montage à partir du serveur bee à l'aide du numéro de port NFS `3000`. Le numéro de port n'est pas requis, et le numéro de port NFS standard `2049` est utilisé par défaut. Vous pouvez choisir d'inclure l'option `public` avec un URL NFS. Sans l'option `public`, le protocole MOUNT est utilisé si le serveur ne prend pas en charge l'identificateur de fichier public. L'option `public` force l'utilisation de l'identificateur de fichier public, et le montage échoue si ce dernier n'est pas pris en charge.

3 **(Facultatif) Si vous utilisé la version 4 de NFS, montez manuellement le système de fichiers à l'aide d'une commande telle que la suivante :**

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

Configuration des services NFS

Cette section décrit quelques-unes des tâches qui sont nécessaires pour effectuer les opérations suivantes :

- démarrer et arrêter le serveur NFS ;
- démarrer et arrêter l'agent de montage automatique ;
- sélectionner une autre version de NFS.

Remarque – À partir de la version Solaris 10, la version 4 de NFS est la valeur par défaut.

TABLEAU 5–3 Liste des tâches pour les services NFS

Tâche	Description	Voir
Démarrage du serveur NFS	Procédure de démarrage du service NFS s'il n'a pas été démarré automatiquement.	“Démarrage des services NFS” à la page 97
Arrêt du serveur NFS	Procédure d'arrêt du service NFS. Normalement, le service ne doit pas être arrêté.	“Arrêt des services NFS” à la page 97
Démarrage de l'agent de montage automatique	Procédure de démarrage de l'agent de montage automatique. Cette procédure est requise lorsque certains mappages de montage automatique sont modifiés.	“Démarrage de l'agent de montage automatique” à la page 98
Arrêt de l'agent de montage automatique	Procédure d'arrêt de l'agent de montage automatique. Cette procédure est requise lorsque certains mappages de montage automatique sont modifiés.	“Arrêt de l'agent de montage automatique” à la page 98
Sélection d'une autre version de NFS sur le serveur	Procédure de sélection d'une autre version de NFS sur le serveur. Si vous choisissez de ne pas utiliser la version 4 de NFS, utilisez cette procédure.	“Sélection de versions différentes de NFS sur un serveur” à la page 98

TABLEAU 5–3 Liste des tâches pour les services NFS *(Suite)*

Tâche	Description	Voir
Sélection d'une autre version de NFS sur le client	Procédure de sélection d'une autre version de NFS sur le client, en modifiant le fichier `/etc/default/nfs`. Si vous choisissez de ne pas utiliser la version 4 de NFS, utilisez cette procédure.	"Sélection de versions différentes de NFS sur un client en modifiant le fichier `/etc/default/nfs`" à la page 100
	Alternez les étapes afin de sélectionner une autre version de NFS sur le client à l'aide de la ligne de commande. Si vous choisissez de ne pas utiliser la version 4 de NFS, utilisez cette autre procédure.	"Utilisation de la commande `mount` pour sélectionner différentes versions de NFS sur un client" à la page 101

▼ Démarrage des services NFS

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Activez le service NFS sur le serveur.**

Saisissez la commande suivante :

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

Cette commande active le service NFS.

Remarque – Le serveur NFS démarre automatiquement lorsque vous initialisez le système. En outre, après l'initialisation du système, les démons du service NFS peuvent être automatiquement activés à tout moment en partageant le système de fichiers NFS. Reportez-vous à la section "Configuration du partage automatique des systèmes de fichiers" à la page 87.

▼ Arrêt des services NFS

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le service NFS sur le serveur.**

Saisissez la commande suivante :

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

▼ Démarrage de l'agent de montage automatique

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Activez le démon autofs.**

Tapez la commande suivante\~:

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

▼ Arrêt de l'agent de montage automatique

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le démon autofs.**

Tapez la commande suivante\~:

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

▼ Sélection de versions différentes de NFS sur un serveur

Si vous choisissez de ne pas utiliser la version 4 de NFS, utilisez cette procédure.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez le fichier `/etc/default/nfs`.**

Par exemple, si vous souhaitez que le serveur fournisse uniquement la version 3, définissez les valeurs pour NFS_SERVER_VERSMAX et NFS_SERVER_VERSMIN sur 3. Pour obtenir une liste des mots-clés et de leurs valeurs, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142.

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

valeur Fournissez le numéro de version.

Remarque – Par défaut, ces lignes sont commentées. N'oubliez pas de supprimer le signe dièse (#).

---

3 (Facultatif) Si vous souhaitez désactiver la délégation de serveur, incluez cette ligne dans le fichier `/etc/default/nfs`.

```
NFS_SERVER_DELEGATION=off
```

Remarque – Dans la version 4 de NFS, la délégation de serveur est activée par défaut. Pour plus d'informations, reportez-vous à la section "Délégation dans la version 4 de NFS" à la page 190.

---

4 (Facultatif) Si vous souhaitez définir un domaine commun pour les clients et les serveurs, ajoutez cette ligne au fichier `/etc/default/nfs`.

`NFSMAPID_DOMAIN=`*my.comany.com*

my.comany.com Indiquez le domaine commun.

Pour plus d'informations, reportez-vous à la section "Démon `nfsmapid`" à la page 148.

5 Vérifiez si le service NFS est en cours d'exécution sur le serveur.

Tapez la commande suivante\~:

```
# svcs network/nfs/server
```

Cette commande indique si le service de serveur NFS est en ligne ou désactivé.

6 (Facultatif) Si nécessaire, désactivez le service NFS.

Si vous avez découvert dans l'étape précédente que le service NFS est en ligne, tapez la commande suivante pour désactiver le service.

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

Remarque – Si vous avez besoin de configurer votre service NFS, reportez-vous à la section "Configuration du partage automatique des systèmes de fichiers" à la page 87.

---

7 Activez le service NFS.

Tapez la commande suivante pour activer le service.

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

Voir aussi "Négociation de version dans NFS" à la page 182

▼ Sélection de versions différentes de NFS sur un client en modifiant le fichier `/etc/default/nfs`

La procédure suivante vous indique comment contrôler la version de NFS utilisée sur le client en modifiant le fichier `/etc/default/nfs`. Si vous préférez utiliser la ligne de commande, reportez-vous à la section "Utilisation de la commande `mount` pour sélectionner différentes versions de NFS sur un client" à la page 101.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Modifiez le fichier `/etc/default/nfs`.

Par exemple, si vous souhaitez uniquement la version 3 sur le client, définissez les valeurs NFS_CLIENT_VERSMAX et NFS_CLIENT_VERSMIN sur 3. Pour obtenir une liste des mots-clés et de leurs valeurs, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142.

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

valeur Fournissez le numéro de version.

Remarque – Par défaut, ces lignes sont commentées. N'oubliez pas de supprimer le signe dièse (#).

---

3 Montez NFS sur le client.

Tapez la commande suivante\~:

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

server-name Indiquez le nom du serveur.

/share-point Indiquez le chemin d'accès du répertoire distant à partager.

/local-dir Indiquez le chemin d'accès du point de montage local.

Voir aussi "Négociation de version dans NFS" à la page 182

▼ Utilisation de la commande `mount` pour sélectionner différentes versions de NFS sur un client

La procédure suivante vous indique comment utiliser la commande `mount` pour contrôler la version de NFS utilisée sur un client pour un montage donné. Si vous préférez modifier la version NFS pour tous les systèmes de fichiers montés par le client, reportez-vous à la section "Sélection de versions différentes de NFS sur un client en modifiant le fichier `/etc/default/nfs`" à la page 100.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Montez la version souhaitée de NFS sur le client.

Tapez la commande suivante\~:

```
# mount -o vers=value server-name:/share-point /local-dir
```

valeur	Fournissez le numéro de version.
server-name	Indiquez le nom du serveur.
/share-point	Indiquez le chemin d'accès du répertoire distant à partager.
/local-dir	Indiquez le chemin d'accès du point de montage local.

Remarque – Cette commande utilise le protocole NFS pour monter le répertoire distant et remplace les paramètres du client dans le fichier `/etc/default/nfs`.

Voir aussi "Négociation de version dans NFS" à la page 182

Administration du système Secure NFS

Afin d'utiliser le système Secure NFS, tous les ordinateurs dont vous êtes responsable doivent posséder un nom de domaine. En règle générale, un domaine est une entité administrative de plusieurs ordinateurs qui fait partie d'un réseau de plus grande taille. Si vous exécutez un service de noms, vous devez également définir le service de noms pour le domaine. Reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

L'authentification via Kerberos 5 est prise en charge par le service NFS. Le Chapitre 21, "Introduction to the Kerberos Service" du *System Administration Guide: Security Services* aborde le service Kerberos.

Vous pouvez également configurer l'environnement Secure NFS pour utiliser l'authentification Diffie-Hellman. Le Chapitre 16, “Using Authentication Services (Tasks)” du *System Administration Guide: Security Services* aborde ce service d'authentification.

▼ Configuration d'un environnement Secure NFS avec l'authentification DH

1 **Affectez un nom à votre domaine, et indiquez-le à tous les ordinateurs du domaine.**

Reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* si vous utilisez le service de noms NIS+.

2 **Définissez les clés publiques et les clés secrètes pour les utilisateurs de vos clients en utilisant les commandes `newkey` ou `nisaddcred`. Faites en sorte que chaque utilisateur définisse son propre mot de passe RPC sécurisé en utilisant la commande `chkey`.**

Remarque – Pour plus d'informations sur ces commandes, reportez-vous aux pages de manuel `newkey`(1M), `nisaddcred`(1M) et `chkey`(1).

Une fois les clés publiques et les clés secrètes générées, les clés publiques et les clés secrètes chiffrées sont stockées dans la base de données `publickey`.

3 **Vérifiez que le service de noms répond.**

Si vous exécutez NIS+, entrez la commande suivante :

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

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

Si vous exécutez NIS, vérifiez que le démon `ypbind` est en cours d'exécution.

4 **Vérifiez que le démon `keyserv` du serveur de clé est en cours d'exécution.**

Saisissez la commande suivante :

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

Si le démon n'est pas en cours d'exécution, démarrez le serveur de clés en tapant la commande suivante :

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

5 Déchiffrez et stockez la clé secrète.

En général, le mot de passe de connexion est identique au mot de passe réseau. Dans cette situation, `keylogin` n'est pas nécessaire. Si les mots de passe sont différents, les utilisateurs doivent se connecter, puis exécuter `keylogin`. Vous avez toujours besoin d'utiliser la commande `keylogin -r` en tant que `root` pour stocker la clé secrète déchiffrée dans `/etc/.rootkey`.

Remarque – Vous devez exécuter `keylogin -r` si la clé secrète root est modifiée ou si `/etc/.rootkey` est perdu.

---

6 Mettez à jour les options de montage pour le système de fichiers.

Pour l'authentification Diffie-Hellman, modifiez le fichier `/etc/dfs/dfstab` et ajoutez l'option `sec=dh` aux entrées appropriées.

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

Reportez-vous à la page de manuel `dfstab(4)` pour obtenir une description de `/etc/dfs/dfstab`.

7 Mettez à jour les mappages de montage automatique pour le système de fichiers.

Modifiez les données `auto_master` pour inclure `sec=dh` en tant qu'option de montage dans les entrées appropriées pour l'authentification Diffie-Hellman :

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

Remarque – Les versions utilisant Solaris 2.5 présentent une limitation. Si un client ne monte pas de manière sécurisée un système de fichiers partagé qui est sécurisé, les utilisateurs ont accès en tant qu'utilisateurs `nobody` plutôt que comme eux-mêmes. Pour les versions ultérieures qui utilisent la version 2, le serveur NFS refuse l'accès si les modes de sécurité ne correspondent pas, sauf si `-sec=none` est inclus dans la ligne de commande `share`. Avec la version 3, le mode est hérité du serveur NFS, de sorte que les clients n'ont pas besoin de spécifier `sec=dh`. Les utilisateurs ont accès aux fichiers en tant qu'eux-mêmes.

Lorsque vous réinstallez, déplacez ou mettez à niveau un ordinateur, n'oubliez pas d'enregistrer `/etc/.rootkey` si vous ne définissez pas de nouvelles clés ou modifiez les clés pour `root`. Si vous supprimez `/etc/.rootkey`, vous pouvez toujours entrer les éléments suivants :

```
# keylogin -r
```

Tâches d'administration WebNFS

Cette section fournit des instructions pour l'administration du système WebNFS. Les tâches connexes sont indiquées ci-après.

TABLEAU 5–4 Liste des tâches pour l'administration WebNFS

Tâche	Description	Voir
Planification pour WebNFS	Points à prendre en considération avant d'activer le service WebNFS.	"Planification de l'accès WebNFS" à la page 104
Activation de WebNFS	Procédure d'activation du montage d'un système de fichiers NFS à l'aide du protocole WebNFS.	"Activation de l'accès WebNFS" à la page 88
Activation de WebNFS par le biais d'un pare-feu	Procédure d'autorisation de l'accès aux fichiers par le biais d'un pare-feu en utilisant le protocole WebNFS.	"Activation de l'accès WebNFS par le biais d'un pare-feu" à la page 106
Navigation à l'aide d'un URL NFS	Instructions d'utilisation d'un URL NFS au sein d'un navigateur Web.	"Navigation à l'aide d'un URL NFS" à la page 105
Utilisation d'un identificateur de fichier public avec autofs	Procédure de forcement de l'utilisation du gestionnaire de fichiers publics lors du montage d'un système de fichiers avec l'agent de montage automatique.	"Utilisation d'un gestionnaire de fichiers publics avec Autofs" à la page 120
Utilisation d'un URL NFS avec autofs	Procédure d'ajout d'un URL NFS aux mappages de montage automatique.	"Utilisation des URL NFS avec Autofs" à la page 121
Autorisation de l'accès à un système de fichiers par le biais d'un pare-feu	Procédure d'autorisation de l'accès à un système de fichiers par le biais d'un pare-feu à l'aide du protocole WebNFS.	"Montage d'un système de fichiers NFS via un pare-feu" à la page 95
Montage d'un système de fichiers à l'aide d'un URL NFS	Procédure d'autorisation de l'accès à un système de fichiers à l'aide d'un URL NFS. Ce processus permet d'accéder à un système de fichiers sans utiliser le protocole MOUNT.	"Montage d'un système de fichiers NFS à l'aide d'un URL NFS " à la page 95

Planification de l'accès WebNFS

Pour utiliser WebNFS, vous avez d'abord besoin d'une application qui est capable d'exécuter et de charger un URL NFS (par exemple, `nfs://server/chemin`). L'étape suivante consiste à choisir le système de fichiers qui peut être exporté pour l'accès WebNFS. Si l'application est basée sur un navigateur Web, la racine de document pour le serveur Web est souvent utilisée. Vous devez tenir compte de plusieurs facteurs lors de la sélection d'un système de fichiers à exporter pour l'accès WebNFS.

1. Chaque serveur possède un gestionnaire de fichiers publics qui est associé par défaut avec le système de fichiers racine du serveur. Le chemin d'accès dans un URL NFS est évalué par rapport au répertoire auquel le gestionnaire des fichiers publics est associé. Si le chemin

mène à un fichier ou un répertoire au sein d'un système de fichiers exporté, le serveur fournit l'accès. Vous pouvez utiliser l'option `public` de la commande `share` afin d'associer le gestionnaire de fichiers publics à un répertoire exporté. Grâce à cette option, les URL sont relatifs au système de fichiers partagé plutôt qu'au système de fichiers root du serveur. Le système de fichiers root n'autorise pas l'accès au Web à moins que le système de fichiers root ne soit partagé.

2. L'environnement WebNFS permet aux utilisateurs qui ont déjà des privilèges de montage d'accéder aux fichiers par le biais d'un navigateur. Cette fonctionnalité est activée indépendamment du fait que le système de fichiers est exporté à l'aide de l'option `public`. Étant donné que les utilisateurs ont déjà accès à ces fichiers par le biais de la configuration NFS, cet accès ne devrait pas créer de risque de sécurité supplémentaire. Vous avez uniquement besoin de partager un système de fichiers en utilisant l'option `public` si les utilisateurs qui ne peuvent pas monter le système de fichiers doivent utiliser l'accès WebNFS.
3. L'option `public` peut être utilisée par exemple avec les systèmes de fichiers qui sont déjà d'accès public. Il peut s'agir par exemple du répertoire supérieur d'une archive ftp ou du répertoire d'URL principal d'un site Web.
4. Vous pouvez utiliser l'option `index` avec la commande `share` pour forcer le chargement d'un fichier HTML. Sinon, vous pouvez lister le répertoire lorsqu'un URL NFS est accessible.

   Après avoir choisi un système de fichiers, passez en revue les fichiers et définissez des droits d'accès pour restreindre la visualisation des fichiers ou répertoires, selon les besoins. Définissez les droits, le cas échéant, pour n'importe quel système de fichiers NFS qui est partagé. Pour de nombreux sites, les droits d'accès `755` et `644` fournissent le niveau d'accès approprié pour les répertoires et les fichiers, respectivement.

   Vous devez tenir compte d'autres facteurs si des URL NFS et HTTP doivent être utilisés pour accéder à un site Web. Ces facteurs sont décrits dans la section "Restrictions WebNFS liées à l'utilisation de navigateur Web" à la page 202.

Navigation à l'aide d'un URL NFS

Les navigateurs qui sont capables de prendre en charge le service WebNFS doivent fournir l'accès à un URL NFS qui ressemble au suivant :

`nfs://`*server*`<:`*port*`>/`*path*

server	Nom du serveur de fichiers
port	Numéro de port à utiliser (`2049`, valeur par défaut)
path	Chemin d'accès du fichier, qui peut être relatif au gestionnaire de fichiers publics ou au système de fichiers root

Remarque – Dans la plupart des navigateurs, le type de service URL (par exemple, `nfs` ou `http`) est mémorisé d'une transaction à l'autre. L'exception se produit lorsqu'un URL qui inclut un autre type de service est chargé. Une fois que vous avez utilisé un URL NFS, une référence à un URL HTTP peut être chargée. Si une telle référence est chargée, les pages suivantes sont chargées en utilisant le protocole HTTP au lieu du protocole NFS.

Activation de l'accès WebNFS par le biais d'un pare-feu

Vous pouvez activer l'accès WebNFS pour les clients qui ne font pas partie du sous-réseau local en configurant le pare-feu pour permettre une connexion TCP sur le port `2049`. L'autorisation de l'accès pour `httpd` ne suffit pas à autoriser l'utilisation des URL NFS.

Présentation des tâches d'administration Autofs

Cette section décrit plusieurs tâches courantes que vous êtes susceptible de rencontrer dans votre propre environnement. Chaque scénario inclut des procédures recommandées pour vous aider à configurer autofs de sorte à répondre aux mieux aux besoins de vos clients.

Remarque – À partir de la version Solaris 10, vous pouvez également utiliser le fichier `/etc/default/autofs` pour configurer votre environnement autofs. Pour plus d'informations, reportez-vous à la section "Utilisation du fichier `/etc/default/autofs` pour configurer votre environnement Autofs" à la page 108

Liste des tâches d'administration Autofs

Le tableau ci-après fournit une description et un renvoi vers un grand nombre de tâches qui sont liées à autofs.

TABLEAU 5–5 Liste des tâches d'administration Autofs

Tâche	Description	Voir
Démarrage d'autofs	Démarrage du service de montage automatique sans avoir à réinitialiser le système	"Démarrage de l'agent de montage automatique" à la page 98
Arrêt d'autofs	Arrêt de la commande de montage automatique sans désactiver d'autres services réseau	"Arrêt de l'agent de montage automatique" à la page 98

TABLEAU 5–5 Liste des tâches d'administration Autofs *(Suite)*

Tâche	Description	Voir
Configuration de votre environnement autofs en utilisant le fichier `/etc/default/autofs`	Affectation de valeurs aux mots-clés dans le fichier `/etc/default/autofs`	"Utilisation du fichier `/etc/default/autofs` pour configurer votre environnement Autofs" à la page 108
Accès aux systèmes de fichiers en utilisant autofs	Accès aux systèmes de fichiers à l'aide du service de montage automatique	"Montage à l'aide de l'agent de montage automatique " à la page 92
Modification des mappages autofs	Procédure de modification du mappage principal, qui doit être utilisé pour indiquer d'autres mappages	"Modification du mappage principal" à la page 110
	Procédure de modification d'un mappage indirect, qui doit être utilisé pour la plupart des mappages	"Modification des mappages indirects" à la page 111
	Procédure de modification d'un mappage direct, qui doit être utilisé lorsqu'une association directe entre un point de montage sur un client et un serveur est nécessaire	"Modification des mappages directs" à la page 111
Modification des mappages autofs pour accéder aux systèmes de fichiers autre que NFS	Procédure de configuration d'un mappage autofs avec une entrée pour une application CD-ROM	"Accès aux applications de CD-ROM avec Autofs" à la page 112
	Procédure de configuration d'un mappage autofs avec une entrée pour une disquette PC-DOS	"Accès aux disquettes de données PC-DOS avec Autofs" à la page 113
	Procédure d'utilisation d'autofs pour accéder à un système de fichiers CacheFS	"Accès aux systèmes de fichiers NFS à l'aide de CacheFS" à la page 114
Utilisation de `/home`	Exemple de configuration d'un mappage `/home` standard	"Configuration d'une vue commune de `/home` " à la page 115
	Procédure de configuration d'un mappage `/home` qui fait référence à plusieurs systèmes de fichiers	"Configuration de `/home` avec plusieurs systèmes de fichiers de répertoires personnels" à la page 115
Utilisation d'un nouveau point de montage autofs	Procédure de configuration d'un mappage autofs lié à un projet	"Consolidation des fichiers associés au projet sous `/ws` " à la page 116
	Procédure de configuration d'un mappage autofs qui prend en charge des architectures client différentes	"Définition d'architectures différentes pour accéder à un espace de noms partagé" à la page 118
	Procédure de configuration d'un mappage autofs qui prend en charge des systèmes d'exploitation différents	"Prise en charge de versions de systèmes d'exploitation client incompatibles" à la page 119
Réplication des systèmes de fichiers avec autofs	Fourniture de l'accès aux systèmes de fichiers qui basculent	"Réplication des fichiers partagés sur plusieurs serveurs" à la page 119

TABLEAU 5–5 Liste des tâches d'administration Autofs *(Suite)*

Tâche	Description	Voir
Utilisation des restrictions en matière de sécurité avec autofs	Fourniture de l'accès aux systèmes de fichiers tout en limitant l'accès `root` à distance aux fichiers	"Application des restrictions de sécurité Autofs" à la page 120
Utilisation d'un gestionnaire de fichiers publics avec autofs	Forcement de l'utilisation du gestionnaire de fichiers publics lors du montage d'un système de fichiers	"Utilisation d'un gestionnaire de fichiers publics avec Autofs" à la page 120
Utilisation d'un URL NFS avec autofs	Ajout d'un URL NFS que l'agent de montage automatique peut utiliser	"Utilisation des URL NFS avec Autofs" à la page 121
Désactivation de la navigabilité autofs	Procédure de désactivation de la navigabilité afin que les points de montage autofs ne soient pas automatiquement remplis sur un seul client	"Désactivation complète de la navigabilité Autofs sur un seul client NFS" à la page 121
	Procédure de désactivation de la navigabilité afin que les points de montage autofs ne soient pas automatiquement remplis sur tous les clients	"Désactivation de la navigabilité Autofs pour tous les clients" à la page 122
	Procédure de désactivation de la navigabilité afin qu'un point de montage autofs spécifique ne soit pas automatiquement rempli sur un client	"Désactivation de la navigabilité Autofs sur un système de fichiers sélectionné" à la page 122

Utilisation du fichier `/etc/default/autofs` pour configurer votre environnement Autofs

À partir de la version Solaris 10, vous pouvez utiliser le fichier `/etc/default/autofs` pour configurer votre environnement autofs. Plus précisément, ce fichier fournit un moyen supplémentaire pour configurer les commandes et démons autofs. Vous pouvez définir dans ce nouveau fichier de configuration les spécifications que vous définiriez sur la ligne de commande. Vous pouvez effectuer vos spécifications en affectant des valeurs à des mots-clés. Pour plus d'informations, reportez-vous à la section "Fichier `/etc/default/autofs`" à la page 141.

La procédure suivante vous indique comment utiliser le fichier `/etc/default/autofs`.

▼ Configuration de votre environnement Autofs à l'aide du fichier `/etc/default/autofs`

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez ou modifiez une entrée dans le fichier `/etc/default/autofs`.**

Par exemple, si vous souhaitez désactiver la navigation pour tous les points de montage autofs, vous pouvez ajouter la ligne suivante.

```
AUTOMOUNTD_NOBROWSE=ON
```

Ce mot-clé est l'équivalent de l'argument `-n` pour `automountd`. Pour obtenir la liste des mots-clés, reportez-vous à la section "Fichier `/etc/default/autofs`" à la page 141.

3 **Redémarrez le démon autofs.**

Tapez la commande suivante\~:

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

Tâches administratives impliquant des mappages

Les tableaux ci-dessous présentent plusieurs des facteurs que vous avez besoin de connaître lors de l'administration des mappages autofs. Votre choix de mappage et de service de noms a une incidence sur le mécanisme que vous avez besoin d'utiliser pour apporter des modifications aux mappages autofs.

Le tableau ci-après décrit les types de mappages et leurs utilisations.

TABLEAU 5–6 Types de mappage autofs et leurs utilisations

Type de mappage	Utilisation
Principal	Associe un répertoire à un mappage
Direct	Dirige autofs vers des systèmes de fichiers spécifiques
Indirect	Dirige autofs vers des systèmes de fichiers orientés références

Le tableau ci-après décrit comment apporter des modifications à votre environnement autofs qui sont basées sur votre service de noms.

TABLEAU 5–7 Maintenance des mappages

Service de noms	Méthode
Fichiers locaux	Éditeur de texte
NIS	Fichiers `make`
NIS+	`nistbladm`

Le tableau suivant indique quand exécuter la commande `automount` , selon la modification que vous avez apportée au type de mappage. Par exemple, si vous avez effectué un ajout ou une

suppression d'un mappage direct, vous devez exécuter la commande `automount` sur le système local. En exécutant la commande, la modification est prise en compte. Toutefois, si vous avez modifié une entrée existante, vous n'avez pas besoin d'exécuter la commande `automount` pour que la modification soit prise en compte.

TABLEAU 5–8 Quand exécuter la commande `automount`

Type de mappage	Redémarrer `automount` ?	
	Ajout ou suppression	Modification
`auto_master`	Y	Y
`direct`	Y	N
`indirect`	N	N

Modification des mappages

Les procédures suivantes exigent que vous utilisiez NIS+ comme service de noms.

▼ Modification du mappage principal

1. **Connectez-vous en tant qu'utilisateur disposant des autorisations de modifier les mappages.**
2. **À l'aide de la commande `nistbladm`, , apportez vos modifications au mappage principal.**

   Reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)*.
3. **Pour chaque client, connectez-vous en tant que superutilisateur ou un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.
4. **Pour chaque client, exécutez la commande `automount` pour vous assurer que vos modifications seront appliquées.**
5. **Informez vos utilisateurs des modifications.**

   La notification est nécessaire pour que les utilisateurs puissent également exécuter la commande `automount` en tant que superutilisateur sur leurs propres ordinateurs. Notez que la commande `automount` rassemble des informations à partir du mappage principal chaque fois qu'elle est exécutée.

▼ Modification des mappages indirects

1. **Connectez-vous en tant qu'utilisateur disposant des autorisations de modifier les mappages.**
2. **À l'aide de la commande `nistbladm`, apportez vos modifications au mappage indirect.**

   Reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)*. Notez que la modification entre en vigueur à la prochaine utilisation du mappage, c'est-à-dire au prochain montage.

▼ Modification des mappages directs

1. **Connectez-vous en tant qu'utilisateur disposant des autorisations de modifier les mappages.**
2. **À l'aide de la commande `nistbladm`,, ajoutez ou supprimez les modifications du mappage direct.**

   Reportez-vous au *System Administration Guide: Naming and Directory Services (NIS+)*.
3. **Informez vos utilisateurs des modifications.**

   La notification est nécessaire pour que les utilisateurs puissent exécuter la commande `automount` en tant que superutilisateur sur leur propre ordinateur, si nécessaire.

Remarque – Si vous modifiez uniquement le contenu d'une entrée de mappage direct existante, vous n'avez pas besoin d'exécuter la commande `automount`.

Par exemple, supposons que vous modifiez le mappage `auto_direct` afin que le répertoire `/usr/src` soit maintenant monté à partir d'un autre serveur. Si `/usr/src` n'est pas monté à ce moment-là, la nouvelle entrée entre en vigueur immédiatement lorsque vous tentez d'accéder à `/usr/src`. Si `/usr/src` est monté maintenant, vous pouvez attendre jusqu'à ce que le démontage automatique se produise, puis accédez au fichier.

Remarque – Utilisez les mappages indirects chaque fois que cela est possible. Les mappages indirects sont plus faciles à construire et sollicitent moins les systèmes de fichiers des ordinateurs. En outre, les mappages indirects n'occupent pas autant d'espace dans la table de montage que les mappages directs.

Éviter les conflits de point de montage

Si vous disposez d'une partition de disque locale qui est montée sur un `/src` et que vous prévoyez d'utiliser le service autofs pour monter d'autres répertoires source, un problème peut survenir. Si vous spécifiez le point de montage `/src`, le service NFS masque la partition locale chaque fois que vous essayez de l'atteindre.

Vous devez monter la partition dans un autre emplacement, par exemple, sur `/export/src`. Vous devez ensuite ajouter une entrée telle que la suivante dans `/etc/vfstab` :

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

Vous devez également ajouter cette entrée dans `auto_src` :

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

`terra` est le nom de l'ordinateur.

Accès aux systèmes de fichiers autres que NFS

Autofs peut également monter des fichiers autres que des fichiers NFS. Autofs monte les fichiers sur des médias amovibles, tels que des disquettes ou des CD-ROM. Normalement, vous montez les fichiers sur des médias amovibles en utilisant le gestionnaire de volumes. Les exemples suivants montrent comment ce montage peut être réalisé par l'intermédiaire d'autofs. Le gestionnaire de volumes et autofs ne peuvent pas fonctionner conjointement. Ces entrées ne peuvent donc être utilisées sans la désactivation préalable du gestionnaire de volumes.

Au lieu de monter un système de fichiers à partir d'un serveur, vous placez le média dans l'unité de disque et faites référence au système de fichiers à partir du mappage. Si vous avez l'intention d'accéder à des systèmes de fichiers autres que NFS et que vous utilisez autofs, reportez-vous aux procédures suivantes.

▼ Accès aux applications de CD-ROM avec Autofs

Remarque – Utilisez cette procédure si vous n'utilisez *pas* le gestionnaire de volumes.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Mettez à jour le mappage autofs.**

Ajoutez une entrée pour le système de fichiers de CD-ROM, qui doit présenter la forme suivante :

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

Le périphérique de CD-ROM que vous avez l'intention de monter doit apparaître sous forme de nom après le signe deux-points.

▼ Accès aux disquettes de données PC-DOS avec Autofs

Remarque – Utilisez cette procédure si vous n'utilisez *pas* le gestionnaire de volumes.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Mettez à jour le mappage autofs.**

Ajoutez une entrée pour le système de fichiers de disquette comme dans l'exemple suivant :

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

Accès aux systèmes de fichiers NFS à l'aide de CacheFS

Le système de fichiers de cache (CacheFS) est un mécanisme de mise en cache générique non volatile. CacheFS améliore la performance de certains systèmes de fichiers par l'utilisation d'un petit disque local rapide. Par exemple, vous pouvez améliorer les performances de l'environnement NFS en utilisant CacheFS.

CacheFS fonctionne différemment selon les versions de NFS. Par exemple, si le client et le système de fichiers d'arrière-plan exécutent la version 2 ou la version 3 de NFS, les fichiers sont mis en cache dans le système de fichiers de premier plan auquel le client peut accéder. Toutefois, si le client et le serveur exécutent la version 4 de NFS, cette fonction est la suivante. Lorsque le client effectue la demande initiale d'accès à un fichier à partir d'un système de fichiers CacheFS, la demande n'est pas adressée au système de fichiers de premier plan (ou mis en cache) et accède directement au système de fichiers d'arrière-plan. Avec la version 4 de NFS, les fichiers ne sont plus mis en cache dans le système de fichiers de premier plan. Tous les accès aux fichiers sont fournis par le système de fichiers d'arrière-plan. De même, aucun fichier n'étant mis en cache dans le système de fichiers de premier plan, les options de montage spécifiques de CacheFS, qui doivent normalement s'appliquer au système de fichiers de premier plan, ne sont pas prises en compte. Les options de montage spécifiques de CacheFS ne s'appliquent pas au système de fichiers d'arrière-plan.

Remarque – La première fois que vous configurez votre système pour la version 4 de NFS, un message d'avertissement apparaît sur la console vous indiquant que la mise en cache n'est plus effectuée.

▼ Accès aux systèmes de fichiers NFS à l'aide de CacheFS

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Exécutez la commande `cfsadmin` pour créer un répertoire de cache sur le disque local.**

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

3 **Ajoutez l'entrée `cachefs` au mappage de montage automatique approprié.**

Par exemple, l'ajout de cette entrée au mappage principal met en cache les répertoires personnels :

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

L'ajout de cette entrée au mappage `auto_home` met en cache uniquement le répertoire personnel de l'utilisateur qui est nommé `rich` :

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

Remarque – Les options étant incluses dans les mappages qui font l'objet de recherches par la suite remplacent les options définies dans les mappages qui font l'objet de recherches antérieurement. Les options utilisées sont les dernières trouvées. Dans l'exemple précédent, une entrée supplémentaire dans le mappage `auto_home` a besoin d'inclure uniquement les options dans les mappages principaux si certaines options ont nécessité des modifications.

Personnalisation de l'agent de montage automatique

Vous pouvez configurer les mappages de montage automatique de plusieurs façons. Les tâches suivantes fournissent des détails sur la manière de personnaliser les mappages de montage automatique afin de fournir une structure de répertoire facile à utiliser.

Configuration d'une vue commune de /home

Idéalement, tous les utilisateurs du réseau doivent être en mesure de localiser leur propre répertoire personnel ou celui de tout utilisateur sous /home. Cette vue doit être commune à tous les ordinateurs, qu'il s'agisse de clients ou de serveurs.

Chaque installation de Solaris inclut un mappage principal : /etc/auto_master.

```
# Master map for autofs
#
+auto_master
/net     -hosts     -nosuid,nobrowse
/home    auto_home  -nobrowse
```

Un mappage pour auto_home est également installé sous /etc.

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

À l'exception d'une référence à un mappage auto_home externe, ce mappage est vide. Si les répertoires sous /home doivent être communs à tous les ordinateurs, ne modifiez pas ce mappage /etc/auto_home. Toutes les entrées du répertoire personnel doivent apparaître dans les fichiers de service de noms, à savoir NIS ou NIS+.

Remarque – Les utilisateurs ne doivent pas être autorisés à exécuter les exécutables setuid à partir de leurs répertoires personnels. Sans cette restriction, tous les utilisateurs pourraient disposer de privilèges de superutilisateur sur tout ordinateur.

▼ Configuration de /home avec plusieurs systèmes de fichiers de répertoires personnels

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Installez les partitions du serveur d'annuaire personnel sous /export/Home.**

   Si le système dispose de plusieurs partitions, installez-les dans des répertoires différents, par exemple, /export/home1 et /export/home2.

3 Utilisez les outils de la console de gestion Solaris afin de créer et de gérer le mappage `auto_home` .

Chaque fois que vous créez un compte utilisateur, tapez l'emplacement du répertoire personnel de l'utilisateur dans le mappage `auto_home`. Les entrées de mappage peuvent être simples, par exemple :

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

Notez l'emploi de l'esperluette (`&`) afin de remplacer la clé de mappage. L'esperluette est l'abréviation de la seconde occurrence de `rusty` dans l'exemple suivant.

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

Une fois le mappage `auto_home` en place, les utilisateurs peuvent faire référence à n'importe quel répertoire personnel (y compris les leurs) avec le chemin `/home/`*user*. *user* est leur nom de connexion et la clé dans le mappage. Cette vue commune de tous les répertoires personnels est utile lors de la connexion à l'ordinateur d'un autre utilisateur. Autofs monte votre répertoire personnel pour vous. De la même façon, si vous exécutez un client système de multifenêtrage distant sur un autre ordinateur, le programme client dispose de la même vue du répertoire `/home`.

Cette vue commune s'étend également au serveur. Dans l'exemple précédent, si `rusty` se connecte au serveur `dragon`, autofs offre ici un accès direct au disque local par le biais du montage loopback de `/export/home1/rusty` sur `/home/rusty`.

Les utilisateurs n'ont pas besoin de connaître l'emplacement réel de leurs répertoires personnels. Si `rusty` nécessite plus d'espace disque et la relocalisation de son répertoire personnel sur un autre serveur, une simple modification suffit. Il vous suffit de modifier l'entrée de `rusty` dans le mappage `auto_home` pour refléter le nouvel emplacement. D'autres utilisateurs peuvent continuer d'utiliser le chemin d'accès `/home/rusty`.

▼ Consolidation des fichiers associés au projet sous `/ws`

Supposez que vous êtes l'administrateur d'un projet de développement logiciel volumineux. Vous avez l'intention de rendre tous les fichiers associés au projet disponibles sous un répertoire nommé `/ws`. Ce répertoire doit être commun à tous les postes de travail au niveau du site.

1 Ajoutez une entrée pour le répertoire `/ws` au mappage `auto_master`, à savoir NIS ou NIS+.

```
/ws     auto_ws     -nosuid
```

Le mappage `auto_ws` détermine le contenu du répertoire `/ws`.

2 Ajoutez l'option `-nosuid` par mesure de précaution.

Cette option empêche les utilisateurs d'exécuter les programmes setuid qui peuvent exister dans un espace de travail.

3 Ajoutez des entrées au mappage `auto_ws`.

Le mappage `auto_ws` est organisé de telle sorte que chaque entrée décrit un sous-projet. Votre première tentative produit une matrice qui ressemble à la suivante :

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

L'esperluette (&) à la fin de chaque entrée correspond à l'abréviation de la clé d'entrée. Par exemple, l'équivalent de la première entrée se présente comme suit :

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

Cette première tentative génère un mappage qui semble simple mais qui n'est pas approprié. L'organisateur du projet décide que la documentation de l'entrée `man` doit être fournie sous la forme d'un sous-répertoire dans chaque sous-projet. En outre, chaque sous-projet nécessite des sous-répertoires pour décrire plusieurs versions du logiciel. Vous devez attribuer chacun de ces sous-répertoires à l'ensemble d'une partition de disque sur le serveur.

Modifiez les entrées dans le mappage comme suit :

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

Bien que le mappage apparaisse maintenant beaucoup plus volumineux, il ne contient encore que les cinq entrées. Chaque entrée est plus volumineuse car elle contient plusieurs montages. Par exemple, une référence à `/ws/compiler` nécessite trois montages pour les répertoires `vers1.0`, `vers2.0` et `man`. La barre oblique inverse à la fin de chaque ligne informe autofs que l'entrée continue sur la ligne suivante. En réalité, l'entrée est une longue ligne, mais des sauts de ligne et la mise en retrait ont été utilisés pour rendre l'entrée plus lisible. Le répertoire `tools` contient des outils de développement de logiciels pour tous les sous-projets, de sorte que ce répertoire n'est pas soumis à la même structure de sous-répertoires. Le répertoire `tools` continue d'être un seul montage.

Cette disposition offre une grande flexibilité à l'administrateur. Généralement, les projets logiciels consomment une grande quantité d'espace disque. Tout au long de la durée de vie de ce

projet, vous pouvez être amené à déplacer et développer différentes partitions de disque. Si ces modifications sont reflétées dans le mappage `auto_ws`, les utilisateurs n'ont pas besoin d'être informés, dans la mesure où l'arborescence des répertoires sous `/ws` n'a pas été modifiée.

Étant donné que les serveurs `alpha` et `bravo` visualisent le même mappage autofs, tous les utilisateurs qui se connectent à ces ordinateurs peuvent trouver l'espace de noms `/ws` comme prévu. Ces utilisateurs disposent d'un accès direct aux fichiers locaux via des montages loopback au lieu de montages NFS.

▼ Définition d'architectures différentes pour accéder à un espace de noms partagé

Vous devez assembler un espace de noms partagé pour les exécutables locaux, et les applications, telles que les tableurs et les packages de traitement de texte. Les clients de cet espace de noms utilisent différentes architectures de station de travail qui requièrent différents formats exécutables. En outre, certaines stations de travail exécutent des versions différentes du système d'exploitation.

1. **Créez le mappage `auto_local`.**

   Reportez-vous au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

2. **Choisissez un seul nom spécifique à un site pour l'espace de noms partagé.**

   Ce nom permet d'identifier facilement les fichiers et répertoires qui appartiennent à cet espace. Par exemple, si vous choisissez `/usr/local` comme nom, le chemin `/usr/local/bin` fait évidemment partie de cet espace de noms.

3. **Pour faciliter la reconnaissance des utilisateurs, créez un mappage autofs indirect.**

   Montez ce mappage sous `/usr/local`. Configurez l'entrée suivante dans le mappage `auto_master` NIS :

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

   Notez que l'option de montage `-ro` implique que les clients ne peuvent pas écrire dans les fichiers ou répertoires.

4. **Exportez le répertoire approprié sur le serveur.**

5. **Incluez une entrée `bin` dans le mappage auto_local.**

   Votre structure de répertoire ressemble à la structure suivante :

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

6 **(Facultatif) Pour servir les clients de différentes architectures, modifiez l'entrée en ajoutant la variable CPU autofs.**

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

- Pour les clients SPARC : placez les exécutables dans `/export/local/bin/sparc`.
- Pour les clients &ia : placez les exécutables dans `/export/local/bin/i386`.

▼ Prise en charge de versions de systèmes d'exploitation client incompatibles

1 **Combinez le type d'architecture avec une variable qui détermine le type de système d'exploitation du client.**

Vous pouvez combiner la variable `OSREL` autofs avec la variable `CPU` pour former un nom qui détermine le type de CPU et la version du système d'exploitation.

2 **Créez l'entrée de mappage suivante.**

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

Pour les clients qui exécutent la version 5.6 du système d'exploitation, exportez les systèmes de fichiers suivants :

- Pour les clients SPARC : exportez `/export/local/bin/sparc5.6` .
- Pour les clients &ia : placez les exécutables dans `/export/local/bin/i3865.6` .

▼ Réplication des fichiers partagés sur plusieurs serveurs

Le meilleur moyen de partager les systèmes de fichiers répliqués qui sont en lecture seule consiste à utiliser le basculement. Reportez-vous à la section "Basculement côté client" à la page 196 qui aborde le basculement.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez l'entrée dans les mappages autofs.**

Créez la liste de tous les serveurs de réplique sous la forme d'une liste séparée par des virgules, comme suit :

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

Autofs choisit le serveur le plus proche. Si un serveur dispose de plusieurs interfaces réseau, répertoriez chaque interface. Autofs choisit l'interface la plus proche du client, en évitant le routage inutile du trafic NFS.

▼ Application des restrictions de sécurité Autofs

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez l'entrée suivante dans le fichier `auto_master` de service de noms, à savoir NIS ou NIS+ :**

```
/home     auto_home     -nosuid
```

L'option `nosuid` empêche les utilisateurs de créer des fichiers avec l'ensemble binaire `setuid` ou `setgid`.

Cette entrée remplace l'entrée pour `/home` dans un fichier `/etc/auto_master` local générique. Reportez-vous à l'exemple précédent. Le remplacement se produit car la référence `+auto_master` au mappage de service de noms externe apparaît avant l'entrée dans le fichier `/home`. Si les entrées du mappage `auto_home` incluent les options de montage, l'option `nosuid` est écrasée. Par conséquent, aucune des options ne doit être utilisée dans le mappage `auto_home` ou l'option `nosuid` doit être incluse avec chaque entrée.

Remarque – Ne montez pas les partitions de disque de répertoire personnel sur ou sous `/home` sur le serveur.

▼ Utilisation d'un gestionnaire de fichiers publics avec Autofs

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez une entrée dans le mappage autofs telle que la suivante :**

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

L'option `public` force l'utilisation du gestionnaire de fichiers publics. Si le serveur NFS ne prend pas en charge un gestionnaire de fichiers publics, le montage échoue.

▼ Utilisation des URL NFS avec Autofs

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez une entrée autofs , telle que la suivante :**

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

   Le service tente d'utiliser le gestionnaire de fichiers publics sur le serveur NFS. Cependant, si le serveur ne prend pas en charge un gestionnaire de fichiers publics, le protocole MOUNT est utilisé.

Désactivation de la navigabilité Autofs

Pour la version par défaut de `/etc/auto_master` qui est installée, l'option `-nobrowse` est ajoutée aux entrées de `/home` et `/net`. En outre, la procédure de mise à niveau ajoute l'option `-nobrowse` aux entrées `/home` et `/net` dans `/etc/auto_master` si ces entrées n'ont pas été modifiées. Cependant, il se peut que vous ayez à effectuer ces modifications manuellement ou à désactiver la navigabilité pour les points de montage autofs spécifiques à un site après l'installation.

Vous pouvez désactiver la fonction de navigabilité de plusieurs façons. Désactivez la fonction à l'aide d'une option de ligne de commande sur le démon `automountd`, ce qui désactive intégralement la navigabilité autofs pour le client. Vous pouvez également désactiver la navigabilité pour chaque entrée de mappage sur tous les clients à l'aide des mappages autofs dans l'espace de noms NIS ou NIS+. Vous pouvez également désactiver la fonction pour chaque entrée de mappage sur chaque client, à l'aide des mappages autofs locaux si aucun espace de noms à l'échelle du réseau n'est en cours d'utilisation.

▼ Désactivation complète de la navigabilité Autofs sur un seul client NFS

1. **Connectez-vous en tant que superutilisateur ou assumez un rôle équivalent sur le client NFS.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Modifiez le fichier `/etc/default/autofs` afin d'inclure le mot-clé et la valeur suivants.**

   ```
   AUTOMOUNTD_NOBROWSE=TRUE
   ```

3 **Redémarrez le service autofs.**

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

▼ Désactivation de la navigabilité Autofs pour tous les clients

Pour désactiver la navigabilité pour tous les clients, vous devez utiliser un service de noms, tel que NIS ou NIS+. Sinon, vous devez modifier manuellement les mappages de montage automatique sur chaque client. Dans cet exemple, la navigabilité du répertoire `/home` est désactivée. Vous devez suivre cette procédure pour chaque nœud autofs indirect qui doit être désactivé.

1 **Ajoutez l'option `-nobrowse` à l'entrée `/home` dans le fichier `auto_master` de service de noms.**

```
/home     auto_home     -nobrowse
```

2 **Exécutez la commande `automount` sur tous les clients.**

Le nouveau comportement entre en vigueur après que vous avez exécuté la commande `automount` sur les systèmes client ou après une réinitialisation.

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

▼ Désactivation de la navigabilité Autofs sur un système de fichiers sélectionné

Dans cet exemple, la navigabilité du répertoire `/net` est désactivée. Vous pouvez utiliser la même procédure pour `/home` ou n'importe quel autre point de montage autofs.

1 **Vérifiez l'entrée `automount` dans `/etc/nsswitch.conf`.**

Pour que les entrées du fichier local soient prioritaires, l'entrée du fichier de commutation de service de noms doit répertorier `files` avant le service de noms. Par exemple :

```
automount:  files nis
```

Cette entrée indique la configuration par défaut dans une installation standard de Solaris.

2 **Vérifiez la position de l'entrée `+auto_master` dans `/etc/auto_master`.**

Pour que les ajouts aux fichiers locaux soient prioritaires sur les entrées dans l'espace de noms, l'entrée `+auto_master` doit être déplacée à la suite de `/net` :

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

Une configuration standard place l'entrée `+auto_master` au début du fichier. Ce positionnement empêche l'utilisation de toutes les modifications locales.

3 **Ajoutez l'option `nobrowse` à l'entrée `/net` dans le fichier `/etc/auto_master`.**

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

4 **Sur tous les clients, exécutez la commande `automount`.**

Le nouveau comportement entre en vigueur après l'exécution de la commande `automount` sur les systèmes client ou après une réinitialisation.

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

Stratégies de dépannage NFS

Lors du suivi d'un problème NFS, n'oubliez pas les principaux points de panne possible : le serveur, le client et le réseau. La stratégie qui est décrite dans cette section tente d'isoler chaque composant individuel pour trouver celui qui ne fonctionne pas. Dans tous les cas, les démons `mountd` et `nfsd` doivent être en cours d'exécution sur le serveur afin que les montages à distance réussissent.

L'option `-intr` est définie par défaut pour tous les montages. Si un programme ne répond pas tout en affichant un message `server not responding`, vous pouvez interrompre le programme à l'aide de la combinaison de touches Ctrl-C du clavier.

Lorsque le réseau ou le serveur rencontre des problèmes, les programmes qui accèdent à des fichiers distants montés de façon inconditionnelle échouent différemment par rapport aux programmes qui accèdent à des fichiers distants montés de façon conditionnelle. Dans le cas des systèmes de fichiers à distance montés de façon inconditionnelle, le noyau du client tente de nouveau les demandes jusqu'à ce que le serveur réponde à nouveau. Dans le cas des systèmes de fichiers à distance montés de façon conditionnelle, le système du client appelle pour renvoyer une erreur après avoir essayé pendant un certain temps. Étant donné que ces erreurs peuvent entraîner des erreurs d'application inattendues et la corruption des données, il est recommandé d'éviter le montage conditionnel.

Lorsqu'un système de fichiers est monté de façon inconditionnelle, un programme qui tente d'accéder au système de fichiers se bloque si le serveur ne répond pas. Dans cette situation, le système NFS affiche le message suivant sur la console :

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

Lorsque le serveur répond, le message suivant s'affiche sur la console :

```
NFS server hostname ok
```

Un programme qui accède à un système de fichiers monté de façon conditionnelle dont le serveur ne répond pas génère le message suivant :

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

Remarque – En raison des erreurs éventuelles, ne montez pas de manière conditionnelle des systèmes de fichiers contenant des données accessibles en lecture-écriture ou des systèmes de fichiers à partir desquels des exécutables sont exécutés. Les données accessibles en écriture peuvent être corrompues si l'application ignore les erreurs. Les exécutables montés peuvent ne pas se charger correctement et échouer.

Procédures de dépannage NFS

Vous devez suivre plusieurs procédures afin d'identifier la panne subie par le service NFS. Vérifiez les éléments suivants :

- Le client peut-il atteindre le serveur ?
- Le client peut-il contacter les services NFS sur le serveur ?
- Les services NFS sont-ils en cours d'exécution sur le serveur ?

Dans le processus de contrôle de ces éléments, vous remarquerez peut-être que d'autres parties du réseau ne fonctionnent pas. Par exemple, le service de noms ou le matériel réseau physique peut ne pas fonctionner. Le *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* contient des procédures de débogage pour plusieurs services de noms. En outre, pendant le processus, vous pouvez constater que le client n'est pas à l'origine du problème. Supposons par exemple que vous obteniez au moins un appel de dépannage de chaque sous-réseau de votre zone de travail. Dans cette situation, vous devez supposer que le problème vient du serveur ou du matériel réseau situé près du serveur. Par conséquent, nous vous recommandons de démarrer le processus de débogage sur le serveur, et non au niveau du client.

▼ Vérification de la connectivité sur un client NFS

1 Vérifiez que le serveur NFS est accessible à partir du client. Sur le client, tapez la commande suivante :

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

Si la commande signale que le serveur est actif, vérifiez à distance le serveur NFS. Reportez-vous à la section "Vérification du serveur NFS à distance " à la page 125.

2 Si le serveur n'est pas accessible à partir du client, assurez-vous que le service de noms local est en cours d'exécution.

Pour les clients NIS+, tapez la commande suivante :

```
% /usr/lib/nis/nisping -u
Last updates for directory eng.acme.com. :
```

```
Master server is eng-master.acme.com.
        Last update occurred at Mon Jun  5 11:16:10 1995

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

3 **Si le service de noms est en cours d'exécution, vérifiez que le client a reçu les informations d'hôte correctes en tapant la commande suivante :**

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

4 **Si les informations d'hôte sont correctes, mais que le serveur n'est pas accessible à partir du client, exécutez la commande `ping` à partir d'un autre client.**

Si l'exécution de la commande à partir d'un deuxième client échoue, reportez-vous à la section “Vérification du service NFS sur le serveur” à la page 127.

5 **Si le serveur est accessible à partir du second client, utilisez la commande `ping` pour vérifier la connectivité du premier client à d'autres systèmes sur le réseau local.**

Si cette commande échoue, vérifiez la configuration du logiciel de gestion de réseau sur le client, par exemple, `/etc/netmasks` et `/etc/nsswitch.conf`.

6 **(Facultatif) Vérifiez la sortie de la commande `rpcinfo`.**

Si la commande `rpcinfo` n'affiche pas `program 100003 version 4 ready and waiting`, la version 4 de NFS n'est pas activée sur le serveur. Pour plus d'informations sur l'activation de la version 4 de NFS, reportez-vous au Tableau 5–3.

7 **Si le logiciel est correct, vérifiez le matériel réseau.**

Essayez de déplacer le client sur un second point de connexion réseau.

▼ Vérification du serveur NFS à distance

Notez que la prise en charge des protocoles UDP et MOUNT n'est pas nécessaire si vous utilisez un serveur de la version 4 de NFS.

1 **Vérifiez que les services NFS ont démarré sur le serveur NFS en tapant la commande suivante :**

```
% rpcinfo -s bee|egrep 'nfs|mountd'
 100003  3,2    tcp,udp,tcp6,upd6               nfs     superuser
 100005  3,2,1  ticots,ticotsord,tcp,tcp6,ticlts,udp,upd6  mountd  superuser
```

Si les démons n'ont pas été démarrés, reportez-vous à la section “Redémarrage des services NFS ” à la page 128.

2 Vérifiez que les processus `nfsd` du serveur répondent.

Sur le client, saisissez la commande suivante pour tester les connexions NFS UDP à partir du serveur.

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

Remarque – La version 4 de NFS ne prend pas en charge UDP.

Si le serveur est en cours d'exécution, il imprime une liste des numéros de programme et de version. À l'aide de l'option `-t`, testez la connexion TCP. Si cette commande échoue, passez à la section "Vérification du service NFS sur le serveur" à la page 127.

3 Vérifiez que le démon `mountd` du serveur répond en entrant la commande suivante.

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

Si le serveur est en cours d'exécution, il imprime une liste de numéros de programme et de version qui sont associés au protocole UDP. À l'aide de l'option `-t`, testez la connexion TCP. Si chaque tentative échoue, passez à la section "Vérification du service NFS sur le serveur" à la page 127.

4 Vérifiez que le service autofs local est en cours d'utilisation :

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

Choisissez un point de montage `/net` ou `/home` dont vous savez qu'il devrait fonctionner correctement. Si cette commande échoue, en tant qu'utilisateur `root` sur le client, saisissez la commande suivante pour redémarrer le service autofs :

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

5 Vérifiez que le système de fichiers est partagé comme prévu sur le serveur.

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

Vérifiez si l'entrée sur le serveur et l'entrée de montage local contiennent des erreurs. Vérifiez également l'espace de noms. Dans cet exemple, si le premier client n'est pas dans le groupe réseau `eng`, ce client ne peut pas monter le système de fichiers `/usr/src`.

Vérifiez toutes les entrées qui contiennent des informations de montage dans tous les fichiers locaux. La liste inclut `/etc/vfstab` et tous les fichiers `/etc/auto_*`.

▼ Vérification du service NFS sur le serveur

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Vérifiez que le serveur peut atteindre les clients.**

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

3. **Si le client n'est pas accessible à partir du serveur, assurez-vous que le service de noms local est en cours d'exécution.**

   Pour les clients NIS+, tapez la commande suivante :

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

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

4. **Si le service de noms est en cours d'exécution, vérifiez la configuration logicielle réseau sur le serveur, par exemple, `/etc/netmasks` et `/etc/nsswitch.conf`.**

5. **Tapez la commande suivante pour vérifier si le démon `rpcbind` est en cours d'exécution.**

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

   Si le serveur est en cours d'exécution, il imprime une liste des numéros de programme et de version qui sont associés au protocole UDP. Si `rpcbind` semble être bloqué, redémarrez le serveur.

6. **Tapez la commande suivante pour vérifier si le démon `nfsd` est en cours d'exécution.**

```
# rpcinfo -u localhost nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
# ps -ef | grep nfsd
root    232      1  0  Apr 07     ?     0:01 /usr/lib/nfs/nfsd -a 16
root   3127   2462  1  09:32:57  pts/3  0:00 grep nfsd
```

Remarque – La version 4 de NFS ne prend pas en charge UDP.

Si le serveur est en cours d'exécution, il imprime une liste de numéros de programme et de version qui sont associés au protocole UDP. Utilisez également l'option `-t` avec `rpcinfo` pour

vérifier la connexion TCP. Si ces commandes échouent, redémarrez le service NFS. Reportez-vous à la section “Redémarrage des services NFS ” à la page 128.

7 Tapez la commande suivante pour vérifier si le démon `mountd` est en cours d'exécution.

```
# /usr/bin/rpcinfo -u localhost mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
# ps -ef | grep mountd
root    145      1 0 Apr 07  ?     21:57 /usr/lib/autofs/automountd
root    234      1 0 Apr 07  ?     0:04  /usr/lib/nfs/mountd
root   3084 2462 1 09:30:20 pts/3  0:00  grep mountd
```

Si le serveur est en cours d'exécution, il imprime une liste de numéros de programme et de version qui sont associés au protocole UDP. Utilisez également l'option `-t` avec `rpcinfo` pour vérifier la connexion TCP. Si ces commandes échouent, redémarrez le service NFS. Reportez-vous à la section “Redémarrage des services NFS ” à la page 128.

▼ Redémarrage des services NFS

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2 Redémarrez le service NFS sur le serveur.

Saisissez la commande suivante :

```
# svcadm restart network/nfs/server
```

Identification de l'hôte fournissant le service de fichiers NFS

Exécutez la commande `nfsstat` avec l'option `-m` pour rassembler les informations NFS actuelles. Le nom du serveur actuel est imprimé après « `currserver=` ».

```
% nfsstat -m
/usr/local from bee,wasp:/export/share/local
 Flags: vers=3,proto=tcp,sec=sys,hard,intr,llock,link,synlink,
        acl,rsize=32768,wsize=32678,retrans=5
 Failover: noresponse=0, failover=0, remap=0, currserver=bee
```

▼ Vérification des options utilisées avec les commandes `mount`

Aucun avertissement n'est émis pour les options non valides. La procédure suivante vous permet de déterminer si les options qui ont été indiquées sur la ligne de commande ou via `/etc/vfstab` étaient valides.

Pour cet exemple, supposons que la commande suivante a été exécutée :

```
# mount -F nfs -o ro,vers=2 bee:/export/share/local /mnt
```

1 Vérifiez les options en exécutant la commande suivante.

```
% nfsstat -m
/mnt from bee:/export/share/local
Flags:  vers=2,proto=tcp,sec=sys,hard,intr,dynamic,acl,rsize=8192,wsize=8192,
        retrans=5
```

Le système de fichiers de bee a été monté à l'aide de la version de protocole définie sur 2. Malheureusement, la commande `nfsstat` n'affiche pas d'informations sur toutes les options. Cependant, la commande `nfsstat` est le moyen le plus précis de vérifier les options.

2 Vérifiez l'entrée dans `/etc/mnttab`.

La commande `mount` n'autorise pas l'ajout d'options non valides à la table de montage. Par conséquent, vous devez vérifier que les options qui sont répertoriées dans le fichier correspondent à celles présentées dans la ligne de commande. De cette façon, vous pouvez vérifier les options qui ne sont pas répertoriées par la commande `nfsstat`.

```
# grep bee /etc/mnttab
bee:/export/share/local /mnt nfs    ro,vers=2,dev=2b0005e 859934818
```

Dépannage d'Autofs

Occasionnellement, vous risquez de rencontrer des problèmes avec autofs. Cette section doit permettre d'améliorer la résolution de problèmes. Elle est divisée en deux sous-sections.

Cette section présente une liste des messages d'erreur qu'autofs génère. La liste est divisée en deux parties :

- Messages d'erreur générés par l'option détaillée (`-v`) de `automount`
- Messages d'erreur qui peuvent s'afficher à tout moment

Chaque message d'erreur est suivi d'une description et de la cause probable du message.

Lors du dépannage, démarrez les programmes autofs avec l'option détaillée (`-v`). Sinon, vous risquez de rencontrer des problèmes sans en connaître la cause.

Les paragraphes suivant présentent les messages d'erreur que vous êtes susceptibles de voir si autofs échoue, et une description du problème éventuel.

Messages d'erreur générés par `automount -v`

`bad key` *key* `in direct map` *mapname*
Description : Lors de l'analyse d'un mappage direct, autofs a trouvé une clé d'entrée sans préfixe /.

Solution : Dans les mappages directs, les clés doivent être des chemins d'accès complets.

`bad key` *key* `in indirect map` *mapname*
Description : Lors de l'analyse d'un mappage indirect, autofs a trouvé une clé d'entrée qui contient une barre oblique (`/`).

Solution : Les clés de mappage indirect doivent être des noms simples, et non des chemins.

`can't mount` *server*`:`*pathname: reason*
Description : Le démon de montage sur le serveur refuse de fournir un gestionnaire de fichiers pour *server*:*pathname*.

Solution : Vérifiez la table d'exportation sur le serveur.

`couldn't create mount point` *mountpoint*`:` *reason*
Description : Autofs n'a pas été en mesure de créer un point de montage qui était nécessaire pour un montage. Ce problème se produit le plus souvent lorsque vous tentez de monter de manière hiérarchique tous les systèmes de fichiers exportés d'un serveur.

Solution : Un point de montage requis ne peut exister que dans un système de fichiers qui ne peut pas être monté, ce qui signifie que le système de fichiers ne peut pas être exporté. Le point de montage ne peut pas être créé, car le système de fichiers parent exporté est exporté en lecture seule.

`leading space in map entry` *entry* `text in` *mapname*
Description : Autofs a découvert une entrée dans un mappage de montage automatique qui contient des espaces de début. Ce problème indique généralement une entrée de mappage qui n'est pas continuée correctement. Exemple :

```
fake
/blat          frobz:/usr/frotz
```

Solution : Dans cet exemple, le message d'avertissement est généré lorsqu'autofs détecte la deuxième ligne car la première ligne doit se terminer par une barre oblique inverse (\).

mapname`: Not found`
Description : Le mappage ne peut pas être localisé. Ce message est généré uniquement lorsque l'option `-v` est utilisée.

Solution : Vérifiez l'orthographe et le chemin d'accès du nom du mappage.

`remount` *server*`:`*pathname* `on` *mountpoint* `: server not responding`
Description : Autofs n'a pas réussi à remonter un système de fichiers précédemment démonté.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

`WARNING:` *mountpoint* `already mounted on`
Description : AutoFS tente de monter par-dessus un point de montage existant. Ce message signifie qu'une erreur interne s'est produite dans autofs (une anomalie).

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

Messages d'erreur divers

`dir` *mountpoint* `must start with '/'`
Solution : Le point de montage automatique doit être indiqué sous la forme d'un chemin d'accès complet. Vérifiez l'orthographe et le chemin d'accès du point de montage.

`hierarchical mountpoint:` *pathname1* `and` *pathname2*
Solution : Autofs n'autorise pas les relations hiérarchiques entre ses points de montage. Un point de montage autofs ne doit pas être contenu dans un autre système de fichiers monté automatiquement.

`host` *server* `not responding`
Description : Autofs a tenté de contacter le serveur (*server*), mais n'a reçu aucune réponse.

Solution : Vérifiez le statut du serveur NFS.

hostname`: exports:` *rpc-err*
Description : Une erreur s'est produite lors de l'obtention de la liste d'exportation de l'hôte (*hostname*). Ce message indique un problème de serveur ou de réseau.

Solution : Vérifiez le statut du serveur NFS.

`map` *mapname*`, key` *key*`: bad`
Description : L'entrée de mappage n'est pas conforme, et autofs ne peut l'interpréter.

Solution : Vérifiez à nouveau l'entrée. Il se peut que l'entrée comporte des caractères qui doivent être remplacés par des caractères d'échappement.

mapname`:` *nis-err*
Description : Une erreur s'est produite lors de la recherche d'une entrée dans un mappage NIS. Ce message peut indiquer des problèmes NIS.

Solution : Vérifiez l'état du serveur NIS.

`mount of` *server*`:`*pathname* `on` *mountpoint*`:`*reason*

Description : Autofs n'a pas réussi à effectuer un montage. Cette occurrence peut indiquer un problème de serveur ou de réseau. La chaîne *reason* définit le problème.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

mountpoint`: Not a directory`

Description : Autofs ne peut pas se monter lui-même sur le point de montage (*mountpoint*) parce qu'il n'est pas un répertoire.

Solution : Vérifiez l'orthographe et le chemin d'accès du point de montage.

`nfscast: cannot send packet:` *reason*

Description : Autofs n'est pas en mesure d'envoyer un paquet de demandes à un serveur d'une liste des emplacements de systèmes de fichiers répliqués. La chaîne *reason* définit le problème.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

`nfscast: cannot receive reply:` *reason*

Description : Autofs ne peut pas recevoir les réponses des serveurs de la liste des emplacements de systèmes de fichiers répliqués. La chaîne *raison* définit le problème.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

`nfscast: select:` *reason*

Description : Tous ces messages d'erreur indiquent des problèmes lors des tentatives de vérification des serveurs pour un système de fichiers répliqué. Ce message peut indiquer un problème de réseau. La chaîne *reason* définit le problème.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est extrêmement rare, et il n'existe pas de solution simple.

`pathconf: no info for` *server*`:`*pathname*

Description : Autofs n'a pas réussi à obtenir les informations `pathconf` pour le chemin d'accès.

Solution : Reportez-vous à la page de manuel `fpathconf(2)`.

`pathconf: server : server not responding`
Description : Autofs n'est pas en mesure de contacter le démon de montage sur le serveur (*server*) qui fournit les informations à `pathconf()`.

Solution : Évitez d'utiliser l'option de montage `POSIX` avec ce serveur.

Autres erreurs avec Autofs

Si les fichiers `/etc/auto*` contiennent le jeu binaire d'exécution, l'agent de montage automatique tente d'exécuter les mappages, ce qui crée des messages tels que le suivant :

```
/etc/auto_home: +auto_home: not found
```

Dans cette situation, le fichier `auto_home` dispose d'autorisations incorrectes. Chaque entrée du fichier génère un message d'erreur qui est similaire à ce message. Les droits d'accès au fichier doivent être réinitialisés en tapant la commande suivante :

```
# chmod 644 /etc/auto_home
```

Messages d'erreur NFS

Cette section présente un message d'erreur qui est suivi d'une description des conditions qui créent l'erreur et d'au moins une solution.

`Bad argument specified with index option - must be a file`
Solution : Vous devez inclure un nom de fichier avec l'option `index`. Vous ne pouvez pas utiliser des noms de répertoires.

`Cannot establish NFS service over /dev/`*`tcp`*`: transport setup problem`
Description : Ce message est souvent créé lorsque les informations sur les services dans l'espace de noms n'ont pas été mises à jour. L'erreur peut également être signalée pour UDP.

Solution : Pour résoudre ce problème, vous devez mettre à jour les données des services dans l'espace de noms.

Pour NIS+, les entrées doivent se présenter comme suit :

```
nfsd nfsd tcp 2049 NFS server daemon
nfsd nfsd udp 2049 NFS server daemon
```

Pour NIS et `/etc/services` , les entrées doivent se présenter comme suit :

```
nfsd    2049/tcp    nfs    # NFS server daemon
nfsd    2049/udp    nfs    # NFS server daemon
```

`Cannot use index option without public option`

Solution : Utilisez l'option `public` avec l'option `index` dans la commande share. Vous devez définir le gestionnaire de fichiers publics afin que l'option `index` fonctionne.

Remarque – La version Solaris 2.5.1 nécessitait que le gestionnaire de fichiers publics soit défini à l'aide de la commande `share`. Suite à une modification dans la version Solaris 2.6, le gestionnaire de fichiers publics est défini par défaut sur `root` (`/`). Ce message d'erreur n'a plus d'importance.

`Could not start` *daemon*`:` *error*

Description : Ce message s'affiche si le démon se termine de façon anormale ou si une erreur d'appel système se produit. La chaîne *error* définit le problème.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est rare, et il n'existe pas de solution simple.

`Could not use public filehandle in request to` *server*

Description : Ce message s'affiche si l'option `public` est spécifiée mais que le serveur NFS ne prend pas en charge le gestionnaire de fichiers publics. Dans cette situation, le montage échoue.

Solution : Pour remédier à cette situation, essayez la demande de montage sans l'aide du gestionnaire de fichiers publics ou reconfigurez le serveur NFS de façon à assurer la prise en charge du gestionnaire de fichiers publics.

daemon `running already with pid` *pid*

Description : Le démon est déjà en cours d'exécution.

Solution : Si vous voulez exécuter une nouvelle copie, interrompez la version actuelle et lancez une nouvelle version.

`error locking` *lock file*

Description : Ce message s'affiche lorsque le fichier de verrouillage (*lock file*) qui est associé à un démon ne peut pas être verrouillé correctement.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est rare, et il n'existe pas de solution simple.

`error checking` *lock file*`:` *error*

Description : Ce message s'affiche lorsque le fichier de verrouillage (*lock file*) qui est associé à un démon ne peut pas être ouvert correctement.

Solution : Contactez Sun pour obtenir de l'aide. Ce message d'erreur est rare, et il n'existe pas de solution simple.

`NOTICE: NFS3: failing over from` *host1* `to` *host2*
Description : Ce message s'affiche sur la console lors d'un basculement. Le message s'affiche à titre informatif uniquement.

Solution : Aucune action n'est requise.

filename`: File too large`
Description : Un client de la version 2 de NFS tente d'accéder à un fichier dont la taille est supérieure à 2 Go.

Solution : Évitez d'utiliser la version 2 de NFS. Montez le système de fichiers avec la version 3 ou 4. Reportez-vous également à la description de l'option `nolargefiles` dans la section "Options `mount` pour les systèmes de fichiers NFS" à la page 160.

`mount: ... server not responding:RPC_PMAP_FAILURE - RPC_TIMED_OUT`
Description : Le serveur qui partage le système de fichiers que vous essayez de monter est arrêté ou inaccessible, au niveau d'exécution incorrect, ou son démon `rpcbind` est bloqué.

Solution : Attendez la réinitialisation du serveur. Si le serveur est bloqué, redémarrez-le.

`mount: ... server not responding: RPC_PROG_NOT_REGISTERED`
Description : La demande de montage a été enregistrée avec `rpcbind`, mais le démon de montage NFS `mountd` n'est pas enregistré.

Solution : Attendez la réinitialisation du serveur. Si le serveur est bloqué, redémarrez-le.

`mount: ... No such file or directory`
Description : Le répertoire distant ou le répertoire local n'existe pas.

Solution : Vérifiez l'orthographe des noms de répertoire. Exécutez `ls` sur les deux répertoires.

`mount: ...: Permission denied`
Description : Le nom de votre ordinateur n'est peut-être pas dans la liste des clients ou groupes réseau qui sont autorisés à accéder au système de fichiers que vous avez tenté de monter.

Solution : À l'aide de la commande `showmount -e`, vérifiez la liste d'accès.

`NFS file temporarily unavailable on the server, retrying ...`
Description : Un serveur de la version 4 de NFS peut déléguer la gestion d'un fichier à un client. Ce message indique que le serveur rappelle une délégation pour un autre client qui est en conflit avec une demande de votre client.

Solution : Le rappel doit se produire avant que le serveur ne puisse traiter la demande de votre client. Pour plus d'informations sur la délégation, reportez-vous à la section "Délégation dans la version 4 de NFS" à la page 190.

`NFS fsstat failed for server` *hostname*`: RPC: Authentication error`
Description : Cette erreur peut être provoquée par de nombreuses situations. L'une des situations les plus difficiles à déboguer est lorsque ce problème survient car un utilisateur fait partie d'un trop grand nombre de groupes. Actuellement, un utilisateur ne peut faire partie de plus de 16 groupes s'il accède aux fichiers via les montages NFS.

Solution : Une alternative existe pour les utilisateurs qui doivent faire partie de plus de 16 groupes. Vous pouvez utiliser les listes de contrôle d'accès pour fournir les privilèges d'accès requis.

`nfs mount: ignoring invalid option "-`*option*`"`
Description : L'indicateur *-option* n'est pas valide.

Solution : Reportez-vous à la page de manuel `mount_nfs(1M)` pour vérifier la syntaxe.

Remarque – Ce message d'erreur n'est pas affiché lors de l'exécution de toute version de la commande `mount` qui est incluse dans une version de Solaris de 2.6 à la version actuelle ou dans des versions précédentes qui ont été corrigées.

`nfs mount: NFS can't support "nolargefiles"`
Description : Un client NFS a essayé de monter un système de fichiers à partir d'un serveur NFS à l'aide de l'option `-nolargefiles` .

Solution : Cette option n'est pas prise en charge pour les types de système de fichiers NFS.

`nfs mount: NFS V2 can't support "largefiles"`
Description : Le protocole de la version 2 de NFS n'est pas en mesure de gérer les fichiers volumineux.

Solution : Vous devez utiliser la version 3 ou la version 4 si l'accès à des fichiers volumineux est requis.

`NFS server` *hostname* `not responding still trying`
Description : Si les programmes se bloquent pendant que vous travaillez sur les fichiers, votre serveur NFS est peut-être en panne. Ce message indique que l'hôte (*hostname*) du serveur NFS est arrêté ou qu'un problème s'est produit sur le serveur ou le réseau.

Solution : Si le basculement est en cours d'utilisation, *hostname* est une liste de serveurs. Commencez à résoudre les problèmes à l'aide de la section "Vérification de la connectivité sur un client NFS " à la page 124.

`Récupération de serveur NFS`
Description : Pendant une partie de la réinitialisation du serveur de la version 4 de NFS, certaines opérations n'ont pas été autorisées. Ce message indique que le client attend que le serveur autorise cette opération pour continuer.

Solution : Aucune action n'est requise. Attendez que le serveur autorise l'opération.

`Autorisation refusée`

Description : Ce message est affiché par les commandes `ls -l`, `getfacl` et `setfacl` pour les raisons suivantes :

- Si l'utilisateur ou le groupe qui existe dans une entrée de liste de contrôle d'accès (ACL) sur un serveur de la version 4 de NFS ne peut pas être mappé à un utilisateur ou groupe valide sur un client de la version 4 de NFS, l'utilisateur n'est pas autorisé à lire l'ACL sur le client.
- Si l'utilisateur ou le groupe qui existe dans une entrée d'ACL qui est en cours de définition sur un client de la version 4 de NFS ne peut pas être mappé à un utilisateur ou groupe valide sur un serveur de la version 4 de NFS, l'utilisateur n'est pas autorisé à écrire ou modifier une liste de contrôle d'accès sur le client.
- Si un client et un serveur de la version 4 de NFS possèdent des valeurs NFSMAPID_DOMAIN incompatibles, le mappage d'ID échoue.

Pour plus d'informations, reportez-vous à la section "Listes de contrôle d'accès (ACL) et `nfsmapid` dans la version 4 de NFS" à la page 192.

Solution : Effectuez les opérations suivantes :

- Assurez-vous que tous les ID utilisateur et de groupe des entrées d'ACL existent à la fois sur le client et le serveur.
- Assurez-vous que la valeur de NFSMAPID_DOMAIN est correctement définie dans le fichier `/etc/default/nfs`. Pour plus d'informations, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142.

Pour déterminer si un utilisateur ou un groupe ne peut pas être mappé sur le serveur ou le client, utilisez le script qui est fourni dans "Vérification d'ID d'utilisateur ou de groupe non mappé" à la page 193.

`port` *number* `in nfs URL not the same as port` *number* `in port option`

Description : Le numéro de port qui est inclus dans l'URL NFS doit correspondre au numéro de port qui est inclus dans l'option `-port` à monter. Si les numéros de port ne correspondent pas, le montage échoue.

Solution : Modifiez la commande pour rendre les numéros de port identiques ou ne spécifiez pas le numéro de port qui est incorrect. En général, vous n'avez pas besoin de spécifier le numéro de port à la fois avec l'URL NFS et l'option `-port`.

`Les répliques doivent être de même version`

Description : Pour que le basculement NFS fonctionne correctement, les serveurs NFS qui sont des répliques doivent prendre en charge la même version du protocole NFS.

Solution : L'exécution de plusieurs versions n'est pas autorisée.

`replicated mounts must be read-only`

Description : Le basculement NFS ne fonctionne pas sur les systèmes de fichiers qui sont montés en lecture-écriture. Le montage du système de fichiers en lecture-écriture augmente la probabilité de modification d'un fichier.

Solution : Le basculement NFS dépend des systèmes de fichiers étant identiques.

`replicated mounts must not be soft`

Description : Les montages répliqués nécessitent que vous attendiez qu'un délai d'attente expire avant que le basculement ne se produise.

Solution : L'option `soft` requiert que le montage échoue immédiatement lorsqu'un délai d'attente commence, de sorte que vous ne puissiez pas inclure l'option `-soft` avec un montage répliqué.

`share_nfs: Cannot share more than one filesystem with 'public' option`

Solution : Vérifiez que le fichier `/etc/dfs/dfstab` n'a qu'un seul système de fichiers sélectionné pour le partage avec l'option `-public`. Un seul gestionnaire de fichiers publics peut être établi par serveur, de sorte qu'un seul système de fichiers par serveur peut être partagé avec cette option.

`WARNING: No network locking on` *hostname*`:` *path*`: contact admin to install server change`

Description : Un client NFS a vainement essayé d'établir une connexion avec le gestionnaire de verrous réseau sur un serveur NFS. Au lieu de faire échouer le montage, cet avertissement est généré pour vous informer que le verrouillage ne fonctionne pas.

Solution : Mettez à niveau le serveur à l'aide d'une nouvelle version du système d'exploitation qui fournit une prise en charge complète du gestionnaire de verrous réseau.

◆ ◆ ◆ CHAPITRE 6

Accès aux systèmes de fichiers réseau (référence)

Ce chapitre décrit les commandes NFS, ainsi que les différentes parties de l'environnement NFS et comment ces parties fonctionnent ensemble.

Remarque – Si votre système comporte des zones activées et que vous souhaitez utiliser cette fonction dans une zone non globale, reportez-vous à la section *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris* pour plus d'informations.

Fichiers NFS

Plusieurs fichiers sont nécessaires pour prendre en charge les activités NFS sur tout ordinateur. La plupart de ces fichiers sont codés en ASCII, mais certains de ces fichiers sont des fichiers de données. Le Tableau 6–1 répertorie ces fichiers et leurs fonctions.

TABLEAU 6–1 Fichiers NFS

Nom de fichier	Fonction
`/etc/default/autofs`	Répertorie les informations de configuration de l'environnement autofs.
`/etc/default/fs`	Indique le type de système de fichiers par défaut pour les systèmes de fichiers locaux.

TABLEAU 6–1 Fichiers NFS *(Suite)*

Nom de fichier	Fonction
`/etc/default/nfs`	Répertorie les informations de configuration `lockd` et `nfsd` . Pour plus d'informations, reportez-vous à la rubrique "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142 et à la page de manuel `nfs(4)`.
`/etc/default/nfslogd`	Répertorie les informations de configuration pour le démon de connexion NFS, `nfslogd`.
`/etc/dfs/dfstab`	Répertorie les ressources locales à partager.
`/etc/dfs/fstypes`	Répertorie les types de systèmes de fichiers par défaut pour les systèmes de fichiers à distance.
`/etc/dfs/sharetab`	Répertorie les ressources locales et distantes qui sont partagés. Reportez-vous à la page de manuel `sharetab(4)`. N'éditez pas ce fichier.
`/etc/mnttab`	Répertorie les systèmes de fichiers qui sont actuellement montés, y compris les répertoires montés automatiquement. Reportez-vous à la page de manuel `mnttab(4)`. N'éditez pas ce fichier.
`/etc/netconfig`	Répertorie les protocoles de transport. N'éditez pas ce fichier.
`/etc/nfs/nfslog.conf`	Répertorie les informations de configuration générale pour la connexion du serveur NFS.
`/etc/nfs/nfslogtab`	Répertorie les informations post-traitement de connexion par `nfslogd`. N'éditez pas ce fichier.
`/etc/nfssec.conf`	Répertorie les services de sécurité NFS.
`/etc/rmtab`	Répertorie les systèmes de fichiers qui sont montés à distance par des clients NFS. Reportez-vous à la page de manuel `rmtab(4)`. N'éditez pas ce fichier.
`/etc/vfstab`	Définit les systèmes de fichiers à monter localement. Reportez-vous à la page de manuel `vfstab(4)`.

La première entrée dans `/etc/dfs/fstypes` est souvent utilisée en tant que type de système de fichiers par défaut pour les systèmes de fichiers à distance. Cette entrée définit le type de système de fichiers NFS en tant que valeur par défaut.

Une seule entrée se trouve dans le fichier `/etc/default/fs` : le type de système de fichiers par défaut pour les disques locaux. Vous pouvez déterminer les types de systèmes de fichiers pris en charge sur un client ou un serveur en consultant les fichiers dans `/kernel/fs`.

Fichier /etc/default/autofs

À partir de la version Solaris 10, vous pouvez utiliser le fichier `/etc/default/autofs` pour configurer votre environnement autofs. Plus précisément, ce fichier fournit un moyen supplémentaire pour configurer les commandes et démons autofs. Vous pouvez définir dans ce nouveau fichier de configuration les spécifications que vous définiriez sur la ligne de commande. En revanche, contrairement à cette dernière méthode, ce fichier conserve les spécifications, même lors de mises à niveau de votre système. De plus, vous n'avez plus besoin de mettre à jour les fichiers de démarrage critiques pour vous assurer que le comportement existant de votre environnement autofs est conservé. Les spécifications sont définies en fournissant les valeurs des mots-clés suivants :

AUTOMOUNT_TIMEOUT
: Détermine la durée d'inactivité d'un système de fichiers avant de le démonter. Ce mot-clé est l'équivalent de l'argument `-t` de la commande `automount`. La valeur par défaut est 600.

AUTOMOUNT_VERBOSE
: Envoie la notification des montages, démontages et autres événements secondaires autofs. Ce mot-clé est l'équivalent de l'argument `-v` de la commande `automount`. La valeur par défaut est false.

AUTOMOUNTD_VERBOSE
: Enregistre les messages d'état sur la console. Il s'agit de l'équivalent de l'argument `-v` du démon `automountd`. La valeur par défaut est false.

AUTOMOUNTD_NOBROWSE
: Active ou désactive la navigation rotations pour tous les points de montage autofs et est l'équivalent de l'argument `-n` pour `automountd`. La valeur par défaut est false.

AUTOMOUNTD_TRACE
: Développe chaque appel de procédure à distance (RPC) et l'affiche sur une sortie standard. Ce mot-clé est l'équivalent de l'argument `-T` de la commande `automountd`. La valeur par défaut est 0. Les valeurs peuvent être comprises entre 0 et 5.

AUTOMOUNTD_ENV
: Permet d'attribuer différentes valeurs aux différents environnements. Ce mot-clé est l'équivalent de l'argument `-D` de la commande `automountd`. Le mot-clé AUTOMOUNTD_ENV peut être utilisé plusieurs fois. Cependant, vous devez utiliser des lignes distinctes pour chaque affectation d'environnement.

Pour plus d'informations, reportez-vous aux pages de manuel `automount(1M)` et `automountd(1M)`. Pour des informations sur les procédures à suivre, reportez-vous à "Configuration de votre environnement Autofs à l'aide du fichier `/etc/default/autofs`" à la page 108.

Mots-clés pour le fichier `/etc/default/nfs`

Dans la version 4 de NFS, les mots-clés suivants peuvent être définis dans le fichier `/etc/default/nfs`. Ces mots-clés contrôlent les protocoles NFS qui sont utilisés par le client et le serveur.

NFS_SERVER_VERSMIN
: Définit la version minimale du protocole NFS à enregistrer et proposée par le serveur. À partir de la version Solaris 10, la valeur par défaut est 2. Les autres valeurs valides incluent 3 ou 4. Reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

NFS_SERVER_VERSMAX
: Définit la version maximale du protocole NFS à enregistrer et proposée par le serveur. À partir de la version Solaris 10, la valeur par défaut est 4. Les autres valeurs valides incluent 2 ou 3. Reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

NFS_CLIENT_VERSMIN
: Définit la version minimale du protocole NFS à utiliser par le client NFS. À partir de la version Solaris 10, la valeur par défaut est 2. Les autres valeurs valides incluent 3 ou 4. Reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

NFS_CLIENT_VERSMAX
: Définit la version maximale du protocole NFS à utiliser par le client NFS. À partir de la version Solaris 10, la valeur par défaut est 4. Les autres valeurs valides incluent 2 ou 3. Reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

NFS_SERVER_DELEGATION
: Détermine si la fonction de délégation de la version 4 de NFS est activée pour le serveur. Si cette fonctionnalité est activée, le serveur tente de fournir des délégations pour le client de la version 4 de NFS. Par défaut, la délégation de serveur est activée. Pour désactiver la délégation de serveur, reportez-vous à la rubrique "Sélection de versions différentes de NFS sur un serveur" à la page 98. Pour plus d'informations, reportez-vous à la rubrique "Délégation dans la version 4 de NFS" à la page 190.

NFSMAPID_DOMAIN
: Définit un domaine commun pour les clients et les serveurs. Remplace le comportement par défaut de l'utilisation d'un nom de domaine DNS local. Pour plus d'informations sur les tâches, reportez-vous à la rubrique "Configuration des services NFS" à la page 96. Reportez-vous également à la rubrique "Démon `nfsmapid`" à la page 148.

Fichier `/etc/default/le`

Ce fichier définit certains des paramètres utilisés lors de l'utilisation de la connexion du serveur NFS. Les paramètres suivants peuvent être définis.

CYCLE_FREQUENCY
: Détermine le nombre d'heures qui doivent s'écouler avant le redémarrage des fichiers journaux. La valeur par défaut est de 24 heures. Cette option est utilisée pour empêcher les fichiers journaux de devenir trop volumineux.

IDLE_TIME
: Définit le nombre de secondes durant lesquelles `nfslogd` doit être mis en veille avant la recherche d'informations supplémentaires dans le tampon. Par ailleurs, ce paramètre détermine la fréquence à laquelle le fichier de configuration est consulté. Ce paramètre, avec MIN_PROCESSING_SIZE, détermine la fréquence à laquelle le tampon est traitée. La valeur par défaut est 300 secondes. Augmenter ce nombre peut améliorer les performances grâce à la réduction du nombre de vérifications.

MAPPING_UPDATE_INTERVAL
: Indique le nombre de secondes entre les mises à jour des enregistrements dans les tables de mappage fichier-identificateur-chemin d'accès. La valeur par défaut est 86 400 secondes ou un jour. Ce paramètre permet de maintenir les tables de mappage fichier-identificateur-chemin d'accès à jour sans avoir à mettre à jour ces tables en permanence.

MAX_LOGS_PRESERVE
: Détermine le nombre de fichiers journaux à enregistrer. La valeur par défaut est 10.

MIN_PROCESSING_SIZE
: Définit le nombre minimal d'octets que le fichier tampon doit atteindre avant le traitement et l'écriture sur le fichier journal. Ce paramètre, avec IDLE_TIME, détermine la fréquence à laquelle le fichier tampon est traitée. La valeur par défaut est 524 288 octets. Augmenter ce nombre peut améliorer les performances en réduisant le nombre de fois où le fichier tampon est traité.

PRUNE_TIMEOUT
: Sélectionne le nombre d'heures qui doit s'écouler avant qu'un enregistrement de mappage fichier-identificateur-chemin d'accès arrive à expiration et peut être réduit. La valeur par défaut est 168 heures ou 7 jours.

UMASK
: Spécifie le masque de création du mode fichier pour les fichiers journaux qui sont créés par `nfslogd`. La valeur par défaut est 0137.

Fichier `/etc/nfs/nfslog.conf`

Ce fichier définit le chemin d'accès, les noms de fichiers, et le type de connexion qu'utilise `nfslogd`. Chaque définition est associée à une *balise*. Pour démarrer la consignation de serveur NFS, vous devez identifier la *balise* pour chaque système de fichiers. La balise globale définit les valeurs par défaut. Vous pouvez utiliser les paramètres suivants avec chaque balise selon les besoins.

defaultdir=*chemin*
: Spécifie le chemin d'accès du répertoire par défaut pour les fichiers journaux. Le répertoire par défaut est `/var/nfs` sauf spécification contraire.

log=*chemin/nom_fichier*
: Définit le chemin d'accès et le nom du fichier pour les fichiers journaux. La valeur par défaut est `/var/nfs/nfslog`.

fhtable=*chemin/nom_fichier*
: Sélectionne le chemin d'accès et le nom du fichier pour les fichiers de base de données fichier-identificateur-chemin d'accès. La valeur par défaut est `/var/nfs/fhtable`.

buffer=*chemin/nom_fichier*
: Détermine le chemin d'accès et le nom du fichier pour les fichiers tampon. La valeur par défaut est `/var/nfs/nfslog_workbuffer`.

logformat=*basique*|*étendu*
: Permet de sélectionner le format à utiliser lors de la création de fichiers journaux lisibles par l'utilisateur. Le format de base génère un fichier journal qui est similaire à certains démons `ftpd`. Le format étendu donne une vue plus détaillée.

Si le chemin d'accès n'est pas spécifié, le chemin d'accès défini par `defaultdir` est utilisé. En outre, vous pouvez remplacer `defaultdir` par un chemin d'accès absolu.

Afin d'identifier les fichiers plus facilement, placez les fichiers dans des répertoires différents. Voici un exemple des changements nécessaires.

```
% cat /etc/nfs/nfslog.conf
#ident  "@(#)nfslog.conf        1.5     99/02/21 SMI"
#
  .
  .
# NFS server log configuration file.
#

global  defaultdir=/var/nfs \
        log=nfslog fhtable=fhtable buffer=nfslog_workbuffer

publicftp log=logs/nfslog fhtable=fh/fhtables buffer=buffers/workbuffer
```

Dans cet exemple, un système de fichiers qui est partagé avec `log=publicftp` utilise les valeurs suivantes :

- Le répertoire par défaut est `/var/nfs`.
- Les fichiers journaux sont stockés dans `/var/nfs/logs/nfslog*`.
- Les tables fichier-identificateur-chemin d'accès sont stockées dans `/var/nfs/fh/fhtables`.
- Les fichiers tampon sont stockés dans `/var/nfs/buffers/workbuffer`.

Pour obtenir des informations sur les procédures à suivre, reportez-vous à la section “Activation de la journalisation de serveur NFS” à la page 89.

Démons NFS

Pour prendre en charge les activités NFS, plusieurs démons sont lancés lorsqu'un système passe en niveau d'exécution 3 ou en mode multi-utilisateur. Les démons `mountd` et `nfsd` sont exécutés sur les systèmes qui sont des serveurs. Le démarrage automatique des démons de serveur dépend de l'existence d'entrées qui sont libellées avec le type de système de fichiers NFS dans `/etc/dfs/sharetab`. Pour prendre en charge le verrouillage de fichiers NFS, les démons `lockd` et `statd` sont exécutés sur les clients et serveurs NFS. Toutefois, contrairement aux précédentes versions de NFS, dans la version 4 de NFS, les démons `lockd`, `statd`, `mountd` et `nfslogd` ne sont pas utilisés.

Cette section décrit les démons suivants :

Démon `automountd`

Ce démon gère les demandes de montage et de démontage du service autofs. La syntaxe de la commande est indiquée ci-après.

`automountd [ -Tnv ] [ -D` *nom*`=` *valeur* `]`

La commande se comporte comme suit :

- `-T` active le suivi.
- `-n` désactive la navigation sur tous les nœuds autofs.
- `-v` consigne tous les messages d'état sur la console.
- `-D` *nom*`=`*valeur* remplace la *valeur* de la variable de mappe de montage automatique indiquée par *nom*.

La valeur par défaut de la mappe de montage automatique est `/etc/auto_master`. Utilisez l'option `-T` pour la résolution de problèmes.

Démon lockd

Ce démon prend en charge les opérations de verrouillage d'enregistrements sur les fichiers NFS. Le démon `lockd` gère les connexions RPC entre le client et le serveur pour le protocole NLM (Network Lock Manager). Le démon est démarré normalement sans aucune option. Vous pouvez utiliser trois options avec cette commande. Reportez-vous à la page de manuel `lockd(1M)`. Ces options peuvent être utilisées à partir de la ligne de commande ou en modifiant la chaîne appropriée dans `/etc/default/nfs`. Vous trouverez ci-après des descriptions des mots-clés qui peuvent être définis dans le fichier`/etc/default/nfs`.

Remarque – À partir de la version Solaris 10, le mot-clé `LOCKD_GRACE_PERIOD` et l'option `-g` ont été abandonnés. Le mot-clé abandonné a été remplacé par le mot-clé `GRACE_PERIOD`. Si les deux mots-clés sont définis, la valeur de `GRACE_PERIOD` remplace celle de `LOCKD_GRACE_PERIOD`. Reportez-vous à la description de `GRACE_PERIOD` qui suit.

Tout comme `LOCKD_GRACE_PERIOD` , `GRACE_PERIOD`=*graceperiod* dans `/etc/default/nfs` définit le nombre de secondes après une réinitialisation du serveur dont disposent les clients pour récupérer les verrous de la version 3 de NFS, fournis par NLM, ainsi que les verrous de la version 4. Par conséquent, la valeur de `GRACE_PERIOD` détermine la longueur de la période de grâce pour la récupération de verrou pour la version 3 et la version 4 de NFS.

Le paramètre `LOCKD_RETRANSMIT_TIMEOUT`=*délai d'attente* dans `/etc/default/nfs` sélectionne le nombre de secondes à attendre avant la retransmission d'une demande de verrou au serveur distant. Cette option a une incidence sur le client NFS côté service. La valeur par défaut pour le *délai d'attente* est de 15 secondes. Le fait de diminuer la valeur du *délai d'attente* valeur peut améliorer le temps de réponse pour les clients NFS sur un réseau "parasité". Cependant, cette modification peut entraîner une charge de serveur supplémentaire en augmentant la fréquence des demandes de verrou externe. Le même paramètre peut être utilisé à partir de la ligne de commande en démarrant le démon avec l'option `-t` *timeout*.

Le paramètre `LOCKD_SERVERS`= *nthreads* dans `/etc/default/nfs` spécifie le nombre maximum de threads simultanés que peut gérer le serveur par connexion. Basez la valeur de *nthreads* sur la charge qui est prévue sur le serveur NFS. La valeur par défaut est 20. Chaque client NFS qui utilise le protocole TCP utilise une connexion unique avec le serveur NFS. Par conséquent, chaque client peut utiliser un maximum de 20 threads simultanés sur le serveur.

Tous les clients NFS qui utilisent UDP partagent une connexion unique avec le serveur NFS. Dans ces conditions, vous pouvez être amené à augmenter le nombre de threads disponibles pour la connexion UDP. Le minimum serait d'autoriser deux threads pour chaque client UDP. Cependant, ce nombre étant spécifique à la charge de travail sur le client, deux threads par client peuvent être insuffisants. L'inconvénient d'utiliser plus de threads est que lorsque les threads sont utilisés, le serveur NFS utilise davantage de mémoire. Si les threads ne sont jamais utilisés, cependant, l'augmentation de *nthreads* n'a aucun effet. Le même paramètre peut être utilisé à partir de la ligne de commande en démarrant le démon à l'aide de l'option `nthreads`.

Démon `mountd`

Ce démon gère les requêtes de montage de système de fichiers provenant de systèmes distants et fournit le contrôle d'accès. Le démon `mountd` consulte `/etc/dfs/sharetab` afin de déterminer quels systèmes de fichiers sont disponibles pour le montage à distance et les systèmes qui sont autorisés à effectuer le montage à distance. Vous pouvez utiliser les options `-v` et `-r` avec cette commande. Reportez-vous à la page de manuel `mountd`(1M).

L'option `-v` exécute la commande en mode détaillé. Chaque fois qu'un serveur NFS détermine l'accès à accorder à un client, un message s'affiche sur la console. Les informations générées peuvent s'avérer utiles lorsque vous essayez de déterminer la raison pour laquelle un client ne peut pas accéder à un système de fichiers.

L'option `-r` refuse toutes les futures demandes de montage à partir des clients. Cette option n'affecte pas les clients qui disposent déjà d'un système de fichiers monté.

Remarque – La version 4 de NFS n'utilise pas ce démon.

Démon `nfs4cbd`

Le démon `nfs4cbd`, qui est destiné à l'utilisation exclusive du client de la version 4 de NFS, gère les points d'extrémité de communication pour le programme de rappel de la version 4 de NFS. Le démon n'a aucune interface accessible par l'utilisateur. Pour plus d'informations, reportez-vous à la page de manuel `nfs4cbd`(1M).

Démon `nfsd`

Ce démon gère les autres demandes de systèmes de fichiers clients. Vous pouvez utiliser plusieurs options avec cette commande. Reportez-vous à la page de manuel `nfsd`(1M) pour obtenir la liste complète. Ces options peuvent être utilisées à partir de la ligne de commande ou en modifiant la chaîne appropriée dans `/etc/default/nfs`.

Le paramètre `NFSD_LISTEN_BACKLOG=`*longueur* dans `/etc/default/nfs` définit la longueur de la file d'attente de connexion sur les transports orientés connexion pour NFS et TCP. La valeur par défaut est 32 entrées. La même sélection peut être effectuée à partir de la ligne de commande en démarrant `nfsd` avec l'option `-l`.

Le paramètre `NFSD_MAX_CONNECTIONS=`*#-conn* dans `/etc/default/nfs` sélectionne le nombre maximum de connexions par transport orienté connexion. La valeur par défaut pour *#-conn* est illimitée. Le même paramètre peut être utilisé à partir de la ligne de commande en démarrant le démon à l'aide de l'option `-c` *#-conn*.

Le paramètre NFSD_SERVER=*nservers* dans /etc/default/nfs sélectionne le nombre maximal de demandes simultanées qu'un serveur peut gérer. La valeur par défaut pour *nservers* est de 16. La même sélection peut être effectuée à partir de la ligne de commande en démarrant nfsd avec l'option nservers.

Contrairement aux versions plus anciennes de ce démon, nfsd ne génère pas plusieurs copies pour traiter les demandes de traitement simultané. La consultation de la table de processus avec ps indique seulement qu'un seul exemplaire du démon est en cours d'exécution.

Démon nfslogd

Ce démon fournit la journalisation opérationnelle. Les opérations NFS qui sont enregistrées sur le serveur sont basées sur les options de configuration qui sont définies dans /etc/default/nfslogd. Lorsque la consignation de serveur NFS est activée, les enregistrements de toutes les opérations RPC sur un système de fichiers sélectionné sont écrites dans un fichier tampon par le noyau. Ensuite, nfslogd effectue un post-traitement de ces demandes. Le commutateur de service de noms est utilisé pour mettre en correspondance les UID avec les informations de connexion et les adresses IP avec les noms d'hôte. Le nombre est enregistré si aucune correspondance ne peut être trouvée par l'intermédiaire des services de noms identifiés.

Le mappage des identificateurs de fichiers vers les chemins d'accès est également géré par nfslogd. Le démon effectue un suivi de ces mappages dans une table de mappage fichier-identificateur-chemin d'accès. Une table de correspondance existe pour chaque balise identifiée dans /etc/nfs/nfslogd. Après le post-traitement, les enregistrements sont écrits dans les fichiers journaux au format ASCII.

Remarque – La version 4 de NFS n'utilise pas ce démon.

Démon nfsmapid

La version 4 du protocole NFS (RFC3530) a modifié la façon dont les UID ou les GID (identificateurs d'utilisateur ou de groupe) sont échangés entre le client et le serveur. Le protocole exige que le propriétaire d'un fichier et que les attributs de groupe soient échangés entre un client de la version 4 de NFS et un serveur de la version 4 de NFS sous la forme de chaînes comme suit : user@nfsv4_domaine ou group@nfsv4_domaine respectivement.

Par exemple, l'utilisateur known_user a un UID 123456 sur un client de la version 4 de NFS dont le nom d'hôte pleinement qualifié est system.example.com. Pour que le client envoie des demandes au serveur de la version 4 de NFS, le client doit faire correspondre l'UID 123456 à utilisateur_connu@exemple.com puis envoyer cet attribut au serveur de la version 4 de NFS. Le serveur de la version 4 de NFS s'attend à recevoir les attributs de fichier utilisateur et de

groupe au format `user_or_group@nfsv4_domain`. Une fois que le serveur reçoit `known_user@example.com` à partir du client, le serveur met en correspondance la chaîne de caractères et l'UID local 123456, qui est interprété par le système de fichiers sous-jacent. Cette fonctionnalité suppose que chaque UID et GID dans le réseau est unique et que les domaines de la version 4 de NFS sur le client correspondent aux domaines de la version 4 de NFS sur le serveur.

Remarque – Si le serveur ne reconnaît pas le nom d'utilisateur ou de groupe donné, même si les domaines de la version 4 de NFS correspondent, le serveur n'est pas en mesure de mapper le nom de l'utilisateur ou du groupe à son ID unique, une valeur entière. Dans de telles circonstances, le serveur mappe le nom de groupe ou d'utilisateur entrant à l'utilisateur `nobody`. Pour éviter de telles occurrences, les administrateurs doivent éviter d'établir des comptes spéciaux qui n'existent que sur le client de la version 4 de NFS.

Le client et le serveur de la version 4 de NFS sont tous deux capables d'exécuter des conversions entier-à-chaîne et chaîne-à-entier. Par exemple, en réponse à une opération GETATTR, le serveur de la version 4 de NFS mappe les UID et GID obtenus dans système de fichiers sous-jacent vers leurs représentations sous forme de chaîne respectives et envoie ces informations au client. Le client doit également faire correspondre les UID et GID dans des représentations sous forme de chaîne. Par exemple, en réponse à la commande `chown`, le client mappe le nouvel UID ou GID vers une représentation sous forme de chaîne avant l'envoi d'une opération SETATTR au serveur.

Notez, cependant, que le client et le serveur répondent différemment aux chaînes non reconnues :

- Si l'utilisateur n'existe pas sur le serveur, même au sein d'une même configuration de domaine de la version 4 de NFS, le serveur rejette l'appel de procédure à distance (RPC) et renvoie un message d'erreur pour le client. Cette situation limite les opérations qui peuvent être effectuées par l'utilisateur distant.
- Si l'utilisateur existe à la fois sur le client et le serveur, mais que les domaines ne correspondent pas, le serveur rejette les opérations de modification d'attribut (tels que SETATTR) qui nécessitent que le serveur mappe la chaîne d'utilisateur entrante sur une valeur entière que le système de fichiers sous-jacent peut comprendre. Pour que les clients de la version 4 de NFS et les serveurs fonctionnent correctement, leurs domaines de la version 4 de NFS et la partie de la chaîne de caractères après le signe `@` doivent correspondre.
- Si le client de la version 4 de NFS ne reconnaît pas un nom d'utilisateur ou de groupe à partir du serveur, le client n'est pas en mesure mapper la chaîne vers son ID unique, une valeur entière. Dans de telles circonstances, le client mappe la chaîne de l'utilisateur ou du groupe entrant à l'utilisateur `nobody`. Cette mise en correspondance avec `nobody` crée divers problèmes pour différentes applications. En ce qui concerne les fonctionnalités de la version 4 de NFS, les opérations qui modifient les attributs de fichiers échouent.

Vous pouvez changer le nom de domaine pour les clients et les serveurs à l'aide de la commande `sharectl` avec l'option suivante.

nfsmapid_domain
: Définit un domaine commun pour les clients et les serveurs. Remplace le comportement par défaut de l'utilisation d'un nom de domaine DNS local. Pour plus d'informations sur les tâches, reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

Fichiers de configuration et `nfsmapid`

La section suivante décrit l'utilisation par le démon `nfsmapid` des fichiers `/etc/nsswitch.conf` et `/etc/resolv.conf` :

- `nfsmapid` utilise des fonctions de bibliothèque C standard pour les demandes de mot de passe et d'informations de groupe aux services de moteur de traitement de noms. Ces services de nom sont contrôlés par les paramètres situés dans le fichier `/etc/nsswitch.conf`. Les modifications apportées au fichier `nsswitch.conf` affectent les opérations `nfsmapid` . Pour plus d'informations sur le fichier `nsswitch.conf`, reportez-vous à la page de manuel `nsswitch.conf(4)`.
- Pour assurer que les clients de la version 4 de NFS sont capables de monter les systèmes de fichiers à partir de différents domaines, `nfsmapid` s'appuie sur la configuration de l'enregistrement de ressource TXT DNS, `_nfsv4idmapdomain` . Pour plus d'informations sur la configuration de l'enregistrement de ressources `_nfsv4idmapdomain` , reportez-vous à la rubrique "`nfsmapid` et enregistrements DNS TXT" à la page 152. En outre, notez les points suivants :
  - L'enregistrement de ressources DNS TXT doit être configuré de manière explicite sur le serveur DNS avec les informations du domaine souhaité.
  - Le fichier `/etc/resolv.conf` doit être configuré avec les paramètres souhaités pour activer `resolver` afin de trouver le serveur DNS et de rechercher les domaines de client et de serveur de la version 4 de NFS dans les enregistrements TXT.

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

  - "Règles de priorité" à la page 151
  - "Configuration du domaine par défaut de la version 4 de NFS" à la page 154
  - Page de manuel `resolv.conf(4)`

Règles de priorité

Pour que `nfsmapid` fonctionne correctement, les clients et serveurs de la version 4 de NFS doivent avoir le même domaine. Pour une mise en correspondance correcte des domaines de la version 4 de NFS, `nfsmapid` suit les règles de priorité strictes suivantes :

1. Il vérifie d'abord le fichier `/etc/default/nfs` pour une valeur attribuée au mot-clé NFSMAPID_DOMAIN. Si une valeur est trouvée, celle attribuée est prioritaire sur tous les autres paramètres. La valeur attribuée est ajoutée aux chaînes des attributs sortants et est comparée aux chaînes des attributs entrants. Pour plus d'informations sur les mots-clés dans le fichier `/etc/default/nfs`, reportez-vous à la rubrique "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142. Pour des informations sur les procédures à suivre, reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

   Remarque – L'utilisation du paramètre NFSMAPID_DOMAIN n'est pas évolutive et n'est pas recommandée pour les déploiements de grande envergure.

2. Si aucune valeur n'a été attribuée à NFSMAPID_DOMAIN, le démon recherche un nom de domaine dans l'enregistrement DNS TXT sur un serveur de noms DNS. `nfsmapid` s'appuie sur des directives dans le fichier `/etc/resolv.conf` et qui sont utilisées par l'ensemble des sous-programmes dans `resolver`. `resolver` effectue une recherche dans les serveurs DNS pour les enregistrements de ressources `_nfsv4idmapdomain`. Notez que l'utilisation des enregistrements DNS TXT est plus évolutive. Pour cette raison, l'utilisation continue des enregistrements TXT est largement préférable à la définition du mot-clé dans le fichier `/etc/default/nfs`.
3. Si aucun enregistrement DNS TXT est configuré de manière à fournir un nom de domaine, le démon `nfsmapid` utilise la valeur indiquée par la directive `domain` ou `search` dans le fichier `/etc/resolv.conf`, avec la directive spécifiée en dernier ayant la priorité.

   Dans l'exemple suivant, où les directives `domain` et `search` sont toutes deux utilisées, le démon `nfsmapid` utilise le premier domaine répertorié après la directive `search`, qui est `company.com`.

   ```
   domain example.company.com
   search company.com foo.bar.com
   ```

4. Si le fichier `/etc/resolv.conf` n'existe pas, `nfsmapid` obtient le nom de domaine de la version 4 de NFS en suivant le comportement de la commande `domainname`. En particulier, si le fichier `/etc/defaultdomain`existe, `nfsmapid` utilise le contenu de ce fichier pour le domaine de la version 4 de NFS. Si le fichier `/etc/defaultdomain` n'existe pas, `nfsmapid` utilise le nom de domaine qui est fourni par le service d'attribution de noms configuré du réseau. Pour plus d'informations, reportez-vous à la page de manuel `domainname(1M)`.

`nfsmapid` et enregistrements DNS TXT

L'ubiquité de DNS fournit un mécanisme de stockage et de distribution efficace pour le nom de domaine de la version 4 de NFS. En outre, du fait de l'évolutivité inhérente de DNS, l'utilisation des enregistrements de ressources DNS TXT est la méthode recommandée pour la configuration du nom de domaine de la version 4 de NFS pour les déploiements de grande envergure. Vous devez configurer l'enregistrement TXT `_nfsv4idmapdomain` au niveau des serveurs DNS au niveau de l'entreprise. Ces configurations assurent que tout client ou serveur de la version 4 de NFS peut trouver son domaine de la version 4 de NFS en parcourant l'arborescence DNS.

Ce qui suit est un exemple d'une entrée préférée pour l'activation du serveur DNS pour fournir le nom de domaine de la version 4 de NFS :

```
_nfsv4idmapdomain       IN      TXT             "foo.bar"
```

Dans cet exemple, le nom de domaine à configurer est la valeur qui est entourée de guillemets. Notez qu'aucun champ `ttl` n'est spécifié et qu'aucun domaine n'est ajouté à `_nfsv4idmapdomain`, qui est la valeur dans le champ `owner`. Cette configuration permet à l'enregistrement TXT d'utiliser l'entrée de la zone `${ORIGIN}` de l'enregistrement SOA (Start-Of-Authority). Par exemple, à des niveaux différents de l'espace de noms de domaine, l'enregistrement peut se lire comme suit :

```
_nfsv4idmapdomain.subnet.yourcorp.com.    IN    TXT    "foo.bar"
_nfsv4idmapdomain.yourcorp.com.           IN    TXT    "foo.bar"
```

Cette configuration offre aux clients DNS la souplesse d'utilisation du fichier `resolv.conf` pour effectuer une recherche dans la hiérarchie de l'arborescence DNS. Reportez-vous à la page de manuel `resolv.conf(4)`. Cette fonctionnalité fournit une plus grande probabilité de trouver l'enregistrement TXT. Pour encore plus de flexibilité, les sous-domaines DNS de niveau inférieur peuvent définir leurs propres enregistrements de ressources DNS TXT. Cette fonction permet aux sous-domaines DNS de niveau inférieur de remplacer l'enregistrement TXT qui est défini par le domaine DNS de niveau supérieur.

Remarque – Le domaine qui est spécifié par l'enregistrement TXT peut être une chaîne arbitraire qui ne correspond pas nécessairement au domaine DNS pour les clients et les serveurs qui utilisent la version 4 de NFS. Vous avez la possibilité de ne pas partager les données de la version 4 de NFS avec d'autres domaines DNS.

Vérification du domaine de la version 4 de NFS

Avant d'attribuer une valeur pour le domaine de la version 4 de NFS de votre réseau, vérifiez si un domaine de la version 4 de NFS a déjà été configuré pour votre réseau. Les exemples suivants constituent des moyens d'identifier le domaine de la version 4 de NFS de votre réseau.

- Pour identifier le domaine de la version 4 de NFS à partir d'un enregistrement de ressources DNS TXT, utilisez la commande `nslookup` ou `dig` :

Le tableau suivant présente un exemple de sortie pour la `nslookup` commande :

```
# nslookup -q=txt _nfsv4idmapdomain
Server:         10.255.255.255
Address:        10.255.255.255#53

_nfsv4idmapdomain.example.company.com text = "company.com"
```

Reportez-vous à cet exemple de sortie pour la commande `dig` :

```
# dig +domain=example.company.com -t TXT _nfsv4idmapdomain
...
;; QUESTION SECTION:
;_nfsv4idmapdomain.example.company.com. IN    TXT

;; ANSWER SECTION:
_nfsv4idmapdomain.example.company.com. 21600 IN TXT   "company.com"

;; AUTHORITY SECTION:
...
```

Pour plus d'informations sur la configuration d'un enregistrement de ressources DNS TXT, voir “`nfsmapid` et enregistrements DNS TXT” à la page 152.

- Si votre réseau n'est pas configuré avec un enregistrement de ressources DNS TXT de la version 4 de NFS, utilisez la commande suivante pour identifier votre domaine de la version 4 de NFS à partir du nom de domaine DNS :

  ```
  # egrep domain /etc/resolv.conf
  domain example.company.com
  ```

- Si le fichier `/etc/resolv.conf` n'est pas configuré pour fournir un nom de domaine DNS au client, utilisez la commande suivante pour identifier le domaine à partir de la configuration de domaine du réseau de la version 4 de NFS :

  ```
  # cat /var/run/nfs4_domain
  company.com
  ```

- Si vous utilisez un autre service d'attribution de noms, tel que NIS, utilisez la commande suivante pour identifier le domaine pour le service d'attribution de nom configuré pour votre réseau :

  ```
  # domainname
  it.example.company.com
  ```

Pour plus d'informations, reportez-vous aux pages de manuel suivantes :

- `nslookup`(1M)
- `dig`(1M)
- `resolv.conf`(4)
- `domainname`(1M)

Configuration du domaine par défaut de la version 4 de NFS

Cette section décrit comment le réseau obtient le domaine par défaut souhaité :

- Pour la plupart des versions actuelles, reportez-vous à la section "Configuration du domaine par défaut de la version 4 de NFS" à la page 154.
- Pour la première version de Solaris 10, reportez-vous à la rubrique "Configuration d'un domaine par défaut de la version 4 de NFS dans la version Solaris 10" à la page 156.

Configuration du domaine par défaut de la version 4 de NFS

Dans la première version de Solaris 10, le domaine était défini lors du premier redémarrage après l'installation du système d'exploitation. Dans les versions ultérieures, le domaine de la version 4 de NFS est défini au cours de l'installation du système d'exploitation. Pour fournir cette fonctionnalité, les fonctions suivantes ont été ajoutées :

- La commande `sysidtool` inclut le programme `sysidnfs4`. Le programme s'exécute pendant la phase d'installation afin de déterminer si un domaine de la version 4 de NFS a été configuré pour le réseau. Reportez-vous aux pages de manuel `sysidtool(1M)` et `sysidnfs4(1M)`.
- Le fichier `sysidcfg` a un nouveau mot-clé, `nfs4_domain`. Ce mot-clé peut être utilisé pour définir le domaine de la version 4 de NFS. Notez que d'autres mots-clés peuvent être définis dans le fichier `sysidcfg`. Reportez-vous à la page de manuel `sysidcfg(4)`.

La section suivante décrit le fonctionnement de la fonctionnalité :

1. Le programme `sysidnfs4` vérifie le fichier `/etc/.sysIDtool.state` afin de déterminer si un domaine de la version 4 de NFS a été identifié.
   - Si le fichier `.sysIDtool.state` indique qu'un domaine de la version 4 de NFS a été configuré pour le réseau, le programme `sysidnfs4` n'effectue pas de contrôles supplémentaires. Voir l'exemple suivant d'un fichier `.sysIDtool.state` :

     ```
     1       # System previously configured?
     1       # Bootparams succeeded?
     1       # System is on a network?
     1       # Extended network information gathered?
     1       # Autobinder succeeded?
     1       # Network has subnets?
     1       # root password prompted for?
     1       # locale and term prompted for?
     1       # security policy in place
     1       # NFSv4 domain configured
     xterms
     ```

     Le `1` qui s'affiche avant `# NFSv4 domain configured` confirme que le domaine de la version 4 de NFS a été configuré.
   - Si le fichier `.sysIDtool.state` indique qu'aucun domaine de la version 4 de NFS n'a été configuré pour le réseau, le programme `sysidnfs4` doit effectuer des contrôles supplémentaires. Voir l'exemple suivant d'un fichier `.sysIDtool.state` :

```
1       # System previously configured?
1       # Bootparams succeeded?
1       # System is on a network?
1       # Extended network information gathered?
1       # Autobinder succeeded?
1       # Network has subnets?
1       # root password prompted for?
1       # locale and term prompted for?
1       # security policy in place
0       # NFSv4 domain configured
xterms
```

Le `0` qui s'affiche avant `# NFSv4 domain configured` confirme qu'aucun domaine de la version 4 de NFS n'a été configuré.

2. Si aucun domaine de la version 4 de NFS n'a été identifié, le programme `sysidnfs4` vérifie le mot-clé `nfs4_domain` dans le fichier `sysidcfg`.
   - Si une valeur pour `nfs4_domain` existe, cette valeur est affectée au mot-clé NFSMAPID_DOMAIN dans le fichier `/etc/default/nfs`. Notez que toute valeur affectée à NFSMAPID_DOMAIN remplace la fonctionnalité de sélection de domaine dynamique du démon `nfsmapid`. Pour plus d'informations sur la fonctionnalité de sélection de domaine dynamique de `nfsmapid`, reportez-vous à la rubrique "Règles de priorité" à la page 151.
   - En l'absence d'une valeur pour `nfs4_domain`, le programme `ysidnfs4` identifie le domaine que `nfsmapid` dérive des services de noms configurés du système d'exploitation. Cette valeur dérivée est présentée en tant que domaine par défaut à une invite de commande interactive qui vous donne la possibilité d'accepter la valeur par défaut ou d'affecter un autre domaine de la version 4 de NFS.

Cette fonctionnalité rend obsolète les suivantes :

- L'exemple de script JumpStart, `set_nfs4_domain` , qui a été fourni dans le média de distribution initial de Solaris 10 n'est plus nécessaire ni recommandé.
- Le fichier `/etc/.NFS4inst_state.domain`, qui a été créé par l'implémentation précédente du programme `sysidnfs4`, n'est plus nécessaire.

Remarque – Compte tenu de la nature évolutive et omniprésente de DNS, l'utilisation des enregistrements DNS TXT pour la configuration du domaine de déploiements de la version 4 de NFS de grande envergure continue d'être préférée et fortement encouragée. Reportez-vous à la rubrique "`nfsmapid` et enregistrements DNS TXT" à la page 152.

Pour obtenir des informations spécifiques sur le processus d'installation de Solaris, reportez-vous aux sections suivantes :

- *Guide d'installation d'Oracle Solaris 10 9/10 : installations de base*
- *Guide d'installation Oracle Solaris 10 9/10 : installations réseau*

Configuration d'un domaine par défaut de la version 4 de NFS dans la version Solaris 10

Dans la première version Solaris 10 de la version 4 de NFS, si votre réseau comporte plusieurs domaines DNS, mais ne dispose que d'un seul espace de noms UID et GID, tous les clients doivent utiliser une valeur pour NFSMAPID_DOMAIN. Pour les sites utilisant DNS, `nfsmapid` résout ce problème en obtenant le nom de domaine à partir de la valeur attribuée à `_nfsv4idmapdomain`. Pour plus d'informations, reportez-vous à la rubrique "`nfsmapid` et enregistrements DNS TXT" à la page 152. Si le réseau n'est pas configuré pour utiliser DNS, lors de la première initialisation du système, le SE utilise l'utilitaire `sysidconfig(1M)` afin de générer les invites suivantes pour le nom de domaine de la version 4 de NFS :

```
This system is configured with NFS version 4, which uses a
domain name that is automatically derived from the system's
name services. The derived domain name is sufficient for most
configurations. In a few cases, mounts that cross different
domains might cause files to be owned by nobody due to the
lack of a common domain name.

Do you need to override the system's default NFS verion 4 domain
name (yes/no)? [no]
```

La réponse par défaut est `[no]`. Si vous choisissez l'option `[no]` , vous pouvez voir les éléments suivants :

```
For more information about how the NFS version 4 default domain name is
derived and its impact, refer to the man pages for nfsmapid(1M) and
nfs(4), and the System Administration Guide: Network Services.
```

Si vous choisissez l'option `[yes]`, vous voyez cette invite :

```
Enter the domain to be used as the NFS version 4 domain name.
NFS version 4 domain name []:
```

Remarque – Si une valeur pour NFSMAPID_DOMAIN existe dans `/etc/default/nfs`, le `[nom_domaine]` que vous fournissez remplace cette valeur.

Informations complémentaires sur `nfsmapid`

Pour plus d'informations sur `nfsmapid`, reportez-vous aux éléments suivants :

- Page de manuel `nfsmapid(1M)`
- Page de manuel `nfs(4)`
- `http://www.ietf.org/rfc/rfc1464.txt`
- "Listes de contrôle d'accès (ACL) et `nfsmapid` dans la version 4 de NFS" à la page 192

Démon `statd`

Ce démon fonctionne avec `lockd` afin de fournir des fonctions de récupération en cas d'arrêt brutal au gestionnaire de verrous. Le démon `statd` permet de suivre les clients qui détiennent les verrous sur un serveur NFS. Si un serveur tombe en panne, au redémarrage, `statd` sur le serveur contacte `statd` sur le client. Le client `statd` peut alors tenter de récupérer les verrous sur le serveur. Le client `statd` informe également le serveur `statd` lorsqu'un client a subi un blocage afin que les verrous du client sur le serveur puissent être effacés. Vous n'avez aucune option à sélectionner avec ce démon. Pour plus d'informations, reportez-vous à la page de manuel `statd(1M)`.

Dans la version Solaris 7, la manière dont `statd` suit les clients a été améliorée. Dans toutes les versions Solaris antérieures, `statd` créé des fichiers dans `/var/statmon/sm` pour chaque client à l'aide du nom d'hôte non qualifié du client. Cette attribution de noms de fichiers provoquait des problèmes si vous aviez deux clients dans des domaines différents partageant un nom d'hôte, ou si les clients ne résidaient pas dans le même domaine que le serveur NFS. Parce que le nom d'hôte non qualifié répertorie uniquement le nom d'hôte, en l'absence de domaine ou d'informations sur l'adresse IP, l'ancienne version de `statd` n'avait aucun moyen de faire la distinction entre ces types de clients. Pour résoudre ce problème, `statd` de Solaris 7 crée un lien symbolique dans `/var/statmon/sm` vers le nom d'hôte non qualifié à l'aide de l'adresse IP du client. Le nouveau lien ressemble à ce qui suit :

```
# ls -l /var/statmon/sm
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv4.192.168.255.255 -> myhost
lrwxrwxrwx   1 daemon          11 Apr 29 16:32 ipv6.fec0::56:a00:20ff:feb9:2734 -> v6host
--w-------   1 daemon          11 Apr 29 16:32 myhost
--w-------   1 daemon          11 Apr 29 16:32 v6host
```

Dans cet exemple, le nom d'hôte du client est `myhost` et l'adresse IP du client est `192.168.255.255`. Si un autre hôte avec le nom `myhost` montait un système de fichiers, deux liens symboliques mèneraient au nom d'hôte.

Remarque – La version 4 de NFS n'utilise pas ce démon.

Commandes NFS

Ces commandes doivent être exécutées en tant que `root` pour être pleinement efficaces, mais les requêtes d'informations peuvent être effectuées par tous les utilisateurs :

- “Commande `setmnt`” à la page 175
- “Commande `share`” à la page 167
- “Commande `shareall`” à la page 173
- “Commande `showmount`” à la page 174
- “Commande `umount`” à la page 165
- “Commande `umountall`” à la page 167
- “Commande `unshare`” à la page 172
- “Commande `unshareall`” à la page 173

Commande `automount`

Cette commande installe les points de montage autofs et associe les informations dans les fichiers automaster à chaque point de montage. La syntaxe de la commande est indiquée ci-après.

`automount [ -t` *durée* `] [ -v ]`

`-t` *durée* définit la durée, en secondes, qu'un système de fichiers doit rester monté, et `-v` sélectionne le mode détaillé. L'exécution de cette commande en mode détaillé facilite le dépannage.

Si elle n'est pas définie de façon spécifique, la valeur de durée est définie sur 5 minutes. Dans la plupart des cas, cette valeur est bonne. Cependant, sur les systèmes qui ont de nombreux systèmes de fichiers montés automatiquement, vous pouvez être amené à augmenter la valeur de durée. En particulier, si un serveur a beaucoup d'utilisateurs actifs, la vérification des systèmes de fichiers montés automatiquement toutes les 5 minutes peut s'avérer inefficace. Une vérification des systèmes de fichiers autofs toutes les 1800 secondes (c'est-à-dire 30 minutes) pourrait être plus optimale. En ne démontant pas les systèmes de fichiers toutes les 5 minutes, la taille de `/etc/mnttab` peut devenir importante. Pour réduire la sortie lorsque `df` vérifie chaque entrée dans `/etc/mnttab`, vous pouvez filtrer la sortie de `df` en utilisant l'option `-F` (voir la page de manuel `df(1M)`) ou en utilisant `egrep`.

Vous pouvez considérer que l'ajustement de la durée modifie également la rapidité avec laquelle les modifications apportées aux mappes de l'agent de montage sont reflétées. Aucune modification n'est visible tant que le système de fichiers n'est pas démonté. Reportez-vous à la rubrique “Modification des mappages” à la page 110 pour obtenir des instructions sur la manière de modifier les mappes de montage automatique.

`clear_locks`, commande

Cette commande vous permet de supprimer tous les verrous de fichiers, d'enregistrement et de partage pour un client NFS. Vous devez être un `superutilisateur` pour exécuter cette commande. À partir d'un serveur NFS, vous pouvez effacer les verrous pour un client

spécifique. À partir d'un client NFS, vous pouvez effacer les verrous pour ce client sur un serveur spécifique. Dans l'exemple suivant, effacez les verrous pour le client NFS nommé `tulip` sur le système actuel.

```
# clear_locks tulip
```

À l'aide de l'option `-s` vous pouvez indiquer de quels hôtes NFS effacer les verrous. Vous devez exécuter cette option à partir du client NFS qui a créé les verrous. Dans cette situation, les verrous provenant du client seraient supprimés du serveur NFS qui est nommé bee.

```
# clear_locks -s bee
```

Attention – Cette commande ne doit être exécutée lorsqu'un client tombe en panne et que vous ne pouvez pas effacer ses verrous externes. Afin d'éviter une altération des données, n'effacez pas les verrous pour un client actif.

Commande `fsstat`

À partir de la version Solaris 10 11/06, l'utilitaire `fsstat` vous permet de surveiller les opérations du système de fichiers par type de système de fichiers et par point de montage. Diverses options permettent de personnaliser la sortie. Reportez-vous aux exemples suivants :

Cet exemple illustre la sortie de la version 3 de NFS, la version 4 et le point de montage `root` .

```
% fsstat nfs3 nfs4 /
  new     name   name    attr    attr   lookup   rddir   read   read   write   write
 file    remov   chng     get     set      ops     ops    ops  bytes     ops   bytes
3.81K      90  3.65K   5.89M   11.9K    35.5M   26.6K   109K   118M   35.0K   8.16G  nfs3
  759     503    457   93.6K   1.44K     454K   8.82K  65.4K   827M     292    223K  nfs4
25.2K   18.1K  1.12K   54.7M    1017     259M   1.76M  22.4M  20.1G   1.43M   3.77G  /
```

Cet exemple utilise l'option `-i` pour fournir des statistiques sur les opérations d'E/S pour la version 3 de NFS, la version 4 et le point de montage `root`.

```
% fsstat -i nfs3 nfs4 /
 read    read    write   write   rddir   rddir   rwlock   rwulock
  ops   bytes      ops   bytes     ops   bytes      ops       ops
 109K    118M    35.0K   8.16G   26.6K   4.45M     170K      170K  nfs3
65.4K    827M      292    223K   8.82K   2.62M    74.1K     74.1K  nfs4
22.4M   20.1G    1.43M   3.77G   1.76M   3.29G    25.5M     25.5M  /
```

Cet exemple utilise l'option `-n` pour fournir des statistiques sur les opérations de dénomination de la version 3 de NFS, de la version 4 et du point de montage `root`.

```
% fsstat -n nfs3 nfs4 /
lookup   creat   remov  link   renam  mkdir  rmdir   rddir  symlnk  rdlnk
 35.5M   3.79K      90     2   3.64K      5      0   26.6K      11   136K  nfs3
  454K     403     503     0     101      0      0   8.82K     356  1.20K  nfs4
  259M   25.2K   18.1K   114    1017     10      2   1.76M      12  8.23M  /
```

Pour plus d'informations, reportez-vous à la page de manuel `fsstat(1M)`.

Commande `mount`

À l'aide de cette commande, vous pouvez joindre un système de fichiers nommé, qu'il soit local ou distant, à un point de montage spécifié. Pour plus d'informations, reportez-vous à la page de manuel `mount(1M)`. Utilisée sans arguments, `mount` affiche la liste des systèmes de fichiers actuellement montés sur votre ordinateur.

De nombreux types de systèmes de fichiers sont inclus dans la version standard de l'installation Solaris. Chaque type de système de fichiers possède une page de manuel spécifique qui répertorie les options pour `mount` qui sont appropriés pour ce type de système de fichiers. La page de manuel pour les systèmes de fichiers NFS est `mount_nfs(1M)`. Pour les systèmes de fichiers UFS, voir `mount_ufs(1M)`.

Solaris 7 inclut la possibilité de sélectionner un nom de chemin d'accès pour monter à partir d'un serveur NFS à l'aide d'un URL NFS au lieu de la syntaxe standard `server:/chemin` . Reportez-vous à la rubrique “Montage d'un système de fichiers NFS à l'aide d'un URL NFS ” à la page 95 pour plus d'informations.

Attention – La version de la commande `mount` n'émet pas d'avertissement à propos des options non valides. La commande ignore de manière silencieuse toutes les options qui ne peuvent pas être interprétées. Assurez-vous de vérifier toutes les options qui ont été utilisées afin d'éviter tout comportement inattendu.

Options `mount` pour les systèmes de fichiers NFS

La suite du texte répertorie certaines des options qui peuvent suivre l'indicateur `-o` lorsque vous montez un système de fichiers NFS. Pour obtenir la liste complète des options, reportez-vous à la page de manuel `mount_nfs(1M)`.

bg|fg
: Ces options peuvent être utilisées pour sélectionner le comportement de relance en cas d'échec d'un montage. L'option `bg` fait que le montage tente de s'exécuter en arrière-plan. L'option `fg` fait que le montage tente de s'exécuter au premier plan. La valeur par défaut est `fg`, qui est le meilleur choix pour les systèmes de fichiers qui doivent être disponibles. Cette option empêche tout traitement supplémentaire tant que le montage n'est pas terminé. `bg` est un bon choix pour les systèmes de fichiers non critiques car le client peut effectuer d'autres traitements tout en attendant que la demande de montage soit terminée.

forcedirectio
: Cette option améliore les performances des transferts de données séquentielles de grande taille. Les données sont copiées directement sur un tampon utilisateur. Aucune mise en cache n'est effectuée dans le noyau sur le client. Cette option est désactivée par défaut.

Auparavant, toutes les requêtes d'écriture étaient numérotées par le client NFS et le serveur NFS. Le client NFS a été modifié pour permettre à une application d'émettre des écritures simultanées, ainsi que des lectures et des écritures simultanées, vers un fichier unique. Vous pouvez activer cette fonctionnalité sur le client à l'aide de l'option de montage `forcedirectio`. Lorsque vous utilisez cette option, vous activez cette fonctionnalité pour tous les fichiers situés dans le système de fichiers monté. Vous pouvez également l'activer sur un seul fichier du client à l'aide de l'interface `directio. ()` Les écritures vers les fichiers sont numérotées si cette fonctionnalité n'est pas activée. D'autre part, si des écritures simultanées ou des lectures et écritures simultanées se produisent, alors la sémantique POSIX n'est plus prise en charge pour ce fichier.

Reportez-vous à la rubrique "Utilisation de la commande `mount`" à la page 163 pour obtenir un exemple d'utilisation de cette option.

largefiles
: Avec cette option, vous pouvez accéder aux fichiers de taille supérieure à 2 Go. La possibilité de consulter ou non un fichier de grande taille est contrôlée uniquement sur le serveur ; cette option est ignorée silencieusement sur les montages de la version 3 de NFS. Par défaut, tous les systèmes de fichiers UFS sont montés avec `largefiles`. Pour les montages qui utilisent le protocole de la version 2 de NFS, l'option `largefiles` entraîne un échec de la commande mount.

nolargefiles
: Cette option destinée aux montages UFS garantit qu'aucun fichier de grande taille ne puisse exister sur le système de fichiers. Reportez-vous à la page de manuel `mount_ufs(1M)`. Étant donné que l'existence de fichiers volumineux peut uniquement être contrôlé sur le serveur NFS, aucune option pour `nolargefiles` n'existe en cas d'utilisation des montages NFS. Les tentatives de montage NFS d'un système de fichiers avec cette option sont rejetées avec une erreur.

nosuid|suid
: À partir de la version Solaris 10, l'option `nosuid` équivaut à spécifier l'option `nodevices` avec l'option `nosetuid`. Lorsque l'option `nodevices` est spécifiée, l'ouverture de fichiers spécifiques à un périphérique dans le système de fichiers monté n'est pas autorisée. Lorsque l'option `nosetuid` n'est pas spécifiée, les bits `setuid` et `setgid` dans les fichiers binaires qui se trouvent dans le système de fichiers sont ignorés. Le processus s'exécute avec les privilèges de l'utilisateur qui exécute le fichier binaire.

  L'option `suid` équivaut à spécifier l'option `devices` avec l'option `setuid`. Lorsque l'option `devices` est spécifiée, l'ouverture de fichiers spécifiques à un périphérique dans le système de fichiers monté est autorisée. Lorsque l'option `setuid` est spécifiée, les bits `setuid` et `setgid` dans les fichiers binaires qui sont situés dans le système de fichiers sont pris en compte par le noyau.

  Si aucune option n'est spécifiée, l'option par défaut est `suid`, qui fournit le comportement par défaut de spécification de l'option `devices` avec l'option `setuid`.

Le tableau suivant décrit l'effet de la combinaison de `nosuid` ou `suid` avec `devices` ou `nodevices`, et `setuid` ou `nosetuid`. Notez que pour chaque combinaison d'options, l'option la plus restrictive détermine le comportement.

Comportement des options combinées	Option	Option	Option
L'équivalent de `nosetuid` avec `nodevices`	`nosuid`	`nosetuid`	`nodevices`
L'équivalent de `nosetuid` avec `nodevices`	`nosuid`	`nosetuid`	`devices`
L'équivalent de `nosetuid` avec `nodevices`	`nosuid`	`setuid`	`nodevices`
L'équivalent de `nosetuid` avec `nodevices`	`nosuid`	`setuid`	`devices`
L'équivalent de `nosetuid` avec `nodevices`	`suid`	`nosetuid`	`nodevices`
L'équivalent de `nosetuid` avec `devices`	`suid`	`nosetuid`	`devices`
L'équivalent de `setuid` avec `nodevices`	`suid`	`setuid`	`nodevices`
L'équivalent de `setuid` avec `devices`	`suid`	`setuid`	`devices`

L'option `nosuid` fournit une sécurité supplémentaire pour les clients NFS qui accèdent à de serveurs qui risque de ne pas être de confiance. Le montage de systèmes de fichiers distants à l'aide de cette option permet de réduire le risque de l'escalade des privilèges via l'importation de périphériques non approuvés ou de l'importation de fichiers binaires `setuid` qui ne sont pas fiables. Toutes ces options sont disponibles dans tous les systèmes de fichiers Solaris.

public
: Cette option force l'utilisation de l'indicateur de fichier public lors du contact du serveur NFS. Si l'identificateur de fichier public est pris en charge par le serveur, l'opération de montage est plus rapide, car le protocole MOUNT n'est pas utilisé. En outre, étant donné que ce protocole n'est pas utilisé, l'option public permet au montage de s'effectuer par le biais d'un pare-feu.

rw|ro
: Les options `-rw` et `-ro` indiquent si un système de fichiers doit être monté en lecture-écriture ou en lecture seule. La valeur par défaut est en lecture-écriture, qui est l'option appropriée pour les répertoires d'accueil distants, les répertoires de spool d'e-mail ou autres systèmes de fichiers qui doivent être modifiés par les utilisateurs. L'option lecture seule est appropriée

pour les répertoires qui ne doivent pas être modifiés par les utilisateurs. Par exemple, les copies partagées des pages de manuel ne doivent pas être accessibles en écriture par les utilisateurs.

sec=*mode*
Vous pouvez utiliser cette option pour spécifier le mécanisme d'authentification à utiliser lors de la transaction de montage. La valeur pour *mode* peut être l'une des suivantes.

- Utilisez `krb5` pour le service d'authentification Kerberos version 5.
- Utilisez `krb5i` pour Kerberos version 5 avec intégrité.
- Utilisez `krb5p` pour Kerberos version 5 avec confidentialité.
- Utilisez `none` pour ne pas avoir d'authentification.
- Utilisez `dh` pour l'authentification Diffie-Hellman (DH).
- Utilisez `sys` pour l'authentification UNIX standard.

Les modes sont également définis dans `/etc/nfssec.conf`.

soft|hard
Un système de fichiers NFS qui est monté avec l'option `soft` renvoie une erreur si le serveur ne répond pas. L'option `hard` option fait que le montage continue les tentatives jusqu'à ce que le serveur réponde. La valeur par défaut est `hard`, qui doit être utilisée pour la plupart des systèmes de fichiers. Il arrive fréquemment que les applications ne vérifient pas les valeurs de retour des systèmes de fichiers montés avec `soft`, ce qui peut faire échouer l'application ou causer des corruptions de fichiers. Si l'application ne vérifie pas les valeurs de retour, des problèmes de routage et autres conditions peuvent toujours confondre l'application ou entraîner une corruption du fichier si l'option `soft` est utilisée. Dans la plupart des cas, il est déconseillé d'utiliser l'option `soft`. Si un système de fichiers est monté à l'aide de l'option `hard`, toute application qui utilise ce système de fichiers se bloque jusqu'à ce que le système de fichiers soit disponible.

Utilisation de la commande `mount`

Reportez-vous aux exemples suivants.

- Dans les versions 2 et 3 de NFS, ces deux commandes montent un système de fichiers NFS à partir du serveur bee en lecture seule.

```
# mount -F nfs -r bee:/export/share/man /usr/man
# mount -F nfs -o ro bee:/export/share/man /usr/man
```

Dans la version 4 de NFS, la ligne de commande suivante permettrait d'obtenir le même montage.

```
# mount -F nfs -o vers=4 -r bee:/export/share/man /usr/man
```

- Dans les versions 2 et 3 de NFS, cette commande utilise l'option `-O` pour forcer le montage des pages de manuel du server bee sur le système local, même si `/usr/man` a déjà été monté. Voir ce qui suit.

```
# mount -F nfs -O bee:/export/share/man /usr/man
```

Dans la version 4 de NFS, la ligne de commande suivante permettrait d'obtenir le même montage.

```
# mount -F nfs -o vers=4 -O bee:/export/share/man /usr/man
```

- Dans les versions 2 et 3 de NFS, cette commande utilise le basculement client.

  ```
  # mount -F nfs -r bee,wasp:/export/share/man /usr/man
  ```

  Dans la version 4 de NFS, la ligne de commande suivante utilise le basculement de client.

  ```
  # mount -F nfs -o vers=4 -r bee,wasp:/export/share/man /usr/man
  ```

  Remarque – Lorsqu'ils sont utilisés à partir de la ligne de commande, les serveurs répertoriés doivent prendre en charge la même version du protocole NFS. N'utilisez pas des serveurs version 2 et 3 en même temps lors de l'exécution de `mount` à partir de la ligne de commande. Vous pouvez utiliser les deux serveurs avec autofs. Autofs sélectionne automatiquement le meilleur sous-ensemble des serveurs version 2 ou 3.

- Voici un exemple d'utilisation d'un URL NFS avec la commande `mount` dans les versions 2 et 3 de NFS.

  ```
  # mount -F nfs nfs://bee//export/share/man /usr/man
  ```

  Voici un exemple d'utilisation d'un URL NFS avec la commande `mount` commande dans la version 4 de NFS.

  ```
  # mount -F nfs -o vers=4 nfs://bee//export/share/man /usr/man
  ```

- Utilisez l'option de montage `forcedirectio` afin de permettre au client d'autoriser les écritures simultanées, ainsi que les lectures et écritures simultanées, sur un fichier. Voici un exemple.

  ```
  # mount -F nfs -o forcedirectio bee:/home/somebody /mnt
  ```

  Dans cet exemple, la commande permet de monter un système de fichiers NFS à partir du serveur bee et permet les lectures et écritures simultanées pour chaque fichier dans le répertoire `/mnt`. Lorsque la prise en charge des lectures et écritures simultanées est activée, ce qui suit se produit.

  - Le client permet aux applications d'écrire dans un fichier en parallèle.
  - La mise en cache est désactivée sur le client. Par conséquent, les données des lectures et des écritures sont conservées sur le serveur. Plus explicitement, puisque le client ne met pas en mémoire cache les données lues ou écrites, toutes les données que l'application n'a pas encore mises en mémoire cache pour elle-même sont lues à partir du serveur. Le système d'exploitation du client n'a pas de copie de ces données. Normalement, le client NFS met en cache les données dans le noyau pour les applications à utiliser.

    Puisque la mise en cache est désactivée sur le client, les processus d'écriture ultérieure et de lecture anticipée sont désactivés. Un processus de lecture anticipée se produit lorsque le noyau anticipe les données qu'une application peut nécessiter par la suite. Le noyau

démarre ensuite le processus de collecte anticipée de données. L'objectif du noyau est d'avoir les données prêtes avant que l'application effectue une demande de données.

Le client utilise le processus d'écriture ultérieure afin d'améliorer le débit d'écriture. Au lieu de commencer immédiatement une opération d'E/S à chaque fois qu'une application écrit des données dans un fichier, les données sont mises en mémoire cache. Les données sont écrites ultérieurement sur le disque.

Le processus d'écriture ultérieure peut permettre aux données d'être écrites en portions plus grandes ou d'être écrites en mode asynchrone à partir de l'application. En règle générale, le résultat de l'utilisation de portions de mémoire plus grandes est une augmentation du débit. Les écritures asynchrones autorisent les chevauchements entre le traitement d'application et le traitement d'E/S. En outre, les écritures asynchrones autorisent le sous-système de stockage afin d'optimiser l'E/S en fournissant un meilleur séquencement des E/S. Les écritures synchrones forcent une séquence d'E/S sur le sous-système de stockage qui pourrait ne pas être optimale.

- Une dégradation importante des performances peut se produire si l'application n'est pas prête à gérer la sémantique des données qui ne sont pas mises en mémoire cache. Les applications multithread évitent ce problème.

Remarque – Si la prise en charge des écritures simultanées n'est pas activée, toutes les demandes d'écriture sont sérialisées. Lorsque les demandes sont sérialisées, ce qui suit se produit. Lorsqu'une demande d'écriture est en cours d'exécution, une deuxième demande d'écriture doit attendre que la première demande d'écriture soit terminé avant de poursuivre.

- Utilisez la commande `mount` sans arguments pour afficher les systèmes de fichiers montés sur un client. Voir ce qui suit.

```
% mount
/ on /dev/dsk/c0t3d0s0 read/write/setuid on Wed Apr 7 13:20:47 2004
/usr on /dev/dsk/c0t3d0s6 read/write/setuid on Wed Apr 7 13:20:47 20041995
/proc on /proc read/write/setuid on Wed Apr 7 13:20:47 2004
/dev/fd on fd read/write/setuid on Wed Apr 7 13:20:47 2004
/tmp on swap read/write on Wed Apr 7 13:20:51 2004
/opt on /dev/dsk/c0t3d0s5 setuid/read/write on Wed Apr 7 13:20:51 20041995
/home/kathys on bee:/export/home/bee7/kathys
  intr/noquota/nosuid/remote on Wed Apr 24 13:22:13 2004
```

Commande `umount`

Cette commande permet de supprimer un système de fichiers actuellement monté. La commande `umount` prend en charge l'option `-V` pour permettre des tests. Vous pouvez également utiliser l'option `-a` pour démonter plusieurs systèmes de fichiers en même temps. Si des *points de montage* sont inclus avec l'option `-a`, ces systèmes de fichiers sont démontés. Si aucun point de montage n'est inclus, une tentative est faite pour démonter tous les systèmes de

fichiers qui sont répertoriés dans `/etc/mnttab` à l'exception des systèmes de fichiers requis tels que `/`, `/usr`, `/var`, `/proc`, `/dev/fd` et `/tmp`. Parce que le système de fichiers est déjà monté et doit disposer d'une entrée dans `/etc/mnttab`, vous n'avez pas besoin d'inclure un indicateur pour le type de système de fichiers.

L'option `-f` force un système de fichiers occupé à être démonté. Vous pouvez utiliser cette option pour débloquer un client bloqué lors de la tentative de montage d'un système de fichiers impossible à monter.

Attention – En forçant le démontage d'un système de fichiers, vous pouvez entraîner une perte de données si les fichiers sont en cours d'écriture.

Reportez-vous aux exemples suivants :

EXEMPLE 6–1 Démontage d'un système de fichiers

Dans cet exemple, un système de fichiers monté sur `/usr/man` est démonté :

```
# umount /usr/man
```

EXEMPLE 6–2 Utilisation d'options avec `umount`

Cet exemple affiche les résultats de l'exécution de `umount -a -V` :

```
# umount -a -V
umount /home/kathys
umount /opt
umount /home
umount /net
```

Notez que cette commande ne démonte pas réellement les systèmes de fichiers.

Commande `mountall`

Utilisez la commande suivante pour monter tous les systèmes de fichiers ou un groupe spécifique de systèmes de fichiers qui sont répertoriés dans une table du système de fichiers. La commande fournit un moyen de réaliser les opérations suivantes :

- sélection du type de système de fichiers auxquels accéder à l'aide de l'option `-F` *FSType* ;
- sélection de tous les systèmes de fichiers distants répertoriés dans une table du système de fichiers avec l'option `-r`.
- Sélection de tous les systèmes de fichiers locaux avec l'option `-l`

Étant donné que tous les systèmes de fichiers libellés en tant que systèmes de fichiers NFS sont des systèmes de fichiers à distance, certaines de ces options sont redondantes. Pour plus d'informations, reportez-vous à la page de manuel `mountall(1M)`.

Notez que les deux exemples ci-dessous d'entrées utilisateur sont équivalents :

```
# mountall -F nfs

# mountall -F nfs -r
```

Commande `umountall`

Utilisez cette commande pour démonter un groupe de systèmes de fichiers. L'option `-k` exécute la commande `fuser -k` *point de montage* pour interrompre tout processus associé au *point de montage*. L'option `-s` indique que le démontage ne doit pas s'effectuer en parallèle. `-l` indique que seuls les systèmes de fichiers locaux sont à utiliser, et `-r` indique que seuls les systèmes de fichiers à distance doivent être utilisés. L'option `-h` *host* indique que tous les systèmes de fichiers de l'hôte nommé doivent être démontés. Vous ne pouvez pas combiner l'option `-h` option avec `-l` ou `-r`.

Ce qui suit est un exemple de démontage de tous les systèmes de fichiers qui sont montés à partir d'hôtes distants :

```
# umountall -r
```

Ce qui suit est un exemple de démontage de tous les systèmes de fichiers qui sont actuellement montés à partir du serveur `bee` :

```
# umountall -h bee
```

Commande `share`

À l'aide de cette commande, vous pouvez rendre un système de fichiers local sur un serveur NFS disponible pour le montage. Vous pouvez également utiliser la commande `share` pour afficher la liste des systèmes de fichiers sur votre système qui sont actuellement partagés. Le serveur NFS doit être en cours d'exécution pour que la commande `share` fonctionne. Le logiciel du serveur NFS est automatiquement lancé lors du démarrage si une entrée est dans `/etc/dfs/dfstab`. La commande ne signale pas d'erreur si le logiciel du serveur NFS n'est pas en cours d'exécution ; vous devez donc vérifier que le logiciel est en cours d'exécution.

Les objets qui peuvent être partagés incluent toute arborescence de répertoires. Cependant, chaque hiérarchie de système de fichiers est limitée par la tranche de disque ou la partition dans laquelle se trouve le système de fichiers. Par exemple, le partage du système de fichiers racine (`/`) ne partagerait pas `/usr`, sauf si ces répertoires sont sur la même partition ou tranche de disque. L'installation normale place le système de fichiers racine sur la tranche 0 et `/usr` sur la tranche 6. En outre, le partage de `/usr` ne partage pas les autres partitions de disque local qui sont montées sur des sous-répertoires de `/usr`.

Un système de fichiers ne peut pas être partagé si ce système de fichiers fait partie d'un plus grand système de fichiers qui est déjà partagé. Si, par exemple, `/usr` et `/usr/local` sont sur une tranche de disque, `/usr` ou `/usr/local` peuvent être partagés. Toutefois, si les deux répertoires doivent être partagés avec différentes options de partage, `/usr/local` doit être déplacé vers une autre tranche de disque.

Vous pouvez accéder à un système de fichiers partagé en lecture seule par l'intermédiaire de l'indicateur de fichier d'un système de fichiers partagé en lecture-écriture. Cependant, les deux systèmes de fichiers doivent être sur la même tranche de disque. Vous pouvez créer une situation plus sécurisée. Placez les systèmes de fichiers qui doivent être en lecture-écriture sur une autre partition ou une tranche de disque distincte des systèmes de fichiers que vous souhaitez partager en lecture seule.

Remarque – Pour plus d'informations sur le fonctionnement de la version 4 de NFS lorsque le partage d'un système de fichiers est annulé puis rétabli, reportez-vous à "Annulation et rétablissement du partage d'un système de fichiers dans la version 4 de NFS" à la page 184.

Options `share` non spécifiques aux systèmes de fichiers

Certaines des options qu'il est possible d'inclure à l'indicateur `-o` sont comme suit.

rw|ro
: Le chemin de fichiers *pathname* est partagé en lecture-écriture ou en lecture seule pour tous les clients.

rw=*accesslist*
: Le système de fichiers est partagé en lecture-écriture uniquement pour les clients répertoriés. Toutes les autres demandes sont refusées. À partir de la version Solaris 2.6, la liste des clients qui sont définis dans *accesslist* a été étendue. Reportez-vous à la rubrique "Définition des listes d'accès avec la commande `share`" à la page 170 pour plus d'informations. Vous pouvez utiliser cette option pour ignorer l'option `-ro`.

Options `share` spécifiques à NFS

Les options que vous pouvez utiliser avec les systèmes de fichiers NFS sont les suivantes.

aclok
: Cette option permet à un serveur NFS qui prend en charge le protocole de la version 2 de NFS d'être configuré afin de pouvoir effectuer un contrôle d'accès pour les clients de la version 2 de NFS. Sans cette option, tous les clients se voient attribuer un accès minimal. Avec cette option, les clients ont un accès maximal. Par exemple, sur les systèmes de fichiers qui sont partagés avec l'option `-aclok`, si une personne dispose d'autorisations en lecture, tout le monde en dispose. Toutefois, sans cette option, vous pouvez refuser l'accès à un client qui doit disposer d'autorisations d'accès. Une décision d'autoriser trop ou pas assez d'accès dépend de la sécurité des systèmes déjà en place. Reportez-vous à la rubrique "Using Access

Control Lists to Protect UFS Files" du *System Administration Guide: Security Services* pour plus d'informations sur les listes de contrôle d'accès (ACL).

Remarque – Pour utiliser des ACL, assurez-vous que les clients et les serveurs exécutent un logiciel qui prend en charge la version 3 de NFS et les protocoles NFS_ACL. Si le logiciel prend en charge uniquement le protocole de la version 3 de NFS, les clients obtiennent un accès correct mais ne peuvent pas manipuler les listes de contrôle d'accès (ACL). Si le logiciel prend en charge le protocole NFS_ACL, les clients obtiennent un accès correct et peuvent manipuler les listes de contrôle d'accès (ACL).

---

anon=*uid*
: Utilisez *uid* pour sélectionner les ID d'utilisateurs non authentifiés. Si vous définissez *uid* sur `-1`, le serveur refuse l'accès aux utilisateurs non authentifiés. Vous pouvez accorder un accès à la racine en définissant `anon=0`, mais cette option permettant aux utilisateurs non authentifiés d'avoir un accès à la racine, il est préférable d'utiliser l'option `root`.

index=*nom_fichier*
: Lorsqu'un utilisateur accède à un URL NFS, l'option `-index=` *nom_fichier* force le chargement du fichier HTML, au lieu d'afficher une liste du répertoire. Cette option imite l'action des navigateurs courants si un fichier `index.html` est trouvé dans le répertoire auquel accède l'URL HTTP. Cette option est l'équivalent de la définition de l'option `DirectoryIndex` pour `httpd`. Par exemple, supposons que l'entrée de fichier `dfstab` ressemble à la suivante :

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

Ces URL affichent ensuite les mêmes informations :

```
nfs://<server>/<dir>
nfs://<server>/<dir>/index.html
nfs://<server>//export/web/<dir>
nfs://<server>//export/web/<dir>/index.html
http://<server>/<dir>
http://<server>/<dir>/index.html
```

log=*balise*
: Cette option spécifie la balise dans `/etc/nfs/nfslog.conf` qui contient les informations de configuration de journalisation du serveur NFS pour un système de fichiers. Cette option doit être sélectionnée pour activer la journalisation du serveur NFS.

nosuid
: Cette option signale que toutes les tentatives d'activation du mode `setuid` ou `setgid` doivent être ignorées. Les clients NFS ne peuvent pas créer de fichiers avec les bits `setuid` ou `setgid` activés.

public
: L'option `-public` a été ajoutée à la commande `share` pour activer la navigation WebNFS. Un seul système de fichiers sur un serveur peut être partagé avec cette option.

root=*accesslist*
: Le serveur donne accès à la racine aux hôtes dans la liste. Par défaut, le serveur ne donne pas accès à la racine aux hôtes distants. Si le mode de sécurité n'est pas `-sec=sys`, vous pouvez inclure uniquement les noms d'hôtes du client dans *accesslist*. À partir de la version Solaris 2.6, la liste des clients qui sont définis dans *accesslist* a été étendue. Reportez-vous à la rubrique "Définition des listes d'accès avec la commande `share`" à la page 170 pour plus d'informations.

Attention – Le fait d'accorder un accès à la racine à d'autres hôtes a des implications significatives en matière de sécurité. Utilisez l'option `-root=` avec la plus grande prudence.

root=*client-name*
: La valeur *client-name* est utilisée avec l'authentification AUTH_SYS pour vérifier l'adresse IP du client sur la base d'une liste d'adresses fournies par `exportfs`(1B). Si une correspondance est trouvée, l'accès `root` est donné à les systèmes de fichiers partagés.

root=*host-name*
: Pour les modes NFS sécurisés tels que AUTH_SYS ou RPCSEC_GSS, le serveur vérifie les noms principaux des clients sur la base d'une liste de noms principaux basées sur l'hôte qui sont dérivés d'une liste d'accès. La syntaxe générique pour le nom principal de client est `root@`*hostname*. Pour Kerberos V la syntaxe est `root/`*hostname.fully.qualified*`@REALM`. Lorsque vous utilisez la valeur *host-name*, les clients sur la liste d'accès doivent avoir les informations d'identification et de connexion d'un nom principal. Pour Kerberos V, le client doit avoir une entrée keytab valide pour son nom principal `root/`*hostname.fully.qualified*`@REALM`. Pour plus d'informations, reportez-vous à "Configuring Kerberos Clients" du *System Administration Guide: Security Services*.

sec=*mode*[:*mode*]
: *mode* sélectionne les modes de sécurité qui sont nécessaires pour obtenir l'accès au système de fichiers. Par défaut, le mode de sécurité est l'authentification UNIX. Vous pouvez spécifier plusieurs modes, mais n'utiliser chaque mode de sécurité qu'une seule fois par ligne de commande. Chaque option `-mode` s'applique à tous les autres options `-rw`, `-ro`, `-rw=`, `-ro=`, `-root=` et `-window=` jusqu'à ce qu'une autre option `-mode` soit détectée. L'utilisation de `-sec=none` mappe tous les utilisateurs vers l'utilisateur `nobody`.

window=*value*
: *value* sélectionne la durée de vie maximale en secondes d'une information d'identification et de connexion sur le serveur NFS. La valeur par défaut est 30 000 secondes ou 8,3 heures.

Définition des listes d'accès avec la commande `share`

Dans les versions de Solaris antérieures à 2.6, l'*accesslist* incluse avec l'option `-ro=`, `-rw=` ou `-root=` de la commande `share` était limitée à une liste de noms d'hôte ou de groupe réseau. À partir de la version Solaris 2.6, la liste d'accès peut également inclure un nom de domaine, un

numéro de sous-réseau, ou une entrée pour refuser l'accès. Ces extensions devraient simplifier le contrôle d'accès aux fichiers sur un seul serveur sans avoir à modifier l'espace de nom ou conserver de longues listes de clients.

Cette commande donne l'accès en lecture seule à la plupart des systèmes mais donne un accès en lecture-écriture pour `rose` et `lilac` :

```
# share -F nfs -o ro,rw=rose:lilac /usr/src
```

Dans l'exemple, l'accès en lecture seule est attribué à tout hôte du groupe réseau `eng`. Le client `rose` se voit spécifiquement attribuer un accès en lecture-écriture.

```
# share -F nfs -o ro=eng,rw=rose /usr/src
```

Remarque – Vous ne pouvez pas spécifier `rw` et `ro` sans arguments. Si aucune option de lecture-écriture n'est spécifiée, la valeur par défaut est lecture-écriture pour tous les clients.

Pour partager un système de fichiers avec plusieurs clients, vous devez saisir toutes les options sur la même ligne. Plusieurs appels de la commande `share` sur le même objet ne se "souviennent" que de la dernière commande exécutée. Cette commande donne l'accès en lecture-écriture à trois systèmes clients, mais seuls `rose` et `tulip` ont accès au système de fichiers en tant que `root`.

```
# share -F nfs -o rw=rose:lilac:tulip,root=rose:tulip /usr/src
```

En cas de partage d'un système de fichiers qui utilise plusieurs mécanismes d'authentification, assurez-vous d'inclure les options `-ro`, `-ro=`, `-rw`, `-rw=`, `-root` et `-window` après les modes de sécurité corrects. Dans cet exemple, l'authentification UNIX est sélectionnée pour tous les hôtes dans le groupe réseau nommé `eng`. Ces hôtes peuvent monter le système de fichiers en lecture seule uniquement. Les hôtes `tulip` et `lilac` peuvent monter le système de fichiers en lecture-écriture s'ils utilisent l'authentification Diffie-Hellman. Avec ces options, `tulip` et `lilac` peuvent monter le système de fichiers en lecture seule même si ces hôtes n'utilisent pas authentification DH. Toutefois, les noms d'hôte doivent être répertoriés dans le groupe réseau `eng`.

```
# share -F nfs -o sec=dh,rw=tulip:lilac,sec=sys,ro=eng /usr/src
```

Même si l'authentification UNIX est le mode de sécurité par défaut, elle n'est pas incluse si l'option `-sec` est utilisée. Par conséquent, vous devez inclure une option `-sec=sys` si l'authentification UNIX doit être utilisée avec tout autre mécanisme d'authentification.

Vous pouvez utiliser un nom de domaine DNS dans la liste d'accès en mettant un point avant le véritable nom de domaine. La chaîne qui suit le point est un nom de domaine, pas un nom d'hôte complet. L'entrée suivante permet l'accès par montage à tous les hôtes dans le domaine `eng.example.com` :

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

Dans cet exemple, le "." unique correspond à tous les hôtes qui sont mis en correspondance par l'intermédiaire des espaces de noms NIS ou NIS+. Les résultats renvoyés à partir de ces services de noms n'incluent pas le nom de domaine. L'entrée `.eng.example.com` correspond à tous les hôtes qui utilisent la résolution d'espaces de noms DNS. DNS renvoie toujours un nom d'hôte complet. Ainsi, l'entrée la plus longue est obligatoire si vous utilisez une combinaison de DNS et des autres espaces de noms.

Vous pouvez utiliser un numéro de sous-réseau dans une liste d'accès en mettant `@` devant le numéro ou le nom du réseau. Ce caractère différencie le nom du réseau provenant d'un groupe réseau ou d'un nom d'hôte complet. Vous devez identifier le sous-réseau dans `/etc/networks` ou dans un espace de noms NIS ou NIS+. Les entrées suivantes ont le même effet si le sous-réseau `192.168` été identifié comme étant le réseau `eng` :

```
# share -F nfs -o ro=@eng /export/share/man
# share -F nfs -o ro=@192.168 /export/share/man
# share -F nfs -o ro=@192.168.0.0 /export/share/man
```

Les deux dernières entrées indiquent que vous n'avez pas besoin d'inclure l'adresse complète du réseau.

Si le préfixe du réseau n'est pas aligné par octets, comme pour CIDR (Classless Inter-Domain Routing), la longueur de masque peut être explicitement spécifiée sur la ligne de commande. La longueur de masque est définie mettant une barre oblique après le nom du réseau ou le numéro de réseau et le nombre de bits significatifs dans le préfixe de l'adresse. Exemple :

```
# share -f nfs -o ro=@eng/17 /export/share/man
# share -F nfs -o ro=@192.168.0/17 /export/share/man
```

Dans ces exemples, le `/17` indique que les premiers 17 bits dans l'adresse sont à utiliser en tant que masque. Pour obtenir des informations supplémentaires sur CIDR, rechercher RFC 1519.

Vous pouvez aussi sélectionner l'accès négatif en mettant un `-` avant l'entrée. Notez que les entrées sont lues de la gauche vers la droite. Par conséquent, vous devez placer les entrées d'accès négatif avant l'entrée à laquelle s'applique l'accès négatif :

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

Cet exemple autoriserait l'accès à tous les hôtes dans le domaine `eng.example.com` , à l'exception de l'hôte nommé `rose`.

Commande `unshare`

Cette commande vous permet d'annuler le partage d'un système de fichiers précédemment disponible au montage par des clients. Vous pouvez utiliser la commande `unshare` pour annuler le partage de n'importe quel système de fichiers, si le système de fichiers a été

explicitement partagé avec la commande `share` commande ou automatiquement par le biais de `/etc/dfs/dfstab`. Si vous utilisez la commande `unshare` pour annuler le référencement d'un système de fichiers partagé par l'intermédiaire du fichier `dfstab`, faites preuve de prudence. N'oubliez pas que le système de fichiers est partagé à nouveau lorsque vous quittez et entrez de nouveau dans le niveau d'exécution 3. Vous devez supprimer l'entrée de ce système de fichiers dans le fichier `dfstab` si le changement doit se poursuivre.

Lorsque vous annulez le partage d'un système de fichiers NFS, l'accès des clients avec les montages existants est bloqué. Le système de fichiers peut être monté sur le client, mais les fichiers ne sont pas accessibles.

Remarque – Pour plus d'informations sur le fonctionnement de la version 4 de NFS lorsque le partage d'un système de fichiers est annulé puis rétabli, reportez-vous à "Annulation et rétablissement du partage d'un système de fichiers dans la version 4 de NFS" à la page 184.

Ce qui suit est un exemple d'annulation du partage d'un système de fichiers spécifique :

```
# unshare /usr/src
```

Commande `shareall`

Cette commande permet de partager plusieurs systèmes de fichiers. Lorsqu'elle est utilisée sans option, la commande partage toutes les entrées de `/etc/dfs/dfstab`. Vous pouvez inclure un nom de fichier pour spécifier le nom d'un fichier qui contient les lignes de commande `share`. Si vous n'incluez pas de nom de fichier, `/etc/dfs/dfstab` est vérifié. Si vous utilisez un `-` pour remplacer le nom de fichier, vous pouvez taper des commandes `share` à partir de l'entrée standard.

Ce qui suit est un exemple de partage de tous les systèmes de fichiers qui sont répertoriés dans un fichier local :

```
# shareall /etc/dfs/special_dfstab
```

Commande `unshareall`

Cette commande annule le partage de la totalité des ressources actuellement partagées. L'option `-F` *FSType* sélectionne une liste de types de systèmes de fichiers définis dans `/etc/dfs/fstypes`. Cet indicateur permet de choisir uniquement certains types de systèmes pour lesquels annuler le partage. Le type de système de fichiers par défaut est défini dans `/etc/dfs/fstypes`. Pour choisir des systèmes de fichiers spécifiques, utilisez la commande `unshare`.

Ce qui suit est un exemple d'annulation de partage de tous les systèmes de fichiers de type NFS :

```
# unshareall -F nfs
```

Commande `showmount`

Cette commande affiche l'un des éléments suivants :

- tous les clients dotés de systèmes de fichiers montés partagés à partir d'un serveur NFS ;
- les systèmes de fichiers montés par des clients uniquement ;
- les systèmes de fichiers partagés avec les informations d'accès client.

Remarque – La commande `showmount` n'affiche que les exportations des versions 2 et 3 de NFS. Cette commande n'affiche pas les exportations de la version 4 de NFS.

La syntaxe de commande est la suivante :

`showmount [ -ade ] [` *hostname* `]`

`-a`	Imprime une liste de tous les montages à distance. Chaque entrée contient le nom du client et du répertoire.
`-d`	Imprime la liste des répertoires qui sont montés à distance par des clients.
`-e`	Imprime la liste des fichiers qui sont partagés ou exportés.
nom_hôte	Sélectionne le serveur NFS à partir duquel recueillir les informations.

Si *hostname* n'est pas spécifié, l'hôte local est interrogé.

La commande suivante répertorie tous les clients et les répertoires locaux montés par les clients :

```
# showmount -a bee
lilac:/export/share/man
lilac:/usr/src
rose:/usr/src
tulip:/export/share/man
```

La commande suivante dresse la liste des répertoires qui ont été montés :

```
# showmount -d bee
/export/share/man
/usr/src
```

La commande ci-dessous répertorie les systèmes de fichiers qui ont été partagés :

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

Commande `setmnt`

Cette commande crée une table `/etc/mnttab`. Les commandes `mount` et `umount` consultent la table. En règle générale, il n'est pas nécessaire d'exécuter cette commande manuellement, car cette commande s'exécute automatiquement lorsqu'un système est démarré.

Commandes pour le dépannage des problèmes liés à NFS

Ces commandes peuvent être utiles lors du dépannage de problèmes liés à NFS.

Commande `nfsstat`

Vous pouvez utiliser cette commande pour collecter des informations statistiques sur les connexion NFS et RPC. La syntaxe de la commande est indiquée ci-après.

`nfsstat [ -cmnrsz ]`

`-c` Affiche des informations côté client

`-m` Affiche les statistiques pour chaque système de fichiers monté NFS

`-n` Indique que les informations NFS doivent être affichées sur le côté client et le côté serveur

`-r` Affiche les statistiques RPC

`-s` Affiche les informations côté serveur

`-z` Spécifie que les statistiques doivent être définies sur zéro

En l'absence d'options spécifiées sur la ligne de commande, les options `-cnrs` utilisées.

La collecte des statistiques côté serveur peut être importante pour le débogage de problèmes lorsqu'un nouveau logiciel ou du nouveau matériel est ajouté à l'environnement informatique. L'exécution de cette commande au moins une fois par semaine et le stockage des chiffres donnent un bon historique des performances précédents.

Reportez-vous à l'exemple ci-dessous :

```
# nfsstat -s

Server rpc:
Connection oriented:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
719949194  0          0          0          0          58478624   33
Connectionless:
calls      badcalls   nullrecv   badlen     xdrcall    dupchecks  dupreqs
```

```
73753609   0          0          0          0          987278     7254

Server nfs:
calls                badcalls
787783794            3516
Version 2: (746607 calls)
null       getattr    setattr    root       lookup     readlink   read
883 0%     60 0%      45 0%      0 0%       177446 23% 1489 0%    537366 71%
wrcache    write      create     remove     rename     link       symlink
0 0%       1105 0%    47 0%      59 0%      28 0%      10 0%      9 0%
mkdir      rmdir      readdir    statfs
26 0%      0 0%       27926 3%   108 0%
Version 3: (728863853 calls)
null          getattr       setattr       lookup        access
1365467 0%    496667075 68% 8864191 1%    66510206 9%   19131659 2%
readlink      read          write         create        mkdir
414705 0%     80123469 10%  18740690 2%   4135195 0%    327059 0%
symlink       mknod         remove        rmdir         rename
101415 0%     9605 0%       6533288 0%    111810 0%     366267 0%
link          readdir       readdirplus   fsstat        fsinfo
2572965 0%    519346 0%     2726631 0%    13320640 1%   60161 0%
pathconf      commit
13181 0%      6248828 0%
Version 4: (54871870 calls)
null                compound
266963 0%           54604907 99%
Version 4: (167573814 operations)
reserved            access              close               commit
0 0%                2663957 1%          2692328 1%          1166001 0%
create              delegpurge          delegreturn         getattr
167423 0%           0 0%                1802019 1%          26405254 15%
getfh               link                lock                lockt
11534581 6%         113212 0%           207723 0%           265 0%
locku               lookup              lookupp             nverify
230430 0%           11059722 6%         423514 0%           21386866 12%
open                openattr            open_confirm        open_downgrade
2835459 1%          4138 0%             18959 0%            3106 0%
putfh               putpubfh            putrootfh           read
52606920 31%        0 0%                35776 0%            4325432 2%
readdir             readlink            remove              rename
606651 0%           38043 0%            560797 0%           248990 0%
renew               restorefh           savefh              secinfo
2330092 1%          8711358 5%          11639329 6%         19384 0%
setattr             setclientid         setclientid_confirm verify
453126 0%           16349 0%            16356 0%            2484 0%
write               release_lockowner   illegal
3247770 1%          0 0%                0 0%

Server nfs_acl:
Version 2: (694979 calls)
null        getacl      setacl      getattr     access      getxattrdir
0 0%        42358 6%    0 0%        584553 84%  68068 9%    0 0%
Version 3: (2465011 calls)
null        getacl      setacl      getxattrdir
0 0%        1293312 52% 1131 0%     1170568 47%
```

La liste précédente est un exemple de statistiques de serveur NFS. Les cinq premières lignes sont relatives à RPC et les autres lignes indiquent les activités NFS. Dans les deux ensembles de statistiques, le fait de connaître le nombre moyen de `badcalls` ou de `calls` et le nombre d'appels par semaine peut aider à identifier un problème. La valeur `badcalls` indique le nombre de mauvais messages à partir d'un client. Cette valeur peut indiquer des problèmes matériels pour le réseau.

Certaines des connexions génèrent des opérations d'écriture sur les disques. Une augmentation soudaine de ces statistiques peut indiquer un problème et doit être examinée. Pour les statistiques de la version 2 de NFS, les connexions à noter sont `setattr`, `write`, `create`, `remove`, `rename` , `link`, `symlink`, `mkdir` et `rmdir`. Pour les statistiques de la version 3 et de la version 4 de NFS, la valeur à surveiller est `commit`. Si le niveau d'opérations `commit` est élevé dans un serveur NFS, comparé à un autre serveur presque identique, vérifiez que les clients NFS ont suffisamment de mémoire. Le nombre d'opérations `commit` sur le serveur s'accroît lorsque les clients n'ont pas de ressources disponibles.

Commande `pstack`

Cette commande affiche un suivi de la pile pour chaque processus. La commande `pstack` doit être exécutée par le propriétaire du processus ou par `root`. Vous pouvez utiliser `pstack` pour déterminer l'endroit où un processus est bloqué. La seule option qui est autorisée avec cette commande est le `PID` du processus que vous souhaitez vérifier. Reportez-vous à la page de manuel `proc(1)`.

L'exemple suivant vérifie que le processus `nfsd` est en cours d'exécution.

```
# /usr/bin/pgrep nfsd
243
# /usr/bin/pstack 243
243:    /usr/lib/nfs/nfsd -a 16
 ef675c04 poll     (24d50, 2, ffffffff)
 000115dc ???????? (24000, 132c4, 276d8, 1329c, 276d8, 0)
 00011390 main     (3, effff14, 0, 0, ffffffff, 400) + 3c8
 00010fb0 _start   (0, 0, 0, 0, 0, 0) + 5c
```

L'exemple indique que le processus est en attente d'une nouvelle demande de connexion, ce qui constitue une réponse normale. Si la pile indique que le processus est toujours interrogé après une requête, le processus peut être bloqué. Suivez les instructions données dans “Redémarrage des services NFS ” à la page 128 pour résoudre ce problème. Passez en revue les instructions dans “Procédures de dépannage NFS ” à la page 124 pour vérifier que votre problème est un programme bloqué.

Commande `rpcinfo`

Cette commande génère des informations sur le service RPC qui est en cours d'exécution sur un système. Vous pouvez également utiliser cette commande pour modifier le service RPC. De nombreuses options sont disponibles avec cette commande. Reportez-vous à la page de manuel `rpcinfo(1M)`. L'exemple suivant est un synopsis raccourci pour certaines des options que vous pouvez utiliser avec la commande.

`rpcinfo [ -m | -s ] [` *nom_hôte* `]`

`rpcinfo -T` *transport nom_hôte* `[` *nomprog* `]`

`rpcinfo [ -t | -u ] [` *nom_hôte* `] [` *nomprog* `]`

`-m`	Affiche une table de statistiques des opérations `rpcbind`
`-s`	Affiche une liste concise de tous les programmes RPC enregistrés
`-T`	Affiche des informations sur les services qui utilisent des transports ou des protocoles spécifiques
`-t`	Teste les programmes RPC qui utilisent TCP
`-u`	Teste les programmes RPC qui utilisent UDP
transport	Sélectionne le transport ou le protocole pour les services
hostname	Sélectionne le nom d'hôte du serveur dont vous souhaitez obtenir des informations
nomprog	Sélectionne le programme RPC sur lequel rassembler des informations

Si aucune valeur n'est donnée pour *nom_hôte*, le nom de l'hôte local est utilisé. Vous pouvez remplacer le numéro de programme RPC pour *nomprog*, mais de nombreux utilisateurs risquent de se souvenir du nom et pas du numéro. Vous pouvez utiliser l'option `-p` à la place de l'option `-s` sur les systèmes qui n'exécutent pas la version 3 du logiciel NFS.

Les données qui sont générés par cette commande peuvent inclure les éléments suivants :

- le numéro de programme RPC ;
- le numéro de version d'un programme spécifique ;
- le protocole de transport en cours d'utilisation ;
- le nom du service RPC ;
- le propriétaire du service RPC.

L'exemple suivant regroupe les informations concernant les services RPC qui sont en cours d'exécution sur un serveur. Le texte qui est générée par la commande est filtrée par la commande `sort` pour rendre la sortie plus lisible. Plusieurs lignes dans lesquelles figurent les services RPC ont été supprimés de l'exemple.

```
% rpcinfo -s bee |sort -n
   program version(s) netid(s)                         service     owner
    100000  2,3,4     udp6,tcp6,udp,tcp,ticlts,ticotsord,ticots rpcbind     superuser
    100001  4,3,2     ticlts,udp,udp6                   rstatd      superuser
    100002  3,2       ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 rusersd     superuser
    100003  3,2       tcp,udp,tcp6,udp6                 nfs         superuser
    100005  3,2,1     ticots,ticotsord,tcp,tcp6,ticlts,udp,udp6 mountd      superuser
    100007  1,2,3     ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 ypbind      superuser
    100008  1         ticlts,udp,udp6                   walld       superuser
    100011  1         ticlts,udp,udp6                   rquotad     superuser
    100012  1         ticlts,udp,udp6                   sprayd      superuser
    100021  4,3,2,1   tcp,udp,tcp6,udp6                 nlockmgr    superuser
    100024  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 status      superuser
    100029  3,2,1     ticots,ticotsord,ticlts           keyserv     superuser
    100068  5         tcp,udp                           cmsd        superuser
    100083  1         tcp,tcp6                          ttdbserverd superuser
    100099  3         ticotsord                         autofs      superuser
    100133  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    100134  1         ticotsord                         tokenring   superuser
    100155  1         ticots,ticotsord,tcp,tcp6         smserverd   superuser
    100221  1         tcp,tcp6                          -           superuser
    100227  3,2       tcp,udp,tcp6,udp6                 nfs_acl     superuser
    100229  1         tcp,tcp6                          metad       superuser
    100230  1         tcp,tcp6                          metamhd     superuser
    100231  1         ticots,ticotsord,ticlts           -           superuser
    100234  1         ticotsord                         gssd        superuser
    100235  1         tcp,tcp6                          -           superuser
    100242  1         tcp,tcp6                          metamedd    superuser
    100249  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    300326  4         tcp,tcp6                          -           superuser
    300598  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
    390113  1         tcp                               -           unknown
 805306368  1         ticots,ticotsord,ticlts,tcp,udp,tcp6,udp6 -           superuser
1289637086  1,5       tcp                               -           26069
```

Les deux exemples suivants montrent comment collecter des informations sur un service RPC en sélectionnant un transport donné sur un serveur. Le premier exemple vérifie le service `mountd` qui est en cours d'exécution sur TCP. Le deuxième exemple vérifie le service NFS qui est en cours d'exécution sur UDP.

```
% rpcinfo -t bee mountd
program 100005 version 1 ready and waiting
program 100005 version 2 ready and waiting
program 100005 version 3 ready and waiting
% rpcinfo -u bee nfs
program 100003 version 2 ready and waiting
program 100003 version 3 ready and waiting
```

Commande `snoop`

Cette commande est souvent utilisée pour surveiller les paquets sur le réseau. La commande `snoop` doit être exécutée en tant que `root`. L'utilisation de cette commande est un bon moyen de

s'assurer que le matériel réseau fonctionne à la fois sur le client et le serveur. De nombreuses options sont disponibles. Reportez-vous à la page de manuel `snoop(1M)`. Un synopsis raccourci de la commande est indiqué ci-après :

`snoop [ -d` *périphérique* `] [ -o` *nom_fichier* `] [ host` *nom_hôte* `]`

`-d` *device*	Spécifie l'interface du réseau local
`-o` *hostname*	Stocke tous les paquets capturés dans le fichier nommé
nom_hôte	Affiche les paquets destinés à et à partir d'un hôte spécifique uniquement

L'option `-d` *périphérique* est utile sur les serveurs qui ont plusieurs interfaces réseau. Vous pouvez utiliser de nombreuses expressions autres que la définition de l'hôte. Une combinaison d'expressions de commande avec `grep` génère souvent des données suffisamment spécifiques pour être utiles.

Lors d'un dépannage, assurez-vous que les paquets vont de et vers l'hôte concerné. Recherchez également les messages d'erreur. L'enregistrement des paquets dans un fichier peut simplifier l'examen des données.

Commande `truss`

Vous pouvez utiliser cette commande pour vérifier si un processus est bloqué. La commande `truss` doit être exécutée par le propriétaire du processus ou par `root`. Vous pouvez utiliser plusieurs options avec cette commande. Reportez-vous à la page de manuel `truss(1)`. Une syntaxe abrégée de la commande est indiquée ci-après.

`truss [ -t` *syscall* `] -p` *pid*

`-t` *syscall*	Sélectionne les appels système à tracer
`-p` *pid*	Indique le PID du processus à tracer

Le *syscall* peut être une liste séparée par des virgules des appels système devant faire l'objet d'un suivi. En outre, si *syscall* commence par un `!`, les appels système répertoriés sont exclus de la trace.

Cet exemple montre que le processus est en attente pour une autre demande de connexion à partir d'un nouveau client.

```
# /usr/bin/truss -p 243
poll(0x00024D50, 2, -1)         (sleeping...)
```

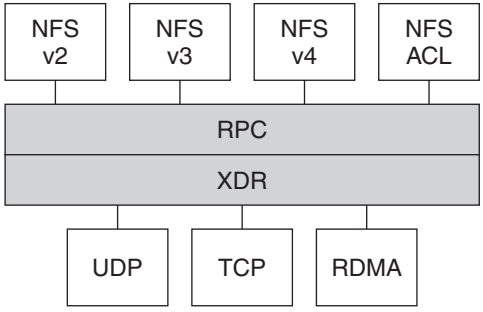
L'exemple précédent montre une réponse normale. Si la réponse ne change pas après l'établissement d'une nouvelle demande de connexion, le processus est bloqué. Suivez les instructions données dans “Redémarrage des services NFS ” à la page 128 pour corriger le

programme bloqué. Passez en revue les instructions dans “Procédures de dépannage NFS ” à la page 124 pour vérifier que votre problème est un programme bloqué.

NFS sur RDMA

La version Solaris 10 inclut le protocole RDMA (Remote Direct Memory Access), qui est une technologie de transfert mémoire-à-mémoire des données sur les réseaux à haut débit. Plus précisément, RDMA fournit un transfert de données distantes directement vers et depuis la mémoire sans intervention de CPU. RDMA fournit également le placement direct de données, ce qui élimine les copie des données, ainsi que toute intervention supplémentaire de la CPU. Par conséquent, RDMA soulage non seulement la CPU de l'hôte, mais réduit également les conflits d'utilisation pour la mémoire de l'hôte et les bus d'E/S. Pour offrir cette possibilité, RDMA combine la structure d'interconnexion d'E/S de technologie InfiniBand sur les plates-formes SPARC avec le système d'exploitation Solaris. La figure ci-après représente la relation de RDMA avec d'autres protocoles, tels que UDP et TCP.

FIGURE 6–1 Relation de RDMA avec d'autres protocoles



NFS est une famille de protocoles en couches sur RPC. La couche XDR (eXternal Data Representation) encode les arguments RPC et les résultats RPC sur l'un des transports RPC, tels que UDP, TCP et RDMA.

Si le transport RDMA n'est pas disponible à la fois sur le client et le serveur, le dispositif de transport TCP est le utilisé, suivi par UDP si TCP n'est pas disponible. Notez, cependant, que si vous utilisez l'option de montage `proto=rdma`, les montages NFS sont forcés d'utiliser RDMA uniquement.

Pour plus d'informations sur les options de montage NFS, reportez-vous à la page de manuel `mount_nfs(1M)` et à “Commande `mount`” à la page 160.

Remarque – RDMA pour InfiniBand utilise le format d'adressage IP et l'infrastructure de recherche par adresse IP pour spécifier les pairs. Cependant, comme RDMA est une pile de protocole distincte, il n'implémente pas totalement toutes les sémantiques d'IP. Par exemple, RDMA n'utilise pas l'adressage IP pour communiquer avec ses pairs. Par conséquent, RDMA peut contourner les configurations de différentes stratégies de sécurité basées sur des adresses IP. Cependant, les stratégies d'administration NFS et RPC, telles que les restrictions `mount` et le RPC sécurisé, ne sont pas contournées.

Fonctionnement du service NFS

Les sections suivantes décrivent certaines des fonctions complexes du logiciel NFS. Notez qu'une partie de la description des fonctions de cette section s'applique exclusivement à la version 4 de NFS.

Remarque – Si votre système comporte des zones activées et que vous souhaitez utiliser cette fonction dans une zone non globale, reportez-vous à la section *Guide d'administration système : Gestion des ressources des conteneurs et des zones Oracle Solaris* pour plus d'informations.

Négociation de version dans NFS

Le processus de lancement de NFS inclut la négociation des niveaux de protocole pour les serveurs et les clients. Si vous ne spécifiez pas le niveau de version, le meilleur niveau est sélectionné par défaut. Par exemple, si le client et le serveur prennent en charge la version 3, cette version est utilisée. Si le client ou le serveur ne peut prendre en charge que la version 2, cette version est utilisée.

À partir de la version Solaris 10, vous pouvez définir les mots clés NFS_CLIENT_VERSMIN, NFS_CLIENT_VERSMAX, NFS_SERVER_VERSMIN, NFS_SERVER_VERSMAX dans le fichier `/etc/default/nfs`. Les valeurs minimum et maximum spécifiées pour le serveur et le client remplacent les valeurs par défaut de ces mots-clés. Pour le client et le serveur, la valeur minimum par défaut est 2 et la valeur maximale par défaut est 4. Reportez-vous à la rubrique "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142. Pour trouver la version prise en charge par le serveur, le client NFS commence avec le paramètre de NFS_CLIENT_VERSMAX et essaie ensuite chaque version jusqu'à atteindre le paramètre de version NFS_CLIENT_VERSMIN. Dès que la version prise en charge est trouvée, le processus se termine. Si, par exemple, NFS_CLIENT_VERSMAX=4 et NFS_CLIENT_VERSMIN=2, le client essaie d'abord la version 4, puis la version 3, et enfin la version 2. Si NFS_CLIENT_VERSMIN et NFS_CLIENT_VERSMAX sont définis sur la même valeur, alors le client utilise toujours cette version et n'essaie pas d'autre version. Si le serveur n'offre pas cette version, le montage échoue.

Remarque – Vous pouvez remplacer les valeurs qui sont déterminées par la négociation en utilisant l'option `vers` avec la commande `mount`. Reportez-vous à la page de manuel `mount_nfs(1M)`.

Pour des informations sur les procédures à suivre, reportez-vous à la rubrique "Configuration des services NFS" à la page 96.

Fonctionnalités de la version 4 de NFS

De nombreuses modifications ont été apportées à NFS dans la version 4. Cette section fournit les descriptions de ces nouvelles fonctionnalités.

Remarque – À partir de la version Solaris 10, la version 4 de NFS ne prend pas en charge la variante de sécurité LIPKEY/SPKM. De plus, la version 4 de NFS n'utilise pas les démons `mountd` , `nfslogd` et `statd`.

Pour des informations sur l'utilisation de la version 4 de NFS, reportez-vous à "Configuration des services NFS" à la page 96.

Annulation et rétablissement du partage d'un système de fichiers dans la version 4 de NFS

Dans les versions 3 et 4 de NFS, si un client tente d'accéder à un système de fichiers dont le partage a été annulé, le serveur renvoie un code d'erreur. Cependant, avec la version 3 de NFS, le serveur conserve tous les verrous que les clients avaient obtenu avant que l'annulation du partage du système de fichiers. Par conséquent, lorsque le partage du système de fichiers est rétabli, les clients de la version 3 de NFS peuvent accéder au système de fichiers comme si son partage n'avait jamais été annulé.

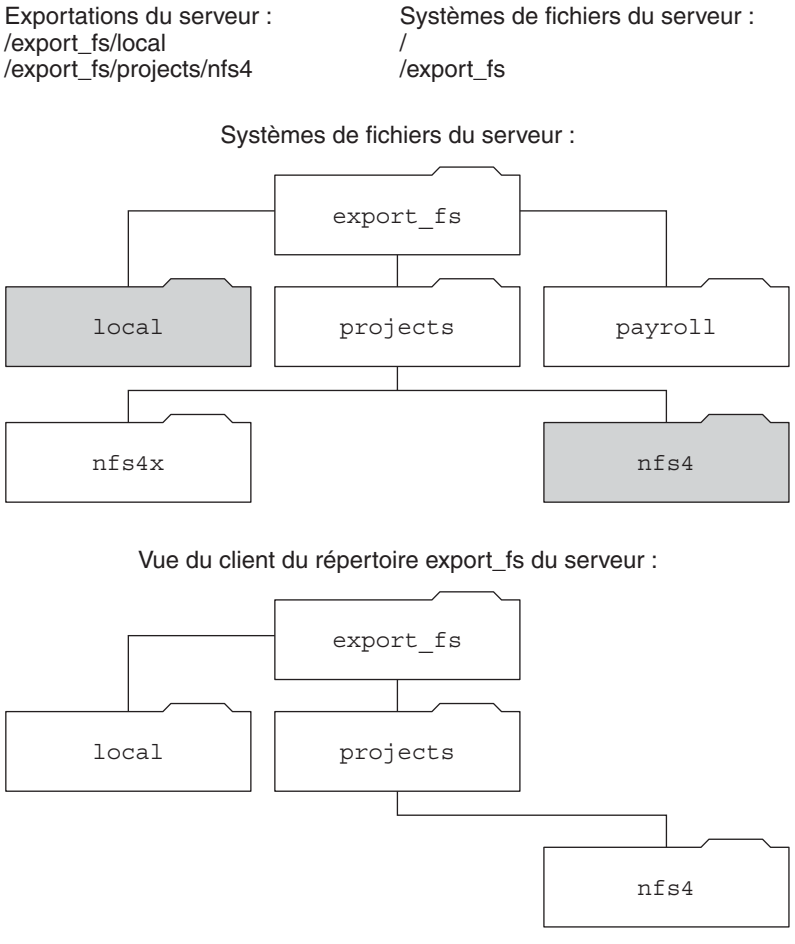
Avec la version 4 de NFS, lorsqu'un système de fichiers n'est pas partagé, tous les états de tout fichier ouvert ou de tout verrou de fichier dans ce système de fichiers sont détruits. Si le client tente d'accéder à ces fichiers ou à ces verrous; il reçoit un message d'erreur. Généralement, cette erreur est signalée comme étant une erreur `I/O` à l'application. Notez, cependant, que le rétablissement du partage d'un système de fichiers partagé pour modifier les options ne détruit aucun état sur le serveur.

Pour obtenir des informations connexes, reportez-vous à la rubrique "Récupération d'un client dans la version 4 de NFS" à la page 187 ou à la page de manuel `unshare_nfs`(1M).

Espace de noms du système de fichiers dans la version 4 de NFS

Les serveurs de la version 4 de NFS créent et mettent à jour un pseudo-système de fichiers qui donne aux clients un accès transparent à tous les objets exportés sur le serveur. Dans les versions antérieures à la version 4 de NFS, le pseudo-système de fichiers n'existait pas. Les clients devaient monter chaque système de fichiers de serveur partagé pour l'accès. Voyez l'exemple suivant :

FIGURE 6–2 Vues du système de fichiers du serveur et du système de fichiers client



Notez que le client ne peut pas voir les répertoires `payroll` et `nfs4x`, car ces répertoires ne sont pas exportés et ne mènent pas à des répertoires exportés. Toutefois, le répertoire `local` est visible pour le client, car `local` est un répertoire exporté. Le répertoire `projects` est visible pour le client, car `projects` mène vers le répertoire exporté, `nfs4`. Par conséquent, certaines parties de l'espace de noms du serveur qui ne sont pas explicitement exportées sont reliées par un pont avec un pseudo-système de fichiers qui affiche uniquement les répertoires exportés et ceux qui mènent à des exports de serveur.

Un pseudo-système de fichiers est une structure qui contient uniquement des répertoires et est créée par le serveur. Le pseudo-système de fichiers permet à un client de parcourir la hiérarchie

des systèmes de fichiers exportés. Par conséquent, la vue du client du pseudo-système de fichiers est limitée aux chemins qui conduisent à systèmes de fichiers exportés.

Les versions précédentes de NFS n'autorisaient pas un client de parcourir les systèmes de fichiers serveur sans monter chaque système de fichiers. Cependant, dans la version 4 de NFS, l'espace de noms de serveur se comporte comme suit :

- Restreint la vue du système de fichiers du client vers des répertoires qui conduisent à des exports de serveur.
- Fournit aux clients un accès continu aux exports de serveur sans nécessiter que le client monte chaque système de fichiers sous-jacent. Reportez-vous à l'exemple précédent. Notez, toutefois, que différents systèmes d'exploitation peuvent nécessiter que le client monte chaque système de fichiers du serveur.

Pour des raisons liées à POSIX, le client de la version 4 de Solaris NFS ne franchit pas les limites du système de fichiers du serveur. En cas de telles tentatives, le client fait que le répertoire semble vide. Pour remédier à cette situation, vous devez effectuer un montage pour chacun des systèmes de fichiers du serveur.

Identificateurs de fichiers volatile de la version 4 de NFS

Les identificateurs de fichiers sont créés sur le serveur et contiennent des informations qui identifient de manière unique les fichiers et les répertoires. Dans les versions 2 et 3 de NFS le serveur renvoyait des identificateurs de fichier persistants. Par conséquent, le client pouvait garantir que le serveur génèrerait un identificateur de fichier qui désigne toujours le même fichier. Exemple :

- Si un fichier est supprimé et remplacé par un autre fichier du même nom, le serveur peut générer un nouvel identificateur de fichier pour le nouveau fichier. Si le client utilise l'ancien identificateur de fichier, le serveur renvoie une erreur d'indicateur de fichier obsolète.
- Si un fichier est renommé, l'indicateur de fichier reste le même.
- En cas de redémarrage du serveur, les identificateurs de fichiers restent les mêmes.

Par conséquent, lorsque le serveur a reçu une demande d'un client qui comporte un identificateur de fichier, la résolution est simple et l'indicateur de fichier désigne toujours le fichier approprié.

Cette méthode d'identification des fichiers et répertoires pour les opérations NFS convient à la plupart des serveurs UNIX. Cependant, elle n'a pas pu être implémentée sur les serveurs s'appuyant sur d'autres méthodes d'identification telles que le chemin d'accès d'un fichier. Pour résoudre ce problème, le protocole de la version 4 de NFS permet à un serveur de déclarer ses identificateurs de fichier comme étant volatiles. Ainsi, un identificateur de fichier peut changer. Si l'identificateur de fichier est modifié, le client doit trouver le nouvel identificateur.

Comme pour les versions 2 et 3 de NFS, le serveur de la version 4 de Solaris NFS fournit toujours des identificateurs de fichier persistants. Toutefois, les clients de la version 4 de Solaris NFS qui accèdent à des serveurs non équipés de la version 4 de Solaris NFS doivent prendre en charge les identificateurs de fichier volatiles si le serveur les utilise. En particulier, lorsque le serveur indique au client que l'indicateur de fichier est volatile, le client doit mettre en cache le mappage entre le nom du chemin d'accès et l'indicateur de fichier. Le client utilise l'identificateur de fichier volatile jusqu'à ce qu'il expire. Lors de son expiration, le client effectue les opérations suivantes :

- efface les informations mises en cache qui se rapportent à cet identificateur de fichier ;
- recherche le nouvel identificateur de fichier ;
- retente l'opération.

Remarque – Le serveur indique toujours au client quels identificateurs de fichier sont persistants ou volatiles.

Les identificateurs de fichier volatiles peuvent expirer pour l'une des raisons suivantes :

- Lorsque vous fermez un fichier.
- Lorsque le système de fichiers de l'identificateur de fichier migre.
- Lorsqu'un client renomme un fichier.
- Lorsque le serveur redémarre.

Notez que si le client n'est pas en mesure de trouver le nouvel identificateur de fichier, un message d'erreur est placé dans le fichier `syslog`. Les autres tentatives d'accès à ce fichier échouent avec une erreur `I/O`.

Récupération d'un client dans la version 4 de NFS

Le protocole de la version 4 de NFS est un protocole avec état. Un protocole est avec état lorsque le client et le serveur assurent la maintenance des informations sur les éléments suivants.

- Fichiers ouverts
- Verrous de fichier

Lorsqu'une panne se produit, comme une panne de serveur, le client et le serveur collaborent pour rétablir les états d'ouverture et de verrouillage qui existaient avant cette panne.

Si un serveur s'arrête brutalement et est redémarré, le serveur perd son état. Le client détecte que le serveur a redémarré et commence le processus pour aider le serveur à reconstruire son état. Ce processus est appelé restauration du client, car le client dirige le processus.

Lorsque le client détecte que le serveur a redémarré, le client suspend immédiatement son activité actuelle et lance le processus de récupération du client. Lorsque le processus de récupération démarre, un message tel que le suivant s'affiche dans le journal d'erreurs système `/var/adm/messages`.

```
NOTICE: Starting recovery server basil.example.company.com
```

Au cours du processus de récupération, le client envoie les informations du serveur à propos de l'état précédent du client. Notez cependant que, pendant cette période, le client n'envoie pas de nouvelles demandes pour le serveur. Toutes les nouvelles demandes d'ouverture de fichiers ou de définition de verrous de fichiers doit attendre que le serveur termine le processus de récupération avant de poursuivre.

Lorsque la récupération du client est terminée, le message suivant s'affiche dans le journal d'erreurs système `/var/adm/messages`.

```
NOTICE: Recovery done for server basil.example.company.com
```

Maintenant, le client a terminé l'envoi des informations d'état pour au serveur. Toutefois, même si le client a terminé ce processus, d'autres clients n'ont peut-être pas été terminé leur processus d'envoi informations d'état au serveur. Par conséquent, le serveur n'accepte pas les demandes d'ouverture ou de verrouillage pendant un certain temps. Cette période appelée délai de grâce, permet à tous les clients de terminer leur processus de récupération.

Au cours de la période de grâce, si le client tente d'ouvrir de nouveaux fichiers ou d'établir de nouveaux verrous, le serveur refuse la demande avec le code d'erreur `GRACE`. À la réception de l'erreur, le client doit attendre la fin de la période de grâce, puis renvoyer la demande au serveur. Pendant la période de grâce, le message suivant s'affiche.

```
NFS server recovering
```

Notez que pendant la période de grâce, les commandes qui n'ouvrent pas les fichiers ou ne définissent pas de verrouillages peuvent s'effectuer. Par exemple, les commandes `ls` et `cd` n'ouvrent par de fichiers ni ne définissent un verrouillage de fichier. Par conséquent, ces commandes ne sont pas suspendues. Toutefois, une commande telle que `cat`, qui ouvre un fichier, serait suspendue jusqu'à ce que la période de grâce se termine.

Lorsque la période de grâce est terminée, le message suivant s'affiche.

```
NFS server recovery ok.
```

Le client peut maintenant envoyer de nouvelles demandes d'ouverture et de verrouillage au serveur.

La récupération du client peut échouer pour diverses raisons. Par exemple, si une partition réseau existe après le redémarrage du serveur, le client peut ne pas être en mesure de rétablir son

état avec le serveur avant la fin de la période de grâce. Lorsque la période de grâce est terminée, le serveur n'autorise pas le client afin de rétablir son état parce que de nouvelles opérations d'état pourraient créer des conflits. Par exemple, un nouveau verrou de fichier peut entrer en conflit avec un ancien verrou de fichier que le client tente de récupérer. Lorsque de telles situations se produisent, le serveur renvoie le code d'erreur `NO_GRACE` au client.

Si la récupération d'une opération d'ouverture pour un fichier en particulier échoue, le client identifie le fichier comme inutilisable et le message suivant s'affiche.

```
WARNING: The following NFS file could not be recovered and was marked dead
(can't reopen:  NFS status 70):  file :  filename
```

Notez que le nombre `70` n'est qu'un exemple.

Si le rétablissement d'un verrou de fichier échoue pendant la restauration, le message d'erreur suivant est publié.

```
NOTICE: nfs4_send_siglost:  pid PROCESS-ID lost
lock on server SERVER-NAME
```

Dans cette situation, le signal `SIGLOST` est publié dans le processus. L'action par défaut pour le signal `SIGLOST` est de mettre fin au processus.

Pour vous permettre de restaurer à partir de cet état, vous devez redémarrer toutes les applications qui avaient des fichiers ouverts au moment de la panne. Notez que les événements suivants peuvent se produire.

- Certains processus qui n'ont pas rouvert le fichier peut recevoir des erreurs d'`E/S`.
- D'autres processus ont rouvert le fichier, ou ont exécuté l'opération d'ouverture après la restauration après panne, sont en mesure d'accéder au fichier sans aucun problème.

Par conséquent, certains processus peuvent accéder à un fichier en particulier tandis que d'autres processus ne le peuvent pas.

Prise en charge du partage `OPEN` dans la version 4 de NFS

Le protocole de la version 4 de NFS offre plusieurs modes partage de fichiers que le client peut utiliser pour contrôler l'accès aux fichiers par d'autres clients. Un client peut spécifier les éléments suivants :

- Le mode `DENY_NONE` donne aux autres clients l'accès en lecture et en écriture à un fichier.
- Le mode `DENY_READ` refuse aux autres clients l'accès en lecture à un fichier.
- Le mode `DENY_WRITE` refuse aux autres clients l'accès en écriture à un fichier.
- Le mode `DENY_BOTH` mode refuse aux autres clients l'accès en lecture et en écriture à un fichier.

Le serveur de la version 4 de Solaris NFS effectue une implémentation complète de ces modes de partage de fichier. Par conséquent, si un client tente d'ouvrir un fichier d'une manière qui entre en conflit avec le mode de partage, le serveur refuse la tentative en faisant échouer l'opération. Lorsque de telles tentatives échouent avec le lancement des opérations de création ou d'ouverture, le client de la version 4 de NFS reçoit une erreur de protocole. Cette erreur est mise en correspondance avec l'erreur d'application `EACCES`.

Même si le protocole offre plusieurs modes de partage, actuellement, l'opération d'ouverture dans Solaris n'offre pas plusieurs modes de partage. Lors de l'ouverture d'un fichier, un client de la version 4 de Solaris NFS peut uniquement utiliser le mode `DENY_NONE`.

Bien que l'appel de système `fcntl` dispose d'une commande `F_SHARE` pour contrôler le partage de fichiers, les commandes `fcntl` ne peuvent pas être implémentées correctement avec la version 4 de NFS. Si vous utilisez ces commandes `fcntl` sur un client de la version 4 de NFS, le client renvoie l'erreur `EAGAIN` à l'application.

Délégation dans la version 4 de NFS

La version 4 de NFS fournit à la fois la prise en charge du client et la prise en charge du serveur pour la délégation. La délégation est une technique par laquelle le serveur délègue la gestion d'un fichier à un client. Par exemple, le serveur peut attribuer une délégation de lecture ou d'écriture à un client. Les délégations de lecture peuvent être accordées à plusieurs clients en même temps, car ces délégations de lecture n'entrent pas en conflit les unes avec les autres. Une délégation d'écriture peut être accordée à un seul client, car une telle délégation peut entrer en conflit avec tout autre accès de fichier par tout autre client. Lorsqu'il détient une délégation d'écriture, le client n'enverrait pas diverses opérations sur le serveur car le client est se voit accorder un accès exclusif à un fichier. De même, le client n'envoie pas diverses opérations au serveur tout en détenant une délégation de lecture. La raison est que le serveur garantit qu'aucun client ne peut ouvrir un fichier en mode écriture. L'effet de la délégation est de réduire considérablement les interactions entre le serveur et le client pour les fichiers délégués. Par conséquent, le trafic réseau est réduit et les performances sur le client et le serveur sont améliorées. Notez, cependant, que le degré d'amélioration des performances dépend du type d'interaction de fichier utilisé par une application et la quantité de surcharge sur le réseau ou le serveur.

La décision d'accorder ou non une délégation revient exclusivement au serveur. Un client ne demande pas de délégation. Le serveur prend des décisions concernant la cession d'une délégation, basée sur les modèles d'accès du fichier. Si différents clients ont récemment accédé à un fichier en mode écriture, le serveur peut ne pas accorder de délégation. La raison est que ce modèle d'accès indique le potentiel de conflits futurs.

Un conflit survient lorsqu'un client accède à un fichier d'une manière qui n'est pas cohérente avec les délégations actuellement accordées à ce fichier. Par exemple, si un client détient une délégation d'écriture sur un fichier et qu'un deuxième client ouvre ce fichier pour lire ou écrire l'accès, le serveur rappelle la délégation d'écriture du premier client. De même, si un client

détient une délégation de lecture et qu'un autre client ouvre le même fichier pour l'écriture, le serveur rappelle la délégation de lecture. Notez que dans les deux cas, le second client ne se voit pas accorder de délégation parce qu'un conflit existe maintenant. Lorsqu'un conflit survient, le serveur utilise un mécanisme de rappel pour contacter le client qui détient actuellement la délégation. Lors de la réception de ce rappel, le client envoie l'état mis à jour du fichier au serveur et renvoie la délégation. Si le client ne répond pas au rappel, le serveur révoque la délégation. Dans de tels cas, le serveur rejette toutes les opérations provenant du client pour ce fichier, et le client rapporte les opérations demandées comme ayant échoué. En règle générale, ces défaillances sont signalées à l'application comme des erreurs d'`E/S`. Pour restaurer à partir de ces erreurs, le fichier doit être fermé, puis rouvert. Les échecs de délégations révoquées peuvent se produire lorsqu'une partition de réseau existe entre le client et le serveur, lorsque le client détient une délégation.

Notez qu'un serveur n'est pas en mesure de résoudre les conflits d'accès à un fichier qui est stocké sur un autre serveur. Par conséquent, un serveur NFS résout uniquement les conflits pour les fichiers qu'il stocke. En outre, en réponse aux conflits causés par des clients qui exécutent différentes versions de NFS, un serveur NFS peut uniquement lancer des rappels pour le client qui exécute la version 4 de NFS. Un serveur NFS ne peut pas initier de rappels pour les clients qui exécutent des versions antérieures de NFS.

Le processus de détection des conflits varie. Par exemple, contrairement à la version 4 de NFS, dans la mesure où les versions 2 et 3 n'ont pas de procédure d'ouverture, le conflit n'est détecté qu'après une tentative de lecture, d'écriture ou de verrouillage d'un fichier par un client. La réponse du serveur à ces conflits varie également. Par exemple :

- Pour la version 3 de NFS, le serveur renvoie l'erreur `juke-box`, ce qui fait que le client interrompt la demande d'accès et réessaie plus tard. Le client imprime le message `File unavailable`.
- Pour la version 2 de NFS 2, l'équivalent de l'erreur `JUKEBOX` n'existant pas, le serveur n'envoie aucune réponse, ce qui fait que le client va attendre, puis réessayer. Le client imprime le message `NFS server not responding`.

Ces conditions sont supprimées une fois le conflit de délégation résolu.

Par défaut, la délégation de serveur est activée. Vous pouvez désactiver la délégation en modifiant le fichier `/etc/default/nfs`. Pour des informations sur les procédures à suivre, reportez-vous à la rubrique “Sélection de versions différentes de NFS sur un serveur” à la page 98.

Aucun mot de passe n'est requis pour la délégation de client. Le démon de rappel de la version 4 de NFS, `nfs4cbd`, fournit le service de rappel sur le client. Ce démon démarre automatiquement dès qu'un montage pour la version 4 de NFS est activé. Par défaut, le client fournit les informations de rappel pour le serveur pour tous les transports Internet répertoriés dans le

fichier système `/etc/netconfig`. Notez que si le client est compatible avec IPv6 et que l'adresse IPv6 pour le nom du client peut être déterminée, le démon de rappel accepte les connexions IPv6.

Le démon de rappel utilise un numéro de programme transitoire et un numéro de port attribué de façon dynamique. Ces informations sont fournies au serveur et ce dernier vérifie le chemin de rappel avant d'accorder les délégations. Si la vérification du chemin de rappel échoue, le serveur n'accorde pas de délégations (il s'agit du seul comportement visible de l'extérieur).

Notez que dans la mesure où les informations de rappel sont intégrées à une demande de la version 4 de NFS, le serveur n'est pas en mesure de contacter le client par le biais d'un périphérique qui utilise la méthode NAT (Network Address Translation). En outre, le démon de rappel utilise un numéro de port dynamique. Par conséquent, le serveur peut ne pas être en mesure de traverser un pare-feu, même si ce pare-feu autorise normalement le trafic NFS sur le port 2049. Dans de telles situations, le serveur n'accorde pas de délégations.

Listes de contrôle d'accès (ACL) et `nfsmapid` dans la version 4 de NFS

Une liste de contrôle d'accès (ACL) offre une meilleure sécurité pour les fichiers en permettant au propriétaire d'un fichier de définir les autorisations de fichier pour un propriétaire du fichier, un groupe et autres utilisateurs et groupes spécifiques. Les ACL sont définies sur le serveur et le client à l'aide de la commande `setfacl`. Pour plus d'informations, reportez-vous à la page de manuel `setfacl(1)`. Dans la version 4 de NFS, le mappeur d'ID, `nfsmapid`, est utilisé pour mettre en correspondance un ID d'utilisateur ou de groupe dans les entrées d'ACL sur un serveur et l'ID d'utilisateur ou de groupe dans entrées d'ACL sur un client. L'inverse est également vrai. Les ID d'utilisateur et de groupe dans les entrées d'ACL doivent exister à la fois sur le client et le serveur.

Motifs d'échecs de mappages d'ID

Les situations suivantes peuvent provoquer un échec de mappage d'ID :

- Si l'utilisateur ou le groupe qui n'existe que dans une entrée d'ACL sur le serveur ne peut pas être mis en correspondance avec un groupe ou un utilisateur valide sur le client, l'utilisateur n'est pas autorisé à lire l'ACL sur le client.

  Par exemple, lorsque vous exécutez les commandes `ls -lv` ou `ls -lV` , vous recevez le message d'erreur `Permission denied` pour les fichiers dotés d'entités ACL d'ID d'utilisateur ou de groupe qui ne peuvent pas être mappées à partir du serveur vers le client. Le mappeur d'ID n'a pas été en mesure d'établir une correspondance entre un utilisateur ou un groupe de l'ACL. Si le mappeur d'ID avait été en mesure de faire correspondre le nom de l'utilisateur ou du groupe, un signe plus (+) aurait été affiché après les autorisations dans la liste de fichiers qui est produite par `ls -l`. Par exemple :

  ```
  % ls -l
  -rw-r--rw-+   1 luis    staff      11968 Aug 12  2005 foobar
  ```

De même, la commande `getfacl` peut renvoyer le message d'erreur `Permission denied` pour la même raison. Pour plus d'informations sur cette commande, reportez-vous à la page de manuel `getfacl(1)`.

- Si l'ID d'utilisateur ou de groupe dans n'importe quelle entrée d'ACL qui est définie sur le client ne peut pas être mappé vers un ID d'utilisateur ou de groupe valide sur le serveur, les commandes `setfacl` ou `chmod` peuvent échouer et renvoyer le message d'erreur `Permission denied`.
- Si les valeurs NFSMAPID_DOMAIN du client et du serveur ne correspondent pas, le mappage d'ID échoue. Pour plus d'informations, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142.

Prévention des problèmes de mappage d'ID avec les ACL

Afin d'éviter les problèmes de mappage d'ID, procédez comme suit :

- Assurez-vous que la valeur de NFSMAPID_DOMAIN est correctement définie dans le fichier `/etc/default/nfs`.
- Assurez-vous que tous les ID d'utilisateur et de groupe dans les entrées d'ACL existent à la fois sur le client et le serveur de la version 4 de NFS.

Vérification d'ID d'utilisateur ou de groupe non mappé

Pour déterminer si un utilisateur ou un groupe ne peut pas être mappé sur le serveur ou le client, utilisez le script suivant :

```
#! /usr/sbin/dtrace -Fs

sdt:::nfs4-acl-nobody
{
     printf("validate_idmapping: (%s) in the ACL could not be mapped!",
stringof(arg0));
}
```

Remarque – Le nom de la sonde utilisée dans ce script est une interface qui est susceptible de changer à l'avenir. Pour plus d'informations, reportez-vous à la rubrique "Niveaux de stabilité" du *Manuel de suivi dynamique Solaris*.

Informations supplémentaires sur les ACL ou nfsmapid

Reportez-vous aux rubriques suivantes :

- "Protecting UFS Files With ACLs (Task Map)" du *System Administration Guide: Security Services*
- Chapitre 8, "Utilisation des ACL et des attributs pour protéger les fichiers Oracle Solaris ZFS" du *Guide d'administration Oracle Solaris ZFS*
- "Démon `nfsmapid`" à la page 148

Négociation UDP et TCP

Pendant l'initialisation, le protocole de transport est également négocié. Par défaut, le premier transport orienté connexion pris en charge à la fois sur le client et le serveur est sélectionné. Si la sélection de cette valeur entraine un échec, le premier protocole de transport sans connexion disponible est utilisé. Les protocoles de transport qui sont pris en charge sur un système sont répertoriés dans `/etc/netconfig`. TCP est le protocole de transport orienté connexion pris en charge par la version. UDP est le protocole de transport sans connexion.

Lorsque les versions du protocole NFS et du protocole de transport sont déterminées par la négociation, la version du protocole NFS est prioritaire sur le protocole de transport. Le protocole de la version 3 de NFS qui utilise UDP a une priorité plus élevée que le protocole de la version 2 de NFS qui utilise TCP. Vous pouvez sélectionner manuellement la version du protocole NFS et le protocole de transport avec la commande `mount`. Reportez-vous à la page de manuel `mount_nfs(1M)`. Dans la plupart des cas, laissez la négociation sélectionner les meilleures options.

Négociation de la taille de transfert de fichiers

La taille de transfert de fichier établit la taille des tampons utilisés lors du transfert des données entre le client et le serveur. En général, les tailles de transfert importantes sont préférables. Le protocole de la version 3 de NFS a une taille de transfert illimitée. Cependant, à partir de la version Solaris 2.6, la taille de tampon par défaut du logiciel est de 32 Ko. Le client peut offrir une plus petite taille de transfert au moment du montage si nécessaire, mais dans la plupart des cas, ce n'est pas nécessaire.

La taille de transfert n'est pas négociée avec des systèmes qui utilisent le protocole de la version 2 de NFS. Dans ces conditions, la taille maximale de transfert est définie sur 8 Ko.

Vous pouvez utiliser les options `-rsize` et `-wsize` pour définir la taille du transfert manuellement avec la commande `mount`. Vous pouvez être amené à réduire la taille de transfert

de certains clients PC. Par ailleurs, vous pouvez augmenter la taille de transfert si le serveur NFS est configuré pour pouvoir utiliser de plus grandes tailles de transfert.

Remarque – À partir de la version Solaris 10, les restrictions concernant les tailles des transferts par câble sont modérées. La taille du transfert dépend des possibilités de transport sous-jacent. Par exemple, la limite du transfert NFS pour le protocole UDP est toujours de 32 Ko. Cependant, TCP étant un protocole de transmission ne possédant pas les limites de datagramme UDP, les tailles maximales de transfert via TCP ont été augmentées à 1 Mo.

Montage des systèmes de fichiers

La description suivante s'applique aux montages de la version 3 de NFS. Le processus de montage de la version 4 de NFS n'inclut ni le service portmap ni le protocole `MOUNT`.

Lorsqu'un client a besoin de monter un système de fichiers à partir d'un serveur, le client doit obtenir un identificateur de fichier auprès du serveur. L'indicateur de fichier doit correspondre à celui du système de fichiers. Cette procédure nécessite que plusieurs transactions s'effectuent entre le client et le serveur. Dans cet exemple, le client tente de monter `/home/terry` à partir du serveur. Un suivi `snoop` pour cette transaction suit.

```
client -> server PORTMAP C GETPORT prog=100005 (MOUNT) vers=3 proto=UDP
server -> client PORTMAP R GETPORT port=33492
client -> server MOUNT3 C Null
server -> client MOUNT3 R Null
client -> server MOUNT3 C Mount /export/home9/terry
server -> client MOUNT3 R Mount OK FH=9000 Auth=unix
client -> server PORTMAP C GETPORT prog=100003 (NFS) vers=3 proto=TCP
server -> client PORTMAP R GETPORT port=2049
client -> server NFS C NULL3
server -> client NFS R NULL3
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

Dans ce suivi, le client demande d'abord le numéro de port de montage au le service portmap sur le serveur NFS. Une fois que le client reçoit le numéro de port de montage (`33492`), ce numéro est utilisé pour tester la disponibilité du service sur le serveur. Une fois que le client a déterminé qu'un service est en cours d'exécution sur ce numéro de port, il effectue une requête de montage. Lorsque le serveur répond à cette demande, le serveur inclut l'identificateur de fichier pour le système de fichiers (`9000`) en cours de montage. Le client envoie ensuite une demande pour le numéro de port NFS. Lorsque le client reçoit le numéro du serveur, il vérifie la disponibilité du service NFS (`nfsd`). En outre, il demande des informations NFS sur le système de fichiers qui utilise l'identificateur de fichier.

Dans le suivi ci-après, le client monte le système de fichiers avec l'option `public`.

```
client -> server NFS C LOOKUP3 FH=0000 /export/home9/terry
server -> client NFS R LOOKUP3 OK FH=9000
client -> server NFS C FSINFO3 FH=9000
server -> client NFS R FSINFO3 OK
client -> server NFS C GETATTR3 FH=9000
server -> client NFS R GETATTR3 OK
```

À l'aide de l'identificateur de fichier public par défaut (`0000`), toutes les transactions devant obtenir des informations à partir du service portmap et déterminer le numéro de port NFS sont ignorées.

Remarque – La version 4 de NFS prend en charge les poignées de fichiers volatiles. Pour plus d'informations, reportez-vous à la section "Identificateurs de fichiers volatile de la version 4 de NFS" à la page 186.

Effets de l'option `-public` et des URL NFS lors du montage

L'option `-public` peut créer des conditions à l'origine de l'échec d'un montage. L'ajout d'un URL NFS peuvent également causer des problèmes. La liste suivante décrit la façon dont un système de fichiers est monté lorsque vous utilisez ces options.

Option public avec URL NFS : force l'utilisation de l'identificateur de fichier public. Le montage échoue si l'identificateur de fichier public n'est pas pris en charge.

Option public avec chemin d'accès ordinaire : force l'utilisation de l'identificateur de fichier public. Le montage échoue si l'identificateur de fichier public n'est pas pris en charge.

URL NFS uniquement : utilise l'identificateur de fichier public si ce dernier est activé sur le serveur NFS. Si le montage échoue lors de l'utilisation de l'identificateur de fichier public, essayez d'effectuer le montage avec le protocole `MOUNT`.

Chemin d'accès ordinaire uniquement : n'utilise par l'identificateur de le fichier public. Le protocole `MOUNT` est utilisé.

Basculement côté client

En utilisant le basculement côté client, un client NFS peut détecter plusieurs serveurs qui rendent les mêmes données disponibles et peuvent passer à un autre serveur lorsque le serveur actuel n'est pas disponible. Le système de fichiers peut devenir indisponible si l'une des conditions suivantes se produit.

- Le système de fichiers est connecté à un serveur qui tombe en panne
- Le serveur est en surcharge.
- Une panne du réseau se produit.

Le basculement, dans ces conditions, est normalement transparent pour l'utilisateur. Par conséquent, le basculement peut se produire à tout moment et sans perturber les processus qui sont en cours d'exécution sur le client.

Le basculement nécessite que le système de fichiers soit monté en lecture seule. Les systèmes de fichiers doivent être identiques pour que le basculement s'effectue avec succès. Reportez-vous à la section "Qu'est-ce qu'un système de fichiers répliqué ?" à la page 197 pour obtenir une description de qui fait qu'un système de fichiers est identique. Un système de fichiers statique ou qui n'a pas été modifiée est souvent le meilleur candidat pour un basculement.

Vous ne pouvez pas utiliser CacheFS et le basculement côté client sur un même montage NFS. Des informations supplémentaires sont enregistrées pour chaque système de fichiers CacheFS. Ces informations ne peuvent pas être mises à jour lors du basculement, de sorte que seule l'une de ces fonctions peut être utilisée lors du montage d'un système de fichiers.

Le nombre de répliques devant être établies pour chaque système de fichiers dépend de nombreux facteurs. Dans l'idéal, vous devez disposer d'au moins deux serveurs. Chaque serveur doit prendre en charge plusieurs sous-réseaux. Cette configuration est préférable au fait d'avoir un serveur unique sur chaque sous-réseau. Le processus exige que chaque serveur répertorié soit vérifié. Par conséquent, si plusieurs serveurs sont répertoriés, chaque montage est plus lent.

Terminologie du basculement

Pour bien comprendre le processus, vous devez comprendre deux termes.

- *Basculement* : le processus de sélection d'un serveur à partir d'une liste de serveurs qui prennent en charge un système de fichiers répliqué. Normalement, le serveur suivant de la liste triée est utilisé, à moins qu'il ne réponde pas.
- *Remappage* : pour utiliser un nouveau serveur. Grâce à une utilisation normale, les clients stockent le nom du chemin d'accès pour chaque fichier actif sur le système de fichiers distant. Au cours du remappage, ces noms de chemin d'accès sont évalués pour détecter les fichiers sur le nouveau serveur.

Qu'est-ce qu'un système de fichiers répliqué ?

Pour les besoins du basculement, un système de fichiers peut être appelé *réplique* lorsque chaque fichier est de la même taille et a la même taille de fichier ou le même type de fichier que le système de fichiers d'origine. Les autorisations, dates de création et autres attributs de fichier ne sont pas pris en compte. Si la taille du fichier ou les types de fichier sont différents, le remappage échoue et le processus se bloque jusqu'à ce que l'ancien serveur devienne disponible. Dans la version 4 de NFS, le comportement est différent. Reportez-vous à la section "Basculement côté client dans la version 4 de NFS" à la page 198.

Vous pouvez conserver la réplication d'un système de fichiers à l'aide de `rdist`, `cpio` ou d'un autre mécanisme de transfert de fichiers. Dans la mesure où la mise à jour des systèmes de fichiers répliqués entraîne des incohérences, prenez les précautions suivantes pour obtenir de meilleurs résultats :

- attribution d'un nouveau nom à l'ancienne version du fichier avant d'installer une nouvelle version du fichier ;
- exécution des mises à jour pendant la nuit lorsque l'utilisation du client est faible ;
- limitation de la taille des mises à jour ;
- réduction du nombre de copies.

Basculement et verrouillage NFS

Certains logiciels requièrent des verrous de lecture sur les fichiers. Pour éviter que ces produits ne dysfonctionnent, les verrous de lecture sur des systèmes de fichiers en lecture seule sont autorisés, mais sont visibles pour le côté client seulement. Les verrous sont conservés par le biais d'un remappage car le serveur n'est pas au courant de l'existence des verrous. Étant donné que les fichiers ne doivent pas changer, vous n'avez pas besoin de verrouiller le fichier sur le côté serveur.

Basculement côté client dans la version 4 de NFS

Dans la version 4 de NFS, si une réplique ne peut pas être établie car les tailles ou les types de fichier sont différents, les événements suivants se produisent.

- Le fichier est inutilisable.
- Un message d'avertissement est imprimé.
- L'application reçoit un échec de l'appel système.

Remarque – Si vous redémarrez l'application et essayez à nouveau d'accéder à un fichier, vous devriez y parvenir.

Dans la version 4 de NFS, vous ne recevez plus d'erreurs de réplication pour les répertoires de tailles différentes. Dans les précédentes versions de NFS, cette condition était considérée comme une erreur et entravait le processus de remappage.

En outre, dans la version 4 de NFS, si une opération de répertoire de lecture est infructueuse, l'opération est exécutée par le serveur suivant de la liste. Dans les précédentes versions de NFS, les opérations de lecture ayant échoué risquaient d'entraîner un échec du remappage et un blocage du processus jusqu'à ce que le serveur d'origine soit disponible.

Fichiers volumineux

Le système d'exploitation prend en charge les fichiers de plus de 2 Go. Par défaut, les systèmes de fichiers UFS sont montés avec l'option `-largefiles` pour prendre en charge la nouvelle fonction. Si nécessaire, reportez-vous à "Désactivation des fichiers volumineux sur un serveur NFS" à la page 93 pour obtenir des instructions.

Si le système de fichiers du serveur est monté avec l'option `-largefiles`, un client NFS Solaris 2.6 peut accéder aux fichiers volumineux sans qu'il ne soit nécessaire d'effectuer des modifications. Toutefois, toutes les commandes Solaris 2.6 ne peuvent pas gérer les fichiers volumineux. Reportez-vous à la page de manuel `largefile(5)` pour obtenir une liste de commandes capables de gérer les grands fichiers. Les clients qui ne peuvent pas prendre en charge le protocole de la version 3 de NFS avec les extensions de fichiers volumineux ne peuvent pas accéder à des fichiers volumineux. Bien que des clients qui exécutent la version 2.5 de Solaris puissent utiliser le protocole de la version 3 de NFS, la prise en charge de fichiers de grande taille n'a pas été incluse dans cette version.

Fonctionnement de la journalisation du serveur NFS

La journalisation du serveur NFS fournit les enregistrements des lectures et écritures NFS, ainsi que des opérations qui modifient le système de fichiers. Ces données peuvent être utilisées pour suivre l'accès aux informations. En outre, ces enregistrements peuvent fournir un moyen quantitatif de mesurer l'intérêt pour l'information.

En cas d'accès à un système de fichiers avec la journalisation activée, le noyau écrit les données brutes dans un fichier tampon. Les données incluent ce qui suit :

- un horodatage ;
- l'adresse IP du client ;
- l'UID du demandeur ;
- l'identificateur de fichier de l'objet fichier ou répertoire objet en cours d'accès ;
- le type de l'opération qui s'est produite.

Le démon `nfslogd` convertit ces données brutes en enregistrements au format ASCII qui sont stockés dans des fichiers journaux. Lors de la conversion, les adresses IP sont modifiées en noms d'hôte et les UID sont modifiés en informations de connexion si le service de noms qui est activé peut trouver des correspondances. Les identificateurs de fichiers sont également convertis en noms de chemin d'accès. Pour accomplir la conversion, le démon assure le suivi des identificateurs de fichiers et stocke les informations dans une table identificateur de fichier-chemin d'accès distincte. De cette façon, le chemin d'accès n'a pas à être identifié à nouveau à chaque accession à un identificateur de fichier. Dans la mesure où aucune

modification n'est apportée aux mappages dans la table identificateur de fichier-chemin lorsque la commande `nfslogd` est désactivée, vous devez conserver le démon en cours d'exécution.

Remarque – La journalisation du serveur n'est pas prise en charge dans la version 4 de NFS.

Fonctionnement du service WebNFS

Le service WebNFS rend les fichiers dans un répertoire accessibles par les clients à l'aide d'un identificateur de fichier. Un identificateur de fichier est une adresse qui est générée par le noyau qui identifie un fichier pour les clients NFS. L'*identificateur de fichier public* a une valeur prédéfinie, de sorte que le serveur n'a pas besoin de générer un identificateur de fichier pour le client. La capacité d'utiliser cet identificateur de fichier prédéfini réduit le trafic réseau en éliminant le protocole `MOUNT`. Cette capacité devrait également accélérer les processus pour les clients.

Par défaut, l'identificateur de fichier public sur un serveur NFS est établi sur le système de fichiers racine. Cette valeur par défaut fournit l'accès WebNFS à tous les clients disposant déjà de privilèges de montage sur le serveur. Vous pouvez modifier l'identificateur de fichier public pour pointer sur n'importe quel système de fichiers en utilisant la commande `share`.

Lorsque le client dispose de l'identificateur de fichier pour le système de fichiers, une commande `LOOKUP` est exécutée pour déterminer l'identificateur du fichier auquel accéder. Le protocole NFS permet l'évaluation d'un seul composant de nom de chemin à la fois. Chaque niveau supplémentaire de hiérarchie de répertoires nécessite une autre opération de `LOOKUP`. Un serveur WebNFS peut évaluer un nom de chemin d'accès entier à l'aide d'une transaction de recherche de composant multi-transaction lorsque la commande `LOOKUP` est relative à l'identificateur de fichier public. La recherche de multi-composant permet au serveur WebNFS de fournir l'identificateur de fichier pour le fichier désiré sans échanger d'identificateurs de fichiers pour chaque niveau de répertoire dans le nom du chemin d'accès.

En outre, un client NFS peut lancer des téléchargements simultanés sur une seule connexion TCP. Cette connexion permet d'avoir un accès rapide sans la charge supplémentaire sur le serveur causée par la configuration de plusieurs connexions. Bien que les applications de navigateur Web prennent en charge le téléchargement de plusieurs fichiers, chaque fichier a sa propre connexion. En utilisant une connexion, le logiciel WebNFS réduit le temps système sur le serveur.

Si le composant final dans le nom de chemin est un lien symbolique vers un autre système de fichiers, le client peut accéder au fichier si le client a déjà un accès par l'intermédiaire des activités NFS normale.

En règle générale, l'URL NFS est évalué par rapport à l'identificateur de fichier public. L'évaluation peut être modifiée de manière à être relative à la racine du serveur du système de

fichiers par l'ajout d'une autre barre oblique au début du chemin d'accès. Dans cet exemple, ces deux URL NFS sont équivalents si l'identificateur de fichier public a été établi sur le système de fichiers `/export/ftp`.

```
nfs://server/junk
nfs://server//export/ftp/junk
```

Remarque – Le protocole de la version 4 de NFS est préféré au service WebNFS. La version 4 de NFS intègre pleinement toutes les négociations de sécurité ajoutées au protocole MOUNT et au service WebNFS.

Fonctionnement de la négociation de sécurité WebNFS

Le service NFS inclut un nouveau protocole qui permet à un client WebNFS de négocier le mécanisme de sécurité sélectionné avec un serveur WebNFS. Le nouveau protocole utilise une recherche de négociation de sécurité multi-composant, qui est une extension de la recherche multi-composant qui a été utilisée dans les versions antérieures du protocole WebNFS.

Le client WebNFS lance le processus en faisant une requête de recherche multi-composant standard en utilisant l'identificateur de fichier public. Puisque le client ne sait pas comment le chemin est protégé par le serveur, le mécanisme de sécurité par défaut est utilisé. Si le mécanisme de sécurité par défaut n'est pas suffisant, la réponse du serveur est une erreur `AUTH_TOOWEAK`. Cette réponse indique que le mécanisme par défaut n'est pas valide. Le client doit utiliser un mécanisme par défaut plus fort.

Lorsque le client reçoit l'erreur `AUTH_TOOWEAK`, le client envoie une requête au serveur pour déterminer quels mécanismes de sécurité sont requis. Si la demande réussit, le serveur répond avec un tableau de mécanismes de sécurité requis pour le chemin d'accès spécifié. En fonction de la taille du tableau de mécanismes de sécurité, le client peut être amené à effectuer des demandes supplémentaires pour obtenir le tableau complet. Si le serveur ne prend pas en charge la négociation de sécurité WebNFS, la demande échoue.

Si la demande aboutit, le client WebNFS sélectionne le premier mécanisme de sécurité à partir du tableau que le client prend en charge. Le client émet ensuite une demande de recherche multi-composant standard à l'aide des mécanismes de sécurité pour acquérir l'identificateur de fichier. Toutes les autres demandes NFS sont effectuées à l'aide du mécanisme de sécurité et de l'identificateur de fichier.

Remarque – Le protocole de la version 4 de NFS est préféré au service WebNFS. La version 4 de NFS intègre pleinement toutes les négociations de sécurité ajoutées au protocole MOUNT et au service WebNFS.

Restrictions WebNFS liées à l'utilisation de navigateur Web

Plusieurs fonctions qu'un site Web utilisant HTTP est capable de fournir ne sont pas prises en charge par le logiciel WebNFS. Ces différences proviennent du fait que le serveur NFS n'envoie que le fichier, de sorte que tout traitement spécial doit être effectué par le client. Si vous avez besoin d'un site web configuré pour l'accès WebNFS et HTTP, vous devez tenir compte des points suivants :

- La navigation sur NFS n'exécute par les scripts CGI. Par conséquent, un système de fichiers avec un site web actif qui utilise de nombreux scripts CGI pourrait ne pas être approprié pour la navigation NFS.
- Le navigateur peut démarrer différents visionneurs pour gérer les identificateurs de fichiers dans différents formats de fichier. L'accès à ces fichiers par le biais d'un URL NFS lance un visionneur externe si le type de fichier peut être déterminé par le nom de fichier. Le navigateur doit reconnaître toute extension de nom de fichier pour un type MIME standard lorsqu'un URL NFS est utilisé. Le logiciel WebNFS n'effectue pas de vérification dans le fichier pour déterminer son type. Par conséquent, le seul moyen de déterminer un type de fichier est son extension de nom.
- La navigation NFS ne peut pas utiliser les mappes d'images côté serveur (images cliquables). Cependant, la navigation NFS peut utiliser les mappes d'image côté client (images cliquables) car les URL sont définis avec l'emplacement. Aucune réponse supplémentaire n'est requise pour le serveur de documents.

Système NFS sécurisé

L'environnement NFS est un moyen efficace et pratique pour partager des systèmes de fichiers sur un réseau doté de diverses architectures et systèmes d'exploitation. Cependant, les mêmes fonctions qui font que le partage des systèmes de fichiers à l'aide des opérations NFS est pratique posent également des problèmes de sécurité. Historiquement, la plupart des implémentations NFS utilisaient l'authentification UNIX (ou AUTH_SYS), mais aussi des méthodes d'authentification plus fortes comme AUTH_DH étaient également disponibles. Lorsque vous utilisez l'authentification UNIX, un serveur NFS authentifie une demande de fichier en authentifiant l'ordinateur qui effectue la demande, mais pas l'utilisateur. Par conséquent, un utilisateur client peut exécuter `su` et usurper l'identité du propriétaire d'un

fichier. Si l'authentification DH est utilisée, le serveur NFS authentifie l'utilisateur, ce qui rend ce type d'usurpation d'identité beaucoup plus difficile.

Avec un accès à la racine et des connaissances en programmation réseau, n'importe qui peut introduire des données arbitraire dans le réseau et extraire des données du réseau. Les attaques les plus dangereuses sont celles qui concernent l'introduction de données. Un exemple est l'usurpation de l'identité d'un utilisateur effectuée en générant les bons paquets ou en enregistrant des conversations et en les rejouant ultérieurement. Ces attaques ont une incidence sur l'intégrité des données. Les attaques qui impliquent l'écoute passive, qui correspond simplement à l'écoute du trafic réseau sans usurpation d'identité, ne sont pas aussi dangereuses, car l'intégrité des données n'est pas compromise. Les utilisateurs peuvent protéger la confidentialité des informations sensibles en chiffrant les données envoyées sur le réseau.

Une approche courante aux problèmes de sécurité réseau consiste à laisser la solution à chaque application. Une meilleure approche consiste à mettre en œuvre un système d'authentification standard à un niveau qui couvre toutes les applications.

Le système d'exploitation Solaris inclut un système d'authentification au niveau de l'appel de procédure à distance (RPC), qui est le mécanisme sur lequel les opérations NFS sont construites. Ce système, appelé appel de procédure à distance sécurisé, améliore considérablement la sécurité d'un environnement réseau et fournit une sécurité supplémentaire pour les services tels que le système NFS. Lorsque le système NFS utilise les fonctions qui sont fournies par l'appel de procédure à distance sécurisé, il est connu comme un système NFS sécurisé.

RPC sécurisé

L'appel de procédure à distance sécurisé est fondamental pour le système NFS sécurisé. L'objectif de l'appel de procédure à distance sécurisé est de construire un système qui est au moins aussi sécurisé qu'un système travaillant en temps partagé. Dans un système travaillant en temps partagé, tous les utilisateurs partagent le même ordinateur. Un système travaillant en temps partagé authentifie un utilisateur par le biais d'un mot de passe de connexion. Avec l'authentification DES (Data Encryption Standard), le même processus d'authentification est terminé. Les utilisateurs peuvent se connecter sur n'importe quel ordinateur distant tout comme les utilisateurs peuvent se connecter sur un terminal local. Les mots de passe de connexion sont leur assurance de la sécurité du réseau. Dans un environnement en temps partagé, l'administrateur système a une obligation éthique de ne pas modifier un mot de passe pour usurper l'identité quelqu'un. Dans l'appel de procédure à distance sécurisé, l'administrateur réseau n'est pas autorisé à modifier les entrées d'une base de données qui stocke *les clés publiques*.

Vous devez être familier avec deux termes pour comprendre un système d'authentification RPC : informations d'identification et de connexion et vérificateurs. Comme pour les cartes

d'identité, les données d'identification sont ce qui identifie une personne : un nom, une adresse et une date de naissance. Le vérificateur est la photo sur la carte. Vous pouvez vérifier que la carte n'a pas été volée en vérifiant la photo sur la carte et en la comparant à la personne qui la détient. Dans RPC, le processus client envoie les informations d'identification et de connexion et un vérificateur au serveur avec chaque requête RPC. Le serveur renvoie uniquement un vérificateur car le client connaît déjà les informations d'identification et de connexion du serveur.

L'authentification RPC est illimitée, ce qui signifie qu'une grande variété de systèmes d'authentification peuvent y être raccordés, comme UNIX, DH et KERB.

Lorsque l'authentification UNIX est utilisée par un service réseau, les informations d'authentification et de connexion contiennent le nom d'hôte du client, l'UID, le GID et la liste d'accès de groupe. Cependant, le vérificateur ne contient rien. Dans la mesure où aucun vérificateur n'existe, un superutilisateur peut falsifier les informations d'identification et de connexion appropriées à l'aide des commandes telles que `su`. Un autre problème de l'authentification UNIX est qu'elle suppose que tous les ordinateurs d'un réseau sont des ordinateurs UNIX. L'authentification UNIX ne fonctionne pas lorsqu'elle est appliquée à d'autres systèmes d'exploitation dans un réseau hétérogène.

Pour surmonter les problèmes de l'authentification UNIX, le RPC sécurisé utilise l'authentification DH.

Authentification DH

L'authentification DH utilise la cryptographie par clé publique DES (Data Encryption Standard) et Diffie-Hellman pour authentifier les utilisateurs et les ordinateurs du réseau. DES est un mécanisme de chiffrement standard. Le chiffrement par clé publique Diffie-Hellman est un système de chiffrement qui implique deux clés : une publique et une secrète. Les clés publiques et secrètes sont stockées dans l'espace de noms. NIS stocke les clés dans la mappe de clé publique. Ces mappes contiennent la clé publique et la clé secrète pour tous les utilisateurs potentiels. Reportez-vous à la section *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)* pour plus d'informations sur la façon de configurer les mappes.

La sécurité de l'authentification DH est basée sur la capacité d'un expéditeur à chiffrer l'heure actuelle, que le destinataire peut ensuite déchiffrer et vérifier par rapport à son propre horloge. L'horodatage est chiffré à l'aide de DES. La configuration requise pour que ce plan fonctionne est la suivante :

- Les deux agents doivent s'accorder sur l'heure actuelle.
- L'expéditeur et le destinataire doivent utiliser la même clé de chiffrement.

Si un réseau exécute un programme de synchronisation d'heure, l'heure sur le client et le serveur est synchronisée automatiquement. Si un programme de synchronisation n'est pas disponible, les horodatages peuvent être calculés à l'aide de l'heure de serveur au lieu de l'heure du réseau.

Le client demande l'heure au serveur avant le démarrage de la session RPC, puis calcule la différence de temps entre sa propre horloge et celle du serveur. Cette différence est utilisée pour compenser l'horloge du client lors du calcul des horodatages. Si les horloges du client et du serveur se désynchronisent, le serveur commence à rejeter les requêtes du client. Le système d'authentification DH sur le client permet d'effectuer une resynchronisation avec le serveur.

Le client et le serveur arrivent à la même clé de chiffrement en générant une *clé* de conversation aléatoire également appelée *clé de session*, et en utilisant le chiffrement par clé publique pour déduire une *clé commune*. La clé commune est une clé que seuls le client et le serveur sont capables de déduire. La clé de conversation est utilisée pour chiffrer et déchiffrer l'horodatage du client. La clé commune est utilisée pour chiffrer et déchiffrer la clé de conversation.

Authentification KERB

Kerberos est un système d'authentification qui a été développé au MIT. Kerberos offre une variété de types de chiffrement, y compris DES. La prise en charge de Kerberos n'est plus fournie dans le cadre du RPC sécurisé, mais cette version inclut une implémentation côté serveur et côté client. Reportez-vous au Chapitre 21, “Introduction to the Kerberos Service” du *System Administration Guide: Security Services* pour plus d'informations sur l'implémentation de l'authentification Kerberos.

Utilisation du RPC sécurisé avec NFS

Tenez compte des points suivants si vous avez l'intention d'utiliser le RPC sécurisé :

- Si un serveur s'arrête brutalement et que personne n'est à proximité (à la suite d'une panne de courant, par exemple), toutes les clés secrètes qui sont stockées dans le système sont supprimées. Maintenant, aucun processus ne peut accéder aux services réseau sécurisés ou monter un système de fichiers NFS. Les processus importants lors d'un redémarrage s'exécutent généralement en tant que `root`. Par conséquent, ces processus fonctionneraient si la clé secrète de la racine était stockée, mais personne n'est disponible pour saisir le mot de passe qui la déchiffre. `keylogin -r` permet à `root` de stocker les clé secrètes effacées dans `/etc/.rootkey`, que `keyserv` lit.
- Certains systèmes démarrent en mode mono-utilisateur, avec un shell de connexion root sur la console et aucune invite de mot de passe. La sécurité physique est indispensable dans de tels cas.
- L'initialisation d'ordinateur sans disque n'est pas totalement sécurisée. Quelqu'un pourrait usurper l'identité du serveur d'amorçage et initialiser un noyau retors qui, par exemple, effectuerait un enregistrement de votre clé secrète sur un ordinateur distant. Le système Secure NFS offre une protection uniquement lorsque le noyau et les clés du serveur sont en cours d'exécution. Dans le cas contraire, aucun moyen ne permet d'authentifier les réponses qui sont données par le serveur d'initialisation. Cette limitation pourrait être un problème grave, mais la limitation nécessite une attaque sophistiquées, à l'aide du code source du

noyau. En outre, il resterait des preuves du crime. Si vous avez interrogiez le réseau pour les serveurs d'amorçage, vous pourriez détecter l'emplacement du serveur d'initialisation retors.

- `root` est le propriétaire de la plupart des programmes setuid. Si la clé secrète pour `root` est stockée dans `/etc/.rootkey` , ces programmes se comportent comme ils ont toujours fait. Si un programme setuid est détenu par un utilisateur, cependant, le programme setuid risque de ne pas toujours fonctionner. Par exemple, supposons qu'un programme setuid est détenu par `dave` et que `dave` ne s'est pas connecté à l'ordinateur depuis qu'il a démarré. Le programme ne sera plus capable d'accéder aux services de réseau sécurisé.
- Si vous vous connectez à un ordinateur distant (avec `login`, `rlogin` ou `telnet`) et utilisez `keylogin` pour obtenir un accès, vous donner l'accès à votre compte. La raison est que votre clé secrète est transmise au serveur de clé de l'ordinateur qui stocke ensuite votre clé secrète. Ce processus est un problème uniquement si vous ne faites pas confiance à l'ordinateur distant. Si vous avez des doutes, cependant, ne vous connectez pas à un ordinateur distant si l'ordinateur distant nécessite un mot de passe. Au lieu de cela, utilisez l'environnement NFS pour monter des systèmes de fichiers qui sont partagés par l'ordinateur distant. Vous pouvez également utiliser `keylogout` pour supprimer la clé secrète du serveur de clés.
- Si un répertoire d'accueil est partagé avec l'option `-o sec=dh`, établir des connexions distantes peut être un problème. Si les fichiers `/etc/hosts.equiv` ou `~/.rhosts` ne sont pas définis pour demander un mot de passe, la connexion est établie. Toutefois, les utilisateurs ne peuvent pas accéder à leurs répertoires d'accueil car aucune authentification n'a été effectuée localement. Si l'utilisateur est invité à saisir un mot de passe, l'utilisateur a le droit d'accéder à son répertoire d'accueil si le mot de passe correspond au mot de passe du réseau.

Mappes Autofs

Autofs utilise trois types de mappes :

- Mappe principale
- Mappe directe
- Mappe indirecte

Mappe principale Autofs

La mappe `auto_master` associe un répertoire à une mappe. La mappe est une liste principale qui indique toutes les mappes qu'autofs doit vérifier. L'exemple suivant montre ce que peut contenir un fichier `auto_master`.

EXEMPLE 6–3 Exemple de fichier `/etc/auto_master`

```
# Master map for automounter
#
```

EXEMPLE 6–3 Exemple de fichier `/etc/auto_master` *(Suite)*

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

Cet exemple illustre le fichier `auto_master` générique avec une addition à la mappe `auto_direct`. Chaque ligne dans la mappe principale `/etc/auto_master` a la syntaxe suivante :

point-de-montage nom-mappe [*options-montage*]

mount-point — *point-montage* est le chemin d'accès complet (absolu) d'un répertoire. Si le répertoire n'existe pas, autofs le crée si possible. Si le répertoire existe déjà et n'est pas vide, le montage sur le répertoire masque son contenu. Dans cette situation, autofs émet un message d'avertissement.

La notation `/-` sous la forme d'un point de montage indique que cette mappe est une mappe directe. Elle signifie également qu'aucun point de montage particulier n'est associé à la mappe.

nom-mappe — *mappe-nom* est la mappe qu'autofs utilise pour trouver l'accès à des emplacements ou des informations de montage. Si le nom est précédé d'une barre oblique (/), autofs interprète le nom comme étant un fichier local. Dans le cas contraire, autofs recherche les informations de montage à l'aide de la recherche qui est spécifiée dans le fichier de configuration du commutateur du service de noms (`/etc/nsswitch.conf`). Les mappes spéciales sont également utilisées pour `/net`. Pour plus d'informations, reportez-vous à la section "Point de montage `/net`" à la page 208.

options-montage — *options-montage* est une liste séparée par des virgules des options qui s'appliquent au montage des entrées spécifiées dans la mappe nom-mappe, sauf si les entrées de cette mappe indiquent d'autres options. Les options pour chaque type de système de fichiers sont répertoriées dans la page de manuel mount pour ce système de fichiers. Par exemple, reportez-vous à la page de manuel `mount_nfs(1M)` pour connaître les options de montage spécifiques à NFS. Pour des points de montage spécifiques à NFS, les options `bg` (arrière-plan) et `fg` (premier plan) ne s'appliquent pas.

Une ligne qui commence avec # est un commentaire. Tout le texte qui suit jusqu'à la fin de la ligne n'est pas pris en compte.

Pour scinder de longues lignes en lignes plus courtes, mettez une barre oblique (\) à la fin de la ligne. Le nombre maximal de caractères d'une entrée est 1024.

Remarque – Si le même point de montage est utilisé dans deux entrées, la première entrée est utilisée par la commande `automount`. La seconde entrée est ignorée.

Point de montage `/home`

Le point de montage `/home` est le répertoire dans lequel les entrées qui sont répertoriées dans `/etc/auto_home` (une mappe indirecte) doivent être montées.

Remarque – Autofs s'exécute sur tous les ordinateurs et prend en charge `/net` et `/home` (répertoires d'accueil montés automatiquement) par défaut. Ces valeurs par défaut peuvent être remplacées par des entrées dans la mappe NIS `auto.master` ou la table NIS+ `auto_master`, ou en modifiant le fichier `/etc/auto_master`.

Point de montage `/net`

Autofs monte sous le répertoire `/net` toutes les entrées dans la mappe spéciale `-hosts`. La mappe est une mappe intégrée qui n'utilise que la base de données hosts. Supposons que l'ordinateur `gumbo` est dans la base de données hosts et qu'il exporte n'importe lequel de ses systèmes de fichiers. La commande suivante change le répertoire actuel pour le répertoire racine de l'ordinateur `gumbo`.

```
% cd /net/gumbo
```

Autofs peut monter uniquement les systèmes de fichiers *exportés* de l'hôte `gumbo`, c'est-à-dire tous les systèmes de fichiers sur un serveur qui sont disponibles pour les utilisateurs du réseau au lieu des systèmes de fichiers sur un disque local. Par conséquent, tous les fichiers et répertoires de `gumbo` pourraient ne pas être disponibles via `/net/gumbo`.

Avec la méthode d'accès `/net`, le nom du serveur est dans le chemin d'accès et dépend de l'emplacement. Si vous souhaitez déplacer un système de fichiers exporté d'un serveur à un autre, le chemin d'accès risque de ne plus fonctionner. Il est donc conseillé de définir une entrée dans une mappe spécifiquement destinée au le système de fichiers que vous souhaitez plutôt que d'utiliser `/net`.

Remarque – Autofs vérifie le serveur de liste d'exportation uniquement au moment du montage. Une fois que le système de fichiers d'un serveur est monté, autofs ne consulte plus le serveur jusqu'à ce que les systèmes de fichiers du serveur soient automatiquement démontés. Par conséquent, les nouveaux systèmes de fichiers exportés ne sont pas visibles tant que les systèmes de fichiers sur le client ne seront pas démontés puis remontés.

Mappe directe autofs

Une mappe directe est un point de montage automatique. Avec une mappe directe, une association directe existe entre un point de montage sur le client et un répertoire sur le serveur. Les mappes directes ont un nom de chemin d'accès complet et indiquent la relation explicitement. L'exemple suivant est une mappe `/etc/auto_direct` standard :

```
/usr/local          -ro \
   /bin                   ivy:/export/local/sun4 \
   /share                 ivy:/export/local/share \
   /src                   ivy:/export/local/src
/usr/man            -ro   oak:/usr/man \
                          rose:/usr/man \
                          willow:/usr/man
/usr/games          -ro   peach:/usr/games
/usr/spool/news     -ro   pine:/usr/spool/news \
                          willow:/var/spool/news
```

Les lignes dans les mappes directes ont la syntaxe suivante :

clé [*options-montage*] *emplacement*

clé — *clé* est le chemin d'accès du point de montage dans une mappe directe.

options-montage — *options-montage* correspond aux options que vous souhaitez appliquer à ce montage particulier. Ces options sont nécessaires uniquement si les options diffèrent de la mappe par défaut. Les options pour chaque type de système de fichiers sont répertoriées dans la page de manuel mount pour ce système de fichiers. Par exemple, reportez-vous à la page de manuel `mount_nfs(1M)` pour connaître les options de montage spécifiques à NFS.

emplacement — *emplacement* est l'emplacement du système de fichiers. Un ou plusieurs systèmes de fichiers sont spécifiés comme *serveur*: *nom_chemin* pour des systèmes de fichiers NFS ou :*nom_périphérique* pour les systèmes de fichiers High Sierra (HSFS).

Remarque – Le *chemin d'accès* ne doit pas inclure un point de montage monté automatiquement. Le *chemin d'accès* doit être le véritable chemin d'accès absolu du système de fichiers. Par exemple, l'emplacement d'un répertoire d'accueil doit être répertorié comme *serveur*:`/export/Home/`*nom utilisateur* et non comme *serveur* :`/home/`*nom utilisateur*.

Comme pour la mappe principale, une ligne qui commence par # est un commentaire. Tout le texte qui suit jusqu'à la fin de la ligne n'est pas pris en compte. Placez une barre oblique à la fin de la ligne pour scinder les lignes longues en lignes plus courtes.

De toutes les mappes, les entrées d'une mappe directe ressemblent le plus aux entrées correspondantes dans `/etc/vfstab`. Une entrée peut figurer dans `/etc/vfstab` comme suit :

```
dancer:/usr/local - /usr/local/tmp nfs - yes ro
```

L'entrée équivalente s'affiche dans une mappe directe comme suit :

```
/usr/local/tmp     -ro     dancer:/usr/local
```

Remarque – Aucune concaténation d'options ne s'effectue entre les mappes de montage automatique. Toutes les options qui sont ajoutées à une mappe de montage automatique remplacent toutes les options qui répertoriées dans les mappes ayant fait l'objet de recherches antérieures. Par exemple, les options qui sont incluses dans la mappe `auto_master` seraient remplacées par les entrées correspondantes dans n'importe quelle autre mappe.

Reportez-vous à la section "Méthode de sélection par autofs des fichiers en lecture seule les plus proches pour les clients (plusieurs emplacements) " à la page 217 pour obtenir des informations sur d'autres fonctionnalités importantes associées à ce type de mappe.

Point de montage `/-`

Dans l'Exemple 6–3, le point de montage `/-` dit à autofs de ne pas associer les entrées dans `auto_direct` avec tout point de montage spécifique. Les mappes indirectes utilisent des points de montage qui sont définis dans le fichier `auto_master`. Les mappes directes utilisant des points de montage qui sont spécifiés dans la mappe nommée. N'oubliez pas que dans une mappe directe, la clé ou point de montage est un nom de chemin d'accès complet.

Un fichier `auto_master` NIS ou NIS+ ne peut avoir qu'une seule entrée de mappe directe car le point de montage doit être une valeur unique dans l'espace de noms. Un fichier `auto_master` qui est un fichier local peut avoir n'importe quel nombre d'entrées de mappe directe entrées si des entrées ne sont pas dupliqués.

Mappe indirecte autofs

Une mappe indirecte utilise une valeur de substitution d'une clé pour établir l'association entre un point de montage sur le client et un répertoire sur le serveur. Les mappes indirectes sont utiles pour accéder à des systèmes de fichiers spécifiques, telles que les dossiers personnels. La mappe `auto_home` est un exemple de mappe indirecte.

Les lignes dans les mappes indirectes ont la syntaxe générale suivante :

clé [*options-montage*] *emplacement*

clé — *clé* est un nom simple sans barres obliques dans une mappe indirecte.

options-montage — *options-montage* correspond aux options que vous souhaitez appliquer à ce montage particulier. Ces options sont nécessaires uniquement si les options diffèrent de la mappe par défaut. Les options pour chaque type de système de fichiers sont répertoriées dans la page de manuel mount pour ce système de fichiers. Par exemple, reportez-vous à la page de manuel `mount_nfs(1M)` pour connaître les options de montage spécifiques à NFS.

emplacement — *emplacement* est l'emplacement du système de fichiers. Un ou plusieurs systèmes de fichiers sont spécifiés comme *server*: *nom_chemin*.

Remarque – Le *chemin d'accès* ne doit pas inclure un point de montage monté automatiquement. Le *chemin d'accès* doit être le véritable chemin d'accès absolu du système de fichiers. Par exemple, l'emplacement d'un répertoire doit être répertorié comme *serveur*`:/usr/local` et non comme *serveur*`:/net/` *serveur*`/usr/local`.

Comme pour la mappe principale, une ligne qui commence par # est un commentaire. Tout le texte qui suit jusqu'à la fin de la ligne n'est pas pris en compte. Placez une barre oblique (\) à la fin de la ligne pour scinder les lignes longues en lignes plus courtes. L'Exemple 6–3 montre une mappe `auto_master` qui contient l'entrée suivante :

```
/home      auto_home        -nobrowse
```

`auto_home` est le nom de la mappe indirecte qui contient les entrées à monter avec `/home`. Une mappe `auto_home` standard peut contenir les éléments suivants :

```
david                 willow:/export/home/david
rob                   cypress:/export/home/rob
gordon                poplar:/export/home/gordon
rajan                 pine:/export/home/rajan
tammy                 apple:/export/home/tammy
jim                   ivy:/export/home/jim
linda    -rw,nosuid   peach:/export/home/linda
```

Pour cet exemple, supposons que l'autre mappe est sur l'hôte `oak`. Supposons que l'utilisateur `linda` dispose d'une entrée dans la base de données de mots de passe qui indique son répertoire d'accueil comme étant `/home/linda`. Chaque fois que `linda` se connecte à l'ordinateur `oak`, autofs monte le répertoire `/export/home/linda` qui réside sur l'ordinateur `peach`. Son répertoire d'accueil est monté en lecture-écriture, nosuid.

Supposons que les conditions suivantes sont réunies : le répertoire d'accueil de Linda figure dans la base de données de mots de passe en tant que `/home/linda`. Quiconque, y compris Linda, peut accéder à ce chemin d'accès à partir de n'importe quel ordinateur qui est configuré avec la mappe principale faisant référence à la mappe dans l'exemple précédent.

Dans ces conditions, l'utilisateur linda peut exécuter `login` ou `rlogin` sur n'importe lequel de ces ordinateurs et son répertoire d'accueil sera monté pour elle.

En outre, Linda peut maintenant également taper la commande suivante :

```
% cd ~david
```

autofs monte le répertoire d'accueil de David pour elle (si tous les droits d'accès le permettent).

Remarque – Aucune concaténation d'options ne s'effectue entre les mappes de montage automatique. Toutes les options qui sont ajoutées à une mappe de montage automatique remplacent toutes les options qui répertoriées dans les mappes ayant fait l'objet de recherches antérieures. Par exemple, les options qui sont incluses dans la mappe `auto_master` sont remplacées par les entrées correspondantes de n'importe quelle autre mappe.

Sur un réseau sans service de noms, vous devez modifier tous les fichiers pertinents (comme `/etc/passwd`) sur tous les systèmes sur le réseau pour permettre à Linda d'accéder à ses fichiers. Avec NIS, apportez les modifications sur le serveur NIS principal et propagez les bases de données pertinentes aux serveurs esclaves. Sur un réseau qui exécute NIS+, la propagation des bases de données pertinentes aux serveurs esclaves s'effectue automatiquement une fois les modifications effectuées.

Fonctionnement d'autofs

Autofs est un service côté client qui monte automatiquement le système de fichiers adéquat. Les composants qui fonctionnent ensemble pour effectuer le montage automatique sont les suivants :

- Commande `automount`
- Système de fichiers `autofs`
- Démon `automountd`

Le service de montage automatique, `svc:/système/système de fichiers/autofs` , qui est appelé au moment du démarrage du système, lit le fichier de mappe principale `auto_master` pour créer l'ensemble initial de montages autofs. Ces montages autofs ne sont pas montés automatiquement lors du démarrage. Ces montages sont des points sous lesquels les systèmes de fichiers seront montés à l'avenir. Ces points sont également appelés nœuds déclencheurs.

Une fois les montages autofs définis, ces montages peuvent déclencher les systèmes de fichiers à monter sous eux. Par exemple, lorsqu'autofs reçoit une demande d'accès à un système de fichiers qui n'est pas actuellement monté, autofs appelle `automountd`, qui permet de monter le système de fichiers demandé.

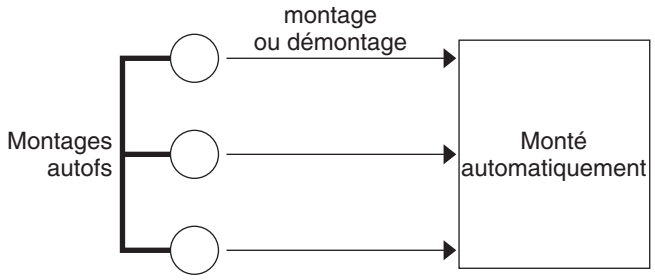
Après le montage initial des montages autofs, la commande `automount` est utilisée pour mettre à jour les montages autofs le cas échéant. La commande compare la liste des montages dans la mappe `auto_master` à la liste des systèmes de fichiers montés dans le fichier de table de montage `/etc/mnttab` (anciennement `/etc/mtab`). `automount` effectue ensuite les modifications appropriées. Ce processus permet aux administrateurs système de modifier des informations de montage dans `auto_master` et que ces modifications soient utilisées par le processus autofs sans arrêter et redémarrer le démon autofs. Une fois que le système de fichiers est monté, tout accès supplémentaire ne nécessite aucune action de `automountd` jusqu'à ce que le système de fichiers soit automatiquement démonté.

Contrairement à `mount`, `automount` ne lit pas le fichier `/etc/vfstab` (qui est spécifique à chaque ordinateur) pour obtenir une liste de systèmes de fichiers à monter. La commande `automount` est contrôlée au sein d'un domaine et sur les ordinateurs via l'espace de nom ou les fichiers locaux.

Vous trouverez ci-après une présentation simplifiée du fonctionnement d'autofs.

Le démon de montage automatique `automountd` est lancé au démarrage par le service `svc:/system/filesystem/autofs`. Reportez-vous à la Figure 6–3. Ce service exécute également la commande `automount` qui lit la mappe principale et installe les points de montage autofs. Pour plus d'informations, reportez-vous à la section "Démarrage du processus de navigation par autofs (mappe principale)" à la page 214.

FIGURE 6–3 Démarrage d'`automount` par le service `svc:/system/filesystem/autofs`



Autofs est un système de fichiers du noyau qui prend en charge le montage et démontage automatiques.

Lorsqu'une demande est effectuée pour accéder à un système de fichiers au niveau d'un point de montage autofs, il se produit ce qui suit :

1. Autofs intercepte la requête.
2. Autofs envoie un message à la commande `automountd` pour que le système de fichiers demandé soit monté.

3. `automountd` localise les informations du système de fichiers dans une mappe, crée les nœuds de déclencheur et exécute le montage.
4. Autofs permet à la requête interceptée de s'effectuer.
5. Autofs démonte le système de fichiers après une période d'inactivité.

Remarque – Les montages qui sont gérés par l'intermédiaire du service autofs ne doit pas être montés ou démontés manuellement. Même si l'opération est réussie, le service autofs ne vérifie pas que l'objet a été démonté, ce qui peut entraîner d'éventuelles incohérences. Un redémarrage efface le contenu de tous les points de montage autofs.

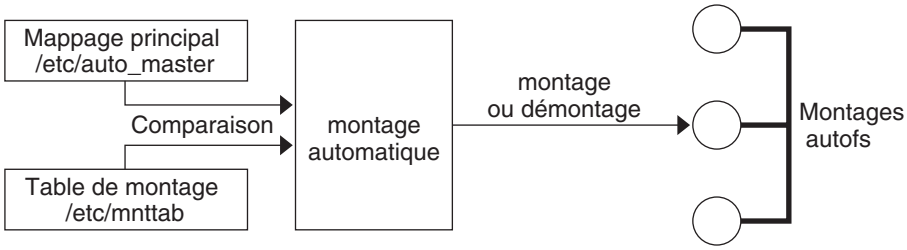
Comment Autofs Permet de naviguer à travers le réseau (cartes)

Autofs recherche une série de mappes pour parcourir le réseau. Les mappes sont des fichiers qui contiennent des informations telles que les entrées de mot de passe de tous les utilisateurs sur un réseau ou les noms de tous les ordinateurs hôte sur un réseau. En réalité, les mappes contiennent des équivalents de fichiers d'administration UNIX à l'échelle du réseau. Les mappes sont disponibles localement ou par l'intermédiaire d'un service de nom de réseau, tel que NIS ou NIS+. Reportez-vous à la rubrique "Modification de la navigation du réseau par autofs (modification des mappes)" à la page 223.

Démarrage du processus de navigation par autofs (mappe principale)

La commande `automount` lit la mappe principale au démarrage du système. Chaque entrée de la mappe principale est un nom de mappe directe ou de mappe indirecte, son chemin d'accès et ses options de montage, tel qu'illustré dans la Figure 6–4. L'ordre des entrées n'est pas important. `automount` compare les entrées dans la mappe principale avec des entrées dans la table de montage pour générer une liste actuelle.

FIGURE 6–4 Navigation par l'intermédiaire de la mappe principale



Processus de montage autofs

Le comportement du service autofs lorsqu'une demande de montage est déclenchée dépend de la façon dont les mappes de montage automatique sont configurées. Le processus de montage est généralement le même pour tous les montages. Cependant, le résultat final change avec le point de montage qui est spécifié et la complexité de ces mappes. Le processus de montage comprend la création des nœuds de déclencheur.

Montage autofs simple

Pour mieux comprendre le processus de montage autofs, supposons que les fichiers suivants sont installés.

```
$ cat /etc/auto_master
# Master map for automounter
#
+auto_master
/net        -hosts        -nosuid,nobrowse
/home       auto_home     -nobrowse
/share      auto_share
$ cat /etc/auto_share
# share directory map for automounter
#
ws          gumbo:/export/share/ws
```

En cas d'accès au répertoire `/share`, le service autofs crée un noeud de déclencheur pour `/share/ws`, qui est une entrée dans `/etc/mnttab` et qui ressemble à l'entrée suivante :

```
-hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
```

En cas d'accès au répertoire `/share/ws`, le service autofs termine le processus avec ces étapes :

1. Vérifie la disponibilité du service de montage du serveur.
2. Monte le système de fichiers demandé sous `/share`. Maintenant le fichier `/etc/mnttab` contient les entrées suivantes.

   ```
   -hosts  /share/ws     autofs  nosuid,nobrowse,ignore,nest,dev=###
   gumbo:/export/share/ws /share/ws   nfs   nosuid,dev=####    #####
   ```

Montage hiérarchique

Lorsque plusieurs couches sont définies dans les fichiers de montage automatique, le processus de montage devient plus complexe. Supposons que vous développez le fichier `/etc/auto_shared` de l'exemple précédent pour qu'il contienne les éléments suivants :

```
# share directory map for automounter
#
ws       /       gumbo:/export/share/ws
         /usr    gumbo:/export/share/ws/usr
```

Le processus de montage est essentiellement le même que dans l'exemple précédent en cas d'accès au point de montage `/share/ws`. En outre, un noeud de déclencheur au niveau suivant (`/usr`) est créé dans le système de fichiers `/share/ws` pour que le niveau suivant puisse être monté si on y accès. Dans cet exemple, `/export/share/ws/usr` doit exister sur le serveur NFS pour le noeud de déclencheur soit créé.

Attention – N'utilisez pas l'option `-soft` lors de la spécification de calques hiérarchiques. Reportez-vous à la rubrique "Démontage autofs" à la page 216 pour obtenir une explication sur cette limite.

Démontage autofs

Le démontage qui se produit après un certain temps d'inactivité suit l'ordre inverse de montage. Si l'un des répertoires à un niveau plus élevé dans la hiérarchie est occupé, seuls les systèmes de fichiers sous ce répertoire sont démontés. Pendant le processus de démontage, les nœuds de déclencheur sont supprimé et le système de fichiers est ensuite démonté. Si le système de fichiers est occupé, le démontage échoue et le nœuds de déclencheur sont réinstallés.

Attention – N'utilisez pas l'option `-soft` lors de la spécification de calques hiérarchiques. Si l'option `-soft` est utilisée, les demandes de réinstallation des nœuds de déclencheur peuvent dépasser le délai imparti. L'échec de réinstallation des nœuds de déclencheur ne laisse aucun accès au niveau suivant de montages. La seule façon de résoudre le problème est de laisser l'agent de montage automatique démonter tous les composants dans la hiérarchie. L'agent de montage automatique peut terminer le démontage soit en attendant que les systèmes de fichiers soient démontés automatiquement, soit le redémarrage du système.

Méthode de sélection par autofs des fichiers en lecture seule les plus proches pour les clients (plusieurs emplacements)

L'exemple de mappe directe contient les éléments suivants :

```
/usr/local          -ro \
   /bin                   ivy:/export/local/sun4\
   /share                 ivy:/export/local/share\
   /src                   ivy:/export/local/src
/usr/man            -ro   oak:/usr/man \
                          rose:/usr/man \
                          willow:/usr/man
/usr/games          -ro   peach:/usr/games
/usr/spool/news     -ro   pine:/usr/spool/news \
                          willow:/var/spool/news
```

Les points de montage `/usr/man` et `/usr/spool/news` répertorient plusieurs emplacements, trois emplacements pour le premier point de montage, et deux emplacements pour le deuxième point de montage. Tous les emplacements répliqués peuvent fournir le même service à n'importe quel utilisateur. Cette procédure est délicate uniquement lorsque vous montez un système de fichiers en lecture seule, dans la mesure où vous devez avoir un contrôle sur les emplacements des fichiers sur lesquels vous écrivez ou que vous modifiez. Vous devez éviter de modifier les fichiers sur un serveur à un moment donné, puis, quelques minutes plus tard, modifier le "même" fichier sur un autre serveur. L'avantage est que le meilleur serveur disponible est utilisé automatiquement sans intervention de l'utilisateur.

Si les systèmes de fichiers sont configurés en tant que répliques (voir “Qu'est-ce qu'un système de fichiers répliqué ?” à la page 197), les clients ont l'avantage de l'utilisation du basculement. Non seulement le meilleur serveur est automatiquement déterminé, mais si ce serveur n'est plus disponible, le client utilise automatiquement le meilleur serveur suivant.

Un exemple d'un bon système de fichiers à configurer est une réplique de pages de manuel. Dans un réseau de grande taille, plusieurs serveurs peuvent exporter l'ensemble actuel de pages de manuel. Le serveur à partir duquel vous montez les pages de manuel n'a pas d'importance s'il est en cours d'exécution et exporte ses systèmes de fichiers. Dans l'exemple précédent, plusieurs emplacements de montage sont exprimés sous forme d'une liste d'emplacements de montage dans l'entrée de mappe.

```
/usr/man -ro oak:/usr/man rose:/usr/man willow:/usr/man
```

Dans cet exemple, vous pouvez monter les pages de manuel à partir des serveurs `oak`, `rose` ou `willow`. Quel serveur est le meilleur dépend d'un certain nombre de facteurs, y compris les éléments suivants :

- le nombre de serveurs qui prennent en charge un niveau donné de protocole NFS ;
- la proximité du serveur ;
- la pondération.

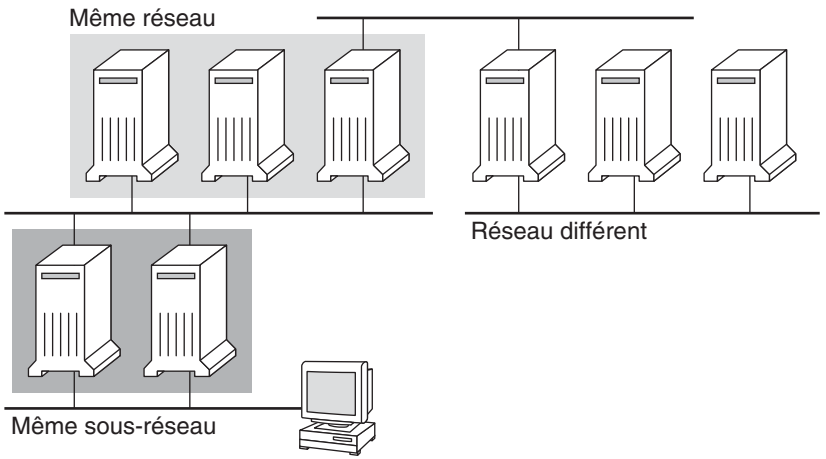
Au cours du processus de tri, le nombre de serveurs qui prennent en charge chaque version du protocole NFS est compté. La version du protocole qui est prise en charge sur la plupart des serveurs devient le protocole par défaut. Cette sélection permet au client de disposer du nombre maximal de serveurs sur lesquels il peut dépendre.

Lorsque le plus grand sous-ensemble de serveurs avec la même version du protocole est trouvé, cette liste de serveurs est triée suivant leur proximité. Pour déterminer la proximité, les adresses IPv4 sont examinées. Les adresses IPv4 indiquent quels serveurs se trouvent dans chaque sous-réseau. Les serveurs d'un sous-réseau local sont préférés aux serveurs sur un sous-réseau distant. La préférence pour le serveur le plus proche réduit les délais d'attente et le trafic sur le réseau.

Remarque – La proximité ne peut pas être déterminée pour les réplications qui utilisent des adresses IPv6.

La Figure 6–5 illustre la proximité de serveur.

FIGURE 6–5 Proximité de serveur



Si plusieurs serveurs qui prennent en charge le même protocole sont sur le sous-réseau local, le temps connexion à chaque serveur est déterminé et le plus rapide des serveurs est utilisé. Le tri peut également être influencé par la pondération (reportez-vous à la section "Autofs et pondération" à la page 220).

Par exemple, si les serveurs version 4 sont plus nombreux, la version 4 devient le protocole utilisé par défaut. Cependant, le processus de tri est maintenant plus complexe. Voici quelques exemples de la manière dont le processus de tri fonctionne :

- Les serveurs sur le sous-réseau local sont préférés aux serveurs sur un sous-réseau distant. Par conséquent, si un serveur version 3 se trouve sur le sous-réseau local et que le serveur version 4 le plus proche est sur un sous-réseau distant, le serveur version 3 se voit donner la préférence. De même, si le sous-réseau local se compose de serveurs version 2, ils sont privilégiés par rapport à des sous-réseaux distants avec des serveurs version 3 et version 4.
- Si le sous-réseau local est constitué d'un nombre varié de serveurs version 2, version 3 et version 4, plus de tri est nécessaire. L'agent de montage automatique préfère la version la plus récente sur le sous-réseau local. Dans cet exemple, la version 4 est la version la plus récente. Toutefois, si le sous-réseau local a plus de serveurs version 3 ou 2 que de serveurs version 4, l'agent de montage automatique "descend" d'une version sur le sous-réseau local. Par exemple, si le sous-réseau local dispose de trois serveurs de version 4, trois serveurs de version 3 et dix serveurs de version 2, un serveur de version 3 est sélectionné.
- De même, si le sous-réseau local est constitué d'un nombre variable de serveurs de version 2 et 3, l'agent de montage automatique examine d'abord la version qui représente la version la plus récente sur le sous-réseau local. Ensuite, l'agent de montage automatique compte le nombre de serveurs qui exécutent chaque version. Si la version la plus récente sur le sous-réseau local représente également la plupart des serveurs, la version la plus élevée est sélectionnée. Si une version inférieure a davantage de serveurs, l'agent de montage automatique descend d'une version sur le sous-réseau local. Par exemple, s'il y a plus de serveurs de version 2 sur le sous-réseau local que de serveurs version 3, un serveur version 2 est sélectionné.

Remarque – La pondération est également influencée par valeurs des mots-clés dans le fichier `/etc/default/nfs`. Plus spécifiquement, les valeurs de NFS_SERVER_VERSMIN, NFS_CLIENT_VERSMIN, NFS_SERVER_VERSMAX et NFS_CLIENT_VERSMAX peuvent exclure certaines versions du processus de tri. Pour plus d'informations sur ces mots-clés, reportez-vous à la section "Mots-clés pour le fichier `/etc/default/nfs`" à la page 142.

Avec le basculement, le tri est vérifié au moment du montage lorsqu'un serveur est sélectionné. Plusieurs emplacements sont utiles dans un environnement où les serveurs individuels peuvent ne pas exporter leurs systèmes de fichiers temporairement.

Le basculement est particulièrement utile dans les réseaux de grande taille avec de nombreux sous-réseaux. Autofs choisit le serveur approprié et est en mesure de limiter le trafic du réseau NFS à un segment de réseau local. Si un serveur dispose de plusieurs interfaces réseau, vous pouvez répertorier le nom d'hôte qui est associé à chaque interface réseau comme si l'interface était un serveur distinct. Autofs sélectionne l'interface la plus proche pour le client.

Remarque – Aucune pondération et aucune vérification de proximité ne sont effectuées avec les montages manuels. La commande `mount` donne la priorité aux serveurs répertoriés de gauche à droite.

Pour plus d'informations, reportez-vous à la page de manuel `automount(1M)`.

Autofs et pondération

Vous pouvez influencer la sélection de serveurs au même niveau de proximité par l'ajout d'une valeur de pondération à la mappe autofs. Par exemple :

```
/usr/man -ro oak,rose(1),willow(2):/usr/man
```

Les nombres entre parenthèses indiquent une pondération. Les serveurs sans pondération ont une valeur de zéro et, par conséquent, sont plus susceptibles d'être sélectionnés. Plus la valeur de pondération est élevée, plus la probabilité que le serveur soit sélectionné est basse.

Remarque – Tous les autres facteurs de sélection de serveur sont plus importants que la pondération. La pondération est uniquement prise en compte lors de la sélection entre serveurs avec la même proximité au réseau.

Variables d'une entrée de mappe

Vous pouvez créer une variable spécifique au client en précédant son nom du signe du dollar (`$`). La variable vous aide à satisfaire à différents types d'architecture qui accèdent au même emplacement du système de fichiers. Vous pouvez également utiliser des accolades pour délimiter le nom de la variable par rapport aux lettres ou chiffres ajoutés. Le Tableau 6–2 montre les variables de mappe prédéfinie.

TABLEAU 6–2 Variables de mappe prédéfinie

Variable	Signification	Dérivées de	Exemple
ARCH	Type d'architecture	`uname -m`	`sun4`

TABLEAU 6–2 Variables de mappe prédéfinie *(Suite)*

Variable	Signification	Dérivées de	Exemple
`CPU`	Type de processeur	`uname -p`	`sparc`
`HOST`	Nom d'hôte	`uname -n`	`dinky`
`OSNAME`	Nom du système d'exploitation	`uname -s`	`SunOS`
`OSREL`	Version du système d'exploitation	`uname -r`	`5.8`
`OSVERS`	Version du système d'exploitation	`uname -v`	`GENERIC`

Vous pouvez utiliser des variables n'importe où dans une ligne de saisie, sauf en tant que clé. Par exemple, supposons que vous disposez d'un serveur de fichiers qui exporte des fichiers binaires SPARC et des architectures `/usr/local/bin/sparc` et `/usr/local/bin/x86` respectivement. Les clients peuvent monter via une entrée de mappe, comme suit :

```
/usr/local/bin        -ro     server:/usr/local/bin/$CPU
```

La même entrée pour tous les clients s'applique maintenant à toutes les architectures.

Remarque – La plupart des applications qui sont écrits pour n'importe laquelle des architectures sun4 peuvent s'exécuter sur toutes les plates-formes sun4. La variable `-ARCH` est codée en dur sur `sun4`.

Mappes faisant référence à d'autres mappes

Une entrée de mappe *+nom-mappe* utilisée dans un fichier de mappe fait qu'automount lit la mappe spécifiée comme si elle était incluse dans le fichier en cours. Si *nom-mappe* n'est pas précédé d'une barre oblique, autofs traite le nom de la mappe comme une chaîne de caractères et utilise la stratégie de changement nom-service pour trouver le nom de la mappe. Si le nom du chemin d'accès est un nom de chemin d'accès absolu, `automount` vérifie une mappe locale de ce nom. Si le nom de la carte commence par un tiret (`-`), `automount` consulte la mappe intégrée appropriée telle que `hosts`.

Ce fichier de changement nom-service contient une entrée pour autofs qui est libellée `automount` et contient l'ordre de recherche des services de noms. Le fichier suivant est un exemple de fichier de changement nom-service.

```
#
# /etc/nsswitch.nis:
#
# An example file that could be copied over to /etc/nsswitch.conf;
# it uses NIS (YP) in conjunction with files.
#
# "hosts:" and "services:" in this file are used only if the /etc/netconfig
```

```
# file contains "switch.so" as a nametoaddr library for "inet" transports.
# the following two lines obviate the "+" entry in /etc/passwd and /etc/group.
passwd:         files nis
group:          files nis

# consult /etc "files" only if nis is down.
hosts:          nis [NOTFOUND=return] files
networks:       nis [NOTFOUND=return] files
protocols:      nis [NOTFOUND=return] files
rpc:            nis [NOTFOUND=return] files
ethers:         nis [NOTFOUND=return] files
netmasks:       nis [NOTFOUND=return] files
bootparams:     nis [NOTFOUND=return] files
publickey:      nis [NOTFOUND=return] files
netgroup:       nis
automount:      files nis
aliases:        files nis
# for efficient getservbyname() avoid nis
services:       files nis
```

Dans cet exemple, les mappes locales sont recherchées avant que les mappes NIS. Par conséquent, il est possible d'avoir peu d'entrées dans la mappe `/etc/auto_home` locale pour les répertoires d'accueil le plus couramment accédés. Vous pouvez ensuite utiliser le commutateur pour restaurer la mappe NIS pour d'autres entrées.

```
bill              cs.csc.edu:/export/home/bill
bonny             cs.csc.edu:/export/home/bonny
```

Après avoir consulté la mappe incluse, si aucune correspondance n'est trouvée, `automount` poursuit l'analyse de la mappe actuelle. Par conséquent, vous pouvez ajouter plusieurs entrées après une entrée `+`.

```
bill              cs.csc.edu:/export/home/bill
bonny             cs.csc.edu:/export/home/bonny
+auto_home
```

La carte qui est incluse peut être un fichier local ou une mappe intégrée. N'oubliez pas que seuls les fichiers locaux peuvent contenir des entrées `+`.

```
+auto_home_finance      # NIS+ map
+auto_home_sales        # NIS+ map
+auto_home_engineering  # NIS+ map
+/etc/auto_mystuff      # local map
+auto_home              # NIS+ map
+-hosts                 # built-in hosts map
```

Remarque – Vous ne pouvez pas utiliser les entrées + entrées dans les mappes NIS+ ou NIS.

Mappes autofs exécutables

Vous pouvez créer une mappe autofs qui exécute des commandes permettant de générer les points de montage autofs. Vous pouvez bénéficier de l'utilisation d'une mappe autofs exécutable si vous devez être en mesure de créer la structure autofs à partir d'une base de données ou d'un fichier plat. L'inconvénient de l'utilisation d'une mappe exécutable est qu'elle doit être installée sur chaque hôte. Une mappe exécutable ne peut pas être incluse ni dans le NIS ni dans le service de noms NIS+.

La mappe exécutable doit disposer d'une entrée dans le fichier `auto_master`.

```
/execute    auto_execute
```

Voici un exemple d'une mappe exécutable :

```
#!/bin/ksh
#
# executable map for autofs
#

case $1 in
             src)  echo '-nosuid,hard bee:/export1' ;;
esac
```

Pour cet exemple fonctionne, le fichier doit être installé comme `/etc/auto_execute` et doit avoir le bit d'exécution défini. Configurer les permissions sur `744`. Dans ces circonstances, l'exécution de la commande ci-dessous est à l'origine du montage du système de fichiers `/export1` de `bee` :

```
% ls /execute/src
```

Modification de la navigation du réseau par autofs (modification des mappes)

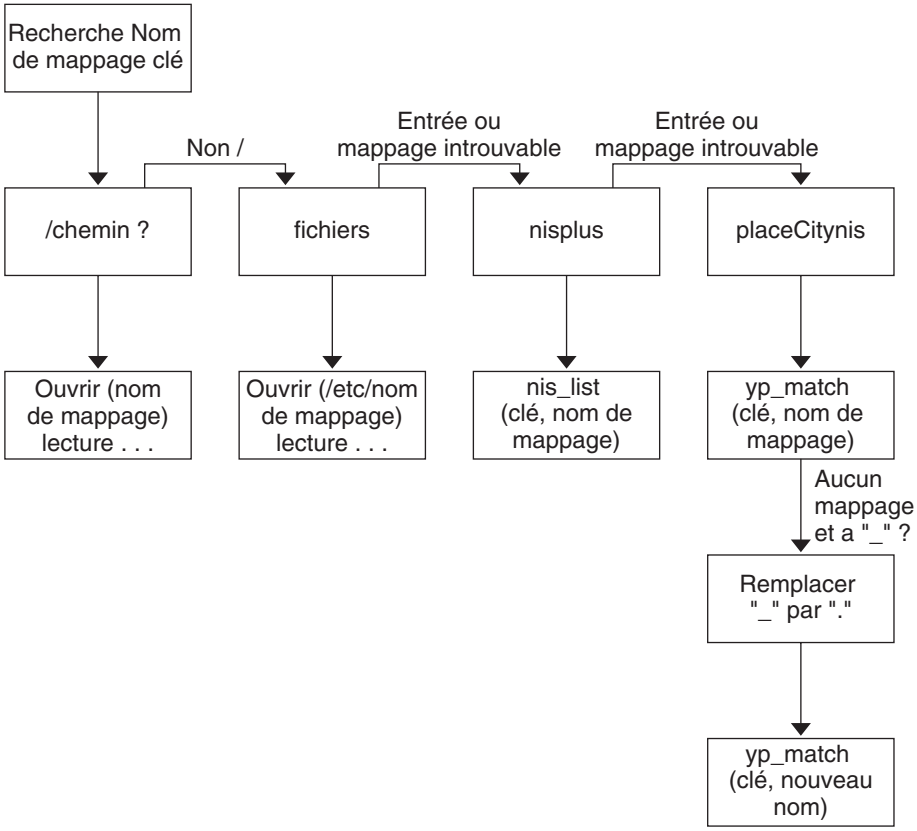
Vous pouvez modifier, supprimer ou ajouter des entrées aux mappes pour répondre aux besoins de votre environnement. Au fur et à mesure du changement de l'emplacement des applications et autres systèmes de fichiers nécessaires pour les utilisateurs, les mappes doivent refléter ces changements. Vous pouvez modifier les mappes autofs à tout moment. L'entrée en vigueur de vos modifications lors du prochain montage d'`automountd` d'un système de fichiers dépend de la mappe que vous modifiez et du type de modification apportée.

Comportement par défaut d'autofs avec les services de noms

Lors du démarrage, autofs est appelé par le service `svc:/system/filesystem/autofs` et autofs vérifie la mappe principale `auto_master`. Autofs est soumis aux règles qui sont traitées par la suite.

Autofs utilise le nom de service qui est spécifié dans l'entrée automount du fichier `/etc/nsswitch.conf`. Si NIS+ est spécifié, par opposition à des fichiers locaux ou NIS, tous les noms de mappe sont utilisés en tant que tels. Si NIS est sélectionné et qu'autofs ne peut pas afficher une mappe dont autofs a besoin, mais trouve un nom de mappe qui contient un ou plusieurs caractères de soulignement, les caractères de soulignement ne sont pas changés en points. Cette modification permet aux anciens noms de fichiers NIS de fonctionner. Ensuite, autofs vérifie à nouveau la mappe, comme illustré dans la Figure 6–6.

FIGURE 6–6 Utilisation du service de noms par autofs



L'activité d'écran pour cette session ressemblerait à l'exemple suivant.

```
$ grep /home /etc/auto_master
/home           auto_home

$ ypmatch brent auto_home
Can’t match key brent in map auto_home.  Reason: no such map in
server’s domain.

$ ypmatch brent auto.home
diskus:/export/home/diskus1/&
```

Si l'option "fichiers" est sélectionnée en tant que service de noms, toutes les mappes sont supposées être des fichiers locaux dans le répertoire `/etc`. Autofs interprète un nom de mappe qui commence par une barre oblique (`/`) comme étant locale quel que soit le service de noms utilisé par autofs.

Référence autofs

Les autres sections de ce chapitre abordent des fonctions et des aspects plus avancés d'autofs.

Autofs et les métacaractères

Autofs reconnaît certains caractères comme ayant une signification particulière. Certains caractères sont utilisés pour les substitutions, et d'autres caractères sont utilisés pour protéger d'autres caractères de l'analyseur syntaxique de mappe autofs.

Esperluette (&)

Si vous possédez une mappe avec de nombreux sous-répertoires spécifiés, comme dans l'exemple suivant, vous pouvez envisager d'utiliser des substitutions de chaîne.

```
john        willow:/home/john
mary        willow:/home/mary
joe         willow:/home/joe
able        pine:/export/able
baker       peach:/export/baker
```

Vous pouvez utiliser le caractère esperluette (&) afin de remplacer la clé partout où elle s'affiche. Si vous utilisez l'esperluette, l'autre mappe change comme suit :

```
john        willow:/home/&
mary        willow:/home/&
joe         willow:/home/&
able        pine:/export/&
baker       peach:/export/&
```

Vous pouvez également utiliser des substitutions de clé dans une mappe directe, notamment dans les situations suivantes :

```
/usr/man                        willow,cedar,poplar:/usr/man
```

Vous pouvez également simplifier davantage l'entrée comme suit :

```
/usr/man                        willow,cedar,poplar:&
```

Notez que la substitution de l'esperluette utilise la chaîne de clé complète. Par conséquent, si la clé dans une mappe directe commence par le signe / (comme elle le devrait), la barre oblique est incluse dans la substitution. Par conséquent, par exemple, vous ne pourriez pas effectuer les opérations suivantes :

```
/progs                &1,&2,&3:/export/src/progs
```

La raison est qu'autofs interpréterait l'exemple comme suit :

```
/progs                 /progs1,/progs2,/progs3:/export/src/progs
```

Astérisque (*)

Vous pouvez utiliser le caractère de substitution universel, l'astérisque (*), pour correspondre à n'importe quelle clé. Vous pouvez monter le système de fichiers `/export` à partir de tous les hôtes à l'aide de cette entrée de mappe.

```
*                       &:/export
```

Chaque esperluette est remplacée par la valeur de n'importe quelle clé donnée. Autofs interprète l'astérisque comme un caractère de fin de fichier.

Autofs et caractères spéciaux

Si vous avez une entrée de mappe qui contient des caractères spéciaux, vous devrez peut-être monter des répertoire avec des noms portant à confusion pour l'analyseur syntaxique de mappes autofs. L'analyseur syntaxique autofs est sensible aux noms contenant par exemple les caractères suivants : deux points, virgules et espaces. Ces noms doivent être entre guillemets, comme dans l'exemple suivant :

```
/vms    -ro    vmsserver: -  -  - "rc0:dk1 - "
/mac    -ro    gator:/ - "Mr Disk - "
```

PARTIE III

SLP

Cette section présente le service SLP (Service Location Protocol) et fournit des informations relatives à sa planification et aux tâches liées, ainsi que des références.

◆ ◆ ◆ CHAPITRE 7

SLP (présentation)

Le protocole SLP (Service Location Protocol) fournit une structure portable, indépendante de la plate-forme pour la découverte et la fourniture de services réseau SLP. Ce chapitre décrit l'architecture SLP et l'implémentation Solaris de SLP pour les Intranet IP.

Architecture SLP

Cette section décrit le fonctionnement de base de SLP, ainsi que les agents et processus utilisés pour l'administration SLP.

SLP fournit automatiquement tous les services suivants, avec peu ou pas de configuration.

- Requêtes des informations nécessaires pour accéder à un service par l'application client
- Annonce des services sur les périphériques matériels réseau ou les serveurs logiciels (par exemple, les imprimantes, serveurs de fichiers, caméras vidéo et serveurs HTTP)
- Restauration gérée en cas de défaillance du serveur principal

En outre, vous pouvez effectuer les opérations suivantes pour gérer et régler les opérations SLP, si nécessaire.

- Organiser les services et les utilisateurs en *étendues* composées de groupes fonctionnels ou logiques
- Activer la journalisation SLP pour surveiller et dépanner le fonctionnement SLP sur votre réseau
- Ajuster les paramètres de synchronisation SLP pour améliorer les performances et l'évolutivité

- Configurer le protocole SLP afin qu'il n'envoie pas et ne traite pas de messages de multidiffusion lorsqu'il est déployé sur des réseaux qui ne prennent pas en charge le routage multidiffusion
- Déployer les agents de répertoire SLP pour améliorer l'évolutivité et les performances

Synthèse de la conception SLP

Les bibliothèques SLP informent les agents conscients du réseau qui annoncent des services afin que ces services puissent être découverts par l'intermédiaire d'un réseau. Les agents SLP maintiennent des informations à jour sur le type et l'emplacement des services. Ces agents peuvent également utiliser des enregistrements de proxy pour annoncer les services sur lesquels SLP n'est pas directement activé. Pour plus d'informations, reportez-vous au Chapitre 10, “Intégration des services hérités”.

Les applications client s'appuient sur les bibliothèques SLP qui envoient des requêtes directement aux agents qui annoncent les services.

Agents et processus SLP

Le tableau suivant décrit les agents SLP. Pour des définitions plus détaillées de ces termes et d'autres termes utilisés dans ce manuel, reportez-vous au Glossaire.

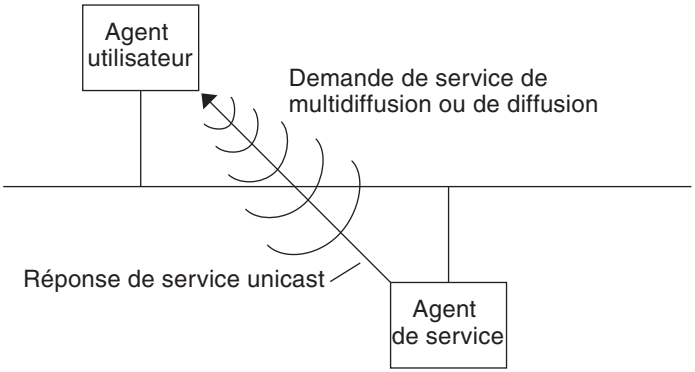
TABLEAU 7–1 Agents SLP

Agent SLP	Description
Agent de répertoire (DA)	Processus qui met en cache les annonces SLP enregistrées par les agents de service (SA). Le DA transfère les annonces de service aux agents utilisateur (UA) à la demande.
Agent de service (SA)	Agent SLP qui agit pour le compte d'un service pour distribuer les annonces de service et enregistrer le service avec les agents de répertoire (DA).
Agent utilisateur (UA)	Agent SLP qui agit pour le compte d'un utilisateur ou d'une application afin d'obtenir des informations sur les annonces de service.
étendue	Groupement administratif ou logique de services.

La figure ci-dessous montre les agents et processus de base qui mettent en œuvre l'architecture SLP. La figure représente un déploiement SLP par défaut. Aucune configuration spéciale n'a été effectuée. Seuls deux agents sont requis : UA et SA. La structure SLP permet à l'UA d'envoyer des requêtes multidiffusion de service au SA. Ce dernier envoie une réponse monodiffusion à l'UA. Par exemple, lorsque l'UA envoie un message de requête de service, le SA répond avec un

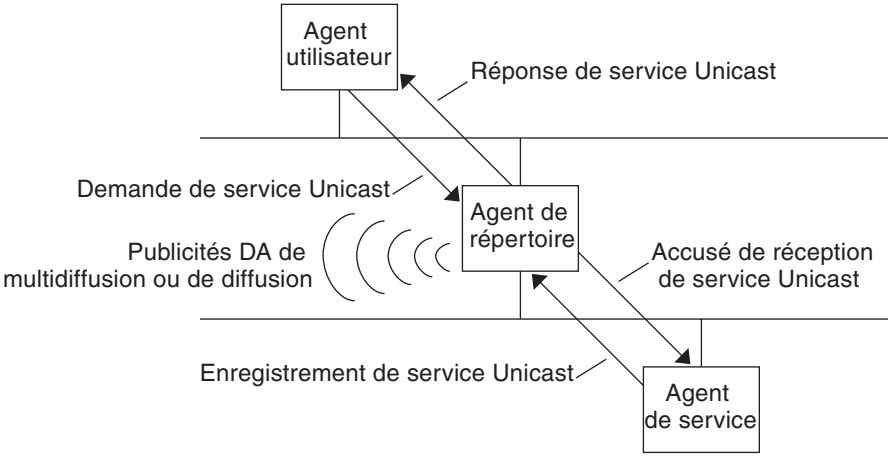
message de réponse de service. La réponse de service contient l'emplacement des services qui répondent aux besoins du client. D'autres requêtes et réponses sont possibles pour les attributs et types de service. Pour plus d'informations, reportez-vous au Chapitre 11, “SLP (références)”.

FIGURE 7–1 Agents et processus SLP de base



La figure ci-dessous montre les agents et processus de base qui mettent en œuvre l'architecture SLP lorsqu'un DA est déployé dans la structure.

FIGURE 7–2 Agents et processus d'architecture SLP mis en œuvre avec un DA



Lorsque vous déployez des agents de répertoire, moins de messages sont envoyés sur le réseau et les agents utilisateur peuvent récupérer les informations beaucoup plus rapidement. Les DA sont cruciaux lorsque la taille d'un réseau augmente ou dans les cas où le routage multidiffusion n'est pas pris en charge. Le DA sert de cache de service pour les annonces de service

enregistrées. Les SA envoient des messages d'enregistrement (`SrvReg`) qui répertorient tous les services qu'ils annoncent aux DA. Les SA reçoivent alors des accusés de réception (`SrvAck`) dans la réponse. Les annonces de service sont actualisées avec le DA ou elles expirent conformément à la durée de vie définie pour l'annonce. Une fois qu'un UA découvre un DA, l'UA envoie une requête monodiffusion au DA plutôt que d'envoyer des requêtes multidiffusion aux SA.

Pour plus d'informations sur les messages SLP Solaris, reportez-vous au chapitre Chapitre 11, “SLP (références)”.

Implémentation SLP

Dans une implémentation SLP Solaris, les SA, UA, DA et serveurs SA SLP, les étendues et autres composants d'architecture décrits dans Tableau 7–1 sont partiellement mappés dans `slpd` et partiellement dans les processus d'application. Le démon SLP, `slpd`, organise certaines interactions SLP hors hôte pour effectuer les opérations suivantes :

- Employer la détection d'agent d'annuaire actif et passif afin de détecter tous les DA sur le réseau
- Maintenir un tableau à jour des DA destiné aux UA et SA sur l'hôte local
- Agir en tant que serveur SA proxy pour les annonces de services hérités (enregistrement de proxy)

Vous pouvez définir la propriété `net.slpisDA` afin d'également configurer `slpd` pour qu'il agisse comme un DA. Reportez-vous au Chapitre 9, “Administration de SLP (tâches)”.

Pour plus d'informations sur le démon SLP, reportez-vous à la page de manuel `slpd(1M)`.

Outre `slpd`, les bibliothèques client C/C++ et Java (`libslp.so` et `slp.jar`) permettent l'accès à la structure SLP pour les clients UA et SA. Les bibliothèques client offrent les fonctions suivantes :

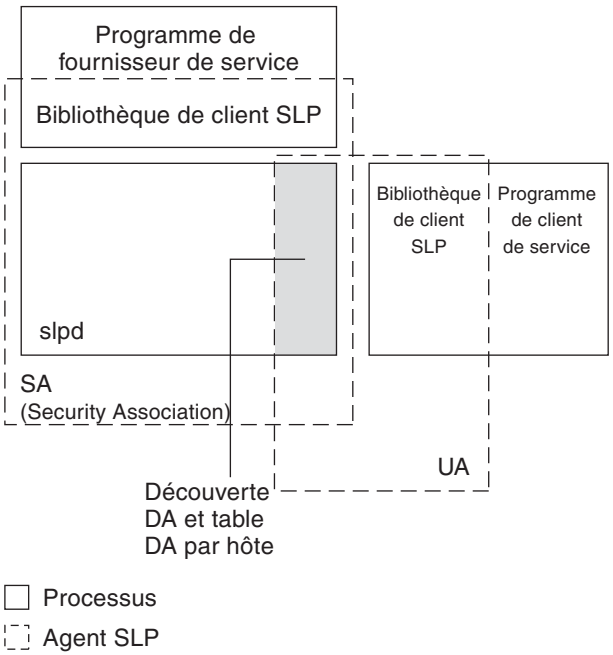
- Logiciel qui offre des services réseau capables d'enregistrer ou annuler l'enregistrement d'annonces de services
- Logiciel client qui peut envoyer des requêtes de services en émettant des requêtes d'annonces de services
- Liste des étendues SLP disponibles pour l'enregistrement et les requêtes

Aucune configuration particulière n'est nécessaire pour activer la communication inter-processus entre `slpd` et les bibliothèques client qui fournissent les services cités précédemment. Néanmoins, vous devez exécuter le processus `slpd` avant de charger les bibliothèques client afin que celles-ci fonctionnent.

Dans la figure ci-dessous, la bibliothèque client SLP dans le programme Fournisseur de services utilise la fonctionnalité SA. Le programme Fournisseur de service utilise la bibliothèque client SLP pour enregistrer ou annuler l'enregistrement de services avec `slpd`. La bibliothèque client

SLP dans le programme Client de service utilise la fonctionnalité UA. Le programme Client de service utilise la bibliothèque client SLP pour envoyer des requêtes. La bibliothèque client SLP envoie des requêtes multidiffusion aux SA ou des requêtes monodiffusion aux DA. Cette communication est transparente pour l'application, à la différence que la méthode de monodiffusion est plus rapide. Il est possible de modifier le comportement de la bibliothèque client en définissant diverses propriétés de configuration SLP. Pour plus d'informations, reportez-vous au Chapitre 9, “Administration de SLP (tâches)”. Le processus `slpd` gère toutes les fonctionnalités SA, telles que la réponse aux requêtes multidiffusion et l'enregistrement avec les DA.

FIGURE 7–3 Implémentation SLP



Autres sources d'informations sur le protocole SLP

Reportez-vous aux documents suivants pour obtenir plus d'informations sur le protocole SLP :

- Kempf, James et Pete Saint Pierre. *Service Location Protocol for Enterprise Networks*. John Wiley & Sons, Inc. ISBN : 0–471–31587–7.
- *Authentication Management Infrastructure Administration Guide*. Numéro de référence : 805-1139-03.

- Guttman, Erik, Charles Perkins, John Veizades et Michael Day. *Service Location Protocol, Version 2, RFC 2608* from the Internet Engineering Task Force (IETF). [http://www.ietf.org/rfc/rfc2608.txt]
- Kempf, James et Erik Guttman. *An API for Service Location, RFC 2614* de l'IETF (Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2614.txt]

◆ ◆ ◆ CHAPITRE 8

Planification et activation de SLP (tâches)

Ce chapitre fournit des informations sur la planification et l'activation de SLP. Les sections suivantes abordent la configuration et le processus d'activation de SLP.

Éléments à prendre en compte pour la configuration de SLP

Le démon SLP est préconfiguré avec des propriétés par défaut. Si les paramètres par défaut conviennent à votre entreprise, le déploiement SLP ne requiert pratiquement aucune administration.

Dans certains cas, cependant, vous pouvez être amené à modifier les propriétés SLP afin d'optimiser le fonctionnement du réseau ou pour activer certaines fonctions. Quelques changements de configuration permettent par exemple d'activer la journalisation SLP. Les informations d'un journal SLP et du suivi `snoop` peuvent vous aider à déterminer si une configuration supplémentaire est nécessaire.

Les propriétés de configuration SLP se trouvent dans le fichier `slp.conf`, disponible sous le répertoire `/etc/inet`. Si vous souhaitez modifier les paramètres par défaut de la propriété, reportez-vous au Chapitre 9, "Administration de SLP (tâches)" pour connaître les procédures appropriées.

Avant de modifier les paramètres de configuration SLP, envisagez les questions suivantes, relatives aux aspects essentiels de l'administration réseau :

- Quelles technologies réseau sont en place dans l'entreprise ?
- Quelle quantité de trafic réseau ces technologies peuvent-elles gérer sans problème ?
- Combien de services, et de quel type, sont-ils disponibles sur le réseau ?
- Combien d'utilisateurs se trouvent-ils sur le réseau ? De quels services ont-ils besoin ? Où se trouvent les utilisateurs par rapport aux services qu'ils utilisent le plus ?

Détermination des éléments à reconfigurer

Vous pouvez utiliser l'utilitaire snoop SLP et les utilitaires de journalisation SLP pour décider si une reconfiguration est nécessaire et les propriétés devant être modifiées. Par exemple, vous pouvez reconfigurer certaines propriétés pour effectuer les opérations suivantes :

- Adapter un ensemble de supports réseau présentant des caractéristiques de latence et de bande passante différentes
- Restaurer le système d'entreprise en cas de pannes de réseau ou de partitionnement non planifié
- Ajouter des DA pour réduire la prolifération des multidiffusions SLP
- Implémenter de nouvelles étendues afin d'organiser les utilisateurs avec les services auxquels ils accèdent le plus souvent

Utilisation de snoop pour surveiller l'activité SLP

L'utilitaire snoop est un outil d'administration passif qui fournit des informations sur le trafic réseau. L'utilitaire lui-même génère un trafic minimal et vous permet de contrôler toutes les activités sur votre réseau en temps réel.

L'utilitaire snoop fournit un suivi de l'ensemble du trafic réel des messages SLP. Par exemple, lorsque vous exécutez snoop avec l'argument de ligne de commande slp, l'utilitaire affiche les suivis avec des informations sur les enregistrements et annulations d'enregistrements SLP. Vous pouvez utiliser ces informations pour évaluer la charge du réseau en vérifiant les services en cours d'enregistrement et l'importance de l'activité d'annulation d'enregistrements en cours.

L'utilitaire snoop est également utile pour observer le flux de trafic entre les hôtes SLP de votre entreprise. Lorsque vous exécutez snoop avec l'argument de ligne de commande slp, vous pouvez surveiller les types d'activités SLP suivants afin de déterminer si la reconfiguration du réseau ou de l'agent est nécessaire :

- Nombre d'hôtes utilisant un DA particulier. Utilisez ces informations pour déterminer s'il est nécessaire de déployer d'autres DA à des fins d'équilibrage de charge.
- Nombre d'hôtes utilisant un DA particulier. Utilisez ces informations pour déterminer s'il est nécessaire de configurer certains hôtes avec de nouvelles étendues ou des étendues différentes.
- Si l'UA demande un délai d'attente ou si un accusé de réception DA est lent. Vous pouvez déterminer si un DA est surchargé en contrôlant les délais d'attente et les retransmissions de l'UA. Vous pouvez également vérifier si le DA nécessite plus de quelques secondes pour envoyer l'accusé de réception d'enregistrement à un SA. Utilisez ces informations pour rééquilibrer la charge du réseau sur le DA, si nécessaire, en déployant des DA ou en modifiant la configuration de l'étendue.

En utilisant snoop avec l'argument de ligne de commande -V (détaillé), vous pouvez obtenir les durées de vie des enregistrements et la valeur du nouvel indicateur dans SrvReg afin de déterminer si le nombre de réenregistrements doit être réduit.

Vous pouvez également utiliser snoop pour suivre d'autres types de trafic SLP, tels que les suivants :

- Trafic entre les clients UA et les DA
- Trafic entre les clients UA de multidiffusion et les SA répondant

Pour plus d'informations relatives à la commande snoop, reportez-vous à la page de manuel snoop(1M).

Astuce – Utilisez la commande netstat avec snoop pour afficher des statistiques sur le trafic et les congestions. Pour plus d'informations relatives à la commande netstat, reportez-vous à la page de manuel netstat(1M).

▼ Utilisation de snoop pour exécuter des suivis SLP

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Exécutez snoop avec l'argument de ligne de commande slp.

```
Brief Mode:
# snoop slp
```

Lorsque vous exécutez snoop en mode *court* par défaut, la sortie en cours est envoyée sur votre écran. Les messages SLP sont tronqués pour tenir sur une seule ligne par suivi SLP.

```
Verbose Mode:
# snoop -v slp
```

Lorsque vous exécutez snoop en mode *détaillé*, snoop envoie la sortie en cours, non abrégée, sur votre écran ; celle-ci fournit les informations suivantes :

- Adresse complète de l'URL du service
- Ensemble des attributs du service
- Durée de vie de l'enregistrement
- Tous les paramètres et indicateurs de sécurité, le cas échéant

Remarque – Vous pouvez utiliser l'argument de ligne de commande `slp` avec d'autres options `snoop`.

Analyse d'un suivi `snoop slp`

Dans l'exemple suivant, `slpd` s'exécute sur *slphost1* dans le mode par défaut comme un serveur SA. Le démon SLP initialise et enregistre *slphost2* en tant que serveur d'écho. Ensuite, le processus `snoop slp` est appelé sur *slphost1*.

Remarque – Pour simplifier la description des résultats du suivi, les lignes dans la sortie `snoop` suivante sont identifiées par des numéros de ligne.

```
(1) slphost1 -> 239.255.255.253 SLP V@ SrvRqst [24487] service:directory-agent []
(2) slphost2 -> slphost1 SLP V2 DAAdvert [24487] service:directory-agent://129
(3) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(4) slphost1 -> 239.255.255.253 SLP V2 SrvRqst [24487] service:directory-agent []
(5) slphost1 -> slphost2 SLP V2 SrvReg [24488/tcp]service:echo.sun:tcp://slphost1:
(6) slphost2 -> slphost1 SLP V2 SrvAck [24488/tcp] ok
(7) slphost1 -> slphost2 SLP V2 SrvDereg [24489/tcp] service:echo.sun:tcp://slphost1:
(8) slphost2 -> slphost1 SLP V2 SrvAck [24489/tcp] ok
```

1. Indique la commande `slpd` sur *slphost1* exécutant la découverte de l'agent du répertoire actif en envoyant une multidiffusion à l'adresse du groupe de multidiffusion SLP à de la recherche d'agents de répertoire. 24487, le numéro du message pour la découverte active, est indiqué entre crochets dans l'affichage du suivi.
2. Indique que `slpd` a répondu à la requête de découverte active 24487 du suivi 1, la commande étant exécutée en tant que DA sur l'hôte *slphost2*. L'URL du service de *slphost2* a été tronquée pour tenir sur une seule ligne. Le DA a envoyé une annonce DA en réponse aux messages de découverte d'un agent de répertoire de multidiffusion, comme indiqué par les numéros de message correspondants dans les suivis 1 et 2.
3. Indique les multidiffusions issues des UA sur *slphost1* pour d'autres DA. *slphost2* a déjà répondu à la requête, de sorte qu'il évite de répondre une autre fois, et aucun autre DA ne répond.
4. Répète l'opération de multidiffusion indiquée dans la ligne précédente.
5. Indique une commande `slpd` sur un hôte *slphost1* transférant les enregistrements client SA au DA sur l'hôte *slphost2*. Un enregistrement de service monodiffusion (`SrvReg`) pour un serveur d'écho est effectué par *slphost1* pour le DA sur *slphost2*.
6. Indique un hôte *slphost2* répondant à *slphost1* `SrvReg` avec un accusé de réception de service (`SrvAck`) qui indique que l'enregistrement a réussi.

Le trafic entre le serveur d'écho qui exécute le client SA et le démon SLP sur *slphost1* n'apparaît pas dans le suivi `snoop`. Cette absence d'informations s'explique par le fait que l'opération `snoop` est exécutée sur le réseau loopback.

7. Indique le serveur d'écho sur *slphost1* qui annule l'enregistrement de l'annonce de service d'écho. Le démon SLP sur *slphost1* transmet l'annulation de l'enregistrement au DA sur l'hôte *slphost2*.
8. Indique l'hôte *slphost2* répondant à l'hôte *slphost1* avec un accusé de réception de service (`SrvAck`) qui indique que l'annulation de l'enregistrement a réussi.

   Le paramètre `/tcp` ajouté au numéro de message sur les lignes 5, 6, 7 et 8 indique que l'échange de messages a été fait par le protocole TCP.

Étape suivante

Après la surveillance du trafic SLP, vous pouvez utiliser les informations collectées à partir des suivis `snoop` pour déterminer si la reconfiguration des valeurs SLP par défaut est nécessaire. Utilisez les informations connexes proposées au Chapitre 9, “Administration de SLP (tâches)” pour configurer les paramètres des propriétés SLP. Pour plus d'informations sur les enregistrements de service et les messages SLP, reportez-vous au Chapitre 11, “SLP (références)”.

◆ ◆ ◆ CHAPITRE 9

Administration de SLP (tâches)

Les sections suivantes fournissent des informations et présentent les tâches de configuration des agents et processus SLP.

Configuration des propriétés SLP

Les propriétés de configuration SLP contrôlent les interactions réseau, les caractéristiques de l'agent SLP, l'état et la connexion. Dans la plupart des cas, la configuration par défaut de ces propriétés ne nécessite aucune modification. Vous pouvez toutefois utiliser les procédures présentées dans ce chapitre lorsque le support ou la topologie du réseau change, ainsi que pour atteindre les objectifs suivants :

- Compensation de la latence du réseau
- Réduction de la congestion du réseau
- Ajout d'agents ou de réallocation d'adresses IP
- Activation de la journalisation SLP

Vous pouvez modifier le fichier de configuration SLP, `/etc/inet/slp.conf`, afin d'effectuer des opérations telles que celles répertoriées dans le tableau ci-après.

TABLEAU 9–1 Opérations de configuration SLP

Opération	Description
Indiquer si `slpd` doit agir comme un serveur DA. Le serveur SA est la valeur par défaut.	Définissez la propriété `net.slpisda` sur `True`.
Définir la synchronisation des messages de multidiffusion du DA.	Définissez la propriété `net.slp.DAHeartBeat` afin de contrôler la fréquence à laquelle un DA envoie une annonce DA non sollicitée en multidiffusion.
Activer la journalisation DA pour surveiller le trafic réseau.	Définissez la propriété `net.slp.traceDATraffic` sur `True` .

Fichier de configuration SLP : éléments de base

Le fichier `/etc/inet/slp.conf` définit et active toutes les activités SLP à chaque redémarrage du démon SLP. Le fichier de configuration est constitué des éléments suivants :

- Propriétés de configuration
- Lignes de commentaire et notations

Propriétés de configuration

Toutes les activités SLP de base, telles que `net.slp.isDA` et `net.slp.DAHeartBeat`, adoptent la convention de nommage suivante.

```
net.slp.<keyword>
```

Le comportement SLP est défini par la valeur d'une propriété ou d'une combinaison de propriétés dans le fichier `slp.conf`. Les propriétés sont structurées en tant que paires clé/valeur dans le fichier de configuration SLP. Comme indiqué dans l'exemple suivant, une paire clé/valeur se compose d'un nom de propriété et d'un paramètre associé.

```
<property name>=<value>
```

La clé pour chaque propriété est le nom de la propriété. La valeur définit la valeur numérique (distance ou durée), l'état true/false ou les paramètres de valeur de chaîne pour la propriété. Les valeurs de propriété sont constituées de l'un des types de données suivants :

- Paramètre True/False (booléen)
- Nombres entiers
- Liste de nombres entiers
- Chaînes de caractères
- Liste de chaînes

Si la valeur définie n'est pas autorisée, la valeur par défaut pour le nom de cette propriété est utilisée. En outre, un message d'erreur est journalisé à l'aide de la commande syslog.

Lignes de commentaire et notations

Vous pouvez ajouter des commentaires décrivant la nature et la fonction de la ligne dans le fichier `slp.conf`. Les lignes de commentaires sont facultatives dans le fichier, mais peuvent s'avérer utiles pour l'administration.

Remarque – Les paramètres du fichier de configuration ne sont pas sensibles à la casse. Pour plus d'informations, reportez-vous au document suivant : Guttman, Erik, James Kempf et Charles Perkins, « Service Templates and service: scheme », RFC 2609 de l'IETF (Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2609.txt]

▼ Modification de votre configuration SLP

Utilisez cette procédure pour modifier les paramètres d'une propriété dans votre fichier de configuration SLP. Un client ou un logiciel de service sur lequel SLP est activé peut également modifier la configuration SLP via l'API SLP. Cette API est décrite dans le document « An API for Service Location », RFC 2614 de l'IETF (Internet Engineering Task Force). [http://www.ietf.org/rfc/rfc2614.txt]

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Modifiez les paramètres de la propriété dans le fichier `/etc/inet/slp.conf`, comme approprié.**

   Reportez-vous à la section "Propriétés de configuration" à la page 244 pour obtenir des informations générales sur les paramètres de propriétés SLP. Consultez les sections qui suivent cette procédure pour obtenir des exemples des différents cas dans lesquels vous pouvez modifier les propriétés `slp.conf` . Reportez-vous à la page de manuel `slp.conf(4)`.

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Remarque – Le démon SLP obtient des informations à partir du fichier de configuration lorsque vous arrêtez ou démarrez `slpd`.

Exemple 9–1 Configuration de `slpd` afin qu'il fonctionne comme un serveur DA

Vous pouvez modifier la valeur par défaut du serveur SA afin que `slpd` puisse fonctionner comme un serveur DA en définissant la propriété `net.slp.isDA` sur `True` dans le fichier `slpd.conf`.

```
net.slp.isDA=True
```

Dans chaque zone, plusieurs propriétés contrôlent les différents aspects de la configuration. Les sections suivantes décrivent différentes situations dans lesquelles vous pouvez modifier les paramètres de propriétés par défaut utilisés dans la configuration SLP.

Modification des annonces DA et de la fréquence de découverte

Dans les cas suivants, vous pouvez modifier les propriétés qui contrôlent la synchronisation des annonces DA et des requêtes de découverte.

- Si vous souhaitez que le SA ou l'UA obtiennent des informations de configuration DA statiquement à partir de la propriété `net.slp.DAAddresses` du fichier `slp.conf`, vous pouvez désactiver la découverte du DA.
- Lorsque le réseau est sujet à un partitionnement récurrent, vous pouvez modifier la fréquence des annonces passives et de la découverte active.
- Si les clients UA et SA accèdent aux DA à l'autre bout d'une connexion commutée, vous pouvez réduire la fréquence du signal d'activité DA et l'intervalle de découverte active afin de diminuer le nombre d'activations de la ligne commutée.
- Si la congestion du réseau est élevée, vous pouvez limiter la multidiffusion.

Les procédures décrites dans cette section expliquent comment modifier les propriétés suivantes.

TABLEAU 9–2 Propriétés de synchronisation d'annonces DA et de requêtes de découverte

Propriétés	Description
`net.slp.passiveDADetection`	Booléen spécifiant si `slpd` est à l'écoute des annonces DA non sollicitées
`net.slp.DAActiveDiscoveryInterval`	Valeur qui spécifie la fréquence à laquelle `slpd` effectue la découverte DA active pour un nouveau DA

TABLEAU 9–2 Propriétés de synchronisation d'annonces DA et de requêtes de découverte *(Suite)*

Propriétés	Description
`net.slp.DAHeartBeat`	Valeur qui spécifie la fréquence à laquelle un DA envoie une annonce DA non sollicitée en multidiffusion

Limitation des UA et SA à des DA configurés de manière statique

Il est parfois nécessaire de limiter les UA et SA afin d'obtenir des adresses DA à partir des informations de configuration statiques dans le fichier `slp.conf`. Dans la procédure suivante, vous pouvez modifier deux propriétés qui permettent à `slpd` d'obtenir des informations DA exclusivement à partir de la propriété `net.slp.DAAddresses`.

▼ Limitation des UA et SA pour obtenir des DA configurés de manière statique

Utilisez la procédure suivante pour modifier les propriétés `net.slp.passivedadetection` et `net.slp.a`.

Remarque – Utilisez cette procédure uniquement sur les hôtes qui exécutent des UA et SA limités aux configurations statiques.

---

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Définissez la propriété `net.slp.passiveDADetection` sur `False` dans le fichier `slp.conf` pour désactiver la découverte passive. `slpd` ignorera alors les annonces DA non sollicitées.**

   ```
   net.slp.passiveDADetection=False
   ```

5. **Définissez la propriété `net.slp.DAActiveDiscoveryInterval` sur `-1` afin de désactiver la découverte active initiale et périodique.**

   ```
   net.slp.DAActiveDiscoveryInterval=-1
   ```

6 **Enregistrez les modifications et fermez le fichier.**

7 **Redémarrez `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Configuration de la découverte DA pour les réseaux commutés

Si les UA ou les SA sont séparés du DA (agent de répertoire) par un réseau commuté, vous pouvez configurer la découverte DA afin de réduire ou d'éliminer le nombre de requêtes de découverte et d'annonces DA. Les réseaux commutés sont généralement facturés lors de leur activation. La réduction des appels superflus peut réduire le coût d'utilisation du réseau commuté.

Remarque – Vous pouvez complètement désactiver la découverte DA en appliquant la méthode décrite à la section "Limitation des UA et SA à des DA configurés de manière statique" à la page 247.

▼ Configuration de la découverte DA pour les réseaux commutés

Vous pouvez utiliser la procédure suivante pour réduire les annonces DA non sollicitées et la découverte active en augmentant la période des signaux d'activité DA et l'intervalle de découverte active.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

```
# svcadm disable network/slp
```

3 **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4 **Augmentez la valeur de la propriété `net.slp.DAHeartbeat` dans le fichier `slpd.conf`.**

`net.slp.DAHeartbeat=`*value*

valeur Nombre entier de 32 bits qui définit le nombre de secondes d'un signal d'activité d'annonce DA passive

Valeur par défaut=10 800 secondes (3 heures)

Plage de valeurs=2 000 à 259 200 000 secondes

Par exemple, vous pouvez définir le signal d'activité DA sur environ 18 heures sur un hôte exécutant un DA :

```
net.slp.DAHeartbeat=65535
```

5 **Augmentez la valeur de la propriété `net.slp.DAActiveDiscoveryInterval` dans le fichier `slpd.conf` :**

`net.slp.DAActiveDiscoveryInterval` *value*

valeur Nombre entier de 32 bits qui définit le nombre de secondes des requêtes de découverte DA active

Valeur par défaut=900 secondes (15 minutes)

Plage de valeurs=300 à 10 800 secondes

Par exemple, vous pouvez définir l'intervalle de découverte DA active sur 18 heures sur un hôte qui exécute un UA et un SA :

```
net.slp.DAActiveDiscoveryInterval=65535
```

6 **Enregistrez les modifications et fermez le fichier.**

7 **Redémarrez `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Configuration du signal d'activité DA pour les partitions fréquentes

Les SA doivent s'enregistrer avec tous les DA qui prennent en charge leurs étendues. Un DA peut apparaître après que `slpd` a effectué une découverte active. Si le DA prend en charge les étendues `slpd`, le démon SLP enregistre toutes les annonces sur son hôte avec le DA.

L'une des méthodes de découverte des DA par `slpd` se produit lors de l'annonce non sollicitée initiale qu'un DA envoie lorsqu'il démarre. Le démon SLP utilise l'annonce périodique non sollicitée (signal d'activité) pour déterminer si un DA est toujours actif. Si le signal d'activité ne s'affiche pas, le démon supprime les DA qu'il utilise et ceux qu'il offre aux UA.

Enfin, lorsqu'un DA subit un arrêt contrôlé, il transmet une annonce DA spéciale qui informe les services SA d'écoute qu'il va être mis hors service. Le démon SLP utilise également cette annonce pour supprimer les DA inactifs du cache.

Si votre réseau est soumis à de fréquentes partitions et les SA durent longtemps, `slpd` peut supprimer les DA mis en cache pendant le partitionnement si aucune annonce de signal d'activité n'est reçue. En diminuant la durée du signal d'activité, vous pouvez réduire le délai de restauration d'un DA désactivé dans le cache une fois la partition réparée.

▼ Configuration du signal d'activité DA pour les partitions fréquentes

Utilisez la procédure suivante pour modifier la propriété `net.slp.DAHeartBeat` afin de réduire la période du signal d'activité DA.

Remarque – Si la découverte DA est complètement désactivée, la propriété `net.slp.DAAddresses` dans le fichier `slp.conf` doit être définie sur les hôtes exécutent les UA et les SA afin qu'ils accèdent au DA correct.

---

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Réduisez la valeur `net.slp.DAHeartBeat` à 1 heure (3 600 secondes). Par défaut, la période du signal d'activité DA est définie sur 3 heures (10 800 secondes).**

   ```
   net.slp.DAHeartBeat=3600
   ```

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Élimination d'une congestion du réseau

Si la congestion est importante, vous pouvez limiter l'activité de multidiffusion. Si les DA n'ont pas déjà été déployés sur le réseau, leur déploiement peut considérablement réduire la quantité de multidiffusion liée au SLP.

Cependant, même après le déploiement des DA, la multidiffusion est toujours nécessaire pour la découverte DA. Vous pouvez réduire la quantité de multidiffusion nécessaire pour la découverte DA à l'aide de la méthode décrite à la section "Configuration de la découverte DA pour les réseaux commutés" à la page 248. Vous pouvez complètement éliminer la multidiffusion pour la découverte DA à l'aide de la méthode décrite à la section "Limitation des UA et SA à des DA configurés de manière statique" à la page 247.

Adaptation d'autres supports réseau, topologies ou configurations

Cette section décrit des scénarios possibles dans lesquels vous pouvez modifier les propriétés suivantes afin de régler les performances SLP.

TABLEAU 9–3 Propriétés des performances SLP

Propriétés	Description
`net.slp.DAAttributes`	Intervalle d'actualisation minimal qu'un DA accepte pour les annonces.
`net.slp.multicastTTL`	Valeur de *durée de vie* spécifiée pour les paquets de multidiffusion.
`net.slp.MTU`	Taille en octets définie pour les paquets réseau. Elle inclut l'adresse IP et les en-têtes TCP ou UDP.
`net.slp.isBroadcastOnly`	Booléen défini pour indiquer si la diffusion doit être utilisée pour la découverte de services DA et non DA.

Réduction des réenregistrements SA

Les SA doivent régulièrement actualiser leurs annonces de service avant qu'elles n'arrivent à expiration. Si un DA gère une très lourde charge provenant de plusieurs UA et SA, des actualisations fréquentes peuvent entraîner la surcharge du DA. Si le DA est surchargé, les requêtes de l'UA commencent à expirer et sont abandonnées. L'expiration des requêtes de l'UA peut avoir plusieurs explications. Avant de supposer que le problème vient de la surcharge du DA, utilisez un suivi `snoop` pour vérifier la durée de vie des annonces de service enregistrées avec un enregistrement de service. Si la durée de vie est courte et si des réenregistrements se produisent souvent, les délais d'expiration sont probablement le résultat de ces réenregistrements fréquents.

Remarque – Un enregistrement de service est un *réenregistrement* si l'indicateur FRESH n'est pas défini. Pour plus d'informations sur les messages d'enregistrement de service, reportez-vous au Chapitre 11, “SLP (références)”.

▼ Réduction des réenregistrements SA

Utilisez la procédure suivante pour augmenter l'intervalle d'actualisation minimal des SA afin de limiter les réenregistrements.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Augmentez la valeur de l'attribut `min-refresh-interval` de la propriété `net.slp.DAAttributes`.**

   La valeur minimale par défaut de la période de réenregistrement est égale à zéro. La valeur zéro par défaut permet aux SA de se réenregistrer à n'importe quel moment. Dans l'exemple suivant, l'intervalle est augmenté à 3 600 secondes (1 heure).

   ```
   net.slp.DAAttributes(min-refresh-interval=3600)
   ```

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Configuration de la propriété de durée de vie de la multidiffusion

La propriété de durée de vie de la multidiffusion (`net.slp.multicastTTL`) détermine la plage sur laquelle un paquet de multidiffusion est propagé sur votre Intranet. La durée de vie de la multidiffusion est configurée en définissant la propriété `net.slp.multicastTTL` sur un nombre entier compris entre 1 et 255. La valeur par défaut du champ TTL de multidiffusion est de 255, de sorte que, en théorie, le routage de paquets n'est pas restreint. Toutefois, une durée de

vie de 255 entraîne la pénétration d'un paquet de multidiffusion sur le réseau Intranet au niveau des routeurs de bordure à la limite de votre domaine d'administration. Une configuration appropriée de la multidiffusion sur les routeurs de bordure est nécessaire pour empêcher la fuite des paquets de multidiffusion dans la dorsale multidiffusion d'Internet ou vers votre fournisseur d'accès Internet.

L'étendue de la durée de vie de multidiffusion est similaire à une durée de vie IP standard, à la différence près qu'une comparaison de durée de vie est effectuée. Une valeur de durée de vie est attribuée à chaque interface d'un routeur sur lequel la multidiffusion est activée. Lorsqu'un paquet de multidiffusion arrive, le routeur compare la valeur de durée de vie du paquet avec celle de l'interface. Si la durée de vie du paquet est supérieure ou égale à celle de l'interface, la durée de vie du paquet est réduite d'un, de même que la durée de vie IP standard. Si la durée de vie est ramenée à zéro, le paquet est rejeté. Lorsque vous utilisez l'étendue de durée de vie pour la multidiffusion SLP, les routeurs doivent être correctement configurés pour limiter les paquets à une sous-section particulière de votre Intranet.

▼ Configuration de la propriété de durée de vie de la multidiffusion

Utilisez la procédure suivante pour réinitialiser la propriété `net.slp.multicastTTL`.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `slpd` et toutes les activités SLP sur l'hôte.

```
# svcadm disable network/slp
```

3 Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.

4 Modifiez la propriété `net.slp.multicastTTL` dans le fichier `slpd.conf` :

`net.slp.multicastTTL=`*value*

valeur Nombre entier positif inférieur ou égal à 255 qui définit la durée de vie de la multidiffusion

Remarque – Vous pouvez réduire la gamme de propagation de la multidiffusion en réduisant la valeur de durée de vie. Si cette valeur est de 1, le paquet est limité au sous-réseau. Si elle est de 32, le paquet est limité au site. Malheureusement, le terme *site* n'est pas défini par le RFC 1075, qui aborde les durées de vie de multidiffusion. Les valeurs supérieures à 32 renvoient au routage théorique sur Internet et ne doivent pas être utilisées. Les valeurs inférieures à 32 peuvent être utilisées pour limiter la multidiffusion à un ensemble de sous-réseaux accessibles, si les durées de vie sur les routeurs sont correctement configurées.

5 **Enregistrez les modifications et fermez le fichier.**

6 **Redémarrez `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Configuration de la taille des paquets

La taille de paquet par défaut pour SLP est de 1 400 octets. Cette taille doit être suffisante pour la plupart les réseaux locaux. Pour les réseaux sans fil ou les réseaux WAN, vous pouvez réduire la taille de paquet afin d'éviter la fragmentation des messages et de réduire le trafic réseau. Pour les réseaux locaux qui ont des paquets plus grands, l'augmentation de la taille des paquets peut améliorer les performances. Vous pouvez déterminer si la taille de paquet doit être réduite en vérifiant la taille minimale des paquets pour votre réseau. Si le support réseau a une taille de paquet plus petite, vous pouvez réduire la valeur `net.slp.MTU` en conséquence.

Vous pouvez augmenter la taille de paquet si votre support réseau a des paquets plus grands. Toutefois, à moins que les annonces de service des SA ou les requêtes des UA dépassent fréquemment la taille de paquet par défaut, il n'est pas nécessaire de modifier la valeur `net.slp.MTU` . Vous pouvez utiliser la commande `snoop` pour déterminer si les requêtes des UA dépassent souvent la taille de paquet par défaut et effectuer une reconduction afin d'utiliser le protocole TCP plutôt que le protocole UDP.

La propriété `net.slp.MTU` mesure la taille de paquet IP complète, y compris l'en-tête de la couche de liaison, l'en-tête IP, l'en-tête du protocole UDP ou TCP et le message SLP.

▼ Configuration de la taille de paquet

Utilisez la procédure suivante pour modifier la taille de paquet par défaut en ajustant la propriété `net.slp.MTU`.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Modifiez la propriété `net.slp.MTU` dans le fichier `slpd.conf` :**

   `net.slp.MTU=`*value*

   valeur Nombre entier de 16 bits qui spécifie la taille du paquet réseau, en octets

   Valeur par défaut=1 400

   Plage de valeurs=128 à 8 192

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Configuration du routage de diffusion

Le protocole SLP est conçu pour utiliser la multidiffusion pour la découverte de services en l'absence de DA et pour la découverte DA. Si votre réseau ne déploie pas de routage multidiffusion, vous pouvez configurer SLP afin d'utiliser la diffusion, en définissant la valeur `net.slp.isBroadcastOnly` sur `True`.

Contrairement à la multidiffusion, les paquets de diffusion ne se propagent pas par défaut sur les sous-réseaux. Pour cette raison, la découverte de services sans DA sur un réseau qui ne prend pas en charge la multidiffusion fonctionne uniquement sur un seul sous-réseau. En outre, des éléments particuliers doivent être pris en compte lors du déploiement de DA et d'étendues sur des réseaux sur lesquels la diffusion est utilisée. Un DA sur un hôte multiréseau peut rapprocher la découverte de services entre plusieurs sous-réseaux sur lesquels la multidiffusion est désactivée. Reportez-vous à la section "Placement du DA et affectation de nom à l'étendue" à la page 271 pour plus d'informations sur le déploiement des DA sur des hôtes multiréseau.

▼ Configuration du routage de diffusion

Utilisez la procédure suivante pour définir la propriété `net.slp.isbroadcastonly` sur `True`.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Modifiez la propriété `net.slp.isBroadcastOnly` dans le fichier `slpd.conf` sur `True` :**

   ```
   net.slp.isBroadcastOnly=True
   ```

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Modification des délais d'attente pour les requêtes de découverte SLP

Deux situations peuvent exiger que vous modifiiez les délais d'attente pour les requêtes de découverte SLP :

- Si les agents SLP sont séparés par plusieurs sous-réseaux, lignes commutées ou autres réseaux WAN, la latence du réseau peut être si élevée que la valeur des délais d'attente par défaut n'est pas suffisante pour exécuter une requête ou un enregistrement. À l'inverse, si la latence de votre réseau est faible, vous pouvez améliorer les performances en réduisant les délais d'expiration.
- Si le réseau est soumis à un trafic important ou un taux de collision élevé, le délai maximal que les SA et les UA doivent attendre avant d'envoyer un message peut être insuffisant pour garantir des transactions sans collision.

Modification des délais d'attente par défaut

Une latence élevée du réseau peut entraîner l'expiration des UA et des SA avant qu'une réponse aux requêtes et enregistrements ne soit renvoyée. La latence peut être un problème si un UA est séparé d'un SA, ou si un UA et un SA sont séparés d'un DA, que ce soit par plusieurs sous-réseaux, une ligne d'appel ou un WAN. Vous pouvez déterminer si la latence est un problème en vérifiant si les requêtes SLP échouent en raison des délais d'attente des requêtes et enregistrements des UA et SA. Vous pouvez également utiliser la commande `ping` pour mesurer la latence réelle.

Le tableau suivant répertorie les propriétés de configuration qui contrôlent les délais d'attente. Vous pouvez utiliser les procédures décrites dans cette section pour modifier ces propriétés.

TABLEAU 9–4 Propriétés des délais d'attente

Propriétés	Description

`net.slp.multicastTimeouts`
`net.slp.DADiscoveryTimeouts`
`net.slp.datagramTimeouts`
	Propriétés qui contrôlent les délais d'attente de transmissions répétées de messages UDP de multidiffusion et monodiffusion avant la l'abandon de la transmission.

`net.slp.multicastMaximumWait`	Propriété qui contrôle la durée maximale pendant laquelle un message de multidiffusion est transmis avant d'être abandonné.
`net.slp.datagramTimeouts`	Limite supérieure d'un délai d'attente DA spécifiée par la somme des valeurs indiquées pour cette propriété. Un datagramme UDP est envoyé à plusieurs reprises à un DA jusqu'à ce qu'une réponse soit reçue ou la limite de délai d'expiration atteinte.

Si des délais d'attente se produisent fréquemment lors de la découverte de service de multidiffusion ou la découverte DA, augmentez la valeur de la propriété `net.slp.multicastMaximumWait` de la valeur par défaut à 15 000 millisecondes (15 secondes). L'augmentation du délai d'attente maximal donne davantage de temps aux requêtes pour s'exécuter sur des réseaux présentant une latence élevée. Une fois la propriété `net.slp.multicastMaximumWait` modifiée, vous devez également modifier les propriétés `net.slp.multicastTimeouts` et `net.slp.DADiscoveryTimeouts` . La somme des valeurs de délai d'attente pour ces propriétés est égale à la valeur `net.slp.multicastMaximumWait`.

▼ Modification des délais d'attente par défaut

Utilisez la procédure suivante pour modifier les propriétés SLP qui contrôlent les délais d'attente.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Modifiez la propriété `net.slp.multicastMaximumWait` dans le fichier `slpd.conf` :**

   `net.slp.multicastMaximumWait=`*value*

   valeur Nombre entier de 32 bits qui répertorie la somme des valeurs définies pour les propriétés `net.slp.multicastTimeouts` et `net.slp.DADiscoveryTimeouts`

   Valeur par défaut=15 000 millisecondes (15 secondes)

   Plage de valeurs=1 000 à 60 000 millisecondes

   Par exemple, si vous déterminez que les requêtes de multidiffusion nécessitent 20 secondes (20 000 millisecondes), vous pouvez ajuster les valeurs répertoriées pour les propriétés `net.slp.multicastTimeouts` et `net.slp.DADiscoveryTimeouts` afin qu'elles soient égales à 20 000 millisecondes.

   ```
   net.slp.multicastMaximumWait=20000
   net.slp.multicastTimeouts=2000,5000,6000,7000
   net.slp.DADiscoveryTimeouts=3000,3000,6000,8000
   ```

5. **Si nécessaire, modifiez la propriété `net.slp.datagramTimeouts` dans le fichier `slpd.conf` :**

   `net.slp.datagramTimeouts=`*value*

   valeur Liste de nombres entiers de 32 bits qui spécifient les délais d'attente, en millisecondes, pour la mise en œuvre de la transmission de datagrammes de monodiffusion aux DA

   Par défaut=3 000, 3 000, 3 000

   Par exemple, vous pouvez augmenter le délai d'attente des datagrammes à 20 000 millisecondes afin d'éviter des délais d'attente fréquents.

   ```
   net.slp.datagramTimeouts=2000,5000,6000,7000
   ```

   Sur des réseaux hautes performances, vous pouvez réduire la limite de délai d'attente pour la transmission de datagrammes UDP de multidiffusion et monodiffusion. Lorsque vous réduisez cette limite, vous réduisez la latence requise pour répondre aux requêtes SLP.

6 **Enregistrez les modifications et fermez le fichier.**

7 **Redémarrez `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Configuration d'une limite d'attente aléatoire

Dans des réseaux soumis à un trafic important ou un taux de collision élevé, la communication avec un DA peut être affectée. Si le taux de collision est élevé, l'agent à l'origine de l'envoi doit retransmettre le datagramme UDP. Vous pouvez déterminer si la retransmission se produit en utilisant la commande `snoop` pour surveiller le trafic sur un réseau d'hôtes qui exécutent `slpd` comme un serveur SA et un hôte qui exécute `slpd` comme un DA. Si plusieurs messages d'enregistrement de service pour le même service s'affichent dans le suivi `snoop` à partir de l'hôte qui exécute `slpd` comme un serveur SA, des collisions de notices peuvent survenir.

Les collisions peuvent s'avérer particulièrement problématiques pendant l'initialisation. Lors du premier démarrage d'un DA, il envoie des annonces non sollicitées et les SA répondent avec des enregistrements. Le protocole SLP demande aux SA d'attendre pendant une durée aléatoire après la réception d'une annonce DA avant de répondre. La limite d'attente aléatoire est uniformément distribuée avec une valeur maximale contrôlée par la propriété `net.slp.randomWaitBound`. La valeur de la limite d'attente aléatoire par défaut est de 1 000 millisecondes (1 seconde).

▼ Configuration de la limite d'attente aléatoire

Utilisez la procédure suivante pour modifier la propriété `net.slp.RandomWaitBound` dans le fichier `slp.conf`.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

```
# svcadm disable network/slp
```

3 **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4 **Modifiez la propriété `net.slp.RandomWaitBound` dans le fichier `slpd.conf` :**

```
net.slp.RandomWaitBound=value
```

valeur Limite supérieure pour le calcul du temps d'attente aléatoire avant d'essayer de contacter un DA

Valeur par défaut=1 000 millisecondes (1 seconde)

Plage de valeurs=1 000 à 3 000 millisecondes

Par exemple, vous pouvez augmenter le temps d'attente maximal à 2 000 millisecondes (2 secondes).

```
net.slp.randomWaitBound=2000
```

Lorsque vous augmentez le temps d'attente aléatoire, un délai d'enregistrement plus long se produit. Les SA peuvent terminer les enregistrements avec les nouveaux DA détectés plus lentement afin d'éviter les collisions et les délais d'expiration.

5 Si nécessaire, modifiez la propriété `net.slp.datagramTimeouts` dans le fichier `slpd.conf` :

```
net.slp.datgramTimeouts=value
```

valeur Liste de nombres entiers de 32 bits qui spécifient les délais d'attente, en millisecondes, pour la mise en œuvre de la transmission de datagrammes de monodiffusion aux DA

Par défaut=3 000, 3 000, 3 000

Par exemple, vous pouvez augmenter le délai d'attente des datagrammes à 20 000 millisecondes afin d'éviter des délais d'attente fréquents.

```
net.slp.datagramTimeouts=2000,5000,6000,7000
```

Sur des réseaux hautes performances, vous pouvez réduire la limite de délai d'attente pour la transmission de datagrammes UDP de multidiffusion et monodiffusion. Ce paramètre permet de réduire la latence pour les requêtes SLP.

6 Enregistrez les modifications et fermez le fichier.

7 Redémarrez `slpd` pour activer vos modifications.

```
# svcadm enable network/slp
```

Étendues de déploiement

Les étendues permettent de fournir des services qui dépendent de groupements d'utilisateurs logiques, physiques et d'administration. Vous pouvez utiliser les étendues pour gérer l'accès aux annonces de service.

Utilisez la propriété `net.slp.useScopes` pour créer des étendues. Par exemple, dans le fichier `/etc/inet/slp.conf` sur un hôte, ajoutez une étendue appelée `newscope`, comme indiqué ci-dessous :

```
net.slp.useScopes=newscope
```

Par exemple, il est possible que votre organisation possède une salle de périphériques réseau (imprimantes, télécopieurs, etc.) située au bout du hall sud au deuxième étage du bâtiment 6. Ces périphériques peuvent être utilisés par toutes les personnes travaillant au deuxième étage, ou vous pouvez limiter leur utilisation aux membres d'un service particulier. Les étendues vous permettent de définir l'accès aux annonces de service pour ces machines.

Si les périphériques sont dédiés à un seul service, vous pouvez créer une étendue portant le nom dudit service, par exemple `mktg`. Les périphériques qui appartiennent à d'autres services peuvent être configurés avec d'autres noms d'étendues.

Dans un autre cas de figure, les services peuvent être éparpillés. Par exemple, les services d'ingénierie mécanique et CAO/FAO peuvent être répartis sur le premier et le deuxième étages. Vous pouvez toutefois allouer les machines du deuxième étage aux hôtes des deux étages en les affectant à la même étendue. Vous pouvez déployer des étendues de la manière la plus appropriée à votre réseau et vos utilisateurs.

Remarque – Les UA possédant une étendue particulière ne sont pas empêchés d'utiliser les services annoncés dans d'autres étendues. La configuration des étendues permet uniquement de contrôler les annonces de service détectées par un UA. Le service est responsable de l'application des restrictions de contrôle d'accès.

Moment adapté à la configuration des étendues

Le SLP peut fonctionner correctement sans étendues configurées. Dans l'environnement d'exploitation Solaris, l'étendue par défaut pour SLP est `default`. Si aucune étendue n'est configurée, `default` est l'étendue pour tous les messages SLP.

Vous pouvez configurer les étendues dans l'un des cas suivants.

- Les organisations que vous prenez en charge souhaitent restreindre l'accès aux annonces de service à leurs propres membres.
- La structure physique de l'organisation suggère que les services dans une zone donnée sont accessibles à des utilisateurs particuliers.
- Les annonces de service que des utilisateurs spécifiques peuvent voir doivent être partitionnées.

Un exemple du premier cas a été cité à la section "Configuration de la découverte DA pour les réseaux commutés" à la page 248. Le second cas correspond à une situation dans laquelle une organisation occupe deux bâtiments, et où vous souhaitez que les utilisateurs d'un bâtiment puissent accéder aux services locaux dans ce bâtiment. Vous pouvez configurer les utilisateurs du bâtiment 1 avec l'étendue `B1` et les utilisateurs du bâtiment 2 avec l'étendue `B2`.

Éléments à prendre en compte lors de la configuration d'étendues

Lorsque vous modifiez la propriété `net.slp.useScopes` du fichier `slpd.conf`, vous configurez les étendues pour tous les agents sur l'hôte. Si l'hôte exécute un SA ou agit comme un DA, vous devez configurer cette propriété si vous souhaitez configurer les SA ou le DA dans des étendues autres que l'étendue `default`. Si seuls des UA sont en cours d'exécution sur la machine et s'ils doivent détecter les SA et les DA prenant en charge les étendues autres que l'étendue `default`, il n'est pas nécessaire de configurer la propriété sauf si vous souhaitez restreindre les étendues utilisées par les UA. Si la propriété n'est pas configuré, les UA peuvent automatiquement découvrir les DA et étendues disponibles via `slpd`. Le démon SLP utilise la découverte DA active et passive pour trouver les DA, ou bien la découverte SA si aucun DA n'est en cours d'exécution. Sinon, si la propriété est configurée, les UA utilisent uniquement les étendues configurées et ne les ignorent pas.

Si vous décidez de configurer des étendues, vous devez prendre envisager de conserver l'étendue `default` dans la liste des étendues configurées, à moins que vous ne soyez certain que tous les SA du réseau disposent d'une étendue configurée. Si des SA restent non configurés, les UA disposant d'étendues configurées ne seront pas en mesure de les détecter. Cette situation se produit car l'étendue `default` est automatiquement appliquée aux SA non configurés, mais les UA disposent d'étendues configurées.

Si vous décidez de configurer également les DA en définissant la propriété `net.slp.DAAddresses`, assurez-vous que les étendues prises en charge par les DA configurés sont les mêmes que les étendues configurées avec la propriété `net.slp.usescopes`. Si les étendues sont différentes, `slpd` imprime un message d'erreur lors de son redémarrage.

▼ Configuration des étendues

Utilisez la procédure suivante pour ajouter des noms d'étendues à la propriété `net.slp.useScopes` du fichier `slp.conf`.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Modifiez la propriété `net.slp.useScopes` dans le fichier `slpd.conf` :**

   `net.slp.useScopes=`*<scope names>*

   scope names Liste de chaînes indiquant les étendues qu'un DA ou SA est autorisé à utiliser lors de l'envoi de requêtes, ou les étendues qu'un DA doit prendre en charge

   Valeur par défaut=Default pour SA et DA/Unassigned pour UA

   Remarque –

   Utilisez les éléments suivants pour créer les noms d'étendues :

   - Caractères alphanumériques, en majuscules ou minuscules
   - Signes de ponctuation (à l'exception de : ", \, *!*, <, =, > et ~)
   - Espaces considérées comme faisant partie du nom
   - Caractères non ASCII

     Utilisez une barre oblique inverse pour neutraliser les caractères non-ASCII. Par exemple, le codage UTF-8 utilise le code hexadécimal `0xc3a9` pour représenter la lettre *e* avec l'accent *aigu* français. Si la plate-forme ne prend pas en charge le format UTF-8, vous pouvez utiliser le code hexadécimal UTF-8 comme séquence d'échappement `\c3\a9`.

   Par exemple, pour spécifier les étendues pour les groupes `eng` et `mktg` dans `bldg6`, modifiez la ligne `net.slp.useScopes` comme suit.

   ```
   net.slp.useScopes=eng,mktg,bldg6
   ```

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Déploiement de DA

Cette section décrit le déploiement stratégique de DA sur un réseau qui exécute SLP.

SLP fonctionne correctement avec uniquement les agents de base (UA et SA), sans DA déployé ni étendue configurée. Tous les agents qui ne disposent pas de configuration spécifique utilisent l'étendue `default`. Les DA servent de caches pour les annonces de service. Le déploiement des DA diminue le nombre de messages envoyés sur le réseau et réduit le temps nécessaire à la réception de réponses aux messages. Cette fonctionnalité permet l'adaptation de SLP à des réseaux de plus grande taille.

Pourquoi déployer un DA SLP ?

La principale raison pour déployer des DA est de réduire la quantité de trafic de multidiffusion et les délais associés à la collecte de réponses monodiffusion. Dans un réseau de grande taille comprenant de nombreux UA et SA, la quantité de trafic de multidiffusion impliquée dans la découverte de services peut devenir importante au point de dégrader les performances de ce réseau. Grâce au déploiement d'un ou plusieurs DA, les UA doivent effectuer une monodiffusion vers les DA associés au service et les SA doivent s'enregistrer avec les DA en utilisant la monodiffusion. La seule multidiffusion enregistrée auprès de SLP sur un réseau comprenant des DA est destinée à la découverte DA active et passive.

Les SA s'enregistrent automatiquement avec les DA qu'ils découvrent au sein d'un ensemble d'étendues commun, plutôt que d'accepter les requêtes de service multidiffusion. Les requêtes de multidiffusion dans les étendues qui ne sont pas prises en charge par le DA sont cependant toujours directement traitées par le SA.

Les requêtes de service émises par les UA sont envoyées en monodiffusion aux DA plutôt qu'en multidiffusion sur le réseau lorsqu'un DA est déployé dans les étendues de l'UA. Par conséquent, les DA au sein des étendues de l'UA réduisent la multidiffusion. En éliminant la multidiffusion pour les requêtes UA normales, le temps requis pour obtenir des réponses aux requêtes est considérablement réduit (de quelques secondes à quelques millisecondes).

Les DA agissent comme un point central pour l'activité des SA et UA. Le déploiement d'un ou plusieurs DA pour un ensemble d'étendues fournit un point centralisé pour la surveillance de l'activité SLP. En activant la journalisation DA, il est plus facile de surveiller les enregistrements et les requêtes qu'en consultant les journaux de plusieurs SA éparpillés sur le réseau. Vous pouvez déployer autant de DA que vous le souhaitez pour une étendue ou des étendues particulières, selon l'équilibre de charge nécessaire.

Dans les réseaux sur lesquels le routage multidiffusion n'est pas activé, vous pouvez configurer SLP pour utiliser la diffusion. Cependant, la diffusion est très peu efficace, car elle exige que chaque hôte traite le message. De plus, la diffusion ne se propage généralement pas sur les

routeurs. Par conséquent, dans le cas d'un réseau ne prenant pas en charge le routage multidiffusion, les services peuvent être découverts uniquement sur le même sous-réseau. Une prise en charge partielle du routage multidiffusion entraîne des incohérences dans la découverte des services sur un réseau. Les messages de multidiffusion sont utilisés pour découvrir les DA. Par conséquent, la prise en charge partielle du routage multidiffusion implique que les UA et les SA enregistrent les services avec tous les DA connus dans l'étendue du SA. Par exemple, si un UA envoie une requête à un DA appelé `DA1` et si le SA possède des services enregistrés avec `DA2`, l'UA échouera à découvrir un service. Pour plus d'informations sur le déploiement de SLP sur des réseaux sur lesquels la multidiffusion n'est pas activée. reportez-vous à la section "Configuration du routage de diffusion" à la page 255.

Sur un réseau présentant une prise en charge incohérente du routage multidiffusion à l'échelle du site, vous devez configurer les UA et SA SLP avec une liste d'emplacements DA cohérente à l'aide de la propriété `net.slp.DAAdresseses`.

Enfin, le DA SLPv2 prend en charge l'interopérabilité avec SLPv1. L'interopérabilité SLPv1 est activée par défaut dans le DA. Si votre réseau contient des périphériques SLPv1, tels que des imprimantes, ou si vous avez besoin d'interagir avec Novell Netware 5, qui utilise SLPv1 pour la découverte de services, vous devez déployer un DA. Sans DA, les UA SLP Solaris ne sont pas en mesure de trouver les services SLPv1 annoncés.

Moment adapté au déploiement des DA

Déployez des DA pour votre entreprise si l'une des conditions suivantes s'applique :

- Le trafic SLP de multidiffusion dépasse 1 % de la bande passante sur votre réseau, selon la mesure de la commande `snoop`.
- Les clients UA rencontrent de longs délais ou des délais d'expiration lors des requêtes de service de multidiffusion.
- Vous souhaitez centraliser le contrôle des annonces de service SLP pour certaines étendues sur un ou plusieurs hôtes.
- La multidiffusion n'est pas activée sur votre réseau, et celui-ci se compose de plusieurs sous-réseaux qui doivent partager des services.
- Votre réseau utilise les périphériques prenant en charge des versions antérieures de SLP (SLPv1) ou vous souhaitez que la découverte de services SLP interagisse avec Novell Netware 5.

▼ Déploiement des DA

Utilisez la procédure suivante pour définir la propriété `net.slp.isda` sur `True` dans le fichier `slp.conf`.

Remarque – Vous pouvez uniquement attribuer un DA par hôte.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

   ```
   # svcadm disable network/slp
   ```

3. **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

4. **Définissez la propriété `net.slp.isda` sur `True` dans le fichier `slpd.conf` :**

   ```
   net.slp.isDA=True
   ```

5. **Enregistrez les modifications et fermez le fichier.**

6. **Redémarrez `slpd` pour activer vos modifications.**

   ```
   # svcadm enable network/slp
   ```

Placement des DA

Cette section suggère des emplacements pour les DA dans différentes situations.

- Le routage multidiffusion n'est pas activé et les DA doivent lier la découverte de services entre les sous-réseaux

  Dans ce cas, un DA doit être placé sur un hôte avec les interfaces et tous les sous-réseaux qui partagent des services. La propriété de configuration `net.slp.interfaces` ne nécessite *pas* d'être définie, sauf si les paquets IP ne sont pas routés entre les interfaces. Pour plus d'informations sur la configuration de la propriété `net.slp.interfaces`, reportez-vous à la section "Configuration multiréseau pour SLP" à la page 268 .

- Les DA sont déployés à des fins d'évolutivité et la principal élément à prendre en compte est l'optimisation de l'accès de l'agent

  Les UA envoient généralement plusieurs requêtes de services aux DA. Un SA s'enregistre une fois auprès du DA, et peut actualiser l'annonce à intervalles réguliers mais peu fréquents. Par conséquent, l'accès de l'UA aux DA est beaucoup plus fréquent que l'accès du SA. Le nombre d'annonces de service est également généralement plus petit que le nombre de requêtes. Par conséquent, la plupart des déploiements DA sont plus efficaces si le déploiement est optimisé pour l'accès UA.

- Placement des DA afin qu'ils soient topologiquement proches des UA sur le réseau afin d'optimiser l'accès UA

  Naturellement, vous devez configurer le DA avec une étendue partagée par les clients UA et SA.

Placement de plusieurs DA à des fins d'équilibrage de charge

Vous pouvez déployer plusieurs DAs pour le même ensemble d'étendues à des fins d'équilibrage de charge. Déployez des DA dans les cas suivants :

- Les requêtes UA envoyées à un DA expirent ou sont renvoyées avec l'erreur `DA_BUSY_NOW`.
- Le journal DA indique que de nombreuses requêtes SLP sont ignorées.
- Le réseau d'utilisateurs qui partagent des services dans les étendues s'étend sur plusieurs bâtiments ou sites physiques.

Vous pouvez exécuter un suivi `snoop` du trafic SLP afin de déterminer combien de requêtes UA reviennent avec l'erreur `DA_BUSY_NOW` . Si le nombre de requêtes UA renvoyées est élevé, les UA dans les bâtiments physiquement et topologiquement éloignées des DA peuvent présenter une réponse lente ou des délais d'attente excessifs. Dans un tel scénario, vous pouvez déployer un DA dans chaque bâtiment pour améliorer la réponse des clients UA dans les bâtiments.

Les liens entre les bâtiments sont souvent plus lents que les réseaux locaux dans les bâtiments. Si votre réseau s'étend sur plusieurs bâtiments ou sites physiques, définissez la propriété `net.slp.DAAddresses` dans le fichier `/etc/inet/slp.conf` sur une liste de noms d'hôtes ou d'adresses spécifiques, afin que les UA accèdent uniquement aux DA spécifiés.

Si un DA particulier utilise une grande quantité de mémoire de l'hôte pour les enregistrements de service, réduisez le nombre d'enregistrements SA en diminuant le nombre d'étendues prises en charge par le DA. Vous pouvez diviser en deux une étendue qui comporte de nombreux enregistrements. Vous pouvez ensuite prendre en charge l'une des nouvelles étendues en déployant un autre DA sur un autre hôte.

SLP et systèmes multiréseau

Un serveur multiréseau agit comme un hôte sur plusieurs sous-réseaux IP. Le serveur peut parfois posséder plusieurs cartes d'interface réseau et agir en tant que routeur. Les paquets IP, y compris les paquets de multidiffusion, sont routés entre les interfaces. Dans certains cas, le routage entre les interfaces est désactivé. Les sections suivantes décrivent la configuration de SLP dans de telles situations.

Configuration multiréseau pour SLP

Sans configuration, `slpd` est à l'écoute de la multidiffusion et de la monodiffusion UDP/TCP sur l'interface réseau par défaut. Si le routage multidiffusion et monodiffusion est activé entre des interfaces sur une machine multiréseau, aucune configuration supplémentaire n'est nécessaire. En effet, les paquets de multidiffusion qui arrivent sur une autre interface sont correctement routés vers l'interface par défaut. Par conséquent, les requêtes multidiffusion pour le DA ou d'autres annonces de service arrivent à `slpd`. Si, pour une raison quelconque, le routage n'est pas activé, la configuration est requise.

Moment adapté à la configuration d'interfaces réseau multiples sans routage

Si l'une des conditions suivantes est remplie, vous pouvez être amené à configurer des machines multiréseau.

- Le routage monodiffusion est activé entre les interfaces et le routage multidiffusion est désactivé.
- Le routage monodiffusion et le routage multidiffusion sont tous deux désactivé entre les interfaces.

Le routage multidiffusion est généralement désactivé entre des interfaces du fait que la multidiffusion n'a pas été déployée sur le réseau. Dans ce cas, la diffusion est normalement utilisée pour la découverte des services qui n'est pas basée sur DA et pour la découverte DA sur des sous-réseaux individuels. La diffusion est activée en définissant la propriété `net.slp.isBroadcastOnly` sur `True`.

Configuration d'interfaces réseau multiples sans routage (liste des tâches)

TABLEAU 9–5 Configuration d'interfaces réseau multiples, sans routage

Tâche	Description	Voir
Configuration de la propriété `net.slp.interfaces`	Définissez cette propriété pour activer `slpd` afin qu'il écoute les requêtes SLP de monodiffusion et multidiffusion/diffusion sur les interfaces spécifiées.	"Configuration de la propriété `net.slp.interfaces`" à la page 269

TABLEAU 9–5 Configuration d'interfaces réseau multiples, sans routage *(Suite)*

Tâche	Description	Voir
Organisation des annonces de services proxy afin que les UA sur les sous-réseaux obtiennent des URL de services avec des adresses accessibles	Restreignez l'annonce de proxy sur une machine qui exécute `slpd` connecté à un seul sous-réseau plutôt qu'un hôte multiréseau.	"Annonce de proxy sur les hôtes multiréseau" à la page 271
Placement des DA et configuration des étendues afin de garantir l'accessibilité entre les UA et les SA	Configurez la propriété `net.slp.interfaces` sur des hôtes multiréseau avec une adresse ou un nom d'hôte d'interface unique. Exécutez un DA sur un hôte multiréseau, mais configurez les étendues de manière à ce que les SA et UA sur chaque sous-réseau utilisent des hôtes différents.	"Placement du DA et affectation de nom à l'étendue" à la page 271

Configuration de la propriété `net.slp.interfaces`

Si la propriété `net.slp.interfaces` est définie, `slpd` est à l'écoute des requêtes SLP de monodiffusion et de multidiffusion/diffusion sur les interfaces répertoriées dans la propriété, plutôt que sur l'interface par défaut.

Généralement, vous définissez la propriété `net.slp.interfaces` en même temps que vous activez la diffusion en définissant la propriété `net.slp.isBroadcastOnly`, car la multidiffusion n'a pas été déployée sur le réseau. Toutefois, si la multidiffusion a été déployée mais n'est pas routée sur cet hôte multiréseau, `slpd` peut recevoir une requête de multidiffusion depuis plusieurs interfaces. Cette situation peut se produire lorsque le routage des paquets est géré par un autre hôte multiréseau ou par un routeur qui connecte les sous-réseaux servis par les interfaces.

Lorsqu'une telle situation se produit, le serveur SA ou l'UA qui envoie la requête reçoit deux réponses de `slpd` sur l'hôte multiréseau. Les réponses sont ensuite filtrées par les bibliothèques client et le client ne les voit pas. Les réponses sont toutefois visibles dans le suivi `snoop`.

Remarque –

Si le routage monodiffusion est désactivé, les services annoncés par les clients SA sur les hôtes multiréseau peuvent ne pas être accessibles à partir de tous les sous-réseaux. Si les services sont inaccessibles, les clients SA peuvent effectuer les opérations suivantes :

- Annoncer une URL de service pour chaque sous-réseau.
- S'assurer que les requêtes émises depuis un sous-réseau particulier font l'objet d'une réponse avec une URL accessible.

La bibliothèque client SA ne fait aucun effort pour garantir que les URL accessibles sont annoncées. Le programme de service, qui peut gérer un hôte multiréseau sans routage ou non, est alors chargé de garantir que les URL accessibles sont annoncées.

Avant le déploiement d'un service sur un hôte multiréseau sur lequel le routage monodiffusion est désactivé, utilisez la commande `snoop` pour déterminer si le service gère correctement les requêtes provenant de plusieurs sous-réseaux. En outre, si vous envisagez de déployer un DA sur l'hôte multiréseau, reportez-vous à la section "Placement du DA et affectation de nom à l'étendue" à la page 271.

▼ Configuration de la propriété `net.slp.interfaces`

Utilisez la procédure suivante pour modifier la propriété `net.slp.interfaces` dans le fichier `slp.conf`.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `slpd` et toutes les activités SLP sur l'hôte.

```
# svcadm disable network/slp
```

3 Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.

4 Modifiez la propriété `net.slp.interfaces` dans le fichier `slpd.conf` :

`net.slp.interfaces=`*value*

valeur Liste d'adresses IPv4 ou de noms d'hôte des cartes d'interface réseau sur lesquels le DA ou le SA doit être à l'écoute de la multidiffusion, la monodiffusion UDP et des messages TCP sur le port 427

Par exemple, un serveur avec trois cartes réseau sur lequel le routage multidiffusion est désactivé est connecté à trois sous-réseaux. Les adresses IP des trois interfaces réseau sont `192.147.142.42`, `192.147.143.42` et `192.147.144.42`. Le masque de sous-réseau est `255.255.255.0` . Si vous réglez la propriété suivante, `slpd` sera à l'écoute des messages de monodiffusion et de multidiffusion/diffusion sur les trois interfaces :

```
net.slp.interfaces=192.147.142.42,192.147.143.42,192.147.144.42
```

Remarque – Vous pouvez spécifier des adresses IP ou noms d'hôte pouvant être résolus pour la propriété `net.slp.interfaces`.

---

5 Enregistrez les modifications et fermez le fichier.

6 **Redémarrez `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Annonce de proxy sur les hôtes multiréseau

Si un hôte comportant plusieurs interfaces annonce des services à l'aide de la commande `slpd` et l'enregistrement de proxy, les URL de service annoncées par `slpd` doivent contenir des noms d'hôte ou des adresses accessibles. Si le routage monodiffusion est activé entre les interfaces, les hôtes sur tous les sous-réseaux peuvent atteindre les hôtes sur d'autres sous-réseaux. Les enregistrements de proxy peuvent également être effectués pour un service sur un sous-réseau. Si, toutefois, le routage monodiffusion est désactivé, les clients de service sur un sous-réseau ne peuvent pas atteindre de services sur un autre sous-réseau via l'hôte multiréseau. Cependant, les clients peuvent être en mesure d'atteindre les services par le biais d'un autre routeur.

Par exemple, supposons que l'hôte avec le nom d'hôte par défaut `bigguy` possède trois cartes d'interface sur trois sous-réseaux non routés. Les noms d'hôte de ces sous-réseaux sont `bigguy`, avec l'adresse IP `192.147.142.42` , `bigguy1`, avec l'adresse IP `192.147.143.42` et `bigguy2`, avec l'adresse IP `192.147.144.42`. Supposons maintenant qu'une imprimante héritée, `oldprinter`, est connectée au sous-réseau `143` et que l'URL `service:printing:lpr://oldprinter/queue1` est configurée avec la valeur `net.slp.interfaces` pour être à l'écoute sur toutes les interfaces. L'URL `oldprinter` fait l'objet d'une annonce de proxy sur toutes les interfaces. Les machines sur les sous-réseaux `142` et `144` reçoivent l'URL en réponse à des requêtes de service, mais ne sont pas en mesure d'accéder au service `oldprinter`.

La solution à ce problème consiste à effectuer l'annonce de proxy avec `slpd` exécuté sur une machine connectée au sous-réseau `143` uniquement, plutôt que sur l'hôte multiréseau. Seuls les hôtes sur le sous-réseau `143` peuvent obtenir l'annonce en réponse à une requête de service.

Placement du DA et affectation de nom à l'étendue

Le placement des DA et l'affectation de nom à une étendue sur un réseau possédant un hôte multiréseau doivent faire l'objet d'une attention particulière afin de s'assurer que les services soient accessibles aux clients. Soyez particulièrement vigilant lorsque le routage est désactivé et la propriété `net.slp.interfaces` configurée. Ici encore, si le routage monodiffusion est activé entre les interfaces sur une machine multiréseau, aucune configuration particulière du DA et de l'étendue n'est nécessaire. Les annonces sont mises en cache avec les services d'identification du DA accessibles à partir de tous les sous-réseaux. Toutefois, si le routage monodiffusion est désactivé, un placement incorrect des DA peut entraîner des problèmes.

Pour voir les problèmes susceptibles de se produire dans l'exemple précédent, envisagez ce qui se passerait si `bigguy` exécutait un DA et les clients sur tous les sous-réseaux avaient les mêmes

étendues. Les SA sur le sous-réseau 143 enregistreraient leurs annonces de service avec le DA. Les UA sur le sous-réseau 144 pourraient obtenir ces annonces de service, bien que les hôtes sur le sous-réseau 143 soient inaccessibles.

Une solution à ce problème consiste à exécuter un DA sur chaque sous-réseau et non sur l'hôte multiréseau. Dans ce cas, la propriété `net.slp.interfaces` sur les hôtes multiréseau doit être configurée avec un nom ou une adresse d'interface hôte unique, ou ne pas être configurée, forçant ainsi l'utilisation de l'interface par défaut. L'inconvénient de cette solution est que les hôtes multiréseau sont souvent de grandes machines plus en mesure de gérer la charge informatique d'un DA.

Une autre solution consiste à exécuter un DA sur l'hôte multiréseau, tout en configurant les étendues de manière à ce que les SA et les UA sur chaque sous-réseau aient une étendue différente. Par exemple, dans l'exemple précédent, les UA et les SA sur le sous-réseau 142 peuvent avoir une étendue appelée `scope142`. Les UA et SA sur le sous-réseau 143 peuvent avoir une autre étendue appelé `scope143` et les UA et SA sur le sous-réseau 144 peuvent avoir une troisième étendue appelée `scope144`. Vous pouvez définir la propriété `net.slp.interfaces` sur `bigguy` avec les trois interfaces afin que le DA serve les trois étendues sur les trois sous-réseaux.

Éléments à prendre en compte lors de la configuration d'interfaces réseau multiples, sans routage

La configuration de la propriété `net.slp.interfaces` permet à un DA sur l'hôte multiréseau de lier les annonces de service entre les sous-réseaux. Par exemple la configuration est utile si le routage multidiffusion est désactivé sur le réseau, mais le routage monodiffusion entre des interfaces sur un hôte multiréseau est activé. Si la monodiffusion est routée entre les interfaces, les hôtes sur un sous-réseau différent de celui sur lequel le service se trouve peuvent contacter le service lorsqu'ils reçoivent l'URL du service. Sans le DA, les serveurs SA sur un sous-réseau particulier ne reçoivent que les diffusions effectuées sur le même sous-réseau, de sorte qu'ils ne peuvent pas localiser les services hors de leur sous-réseau.

La situation la plus courante qui nécessite la configuration de la propriété `net.slp.interfaces` se produit lorsque la multidiffusion n'est pas déployée sur le réseau et que la diffusion est utilisée à la place. D'autres situations nécessitent une réflexion et une planification minutieuses pour éviter les réponses en double ou les services inaccessibles.

◆ ◆ ◆ CHAPITRE 10

Intégration des services hérités

Les services hérités sont les services réseau qui précèdent le développement et la mise en œuvre de SLP. Les services tels que le démon d'imprimante ligne (`lpsched`), le service de fichiers NFS et le service de noms NIS/NIS+, par exemple, ne contiennent pas d'agent de service interne pour SLP. Ce chapitre décrit quand et comment annoncer les services hérités.

Moment adapté pour l'annonce des services hérités

Grâce à l'annonce de services hérités, vous pouvez activer les agents utilisateur SLP pour trouver des périphériques et des services, tels que les éléments suivants, sur les réseaux. Vous pouvez trouver des périphériques matériels et services logiciels qui ne contiennent pas d'agent de service SLP. Lorsque des applications comportant des agents utilisateur SLP nécessitent de rechercher des imprimantes ou des bases de données qui ne contiennent pas d'agent de service SLP, par exemple, les annonces héritées peuvent s'avérer nécessaires.

Annonce de services hérités

Vous pouvez utiliser l'une des méthodes suivantes pour annoncer les services hérités :

- Modifier le service pour incorporer un agent de service SLP.
- Écrire un petit programme qui annonce pour le compte d'un service pour lequel SLP n'est pas activé.
- Utiliser l'annonce de proxy pour que `slpd` annonce le service.

Modification du service

Si le code source du serveur logiciel est disponible, vous pouvez incorporer un agent de service SLP. Les API C et Java pour SLP sont relativement simples à utiliser. Pour plus d'informations, reportez-vous aux pages de manuel relatives à l'API C et à la documentation sur l'API Java. Si le service est un périphérique matériel, le fabricant peut avoir une PROM mise à jour qui intègre SLP. Contactez le fabricant du périphérique pour obtenir davantage d'informations.

Annonce d'un service pour lequel SLP n'est pas activé

Si le code source ou une PROM mise à jour qui contient SLP n'est pas disponible, vous pouvez écrire une petite application qui utilise la bibliothèque client SLP afin d'annoncer le service. Cette application peut fonctionner comme un petit démon que vous pouvez démarrer ou arrêter à partir du même script shell que vous utilisez pour démarrer et arrêter le service.

Enregistrement de proxy SLP

Solaris `slpd` prend en charge l'annonce des services hérités avec un fichier d'enregistrement de proxy Le fichier d'enregistrement de proxy est une liste d'annonces de service dans un format portable.

▼ Activation de l'enregistrement de proxy SLP

1 **Créez un fichier d'enregistrement de proxy sur le système de fichiers hôte ou dans n'importe quel répertoire réseau auquel le protocole HTTP peut accéder.**

2 **Déterminez si un modèle de type de service existe pour le service.**

Le modèle est une description de l'URL du service et des attributs d'un type de service. Un modèle est utilisé pour définir les composants d'une annonce pour un type de service précis :

- Si un modèle de type de service existe, utilisez le modèle pour construire l'enregistrement de proxy. Pour obtenir davantage d'informations sur les modèles de type de service, reportez-vous au RFC 2609.
- Si aucun modèle de type de service n'est disponible pour le service, sélectionnez un ensemble d'attributs qui décrit précisément le service. Utilisez une autorité de nommage autre que l'autorité par défaut pour l'annonce. L'autorité de nommage par défaut est activée uniquement pour les types de services normalisés. Pour obtenir davantage d'informations sur les autorités de nommage, reportez-vous au RFC 2609.

Par exemple, supposons qu'une entreprise appelée *BizApp* possède une base de données locale utilisée pour suivre les défaillances logicielles. Pour annoncer la base de données, l'entreprise peut utiliser une URL avec le type de service `service:bugdb.bizapp`. L'autorité de nommage serait alors `bizapp`.

3 **Suivez les étapes suivantes pour configurer la propriété `net.slp.serializedRegURL` dans le fichier `/etc/inet/slp.conf` avec l'emplacement du fichier d'enregistrement créé au cours des étapes précédentes.**

4 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

5 **Arrêtez `slpd` et toutes les activités SLP sur l'hôte.**

```
# svcadm disable network/slp
```

6 **Sauvegardez le fichier `/etc/inet/slp.conf` par défaut avant de modifier les paramètres de configuration.**

7 **Spécifiez l'emplacement du fichier d'enregistrement de proxy dans la propriété `net.slp.serializedRegURL` du fichier `/etc/inet/slp.conf`.**

`net.slp.net.slp.serializedRegURL=`*proxy registration file URL*

Par exemple, si le fichier d'enregistrement sérialisé est `/net/inet/slp.reg` , configurez la propriété comme indiqué dans l'exemple suivant :

```
net.slp.serializedRegURL=file:/etc/inet/slp.reg
```

8 **Enregistrez les modifications et fermez le fichier.**

9 **Redémarrez la commande `slpd` pour activer vos modifications.**

```
# svcadm enable network/slp
```

Utilisation de l'enregistrement de proxy SLP pour l'annonce

Une annonce de service est formée de lignes qui identifient l'URL du service, d'une étendue facultative et d'une série de définitions d'attributs. Le démon SLP lit, enregistre et conserve les annonces de proxy exactement comme le ferait un client SA. L'exemple suivant présente un exemple d'annonce issue d'un fichier d'enregistrement de proxy.

Dans l'exemple, une imprimante héritée prenant en charge le protocole LPR et un serveur FTP sont annoncés. Les numéros de ligne ont été ajoutés à des fins de description et ne font pas partie du fichier.

```
(1) #Advertise legacy printer.
(2)
(3) service:lpr://bizserver/mainspool,en,65535
(4) scope=eng,corp
(5) make-model=Laserwriter II
(6) location-description=B16-2345
(7) color-supported=monochromatic
(8) fonts-supported=Courier,Times,Helvetica 9 10
(9)
(10) #Advertise FTP server
(11)
(12) ftp://archive/usr/src/public,en,65535,src-server
(13) content=Source code for projects
(14)
```

Remarque – Le fichier d'enregistrement de proxy prend en charge la même convention d'échappement des caractères non ASCII que le fichier de configuration. Pour plus d'informations sur le format du fichier d'enregistrement de proxy, reportez-vous au RFC 2614.

TABLEAU 10–1 Description du fichier d'enregistrement de proxy SLP

Numéros de ligne	Description
1 et 10	Lignes de commentaires qui commencent par un symbole dièse (#) et n'affectent en aucun cas le fonctionnement du fichier. Tous les caractères jusqu'à la fin d'une ligne de commentaire sont ignorés.
2, 9 et 14	Lignes vides qui délimitent les annonces.

TABLEAU 10–1 Description du fichier d'enregistrement de proxy SLP *(Suite)*

Numéros de ligne	Description
3, 12	URL de service qui ont chacune trois champs obligatoires et un champ facultatif séparés par des virgules : ■ `service : URL` ou générique annoncée Reportez-vous au RFC 2609 pour connaître la procédure de création d'une URL : service. ■ Langue de l'annonce. Dans l'exemple précédent, le champ est désigné en anglais, *en*. La langue est une balise de langue RFC 1766. ■ Durée de l'annonce, en secondes. La durée de vie est limitée à un entier non signé de 16 bits. Si la durée de vie est inférieure au maximum, 65 535, `slpd` met fin à l'annonce. Si la durée de vie est de 65 535, `slpd` actualise régulièrement l'annonce et la durée de vie est considérée comme permanente, jusqu'à ce que `slpd` s'arrête. ■ (Facultatif) Champ de type de service : s'il est utilisé, ce champ définit le type de service. Si l'URL du service est définie, vous pouvez modifier le type de service sous lequel l'URL est annoncée. Dans l'exemple de fichier d'enregistrement de proxy précédent, la ligne 12 contient une URL de FTP générique. Le champ de type facultatif entraîne l'annonce de l'URL sous le nom de type de service *src-server*. Le préfixe `service` n'est pas ajouté par défaut pour le nom de type.
4	Désignation de l'étendue. La ligne facultative se compose du jeton `scope`, suivi d'un signe égale et d'une liste séparée par des virgules des noms d'étendues. Les noms d'étendues sont définis par la propriété de configuration `net.slp.useScopes`. Seules les étendues configurées pour l'hôte doivent être incluses dans la liste. Si aucune ligne d'étendue n'est ajoutée, l'enregistrement est effectué dans toutes les étendues avec lesquelles `slpd` est configuré. La ligne d'étendue doit apparaître immédiatement après la ligne d'URL. Sinon, les noms d'étendues sont reconnus comme des attributs.
5–8	Définitions d'attributs. Après la ligne d'étendue facultative, le corps de l'annonce de service contient les lignes de paires de liste attribut/valeur. Chaque paire se compose du descripteur de l'attribut, suivi d'un signe égale et d'une valeur d'attribut ou une liste de valeurs séparées par des virgules. Dans l'exemple de fichier d'enregistrement de proxy précédent, la ligne 8 illustre une liste d'attributs avec plusieurs valeurs. Toutes les autres listes ont des valeurs uniques. Le format des noms et valeurs d'attributs est le même que pour les messages SLP simultanés.

Considérations à prendre en compte lors de l'annonce de services hérités

En règle générale, la modification du code source pour ajouter le protocole SLP est préférable à l'écriture d'un service SLP qui utilise l'API SLP pour effectuer une annonce pour le compte d'autres services. La modification du code source est également préférable à l'utilisation de l'enregistrement de proxy. Lorsque vous modifiez le code source, vous pouvez ajouter des

fonctionnalités spécifiques au service et suivre de près la disponibilité du service. Si le code source n'est pas disponible, l'écriture d'un service d'assistance SLP qui effectuera les annonces pour le compte d'autres services est préférable à l'utilisation de l'enregistrement de proxy. Idéalement, ce service d'assistance est intégré à la procédure de démarrage et d'arrêt du service, utilisée pour contrôler l'activation et la désactivation. L'annonce de proxy est généralement le troisième choix, si aucun code source n'est disponible et si l'écriture d'un agent de service autonome n'est pas pratique.

Les annonces de proxy sont uniquement conservées si `slpd` est en cours d'exécution pour lire le fichier d'enregistrement de proxy. Aucune connexion directe n'existe entre l'annonce de proxy et le service. Si une annonce arrive à expiration ou si `slpd` est arrêté, l'annonce proxy n'est plus disponible.

Si le service est arrêté, `slpd` doit être arrêté. Le fichier d'enregistrement sérialisé est modifié pour commenter ou supprimer l'annonce de proxy, et `slpd` est redémarré. Suivez la même procédure lorsque le service est redémarré ou réinstallé. L'absence de connexion entre l'annonce de proxy et le service est un inconvénient majeur des annonces de proxy.

◆ ◆ ◆ CHAPITRE 11

SLP (références)

Ce chapitre décrit les codes d'état et les types de messages SLP. Les types de messages SLP sont répertoriés avec les abréviations et des codes de fonction. Les codes d'état SLP sont affichés avec des descriptions et des codes de fonction qui permettent d'indiquer qu'une requête est reçue (code 0) ou que le récepteur est occupé.

Remarque – Le démon SLP (`slpd`) renvoie des codes d'état uniquement pour les messages de monodiffusion.

Codes d'état SLP

TABLEAU 11–1 Codes d'état SLP

Type d'état	Code d'état	Description
aucune erreur	0	La requête a été traitée sans erreur.
LANGUAGE_NOT_SUPPORTED	1	Pour une requête AttrRqst ou SrvRqst, il existe des données pour le type de service dans l'étendue, mais aucune langue n'est indiquée.
PARSE_ERROR	2	Le message échoue à suivre la syntaxe SLP.
INVALID_REGISTRATION	3	Le message SrvReg présente des problèmes, tels qu'une durée de vie égale à zéro ou une balise de langue omise.
SCOPE_NOT_SUPPORTED	4	Le message SLP n'inclut pas d'étendue dans sa liste d'étendues prises en charge par le SA ou le DA qui répond à la requête.
AUTHENTICATION_UNKNOWN	5	Le DA ou le SA a reçu une requête pour une SPI SLP non prise en charge.

TABLEAU 11–1 Codes d'état SLP *(Suite)*

Type d'état	Code d'état	Description
AUTHENTICATION_ABSENT	6	L'UA ou le DA attendait l'URL et l'authentification d'attribut dans le SrvReg et ne les a pas reçus.
AUTHENTICATION_FAILED	7	L'UA ou le DA a détecté une erreur d'authentification dans un bloc d'authentification.
VER_NOT_SUPPORTED	9	Numéro de version non pris en charge dans le message.
INTERNAL_ERROR	10	Une erreur inconnue s'est produite dans le DA ou le SA. Par exemple, il n'y a plus d'espace fichiers sur le système d'exploitation.
DA_BUSY_NOW	11	L'UA ou le SA doit effectuer une nouvelle tentative, à l'aide d'un temps d'attente exponentiel. Le DA est occupé à traiter d'autres messages.
OPTION_NOT_UNDERSTOOD	12	Le DA ou le SA a reçu une option inconnue dans la plage obligatoire.
INVALID_UPDATE	13	Le DA a reçu un message SrvReg sans ensemble FRESH pour un service non enregistré ou avec des types de service incohérents.
MSG_NOT_SUPPORTED	14	Le SA a reçu une requête AttrRqst ou SrvTypeRqst et ne la prend pas en charge.
REFRESH_REJECTED	15	Le SA a envoyé un message SrvReg ou SrvDereg partiel à un DA à un intervalle plus fréquent que l'intervalle d'actualisation minimal du DA.

Types de message SLP

TABLEAU 11–2 Types de message SLP

Type de message	Abréviation	Code de fonction	Description
Requête de service	`SrvRqst`	1	Émise par un UA pour trouver des services ou par un serveur UA ou SA pendant la découverte DA active.
Réponse de service	`SrvRply`	2	Réponse du DA ou du SA à une requête de service.
Enregistrement de service	`SrvReg`	3	Permet aux SA d'enregistrer de nouvelles annonces, de mettre à jour les annonces existantes avec des attributs nouveaux ou modifiés et d'actualiser la durée de vie de l'URL.

TABLEAU 11–2 Types de message SLP *(Suite)*

Type de message	Abréviation	Code de fonction	Description
Annulation de l'enregistrement de service	`SrvDereg`	4	Utilisé par le SA pour annuler l'enregistrement de ses annonces lorsque le service qu'elles représentent n'est plus disponible.
Accusé de réception	`SrvAck`	5	Réponse du DA à une requête de service d'un SA ou à un message d'annulation d'un enregistrement de service.
Requête d'attribut	`AttrRqst`	6	Effectuée via l'URL ou le type de service pour demander une liste d'attributs.
Réponse d'attribut	`AttrRply`	7	Permet de renvoyer la liste des attributs.
Annonce DA	`DAAdvert`	8	Réponse du DA aux requêtes de service de multidiffusion.
Requête de type de service	`SrvTypeRqst`	9	Permet d'obtenir des renseignements sur les types de services enregistrés possédant une autorité de nommage particulière et se trouvant dans un ensemble d'étendues spécifique.
Réponse de type de service	`SrvTypeRply`	10	Message renvoyé en réponse à la requête de type de service.
Annonce SA	`SAAdvert`	11	Les UA utilisent le message `SAAdvert` pour découvrir les SA et leurs étendues sur les réseaux où aucun DA n'est déployé.

PARTIE IV

Sujets relatifs aux services de messagerie

Cette section fournit une présentation, des listes de tâches et des informations de référence sur le service de messagerie.

◆ ◆ ◆ CHAPITRE 12

Services de messagerie (présentation)

La configuration et la mise à jour d'un service de messagerie électronique impliquent des tâches complexes qui sont cruciales pour les opérations quotidiennes de votre réseau. En tant qu'administrateur réseau, vous pouvez être amené à étendre un service de messagerie existant. Sinon, vous devrez peut-être configurer un service de messagerie sur un nouveau réseau ou sur un sous-réseau. Les chapitres sur les services de messagerie peuvent vous aider à planifier et à configurer un service de messagerie pour votre réseau. Ce chapitre fournit des liens vers les descriptions des nouvelles fonctions de la commande `sendmail`, ainsi qu'une liste d'autres sources d'informations. En outre, ce chapitre fournit une présentation des composants matériels et logiciels qui sont nécessaires pour établir un service de messagerie.

Pour des informations sur les procédures à suivre pour configurer et administrer les services de messagerie, reportez-vous au Chapitre 13, "Services de messagerie (tâches)". Pour plus d'informations, reportez-vous à la section "Liste des tâches pour les services de messagerie" à la page 291.

Pour une description détaillée des composants des services de messagerie, reportez-vous au Chapitre 14, "Services de messagerie (référence)". Ce chapitre décrit également les programmes et les fichiers de services de messagerie, le processus d'acheminement du courrier, les interactions de la commande `sendmail` avec les services de noms et les fonctions de la version 8.13 de `sendmail`. Reportez-vous à la section "Modifications de la version 8.13 de `sendmail`" à la page 383.

Nouveautés des services de messagerie

Cette section fournit des informations sur les nouvelles fonctions dans les différentes versions de Solaris.

Modifications apportées dans cette version

Les modifications suivantes ont été apportées dans Oracle Solaris version 10 mise à jour 10 :

- La version par défaut de la commande sendmail a été mise à jour dans 8.14.
- L'instance sendmail a été divisée en deux instances pour assurer une meilleure gestion du démon classique (`svc:/network/smtp:sendmail`) et du programme d'exécution de file d'attente client (`svc:/network/smtp:sendmail-client`).
- Le système peut être configuré pour reconstituer automatiquement le fichier `sendmail.cf` et les fichiers de configuration `submit.mc`. Les étapes nécessaires sont documentées à la section "Reconstruction automatique d'un fichier de configuration" à la page 308.
- Par défaut, le démon sendmail s'exécute dans le nouveau mode démon local. Le mode local uniquement n'accepte que les messages entrants provenant des connexions de l'hôte local ou SMTP loopback. Par exemple, un message provenant d'une tâche cron ou entre des utilisateurs locaux serait accepté. Le courrier sortant est acheminé normalement, seul le courrier entrant est modifié. L'option `-bl` est utilisée pour sélectionner le mode local uniquement, également connu comme le mode Devenir local (become local). Pour plus d'informations sur ce mode, reportez-vous à la page de manuel `sendmail(1M)`. Pour obtenir des instructions sur la façon de revenir au mode `-bd` ou Devenir démon (become daemon), reportez-vous à la section "Utilisation de `sendmail` en mode ouvert" à la page 308.

Modifications apportées dans la version Solaris 10 1/06

À partir de la version Solaris 10 1/06, `sendmail` prend en charge le protocole SMTP avec TLS (Transport Layer Security). Pour plus d'informations, reportez-vous aux références suivantes :

- "Prise en charge de l'exécution de SMTP avec TLS dans la version 8.13 de `sendmail`" à la page 384
- "Configuration de SMTP pour utiliser le protocole TLS" à la page 309

Pour obtenir la liste complète des fonctionnalités de la version Solaris 10 1/06, reportez-vous au document *Nouveautés apportées à Oracle Solaris 10 8/11*.

Modifications apportées dans la version Solaris 10

La version 8.13 est la version par défaut pour `sendmail`. Pour plus d'informations sur la version 8.13 et d'autres modifications, reportez-vous aux sections suivantes :

- “Indicateurs utilisés et non utilisés pour compiler `sendmail`” à la page 344
- “`MILTER`, API de filtre de courrier pour `sendmail`” à la page 345
- “Versions du fichier de configuration” à la page 346
- “Amélioration de l'utilitaire `vacation`” à la page 359
- “Contenu du répertoire `/etc/mail/cf`” à la page 361
- “Modifications de la version 8.13 de `sendmail`” à la page 383
- “Prise en charge des wrappers TCP à partir de la version 8.12 de `sendmail`” à la page 393

En outre, le service de messagerie est géré par l'utilitaire de gestion des services. Les actions administratives appliquées à ce service (activation, désactivation ou redémarrage, par exemple), peuvent être réalisées à l'aide de la commande `svcadm`. Servez-vous de la commande `svcs` pour connaître l'état du service. Pour plus d'informations sur l'utilitaire de gestion des services, reportez-vous à la page de manuel `smf(5)` et le Chapitre 18, “Gestion des services (présentation)” du *Guide d'administration système : administration de base*.

Autres sources d'informations `sendmail`

Ce qui suit est une liste des autres sources d'informations sur `sendmail`.

- Costales, Bryan. *sendmail, Third Edition*. O'Reilly & Associates, Inc., 2002.
- Page d'accueil pour `sendmail` – `http://www.sendmail.org`.
- FAQ pour `sendmail` – `http://www.sendmail.org/faq`.
- Fichier README relatifs aux nouveaux fichiers de configuration `sendmail` – `http://www.sendmail.org/m4/readme.html`.
- Guide pour les problèmes liés à la migration vers les versions les plus récentes de `sendmail` – `http://www.sendmail.org/vendor/sun/`.

Introduction aux composants des services de messagerie

De nombreux composants matériels et logiciels sont nécessaires pour établir un service de messagerie. Les sections suivantes fournissent une introduction rapide à ces composants. Elles introduisent également certains des termes qui sont utilisés pour décrire les composants.

La première section, “Présentation des composants logiciels” à la page 288, définit les termes qui sont utilisés lorsqu'on parle des parties logicielles du système de distribution du courrier. La section suivante, “Présentation des composants matériels” à la page 288, se concentre sur les fonctions des systèmes matériels dans une configuration de messagerie.

Présentation des composants logiciels

Le tableau ci-dessous présente quelques-uns des composants logiciels d'un système de messagerie. Reportez-vous à la section "Composants logiciels" à la page 347 pour une description complète de tous les composants logiciels.

Composant	Description
Fichiers `.forward`	Fichiers que vous pouvez configurer dans un répertoire personnel d'un l'utilisateur pour rediriger ou envoyer les messages à un programme automatiquement
Boîte à lettres	Fichier sur un serveur de courrier qui est la destination finale pour les messages électroniques
Adresses e-mail	Adresses qui contiennent le nom du destinataire et le système auquel un message électronique est distribué
Alias de messagerie	Nom alternatif utilisé dans une adresse e-mail
File d'attente de messages	Ensemble de messages électroniques qui doit être traité par le serveur de courrier
Administrateur du courrier	Alias de messagerie spécial qui est utilisé pour signaler des problèmes et poser des questions sur le service de messagerie
Fichier de configuration sendmail	Fichier qui contient toutes les informations nécessaires pour l'acheminement du courrier

Présentation des composants matériels

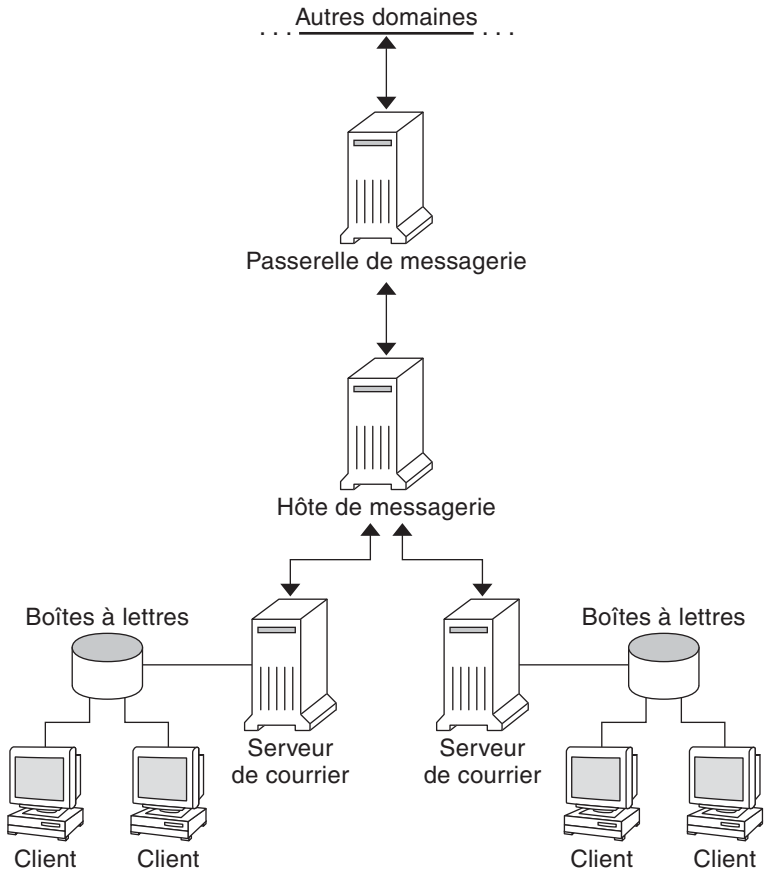
Une configuration de messagerie nécessite trois éléments, que vous pouvez combiner sur le même système ou fournir dans des systèmes distincts.

- Un hôte de messagerie – Système qui est configuré pour gérer les adresses e-mail qui sont difficiles à résoudre
- Un minimum d'un serveur de courrier – Système qui est configuré pour contenir une ou plusieurs boîtes à lettres
- Des clients de messagerie – Systèmes qui accèdent aux messages à partir d'un serveur de courrier

Si les utilisateurs doivent communiquer avec des réseaux en dehors de votre domaine, vous devez également ajouter un quatrième élément, une passerelle de messagerie.

La Figure 12–1 présente une configuration de messagerie électronique habituelle, utilisant les trois éléments de messagerie de base, plus une passerelle de messagerie.

FIGURE 12–1 Configuration de messagerie électronique habituelle



Chaque élément est décrit en détail à la section "Composants matériels" à la page 355.

◆ ◆ ◆ CHAPITRE 13

Services de messagerie (tâches)

Ce chapitre explique comment configurer et administrer des services de messagerie. Si vous n'êtes pas familiarisé avec l'administration des services de messagerie, lisez le Chapitre 12, “Services de messagerie (présentation)” pour une introduction aux composants des services de messagerie. Ce chapitre propose également une description de la configuration typique d'un service de messagerie, comme illustré dans la Figure 12–1. La liste ci-dessous peut vous aider à trouver les groupes de procédures connexes qui sont traitées dans ce chapitre.

Pour une description détaillée des composants des services de messagerie, reportez-vous au Chapitre 14, “Services de messagerie (référence)”. Ce chapitre décrit également les programmes et fichiers du service de messagerie, le processus d'acheminement du courrier, les interactions de `sendmail` avec les services de noms et les fonctions de la version 8.13 de `sendmail` qui ne sont pas entièrement décrites dans la page de manuel `sendmail(1M)`.

Liste des tâches pour les services de messagerie

Le tableau ci-dessous vous renvoie à d'autres listes de tâches qui se concentrent sur un groupe spécifique de procédures.

Tâche	Description	Voir
Configuration des services de messagerie	Utilisez ces procédures pour configurer chaque composant de votre service de messagerie. Apprenez à configurer un serveur de courrier, un client de messagerie, un hôte de messagerie et une passerelle de messagerie. Apprenez à utiliser le serveur DNS avec `sendmail`.	"Configuration des services de messagerie (liste des tâches)" à la page 296
Modification de la configuration sendmail	Utilisez ces procédures pour modifier vos fichiers de configuration ou les propriétés du service.	"Modification de la configuration sendmail (liste des tâches)" à la page 305
Administration des fichiers d'alias de messagerie	Utilisez ces procédures pour fournir une définition d'alias sur votre réseau. Apprenez à gérer les entrées de tables NIS+. Apprenez également à configurer une carte NIS, un alias de messagerie locale, un fichier de configuration à clé et un alias d'administrateur du courrier.	"Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315
Administration de la file d'attente de messages	Utilisez ces procédures pour permettre un traitement de la file d'attente progressif. Apprenez à afficher et déplacer la file d'attente de messages, forcer le traitement des files d'attente de messages et exécuter un sous-ensemble de la file d'attente de messages. En outre, apprenez à exécuter l'ancienne file d'attente de messages.	"Administration des répertoires de file d'attente (liste des tâches)" à la page 327
Administration des fichiers `.forward`	Utilisez ces procédures pour désactiver les fichiers `.forward` ou modifier le chemin de recherche du fichier `.forward`. Apprenez également à autoriser les utilisateurs à utiliser le fichier `.forward` en créant et alimentant le fichier `/etc/shells`.	"Administration des fichiers `.forward` (liste des tâches)" à la page 331
Procédures de dépannage et conseils pour les services de messagerie	Utilisez ces procédures et conseils pour résoudre les problèmes rencontrés avec votre service de messagerie. Apprenez à tester la configuration de la messagerie, à vérifier les alias de messagerie, à tester les ensembles de règles `sendmail`, à vérifier les connexions à d'autres systèmes et à consigner les messages. Apprenez également à rechercher d'autres informations de diagnostic pour la messagerie.	"Procédures de dépannage et conseils pour les services de messagerie (liste des tâches)" à la page 334

Tâche	Description	Voir
Résolution des messages d'erreur	Utilisez les informations de cette section pour résoudre certains messages d'erreur relatifs à la messagerie.	"Résolution des messages d'erreur" à la page 339

Planification de votre système de messagerie

La liste ci-après décrit certains points à prendre en compte lors du processus de planification.

- Déterminez le type de configuration de messagerie qui répond à vos besoins. Cette section décrit deux types de base de configuration de la messagerie et répertorie brièvement ce que vous devez paramétrer dans chacune d'entre elles. Consultez cette section si vous avez besoin de configurer un nouveau système de messagerie ou si vous développez un système existant. Le premier type de configuration est décrit dans la section "Courrier local uniquement" à la page 293 et le deuxième dans la section "Courrier local et connexion à distance" à la page 295.
- Si nécessaire, choisissez les systèmes qui devront agir en tant que serveurs de courrier, hôtes de messagerie et passerelles de messagerie.
- Créez une liste de tous les clients de messagerie pour lesquels vous fournissez des services et incluez l'emplacement de leurs boîtes à lettres. Cette liste peut vous aider lorsque vous êtes prêt à créer les alias de messagerie de vos utilisateurs.
- Décidez comment mettre à jour les alias et transférer les messages électroniques. Vous pouvez configurer une boîte à lettres d'`alias` en tant qu'emplacement de destination des demandes de transfert de courrier des utilisateurs. Les utilisateurs peuvent également utiliser cette boîte à lettres pour envoyer les demandes de modifications à apporter à leurs alias de messagerie par défaut. Si votre système utilise NIS ou NIS+, vous pouvez administrer le transfert de courrier en lieu et place des utilisateurs. La section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 propose une liste des tâches qui sont liées à la définition d'alias. La section "Administration des fichiers `.forward` (liste des tâches)" à la page 331 dresse une liste des tâches relatives à la gestion des fichiers `.forward`.

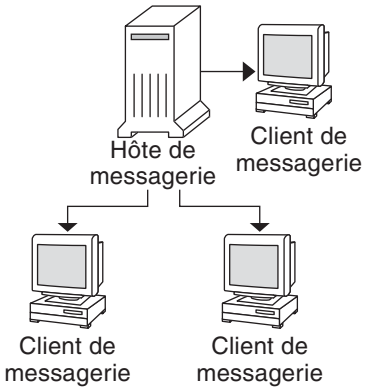
Une fois le processus de planification terminé, configurez les systèmes sur votre site pour effectuer les fonctions qui sont décrites dans la section "Configuration des services de messagerie (liste des tâches)" à la page 296. Pour plus d'informations sur les tâches, reportez-vous à la section "Liste des tâches pour les services de messagerie" à la page 291.

Courrier local uniquement

La configuration de messagerie la plus simple, telle qu'illustrée à la Figure 13–1, se compose d'au moins deux stations de travail connectées à un hôte de messagerie. Le courrier est uniquement

local. Tous les clients stockent le courrier sur leurs disques locaux et agissent en tant que serveurs de courrier. Les adresses e-mail sont analysées à l'aide des fichiers `/etc/mail/aliases`.

FIGURE 13–1 Configuration du courrier local



Pour ce type de configuration de messagerie, vous avez besoin des éléments suivants.

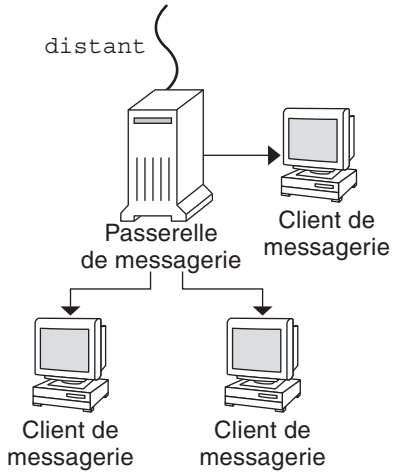
- Le fichier `/etc/mail/sendmail.cf` par défaut, qui ne nécessite aucune modification, sur chaque système client de messagerie.
- Un serveur désigné en tant qu'hôte de messagerie. Si vous exécutez NIS ou NIS+, vous pouvez effectuer cette désignation en ajoutant `mailhost.`*domain-name* au fichier `/etc/hosts` placé sur l'hôte de messagerie. Si vous exécutez un autre service de noms, tel que DNS ou LDAP, vous devez fournir des informations supplémentaires dans le fichier `/etc/hosts`. Reportez-vous à la section "Configuration d'un hôte de messagerie" à la page 301.
- Si vous utilisez un service de noms autre que NIS ou NIS+, vous devez d'abord faire correspondre les fichiers `/etc/mail/aliases` sur n'importe quel système doté d'une boîte à lettres locale.
- Un espace suffisant dans `/var/mail` sur chaque système client de messagerie pour contenir les boîtes à lettres.

Pour plus d'informations sur les tâches de configuration de votre service de messagerie, reportez-vous à la section "Configuration des services de messagerie" à la page 296. Si vous recherchez une procédure liée à la configuration de votre service de messagerie, reportez-vous à la section "Configuration des services de messagerie (liste des tâches)" à la page 296.

Courrier local et connexion à distance

La configuration de messagerie la plus répandue pour un petit réseau est illustrée à la Figure 13–2. Un système inclut le serveur de courrier, l'hôte de messagerie et la passerelle de messagerie qui fournit la connexion à distance. Le courrier est distribué à l'aide des fichiers `/etc/mail/aliases` sur la passerelle de messagerie. Aucun service de noms n'est requis.

FIGURE 13–2 Configuration du courrier local avec une connexion UUCP



Dans cette configuration, vous pouvez supposer que les clients de messagerie montent leurs fichiers de courrier de `/var/mail` sur l'hôte de messagerie. Pour ce type de configuration de messagerie, vous avez besoin des éléments suivants.

- Le fichier `/etc/mail/sendmail.cf` par défaut sur chaque système client de messagerie. Ce fichier n'a pas besoin d'aucune modification.
- Un serveur désigné en tant qu'hôte de messagerie. Si vous exécutez NIS ou NIS+, vous pouvez effectuer cette désignation en ajoutant `mailhost.`*domain-name* au fichier `/etc/hosts` placé sur l'hôte de messagerie. Si vous exécutez un autre service de noms, tel que DNS ou LDAP, vous devez fournir des informations supplémentaires dans le fichier `/etc/hosts`. Reportez-vous à la section "Configuration d'un hôte de messagerie" à la page 301.
- Si vous utilisez un service de noms autre que NIS ou NIS+, vous devez d'abord faire correspondre les fichiers `/etc/mail/aliases` sur n'importe quel système doté d'une boîte à lettres locale.
- Un espace suffisant dans `/var/mail` sur le serveur de courrier pour contenir les boîtes à lettres client.

Pour plus d'informations sur les tâches de configuration de votre service de messagerie, reportez-vous à la section "Configuration des services de messagerie" à la page 296. Si vous recherchez une procédure liée à la configuration de votre service de messagerie, reportez-vous à la section "Configuration des services de messagerie (liste des tâches)" à la page 296.

Configuration des services de messagerie (liste des tâches)

Le tableau suivant décrit les procédures relatives à la configuration des services de messagerie.

Tâche	Description	Voir
Configuration d'un serveur de courrier	Étapes pour permettre à un serveur d'acheminer le courrier	"Configuration d'un serveur de courrier" à la page 297
Configuration d'un client de messagerie	Étapes pour permettre à un utilisateur de recevoir le courrier	"Configuration d'un client de messagerie" à la page 299
Configuration d'un hôte de messagerie	Étapes pour établir un hôte de messagerie capable de résoudre les adresses e-mail	"Configuration d'un hôte de messagerie" à la page 301
Configuration d'une passerelle de messagerie	Étapes pour gérer la communication avec les réseaux en dehors de votre domaine	"Configuration d'une passerelle de messagerie" à la page 303
Utilisation d'un DNS avec `sendmail`	Étapes pour activer les recherches d'hôtes DNS	"Utilisation de DNS avec `sendmail`" à la page 304

Configuration des services de messagerie

Vous pouvez facilement configurer un service de messagerie si votre site n'établit pas de connexion avec des services de messagerie en dehors de votre entreprise ou si votre entreprise se trouve dans un domaine unique.

Deux types de configuration sont nécessaires pour le courrier local. Pour une représentation de ces configurations, reportez-vous à la Figure 13–1 de la section "Courrier local uniquement" à la page 293. Deux configurations supplémentaires sont nécessaires pour la communication avec des réseaux situés à l'extérieur de votre domaine. Pour une représentation de ces configurations, reportez-vous à la Figure 12–1 de la section "Présentation des composants matériels" à la page 288 ou à la Figure 13–2 de la section "Courrier local et connexion à distance" à la page 295. Vous pouvez combiner ces configurations sur le même système ou fournir ces configurations sur des systèmes distincts. Par exemple, si les fonctions de vos serveur de courrier et hôte de messagerie sont sur le même système, suivez les instructions de cette section pour configurer ce système en tant qu'hôte de messagerie. Suivez ensuite les instructions de cette section pour configurer le même système en tant que serveur de courrier.

Remarque – Les procédures suivantes de configuration d'un serveur de courrier et d'un client de messagerie s'appliquent lorsque les boîtes à lettres sont montées via NFS. Cependant, les boîtes à lettres sont généralement conservées dans des répertoires `/var/mail` montés localement, ce qui rend ces procédures inutiles.

Configuration d'un serveur de courrier

Aucune étape particulière n'est nécessaire pour configurer un serveur de courrier servant uniquement le courrier pour les utilisateurs locaux. L'utilisateur doit disposer d'une entrée dans le fichier de mot de passe ou dans l'espace de noms. En outre, pour le courrier à distribuer, l'utilisateur doit avoir un répertoire personnel local pour la vérification du fichier `~/.forward`. Pour cette raison, les serveurs d'annuaire personnel sont souvent configurés en tant que serveur de courrier. La section "Composants matériels" à la page 355 du Chapitre 14, "Services de messagerie (référence)" fournit plus d'informations sur le serveur de courrier.

Le serveur de courrier peut acheminer le courrier pour de nombreux clients de messagerie. Ce type de serveur doit disposer d'un espace de spool adéquat pour les boîtes à lettres client.

Remarque – Le programme `mail.local` crée automatiquement des boîtes à lettres dans le répertoire `/var/mail` la première fois qu'un message est transmis. Vous n'avez pas besoin de créer des boîtes à lettres individuelles pour vos clients de messagerie.

Pour que les clients accèdent à leurs boîtes à lettres, le répertoire `/var/mail` doit être disponible pour le montage à distance. Sinon, un service comme le protocole POP (Post Office Protocol) ou le protocole IMAP (Internet Message Access Protocol) doit être disponible à partir du serveur. La tâche suivante vous montre comment configurer un serveur de courrier à l'aide du répertoire `/var/mail`. Cette section ne donne aucune instruction de configuration pour les protocoles POP ou IMAP.

Pour la tâche suivante, assurez-vous que le fichier `/etc/dfs/dfstab` montre que le répertoire `/var/mail` est exporté.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Vérifiez si le répertoire `/var/mail` est disponible pour l'accès à distance.

```
# share
```

Si le répertoire `/var/mail` est listé, passez à l'étape 5.

Si le répertoire `/var/mail` n'apparaît pas ou si aucune liste ne s'affiche, passez à la sous-étape appropriée.

a. (Facultatif) Si aucune liste ne s'affiche, démarrez les services NFS.

Suivez la procédure, "Configuration du partage automatique des systèmes de fichiers" à la page 87, pour utiliser le répertoire `/var/mail` pour démarrer les services NFS.

b. (Facultatif) Si le répertoire `/var/mail` n'est pas inclus dans la liste, ajoutez-le à `/etc/dfs/dfstab`.

Ajoutez la ligne de commande suivante au fichier `/etc/dfs/dfstab`.

```
share -F nfs -o rw /var/mail
```

4 Rendez le système de fichiers disponible au montage.

```
# shareall
```

5 Assurez-vous que votre service de noms a été démarré.

a. (Facultatif) Si vous exécutez NIS, utilisez cette commande.

```
# ypwhich
```

Pour plus d'informations, reportez-vous à la page de manuel `ypwhich(1)`.

b. (Facultatif) Si vous exécutez NIS+, utilisez cette commande.

```
# nisls
```

Pour plus d'informations, reportez-vous à la page de manuel `nisls(1)`.

c. (Facultatif) Si vous exécutez DNS, utilisez cette commande.

```
# nslookup hostname
```

hostname Utilisez votre nom d'hôte.

Pour plus d'informations, reportez-vous à la page de manuel `nslookup(1M)`.

d. (Facultatif) Si vous exécutez LDAP, utilisez cette commande.

```
# ldaplist
```

Pour plus d'informations, reportez-vous à la page de manuel `ldaplist(1)`.

6 Redémarrez `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

Configuration d'un client de messagerie

Un client de messagerie est un utilisateur de services de messagerie avec une boîte à lettres sur un serveur de courrier. En outre, le client de messagerie possède un alias de messagerie dans le fichier `/etc/mail/aliases` qui pointe vers l'emplacement de la boîte à lettres.

Remarque – Vous pouvez également effectuer la tâche de configuration d'un client de messagerie à l'aide d'un service, tel que le protocole POP (Post Office Protocol) ou le protocole IMAP (Internet Message Access Protocol). Cette section ne donne toutefois aucune instruction de configuration pour les protocoles POP ou IMAP.

---

1 Connectez-vous en tant que superutilisateur (ou équivalent) sur le système du client de messagerie.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Vérifiez qu'un point de montage `/var/mail` existe sur le système du client de messagerie.

Le point de montage doit avoir été créé au cours du processus d'installation. Vous pouvez utiliser `ls` pour vous assurer que le système de fichiers existe. L'exemple suivant montre la réponse que vous recevez lorsque le système de fichiers n'a pas été créé.

```
# ls -l /var/mail
/var/mail not found
```

4 Assurez-vous qu'aucun fichier n'est présent dans le répertoire `/var/mail`.

Si des fichiers de courrier existent dans ce répertoire, vous devez les déplacer afin qu'ils ne soient pas pris en compte lorsque le répertoire `/var/mail` est monté à partir du serveur.

5 Montez le répertoire `/var/mail` à partir du serveur de courrier.

Vous pouvez monter le répertoire de courrier automatiquement ou à l'initialisation.

a. (Facultatif) Montez `/var/mail` automatiquement.

Ajoutez une entrée, telle que celle présentée ci-après, au fichier `/etc/auto_direct`.

```
/var/mail -rw,hard,actimeo=0 server:/var/mail
```

server Utilisez le nom du serveur assigné.

b. (Facultatif) Montez `/var/mail` à l'initialisation.

Ajoutez l'entrée suivante au fichier `/etc/vfstab`. Cette entrée autorise le répertoire `/var/mail` sur le serveur de courrier qui est spécifié pour monter le répertoire `/var/mail` local.

server`:/var/mail - /var/mail nfs - no rw,hard,actimeo=0`

La boîte à lettres du client est montée automatiquement chaque fois que le système est redémarré. Si vous ne réinitialisez pas le système, tapez la commande suivante pour monter la boîte à lettres client.

```
# mountall
```

Attention – Pour que le verrouillage et l'accès à la boîte à lettres fonctionnent correctement, vous devez inclure l'option `actimeo=0` lors du montage d'une messagerie à partir d'un serveur NFS.

6 Mettez à jour le fichier `/etc/hosts`.

Modifiez le fichier `/etc/hosts` et ajoutez une entrée pour le serveur de courrier. Cette étape n'est pas nécessaire si vous utilisez un service de noms.

```
# cat /etc/hosts
#
# Internet host table
#
..
IP-address      mailhost  mailhost  mailhost.example.com
```

IP-address Utilisez les adresses IP assignées.

example.com Utilisez le domaine assigné.

mailhost Utilisez l'hôte de messagerie assigné.

Pour plus d'informations, reportez-vous à la page de manuel `hosts(4)`.

7 Ajoutez une entrée pour le client à l'un des fichiers d'alias.

Pour obtenir la liste des tâches sur l'administration des fichiers d'alias de messagerie, reportez-vous à la section “Administration des fichiers d'alias de messagerie (liste des tâches)” à la page 315. Notez que le programme `mail.local` crée automatiquement des boîtes à lettres dans le répertoire `/var/mail` la première fois qu'un message est transmis. Vous n'avez pas besoin de créer des boîtes à lettres individuelles pour vos clients de messagerie.

8 Redémarrez `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

Configuration d'un hôte de messagerie

Un hôte de messagerie résout les adresses e-mail et réachemine le courrier au sein de votre domaine. Un bon candidat pour un hôte de messagerie est un système qui fournit à votre réseau une connexion à distance ou qui connecte votre réseau à un domaine parent. La procédure ci-après illustre la configuration d'un hôte de messagerie.

1 Connectez-vous en tant que superutilisateur (ou équivalent) sur le système de l'hôte de messagerie.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Vérifiez la configuration du nom d'hôte.

Exécutez le script `check-hostname` pour vérifier que `sendmail` peut identifier le nom d'hôte complet de ce serveur.

```
% /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

Si ce script ne parvient pas à identifier le nom d'hôte complet, vous devez ajouter ce dernier en tant que premier alias de l'hôte dans le fichier `/etc/hosts`.

4 Mettez à jour le fichier `/etc/hosts`.

Choisissez l'étape qui correspond à votre cas.

a. (Facultatif) Si vous utilisez NIS ou NIS+, modifiez le fichier `/etc/hosts` sur le système qui sera le nouvel hôte de messagerie.

Ajoutez les mots `mailhost` et `mailhost.`*domain* après l'adresse IP et le nom du système de l'hôte de messagerie.

IP-address mailhost `mailhost mailhost.`*domain* `loghost`

IP-address	Utilisez l'adresse IP assignée.
mailhost	Utilisez le nom du système de l'hôte de messagerie.
domain	Utilisez le nom de domaine développé.

Le système est maintenant défini en tant qu'hôte de messagerie. Le domaine *domain* doit être identique à la chaîne qui est donnée en tant que nom de sous-domaine dans la sortie de la commande suivante.

```
% /usr/lib/sendmail -bt -d0 </dev/null
Version 8.13.1+Sun
 Compiled with: LDAPMAP MAP_REGEX LOG MATCHGECOS MIME7TO8 MIME8TO7
                NAMED_BIND NDBM NETINET NETINET6 NETUNIX NEWDB NIS
                NISPLUS QUEUE SCANF SMTP USERDB XDEBUG

============ SYSTEM IDENTITY (after readcf) ============
      (short domain name) $w = phoenix
  (canonical domain name) $j = phoenix.example.com
         (subdomain name) $m = example.com
              (node name) $k = phoenix
========================================================
```

Reportez-vous à l'exemple suivant qui montre à quoi le fichier `hosts` doit ressembler après ces modifications.

```
# cat /etc/hosts
#
# Internet host table
#
172.31.255.255   localhost
192.168.255.255  phoenix mailhost mailhost.example.com loghost
```

b. (Facultatif) Si vous n'utilisez pas NIS ou NIS+, modifiez le fichier `/etc/hosts` sur chaque système du réseau.

Créez l'entrée suivante.

IP-address *mailhost* `mailhost` *mailhost*`.`*domain* `loghost`

5 Redémarrez `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

6 Testez votre configuration de messagerie.

Pour obtenir des instructions, reportez-vous à la section “Test de la configuration de la messagerie” à la page 335.

Remarque – Pour plus d'informations sur les hôtes de messagerie, reportez-vous à la section “Composants matériels” à la page 355 du Chapitre 14, “Services de messagerie (référence)”.

Configuration d'une passerelle de messagerie

Une passerelle de messagerie gère la communication avec les réseaux situés en dehors de votre domaine. Le logiciel de messagerie sur la passerelle de messagerie d'envoi peut correspondre à celui sur le système de réception.

Un système attaché à Ethernet et aux lignes téléphoniques est un candidat pour une passerelle de messagerie. Tout comme l'est un système configuré en tant que routeur vers Internet. Vous pouvez configurer l'hôte de messagerie ou un autre système en tant que passerelle de messagerie. Vous pouvez choisir de configurer plusieurs passerelles de messagerie pour votre domaine. Si vous disposez de connexions UUCP (UNIX-to-UNIX Copy Program), vous devez configurer le(s) système(s) doté(s) des connexions UUCP en tant que passerelle de messagerie.

1 **Connectez-vous en tant que superutilisateur (ou équivalent) sur la passerelle de messagerie.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Arrêtez `sendmail`.**

```
# svcadm disable -t network/smtp:sendmail
```

3 **Vérifiez la configuration du nom d'hôte.**

Exécutez le script `check-hostname` pour vérifier que `sendmail` peut identifier le nom d'hôte complet de ce serveur.

```
# /usr/sbin/check-hostname
hostname phoenix OK: fully qualified as phoenix.example.com
```

Si ce script ne parvient pas à identifier le nom d'hôte complet, vous devez ajouter ce dernier en tant que premier alias de l'hôte dans le fichier `/etc/hosts`. Si vous avez besoin d'aide pour procéder à cette étape, reportez-vous à l'Étape 4 de la section "Configuration d'un hôte de messagerie" à la page 301.

4 **Assurez-vous que votre service de noms a été démarré.**

a. **(Facultatif) Si vous exécutez NIS, utilisez cette commande.**

```
# ypwhich
```

Pour plus d'informations, reportez-vous à la page de manuel `ypwhich(1)`.

b. **(Facultatif) Si vous exécutez NIS+, utilisez cette commande.**

```
# nisls
```

Pour plus d'informations, reportez-vous à la page de manuel `nisls(1)`.

c. (Facultatif) Si vous exécutez DNS, utilisez cette commande.

```
# nslookup hostname
```

hostname Utilisez votre nom d'hôte.

Pour plus d'informations, reportez-vous à la page de manuel `nslookup(1M)`.

d. (Facultatif) Si vous exécutez LDAP, utilisez cette commande.

```
# ldaplist
```

Pour plus d'informations, reportez-vous à la page de manuel `ldaplist(1)`.

5 Redémarrez `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

6 Testez votre configuration de messagerie.

Pour obtenir des instructions, reportez-vous à la section "Test de la configuration de la messagerie" à la page 335.

Remarque – Pour plus d'informations sur la passerelle de messagerie, reportez-vous à la section "Composants matériels" à la page 355 du Chapitre 14, "Services de messagerie (référence)".

▼ Utilisation de DNS avec `sendmail`

Le service de noms DNS ne prend pas en charge les alias d'individus. Ce service de noms prend en charge les alias d'hôtes ou de domaines qui utilisent les enregistrements Mail eXchanger (MX) et `CNAME`. Vous pouvez spécifier les noms d'hôte et/ou de domaine dans la base de données DNS. Pour plus d'informations sur la commande `sendmail` et DNS, reportez-vous à la section "Interactions de `sendmail` avec des services de noms" à la page 378 du Chapitre 14, "Services de messagerie (référence)" ou au *Guide d'administration système : Services d'annuaire et de nommage (DNS, NIS et LDAP)*.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Activez les recherches d'hôtes DNS (NIS+ uniquement).

Modifiez le fichier `/etc/nsswitch.conf` et supprimez le caractère `#` de la définition `hosts` qui inclut l'indicateur `dns`. L'entrée de l'hôte doit inclure l'indicateur `dns`, comme le montre l'exemple suivant, pour que les alias de l'hôte DNS soient utilisés.

```
# grep hosts /etc/nsswitch.conf
#hosts:     nisplus [NOTFOUND=return] files
```

```
hosts:      dns nisplus [NOTFOUND=return] files
```

3 **Vérifiez la présence des entrées `mailhost` et `mailhost.`*domain*.**

Utilisez la commande `nslookup` pour vous assurer qu'une entrée existe pour `mailhost` et `mailhost.`*domain* dans la base de données DNS. Pour plus d'informations, reportez-vous à la page de manuel `nslookup(1M)`.

Modification de la configuration sendmail (liste des tâches)

Tâche	Description	Voir
Création d'un fichier de configuration `sendmail`	Utilisez cette procédure pour modifier votre fichier `sendmail.cf`. Un exemple d'activation du masquerading de domaine est également inclus.	"Création d'un fichier `sendmail.cf`" à la page 306
Configuration d'un hôte virtuel	Utilisez cette procédure pour configurer sendmail pour que le courrier soit accepté pour plus d'un domaine.	"Configuration d'un hôte virtuel" à la page 307
Configuration de la reconstruction automatique du fichier de configuration sendmail	Utilisez cette procédure pour modifier le service sendmail afin que les fichiers de configuration `sendmail.cf` et `submit.mc` soient automatiquement reconstruits après une mise à niveau.	"Reconstruction automatique d'un fichier de configuration" à la page 308
Exécution de `sendmail` en mode ouvert	Utilisez cette procédure pour modifier les propriétés du service sendmail afin d'activer le mode ouvert.	"Utilisation de `sendmail` en mode ouvert" à la page 308
Configuration de SMTP pour utiliser TLS (Transport Layer Security)	Utilisez cette procédure pour activer les connexions sécurisées SMTP avec TLS.	"Configuration de SMTP pour utiliser le protocole TLS" à la page 309
Gestion de la distribution du courrier à l'aide d'une autre configuration	Utilisez cette procédure pour éviter d'éventuels problèmes de distribution du courrier qui peuvent se produire si le démon principal est désactivé.	"Gestion de la distribution du courrier à l'aide d'une autre configuration de `sendmail.cf`" à la page 314

Modification de la configuration sendmail

La section "Création d'un fichier `sendmail.cf`" à la page 306 vous montre comment créer le fichier de configuration. Bien que vous puissiez toujours utiliser des versions plus anciennes des fichiers `sendmail.cf`, il est recommandé d'utiliser le nouveau format.

Pour plus de détails, reportez-vous à la documentation suivante.

- Le fichier `/etc/mail/cf/README` fournit une description complète du processus de configuration.
- Le site Web `http://www.sendmail.org` offre des informations en ligne à propos de la configuration `sendmail`.
- Les sections "Versions du fichier de configuration" à la page 346 et "Fichier de configuration `sendmail`" à la page 370 du Chapitre 14, "Services de messagerie (référence)" fournissent des indications.
- La section "Macros de configuration `m4` supplémentaires et révisées à partir de la version 8.12 de `sendmail`" à la page 400 est également utile.

▼ Création d'un fichier `sendmail.cf`

La procédure suivante vous montre comment créer un fichier de configuration.

Remarque – Le fichier `/usr/lib/mail/cf/main-v7sun.mc` est désormais `/etc/mail/cf/cf/sendmail.mc`.

---

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Arrêtez `sendmail`.

```
# svcadm disable -t network/smtp:sendmail
```

3 Faites une copie des fichiers de configuration que vous modifiez.

```
# cd /etc/mail/cf/cf
# cp sendmail.mc myhost.mc
```

myhost Sélectionnez un nouveau nom pour votre fichier `.mc`.

4 Modifiez les nouveaux fichiers de configuration (par exemple, *myhost*`.mc`), si nécessaire.

Par exemple, ajoutez la ligne de commande suivante pour activer le masquerading du domaine.

```
# cat myhost.mc
..
MASQUERADE_AS('host.domain')
```

host.domain Utilisez le nom d'hôte et le nom de domaine souhaités.

Dans cet exemple, la commande `MASQUERADE_AS` entraîne l'étiquetage du courrier envoyé pour indiquer sa provenance de *host.domain*, plutôt que de `$j`.

5 **Créez le fichier de configuration en utilisant `m4`.**

```
# /usr/ccs/bin/make myhost.cf
```

6 **Testez le nouveau fichier de configuration en utilisant l'option `-C` pour spécifier le nouveau fichier.**

```
# /usr/lib/sendmail -C myhost.cf -v testaddr </dev/null
```

Bien que cette commande affiche des messages, elle envoie un message à `testaddr`. Seul le courrier sortant peut être testé sans redémarrer le service `sendmail` sur le système. Pour les systèmes qui ne gèrent pas encore le courrier, utilisez la procédure de test complet de la section "Test de la configuration de la messagerie" à la page 335.

7 **Installez le nouveau fichier de configuration après avoir fait une copie de l'original.**

```
# cp /etc/mail/sendmail.cf /etc/mail/sendmail.cf.save
# cp myhost.cf /etc/mail/sendmail.cf
```

8 **Redémarrez le service `sendmail`.**

```
# svcadm enable network/smtp:sendmail
```

Configuration d'un hôte virtuel

Si vous devez assigner plusieurs adresses IP à un hôte, reportez-vous au site Web : `http://www.sendmail.org/tips/virtualHosting`. Ce site fournit des instructions complètes sur la façon d'utiliser `sendmail` pour configurer un hôte virtuel. Cependant, à la section "Sendmail Configuration", n'effectuez pas l'étape 3b, comme présenté ci-dessous.

```
# cd sendmail-VERSION/cf/cf
# ./Build mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

Effectuez plutôt les étapes suivantes pour le système d'exploitation Solaris.

```
# cd /etc/mail/cf/cf
# /usr/ccs/bin/make mailserver.cf
# cp mailserver.cf /etc/mail/sendmail.cf
```

mailserver Utilisez le nom du fichier `.cf`.

La section "Modification de la configuration sendmail" à la page 305 présente les trois mêmes étapes dans le cadre du processus de création.

Une fois que vous avez généré votre fichier `/etc/mail/sendmail.cf`, vous pouvez passer aux étapes suivantes pour créer une table d'utilisateurs virtuels.

▼ Reconstruction automatique d'un fichier de configuration

Si vous avez créé votre propre copie de `sendmail.cf` ou `submit.cf`, le fichier de configuration n'est pas remplacé pendant le processus de mise à niveau. La procédure suivante présente la configuration des propriétés du service sendmail pour que le fichier `sendmail.cf` soit automatiquement reconstruit. Pour obtenir des instructions sur la création automatique du fichier de configuration `submit.cf` , reportez-vous à l'Exemple 13–1. Vous pouvez combiner ces procédures si vous avez besoin de construire les deux fichiers.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Définissez les propriétés sendmail.

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/path_to_sendmail_mc=/etc/mail/cf/cf/myhost.mc
svc:/network/smtp:sendmail> quit
```

3 Actualisez et redémarrez le service sendmail.

La première commande transmet les modifications dans l'instantané en cours d'exécution. La deuxième commande redémarre le service sendmail à l'aide des nouvelles options.

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

Exemple 13–1 Établissement d'une reconstruction automatique de `submit.cf`

Cette procédure permet de configurer le service sendmail, de manière à ce que le fichier de configuration `submit.mc` soit reconstruit automatiquement.

```
# svccfg -s sendmail-client:default
svc:/network/smtp:sendmail> setprop config/path_to_submit_mc=/etc/mail/cf/cf/submit-myhost.mc
svc:/network/smtp:sendmail> exit
# svcadm refresh svc:/network/sendmail-client
# svcadm restart svc:/network/sendmail-client
```

▼ Utilisation de `sendmail` en mode ouvert

Dans la version Solaris 10, le service sendmail a été modifié de façon à ce qu'il s'exécute par défaut en mode local uniquement. Le mode local uniquement signifie que seul le courrier issu de l'hôte local est accepté. Les messages provenant de n'importe quel autre système sont rejetés. Les versions antérieures étaient configurées pour accepter le courrier entrant provenant de tous

les systèmes distants, cette configuration étant connue comme étant le mode ouvert. Pour utiliser le mode ouvert, utilisez la procédure suivante.

Attention – L'exécution de sendmail en mode local uniquement est beaucoup plus sûre que son exécution en mode ouvert. Assurez-vous que vous connaissez les risques de sécurité potentiels si vous suivez cette procédure.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Définissez les propriétés sendmail.**

```
# svccfg -s sendmail
svc:/network/smtp:sendmail> setprop config/local_only = false
svc:/network/smtp:sendmail> quit
```

3. **Actualisez et redémarrez le service sendmail.**

```
# svcadm refresh svc:/network/smtp:sendmail
# svcadm restart svc:/network/smtp:sendmail
```

▼ Configuration de SMTP pour utiliser le protocole TLS

À partir de la version Solaris 10 1/06, SMTP peut utiliser le protocole TLS (Transport Layer Security) dans la version 8.13 de `sendmail`. Ce service aux serveurs et clients SMTP fournit des communications privées et authentifiées sur Internet, ainsi qu'une protection contre les écoutes clandestines et les pirates. Notez que ce service n'est pas activé par défaut.

La procédure suivante utilise des données d'exemple pour vous montrer comment configurer les certificats qui permettent à `sendmail` d'utiliser TLS. Pour plus d'informations, reportez-vous à la section "Prise en charge de l'exécution de SMTP avec TLS dans la version 8.13 de `sendmail`" à la page 384.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez `sendmail`.**

```
# svcadm disable -t network/smtp:sendmail
```

3 Configurez les certificats qui permettent à `sendmail` d'utiliser TLS.

a. Exécutez ce qui suit :

```
# cd /etc/mail
# mkdir -p certs/CA
# cd certs/CA
# mkdir certs crl newcerts private
# echo "01" > serial
# cp /dev/null index.txt
# cp /etc/sfw/openssl/openssl.cnf .
```

b. Utilisez l'éditeur de texte de votre choix pour faire passer la valeur `dir` située dans le fichier `openssl.cnf` de `/etc/sfw/openssl` à `/etc/mail/certs/CA`.

c. Utilisez l'outil de ligne de commande `openssl` pour mettre en œuvre TLS.

Notez que la ligne de commande suivante génère du texte interactif.

```
# openssl req -new -x509 -keyout private/cakey.pem -out cacert.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
.....................................++++++
.....................................++++++
writing new private key to 'private/cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

`req`	Cette commande crée et traite des demandes de certificats.
`-new`	Cette option de `req` génère une nouvelle demande de certificat.
`-x509`	Cette option de `req` crée un certificat autosigné.
`-keyout private/cakey.pem`	Cette option de `req` vous permet d'assigner `private/fichier.pem` en tant que nom de fichier pour la clé privée que vous venez de créer.

`-out cacert.pem`	Cette option de `req` vous permet d'assigner `cacert.pem` en tant que fichier de sortie.
`-days 365`	Cette option de `req` vous permet d'obtenir le certificat pour `365` jours. La valeur par défaut est `30`.
`-config openssl.cnf`	Cette option de `req` vous permet de spécifier `openssl.cnf` en tant que fichier de configuration.

Notez que cette commande requiert que vous fournissiez les informations suivantes :

- `Country Name` (nom du pays), comme `US`.
- `State or Province Name` (nom de l'État ou de la province), comme `California`.
- `Locality Name` (nom de la localité), comme `Menlo Park`.
- `Organization Name` (nom de l'organisation), comme `Sun Microsystems`.
- `Organizational Unit Name` (nom du service dans l'organisation), comme `Solaris` .
- `Common Name` (nom commun), qui correspond au nom d'hôte complet de la machine. Pour plus d'informations, reportez-vous à la page de manuel `check-hostname(1M)`.
- `Email Address` (adresse e-mail), comme `someuser@example.com`.

4 (Facultatif) Si vous avez besoin d'une nouvelle connexion sécurisée, créez un nouveau certificat et signez-le avec l'autorité de certification.

a. Créez un certificat.

```
# cd /etc/mail/certs/CA
# openssl req -nodes -new -x509 -keyout newreq.pem -out newreq.pem -days 365 \
-config openssl.cnf
Generating a 1024 bit RSA private key
..............++++++
..............++++++
writing new private key to 'newreq.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:California
Locality Name (eg, city) []:Menlo Park
Organization Name (eg, company) [Unconfigured OpenSSL Installation]:Sun Microsystems
Organizational Unit Name (eg, section) []:Solaris
Common Name (eg, YOUR name) []:somehost.somedomain.example.com
Email Address []:someuser@example.com
```

Cette commande requiert que vous fournissiez les mêmes informations que vous avez fournies à l'étape 3c.

Notez que dans cet exemple, le certificat et la clé privée se trouvent dans le fichier `newreq.pem`.

b. Signez le certificat avec l'autorité de certification.

```
# cd /etc/mail/certs/CA
# openssl x509 -x509toreq -in newreq.pem -signkey newreq.pem -out tmp.pem
Getting request Private Key
Generating certificate request
# openssl ca -config openssl.cnf -policy policy_anything -out newcert.pem -infiles tmp.pem
Using configuration from openssl.cnf
Enter pass phrase for /etc/mail/certs/CA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 1 (0x1)
        Validity
            Not Before: Jun 23 18:44:38 2005 GMT
            Not After : Jun 23 18:44:38 2006 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = California
            localityName              = Menlo Park
            organizationName          = Sun Microsystems
            organizationalUnitName    = Solaris
            commonName                = somehost.somedomain.example.com
            emailAddress              = someuser@example.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                93:D4:1F:C3:36:50:C5:97:D7:5E:01:E4:E3:4B:5D:0B:1F:96:9C:E2
            X509v3 Authority Key Identifier:
                keyid:99:47:F7:17:CF:52:2A:74:A2:C0:13:38:20:6B:F1:B3:89:84:CC:68
                DirName:/C=US/ST=California/L=Menlo Park/O=Sun Microsystems/OU=Solaris/\
                CN=someuser@example.com/emailAddress=someuser@example.com
                serial:00

Certificate is to be certified until Jun 23 18:44:38 2006 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
# rm -f tmp.pem
```

Dans cet exemple, le fichier `newreq.pem` contient le certificat et la clé privée non signés. Le fichier `newcert.pem` contient le certificat signé.

Utilitaire `x509` — Affiche les informations sur les certificats, convertit les certificats sous différentes formes et signe les demandes de certificats.

Application ca — Utilisée pour signer les demandes de certificats sous différentes formes et générer des listes de révocation de certificats (LRC).

5 **Activez `sendmail` pour utiliser les certificats en ajoutant les lignes suivantes à votre fichier `.mc`.**

```
define('confCACERT_PATH', '/etc/mail/certs')dnl
define('confCACERT', '/etc/mail/certs/CAcert.pem')dnl
define('confSERVER_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confSERVER_KEY', '/etc/mail/certs/MYkey.pem')dnl
define('confCLIENT_CERT', '/etc/mail/certs/MYcert.pem')dnl
define('confCLIENT_KEY', '/etc/mail/certs/MYkey.pem')dnl
```

Pour plus d'informations, reportez-vous à la section "Options du fichier de configuration pour l'exécution de SMTP avec TLS" à la page 385.

6 **Recréez et installez le fichier `sendmail.cf` dans le répertoire `/etc/mail`.**

Pour obtenir des instructions détaillées, reportez-vous à la section "Modification de la configuration sendmail" à la page 305.

7 **Créez des liens symboliques à partir des fichiers que vous avez créés avec `openssl` vers les fichiers que vous avez définis dans votre fichier `.mc`.**

```
# cd /etc/mail/certs
# ln -s CA/cacert.pem CAcert.pem
# ln -s CA/newcert.pem MYcert.pem
# ln -s CA/newreq.pem MYkey.pem
```

8 **Pour plus de sécurité, refusez les autorisations en lecture aux groupes (et autres) pour `MYkey.pem`.**

```
# chmod go-r MYkey.pem
```

9 **Utilisez un lien symbolique pour installer des certificats d'AC dans le répertoire assigné à `confCACERT_PATH`.**

```
# C=CAcert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

10 **Pour un système de messagerie sécurisé avec d'autres hôtes, installez leurs certificats d'hôte.**

a. **Copiez le fichier défini par l'option `confCACERT` de l'autre hôte dans `/etc/mail/certs/`*host.domain*`.cert.pem`.**

Remplacez *host.domain* par le nom d'hôte complet de l'autre hôte.

b. **Utilisez un lien symbolique pour installer des certificats d'AC dans le répertoire assigné à `confCACERT_PATH`.**

```
# C=host.domain.cert.pem
# ln -s $C 'openssl x509 -noout -hash < $C'.0
```

Remplacez *host.domain* par le nom d'hôte complet de l'autre hôte.

11 Redémarrez `sendmail`.

```
# svcadm enable network/smtp:sendmail
```

Exemple 13–2 En-tête de courrier `Received` :

Ce qui suit est un exemple de l'en-tête `Received` : pour le courrier sécurisé avec TLS.

```
Received: from his.example.com ([IPv6:2001:db8:3c4d:15::1a2f:1a2b])
        by her.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNUB8i242496
        (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:11 -0800 (PST)
Received: from her.example.com (her.city.example.com [192.168.0.0])
        by his.example.com (8.13.4+Sun/8.13.4) with ESMTP id j2TNU7cl571102
        version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=OK)
        for <janepc@her.example.com>; Tue, 29 Mar 2005 15:30:07 -0800 (PST)
```

Notez que la valeur de `verify` est `OK`, ce qui signifie que l'authentification a réussi. Pour plus d'informations, reportez-vous à la section "Macros pour l'exécution de SMTP avec TLS" à la page 387.

Voir aussi Les pages de manuel OpenSSL suivantes :

- openssl(1) (`http://www.openssl.org/docs/apps/openssl.html`).
- req(1) (`http://www.openssl.org/docs/apps/req.html`).
- x509(1) (`http://www.openssl.org/docs/apps/x509.html`).
- ca(1) (`http://www.openssl.org/docs/apps/ca.html`).

▼ Gestion de la distribution du courrier à l'aide d'une autre configuration de `sendmail.cf`

Pour faciliter le transport du courrier entrant et sortant, la nouvelle configuration par défaut de `sendmail` utilise un démon et un programme d'exécution de file d'attente client. Ce programme doit être en mesure de soumettre le courrier au démon sur le port SMTP local. Si le démon n'écoute pas sur le port SMTP, le courrier reste dans la file d'attente. Pour éviter ce problème, effectuez la tâche suivante. Pour plus d'informations sur le démon et le programme d'exécution de file d'attente client, et pour comprendre pourquoi vous devrez peut-être utiliser cette configuration alternative, reportez-vous à la section "Fichier de configuration `submit.cf` à partir de la version 8.12 de `sendmail`" à la page 393.

Cette procédure permet de s'assurer que le démon s'exécute uniquement pour accepter les connexions de l'hôte local.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez le service client `sendmail`.**

   ```
   # svcadm disable -t sendmail-client
   ```

3. **Faites une copie du fichier de configuration que vous modifiez.**

   ```
   # cd /etc/mail/cf/cf
   # cp submit.mc submit-myhost.mc
   ```

   myhost Sélectionnez un nouveau nom pour votre fichier `.mc`.

4. **Modifiez le nouveau fichier de configuration (par exemple, `submit-` *myhost*`.mc`).**

   Modifiez l'adresse IP de l'hôte d'écoute dans la définition `msp`.

   ```
   # grep msp submit-myhost.mc
   FEATURE('msp', '[#.#.#.#]')dnl
   ```

5. **Créez le fichier de configuration en utilisant `m4`.**

   ```
   # /usr/ccs/bin/make submit-myhost.cf
   ```

6. **Installez le nouveau fichier de configuration après avoir fait une copie de l'original.**

   ```
   # cp /etc/mail/submit.cf /etc/mail/submit.cf.save
   # cp submit-myhost.cf /etc/mail/submit.cf
   ```

7. **Redémarrez le service client `sendmail`.**

   ```
   # svcadm enable sendmail-client
   ```

Administration des fichiers d'alias de messagerie (liste des tâches)

Le tableau ci-dessous décrit les procédures d'administration des fichiers d'alias de messagerie. Pour plus d'informations sur ce sujet, reportez-vous à la section "Fichiers d'alias de messagerie" à la page 371 du Chapitre 14, "Services de messagerie (référence)".

Tâche	Description	Voir
Gestion des entrées d'alias dans une table `mail_aliases` NIS+	Si votre service de noms est NIS+, utilisez ces procédures pour gérer le contenu de votre table `mail_aliases`. Lancez une table `mail_aliases` NIS+.	"Initiation d'une table `mail_aliases` NIS+" à la page 317
	Répertoriez le contenu de la table `mail_aliases` NIS+. Cette procédure comprend des exemples de création de liste d'entrées individuelles et de correspondances partielles.	"Création d'une liste du contenu de la table `mail_aliases` NIS+" à la page 318
	Ajoutez des alias à la table `mail_aliases` NIS+ à partir de la ligne de commande.	"Ajout d'alias à la table `mail_aliases` NIS+ à partir de la ligne de commande" à la page 319
	Ajoutez des entrées en modifiant une table `mail_aliases` NIS+.	"Ajout d'entrées par la modification d'une table `mail_aliases` NIS+" à la page 320
	Modifiez des entrées dans une table `mail_aliases` NIS+. Cette procédure comprend un exemple de suppression d'une entrée.	"Modification d'entrées dans une table `mail_aliases` NIS+" à la page 321
Configuration d'une carte `mail.alias` NIS	Si votre service de noms est NIS, suivez ces instructions pour faciliter la définition d'alias avec une carte `mail.alias`.	"Configuration d'une carte `mail.alias` NIS" à la page 322
Configuration d'un fichier d'alias de messagerie locale	Si vous n'utilisez pas de service de noms (tel que NIS ou NIS+), suivez ces instructions afin de faciliter la définition d'alias avec le fichier `/etc/mail/aliases`.	"Configuration d'un fichier d'alias de messagerie locale" à la page 323
Création d'un fichier de configuration à clé	Suivez ces étapes pour faciliter la définition d'alias avec un fichier de configuration à clé.	"Création d'un fichier de configuration à clé" à la page 324
Configuration de l'alias `postmaster`	Utilisez les procédures décrites dans cette section pour gérer l'alias `postmaster`. Vous devez avoir cet alias.	"Gestion de l'alias `postmaster`" à la page 325

Administration des fichiers d'alias de messagerie

Les alias de messagerie doivent être uniques au sein d'un domaine. Cette section fournit les procédures de gestion des fichiers d'alias de messagerie. Alternativement, vous pouvez utiliser la fonction de liste de diffusion dans la console de gestion Solaris pour effectuer ces tâches sur la base de données d'alias.

En outre, vous pouvez créer des fichiers de base de données pour l'hôte de messagerie locale en utilisant `makemap`. Reportez-vous à la page de manuel `makemap(1M)`. L'utilisation de ces fichiers de base de données n'offre pas tous les avantages de l'utilisation d'un service de noms, tel que NIS ou NIS+. Toutefois, vous devriez être en mesure de récupérer les données à partir de ces fichiers de base de données locaux plus rapidement, car aucune recherche sur réseau n'est impliquée. Pour plus d'informations, reportez-vous aux sections "Interactions de `sendmail` avec des services de noms" à la page 378 et "Fichiers d'alias de messagerie" à la page 371 du Chapitre 14, "Services de messagerie (référence)".

Choisissez parmi les procédures suivantes :

Initiation d'une table `mail_aliases` NIS+

Vous pouvez utiliser la commande `aliasadm` pour gérer les entrées d'une table NIS+. Pour créer une table, suivez les instructions ci-après. Pour plus d'informations, reportez-vous à la page de manuel `aliasadm(1M)`.

1 Soyez membre du groupe NIS+ propriétaire de la table ou devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Initiez une table NIS+.

```
# aliasadm -I
```

3 Ajoutez des entrées à la table.

- Pour ajouter deux ou trois alias, reportez-vous à la section "Ajout d'alias à la table `mail_aliases` NIS+ à partir de la ligne de commande" à la page 319.
- Pour ajouter plus de deux ou trois alias, reportez-vous à la section "Ajout d'entrées par la modification d'une table `mail_aliases` NIS+" à la page 320.

▼ Création d'une liste du contenu de la table `mail_aliases` NIS+

Pour voir la liste complète du contenu de la table, suivez ces instructions.

1 **Soyez membre du groupe NIS+ propriétaire de la table ou devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Dressez la liste de toutes les entrées dans l'ordre alphabétique, par alias.**

```
# aliasadm -l
```

Pour plus d'informations, reportez-vous à la page de manuel `aliasadm(1M)`.

Exemple 13–3 Insertion d'une entrée d'une table `mail_aliases` NIS+ dans une liste

Alternativement, vous pouvez utiliser la commande `aliasadm` pour répertorier des entrées individuelles. Une fois que vous avez terminé la première étape de cette procédure, saisissez ce qui suit :

```
# aliasadm -m ignatz
ignatz: ignatz@saturn # Alias for Iggy Ignatz
```

La commande correspond uniquement au nom d'alias complet, et non à des chaînes partielles. Vous ne pouvez pas utiliser des métacaractères, tels que `*` et `?`, avec `aliasadm -m`.

Exemple 13–4 Insertion de correspondances partielles d'une table `mail_aliases` NIS+ dans une liste

Vous pouvez également utiliser la commande `aliasadm` pour répertorier des correspondances partielles. Une fois que vous avez terminé la première étape de cette procédure, saisissez ce qui suit :

```
# aliasadm -l | grep partial-string
```

Remplacez *partial-string* par la chaîne souhaitée pour votre recherche.

▼ Ajout d'alias à la table `mail_aliases` NIS+ à partir de la ligne de commande

Pour ajouter deux ou trois alias à la table, suivez les instructions ci-dessous. Si vous ajoutez plus de deux ou trois alias, reportez-vous à la section "Ajout d'entrées par la modification d'une table `mail_aliases` NIS+" à la page 320.

1 Compilez une liste de chacun de vos clients de messagerie, de l'emplacement de leurs boîtes à lettres et des noms des systèmes de serveur de courrier.

2 Soyez membre du groupe NIS+ propriétaire de la table ou devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 (Facultatif) Si nécessaire, lancez une table NIS+.

Si vous êtes en train de créer une toute nouvelle table `mail_aliases` NIS+, vous devez d'abord lancer la table. Pour terminer cette tâche, reportez-vous à la section "Initiation d'une table `mail_aliases` NIS+" à la page 317.

4 Ajoutez des alias à la table.

Reportez-vous à cet exemple d'une entrée typique.

```
# aliasadm -a iggy iggy.ignatz@saturn "Iggy Ignatz"
```

La liste ci-après décrit l'entrée par rapport à l'exemple précédent.

`-a`	Option permettant d'ajouter un alias
`iggy`	Forme abrégée du nom d'alias
`iggy.ignatz@saturn`	Forme développée du nom d'alias
`"Iggy Ignatz"`	Nom de l'alias entre guillemets

5 Affichez l'entrée que vous avez créée et assurez-vous qu'elle est correcte.

```
# aliasadm -m alias
```

alias	Entrée créée

Pour plus d'informations, reportez-vous à la page de manuel `aliasadm`(1M).

▼ Ajout d'entrées par la modification d'une table `mail_aliases` NIS+

Vous pouvez utiliser la commande `aliasadm` pour gérer les entrées d'une table NIS+. Pour ajouter plus de deux ou trois alias à la table, suivez les instructions ci-après.

1 Compilez une liste de chacun de vos clients de messagerie, de l'emplacement de leurs boîtes à lettres et des noms des systèmes de serveur de courrier.

2 Soyez membre du groupe NIS+ propriétaire de la table ou devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 Affichez et modifiez la table d'alias.

```
# aliasadm -e
```

Cette commande affiche la table et vous permet de la modifier. L'éditeur que vous utilisez a été défini avec la variable d'environnement `$EDITOR`. Si cette variable n'est pas définie, `vi` est l'éditeur par défaut.

4 Utilisez le format suivant pour saisir chaque alias sur une ligne distincte.

alias`:` *expanded-alias* `# ["`*option*`" # "`*comments*`"]`

alias	Cette colonne reçoit la forme abrégée du nom d'alias.
expanded-alias	Cette colonne reçoit la forme développée du nom d'alias.
option	Cette colonne est réservée à une utilisation future.
comments	Cette colonne reçoit des commentaires sur des alias particuliers, tel qu'un nom d'alias.

Si vous laissez la colonne option vide, tapez une paire de guillemets (`""`) vide et ajoutez des commentaires.

L'ordre des entrées n'est pas important dans la table `mail_aliases` NIS+. La commande `aliasadm -l` trie la liste et affiche les entrées dans l'ordre alphabétique.

Pour plus d'informations, reportez-vous à la section "Fichiers d'alias de messagerie" à la page 371 et à la page de manuel `aliasadm`(1M).

▼ Modification d'entrées dans une table `mail_aliases` NIS+

Pour modifier des entrées de la table, suivez ces instructions.

1 Soyez membre du groupe NIS+ propriétaire de la table ou devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Affichez l'entrée d'alias.

```
# aliasadm -m alias
```

Remplacez *alias* par le nom d'alias assigné.

3 Modifiez l'entrée d'alias, si nécessaire.

```
# aliasadm -c alias expanded-alias [options comments]
```

alias	Si nécessaire, modifiez le nom de l'alias.
expanded-alias	Si nécessaire, modifiez le nom développé de l'alias.
options	Si nécessaire, modifiez l'option.
comments	Si nécessaire, modifiez le commentaire pour cette entrée.

Pour plus d'informations, reportez-vous à la page de manuel `aliasadm`(1M), ainsi qu'à la section "Fichiers d'alias de messagerie" à la page 371.

4 Affichez l'entrée que vous avez modifiée et assurez-vous qu'elle est correcte.

```
# aliasadm -m alias
```

Pour plus d'informations, reportez-vous à la page de manuel `aliasadm`(1M).

Exemple 13–5 Suppression d'entrées d'une table `mail_aliases` NIS+

Pour supprimer des entrées de la table, utilisez la syntaxe ci-dessous une fois que vous avez terminé la première étape de cette procédure :

```
# aliasadm -d alias
```

Remplacez *alias* par le nom de l'alias pour l'entrée que vous souhaitez supprimer.

▼ Configuration d'une carte `mail.alias` NIS

Utilisez la procédure suivante pour faciliter une définition d'alias avec une carte `mail.alias` NIS.

1 Compilez une liste de chacun de vos clients de messagerie, de l'emplacement de leurs boîtes à lettres et des noms des systèmes de serveur de courrier.

2 Devenez utilisateur `root` (ou équivalent) sur le serveur maître NIS.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3 Modifiez le fichier `/etc/mail/aliases` et créez les entrées suivantes.

a. Ajoutez une entrée pour chaque client de messagerie.

```
# cat /etc/mail/aliases
..
alias:expanded-alias
```

alias — Utilisez le nom d'alias court.

expanded-alias — Utilisez le nom d'alias complet (`user@host.domain.com`).

b. Assurez-vous que vous avez une entrée `Postmaster: root`.

```
# cat /etc/mail/aliases
..
Postmaster: root
```

c. Ajoutez un alias pour l'utilisateur `root`. Utilisez l'adresse e-mail de la personne désignée administrateur du courrier.

```
# cat /etc/mail/aliases
..
root: user@host.domain.com
```

user@host.domain.com — Utilisez l'adresse assignée de l'administrateur du courrier désigné.

4 Assurez-vous que le serveur maître NIS exécute un service de noms pour résoudre les noms d'hôte sur chaque serveur de courrier.

5 Passez au répertoire `/var/yp`.

```
# cd /var/yp
```

6 Appliquez la commande `make`.

```
# make
```

Les modifications apportées aux fichiers `/etc/hosts` et `/etc/mail/aliases` sont propagées aux systèmes esclaves NIS. Les modifications ne restent actives que pendant quelques minutes, au plus.

Configuration d'un fichier d'alias de messagerie locale

Utilisez la procédure suivante pour résoudre les alias avec un fichier d'alias de messagerie locale.

1. **Compilez une liste de chacun de vos utilisateurs et de l'emplacement de leurs boîtes à lettres.**

2. **Devenez utilisateur `root` (ou équivalent) sur le serveur de courrier.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

3. **Modifiez le fichier `/etc/mail/aliases` et créez les entrées suivantes.**

   a. **Ajoutez une entrée pour chaque utilisateur.**

      user1 : *user2@host.domain*

user1	Utilisez le nouveau nom d'alias.
user2@host.domain	Utilisez l'adresse réelle pour le nouvel alias.

   b. **Assurez-vous que vous avez une entrée `Postmaster: root`.**

      ```
      # cat /etc/mail/aliases
      ..
      Postmaster: root
      ```

   c. **Ajoutez un alias pour l'utilisateur `root`. Utilisez l'adresse e-mail de la personne désignée administrateur du courrier.**

      ```
      # cat /etc/mail/aliases
      ..
      root: user@host.domain.com
      ```

user@host.domain.com	Utilisez l'adresse assignée de l'administrateur du courrier désigné.

4. **Recréez la base de données d'alias.**

   ```
   # newaliases
   ```

   La configuration de l'option `AliasFile` dans `/etc/mail/sendmail.cf` détermine si cette commande génère sous forme binaire le fichier unique, `/etc/mail/aliases.db`, ou la paire de fichiers, `/etc/mail/aliases.dir` et `/etc/mail/aliases.pag`.

5 Effectuez l'une des étapes suivantes pour copier le ou les fichiers qui ont été générés.

a. (Facultatif) Copiez les fichiers `/etc/mail/aliases`, `/etc/mail/aliases.dir` et `/etc/mail/aliases.pag` dans chacun des autres systèmes.

Vous pouvez copier les trois fichiers en utilisant les commandes `rcp` ou `rdist`. Pour plus d'informations, reportez-vous aux pages de manuel `rcp(1)` ou `rdist(1)`. Sinon, vous pouvez créer un script dans ce but.

Lorsque vous copiez ces fichiers, vous n'avez pas besoin d'exécuter la commande `newaliases` sur chacun des autres systèmes. Cependant, n'oubliez pas de mettre à jour tous les fichiers `/etc/mail/aliases` chaque fois que vous ajoutez ou supprimez un client de messagerie.

b. (Facultatif) Copiez les fichiers `/etc/mail/aliases` et `/etc/mail/aliases.db` dans chacun des autres systèmes.

Vous pouvez copier ces fichiers en utilisant les commandes `rcp` ou `rdist`. Pour plus d'informations, reportez-vous aux pages de manuel `rcp(1)` ou `rdist(1)`. Sinon, vous pouvez créer un script dans ce but.

Lorsque vous copiez ces fichiers, vous n'avez pas besoin d'exécuter la commande `newaliases` sur chacun des autres systèmes. Cependant, n'oubliez pas de mettre à jour tous les fichiers `/etc/mail/aliases` chaque fois que vous ajoutez ou supprimez un client de messagerie.

▼ Création d'un fichier de configuration à clé

Pour créer un fichier de configuration à clé, suivez les instructions ci-après.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Créez un fichier d'entrée.

Les entrées peuvent avoir la syntaxe suivante.

old-name@newdomain.com *new-name@newdomain.com*
old-name@olddomain.com `error:nouser No such user here`
@olddomain.com `%1@`*newdomain.com*

old_name@newdomain.com	Utilisez le nom d'utilisateur qui était auparavant assigné avec le domaine qui vient d'être assigné.
new_name@newdomain.com	Utilisez l'adresse qui vient d'être assignée.

old_name@olddomain.com	Utilisez le nom d'utilisateur qui était auparavant assigné avec le domaine qui était assigné.
olddomain.com	Utilisez le domaine qui était assigné auparavant.
newdomain.com	Utilisez le domaine qui vient d'être assigné.

La première entrée redirige le courrier vers un nouvel alias. L'entrée suivante crée un message lorsqu'un alias erroné est utilisé. La dernière entrée redirige tous les courriers entrants de `olddomain` vers `newdomain`.

3 Créez le fichier de base de données.

```
# /usr/sbin/makemap maptype newmap < newmap
```

maptype	Sélectionnez un type de base de données, tel que `dbm`, `btree` ou `hash`.
newmap	Utilisez le nom du fichier d'entrée et la première partie du nom du fichier de base de données. Si le type de base de données `dbm` est sélectionné, les fichiers de base de données sont créés en utilisant des suffixes `.pag` et `.dir`. Pour les deux autres types de base de données, le nom du fichier est suivi par `.db`.

Gestion de l'alias `postmaster`

Chaque système doit être en mesure d'envoyer du courrier à une boîte à lettres `postmaster`. Vous pouvez créer un alias NIS ou NIS+ pour `postmaster`, ou vous pouvez créer un alias dans chaque fichier `/etc/mail/aliases` local. Reportez-vous à ces procédures.

- "Création d'un alias `postmaster` dans chaque fichier `/etc/mail/aliases` local" à la page 325
- "Création d'une autre boîte à lettres pour `postmaster`" à la page 326
- "Ajout de la boîte à lettres `postmaster` aux alias dans le fichier `/etc/mail/aliases`" à la page 327

▼ Création d'un alias `postmaster` dans chaque fichier `/etc/mail/aliases` local

Si vous créez l'alias `postmaster` dans chaque fichier `/etc/mail/aliases` local, suivez les instructions ci-dessous.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Affichez l'entrée `/etc/mail/aliases`.**

```
# cat /etc/mail/aliases
# Following alias is required by the mail protocol, RFC 2821
# Set it to the address of a HUMAN who deals with this system's
# mail problems.
Postmaster: root
```

3 **Modifiez le fichier `/etc/mail/aliases` de chaque système.**

Passez de l'utilisateur `root` à l'adresse e-mail de la personne désignée administrateur du courrier.

`Postmaster:` *mail-address*

mail-address Utilisez l'adresse assignée de la personne désignée administrateur du courrier.

4 **(Facultatif) Créez une boîte à lettres séparée pour l'administrateur du courrier.**

Vous pouvez créer une autre boîte à lettres pour l'administrateur du courrier pour maintenir son courrier séparé du courrier personnel. Si vous créez une autre boîte à lettres, utilisez l'adresse de la boîte à lettres à la place de l'adresse e-mail personnelle de l'administrateur du courrier lorsque vous modifiez les fichiers `/etc/mail/aliases`. Pour plus d'informations, reportez-vous à la section "Création d'une autre boîte à lettres pour `postmaster`" à la page 326.

▼ Création d'une autre boîte à lettres pour `postmaster`

Si vous souhaitez créer une autre boîte à lettres pour `postmaster`, suivez ces instructions.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez un compte utilisateur pour la personne désignée `postmaster`. Placez un astérisque (`*`) dans le champ de mot de passe.**

Pour plus d'informations sur l'ajout d'un compte utilisateur, reportez-vous à "Configuration des comptes utilisateur (liste des tâches) " du *Guide d'administration système : administration de base*.

3 **Une fois le courrier distribué, donnez au programme `mail` les autorisations en lecture et en écriture sur le nom de la boîte à lettres.**

`# mail -f` *postmaster*

postmaster Utilisez l'adresse assignée.

▼ Ajout de la boîte à lettres `postmaster` aux alias dans le fichier `/etc/mail/aliases`

Si vous ajoutez une boîte à lettres `postmaster` aux alias dans le fichier `/etc/mail/aliases`, suivez les instructions ci-dessous.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Ajoutez un alias pour l'utilisateur `root`. Utilisez l'adresse e-mail de la personne désignée administrateur du courrier.**

   ```
   # cat /etc/mail/aliases
   ..
   root: user@host.domain.com
   ```

   user@host.domain.com Utilisez l'adresse assignée de la personne désignée administrateur du courrier.

3. **Sur le système local de l'administrateur du courrier, créez une entrée dans le fichier `/etc/mail/aliases` qui définit le nom de l'alias. `sysadmin` est un exemple. Incluez également le chemin d'accès à la boîte à lettres locale.**

   ```
   # cat /etc/mail/aliases
   ..
   sysadmin: /usr/somewhere/somefile
   ```

   sysadmin Créez un nom pour un nouvel alias.

   /usr/somewhere/somefile Utilisez le chemin d'accès à la boîte à lettres locale.

4. **Recréez la base de données d'alias.**

   ```
   # newaliases
   ```

Administration des répertoires de file d'attente (liste des tâches)

Le tableau suivant décrit les procédures d'administration de la file d'attente de messages.

Tâche	Description	Voir
Affichage du contenu de la file d'attente de messages, `/var/spool/mqueue`	Utilisez cette procédure pour connaître le nombre de messages dans la file d'attente et la vitesse à laquelle ils sont effacés de la file d'attente.	"Affichage du contenu de la file d'attente de messages, `/var/spool/mqueue`" à la page 329
Traitement forcé de la file d'attente de messages, `/var/spool/mqueue`	Utilisez cette procédure pour acheminer les messages vers un système qui, auparavant, n'était pas en mesure de recevoir des messages.	"Traitement forcé de la file d'attente de messages, `/var/spool/mqueue`" à la page 329
Exécution d'un sous-ensemble de la file d'attente de messages, `/var/spool/mqueue`	Utilisez cette procédure pour forcer le traitement d'une sous-chaîne d'une adresse, tel qu'un nom d'hôte. Vous pouvez également utiliser cette procédure pour forcer la sortie d'un message hors de la file d'attente.	"Exécution d'un sous-ensemble de la file d'attente de messages, `/var/spool/mqueue`" à la page 330
Déplacement de la file d'attente de messages, `/var/spool/mqueue`	Utilisez cette procédure pour déplacer la file d'attente de messages.	"Déplacement de la file d'attente de messages, `/var/spool/mqueue`" à la page 330
Exécution de l'ancienne file d'attente de messages, `/var/spool/omqueue`	Utilisez cette procédure pour exécuter une ancienne file d'attente de messages.	"Exécution de l'ancienne file d'attente de messages, `/var/spool/omqueue` " à la page 331

Administration des répertoires de file d'attente

Cette section décrit certaines tâches utiles à l'administration de files d'attente. Pour plus d'informations sur la file d'attente du client uniquement, reportez-vous à la section "Fichier de configuration `submit.cf` à partir de la version 8.12 de `sendmail`" à la page 393. Pour obtenir d'autres informations connexes, vous pouvez vous reporter à la section "Fonctions de file d'attente supplémentaires à partir de la version 8.12 de `sendmail`" à la page 406.

Reportez-vous aux sections suivantes :

▼ Affichage du contenu de la file d'attente de messages, /var/spool/mqueue

- **Affichez le nombre de messages dans la file d'attente et la vitesse à laquelle ils sont effacés de la file d'attente.**

  Entrez la commande suivante :

  ```
  # /usr/bin/mailq | more
  ```

  Cette commande fournit les informations suivantes.

  - Les ID de file d'attente
  - La taille du message
  - La date à laquelle le message a rejoint la file d'attente
  - L'état du message
  - L'expéditeur et les destinataires

  En outre, cette commande vérifie désormais l'attribut d'autorisation, `solaris.admin.mail.mailq`. Si la vérification réussit, l'équivalent de la spécification de l'indicateur `-bp` avec `sendmail` est exécuté. Si la vérification échoue, un message d'erreur est imprimé. Par défaut, cet attribut d'autorisation est activé pour tous les utilisateurs. L'attribut d'autorisation peut être désactivé en modifiant l'entrée utilisateur dans `prof_attr`. Pour plus d'informations, reportez-vous aux pages de manuel pour `prof_attr(4)` et `mailq(1)`.

▼ Traitement forcé de la file d'attente de messages, /var/spool/mqueue

Utilisez cette procédure, par exemple, pour acheminer les messages vers un système qui, auparavant, n'était pas en mesure de recevoir des messages.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Forcez le traitement de la file d'attente et affichez l'avancement des tâches au fur et à mesure que la file d'attente est vidée.**

   ```
   # /usr/lib/sendmail -q -v
   ```

▼ Exécution d'un sous-ensemble de la file d'attente de messages, `/var/spool/mqueue`

Utilisez cette procédure, par exemple, pour forcer le traitement d'une sous-chaîne d'une adresse, telle qu'un nom d'hôte. Vous pouvez également utiliser cette procédure pour forcer le traitement d'un message de la file d'attente.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Exécutez un sous-ensemble de la file d'attente de messages à tout moment avec `-qR`*string*.

```
# /usr/lib/sendmail -qRstring
```

string Utilisez l'alias d'un destinataire ou une sous-chaîne de *user@host.domain*, telle qu'un nom d'hôte.

Vous pouvez également exécuter un sous-ensemble de la file d'attente de messages avec `-qI` *nnnnn*.

```
# /usr/lib/sendmail -qInnnnn
```

nnnnn Utilisez un ID de file d'attente.

▼ Déplacement de la file d'attente de messages, `/var/spool/mqueue`

Si vous déplacez la file d'attente de messages, suivez ces instructions.

1 Devenez utilisateur `root` (ou équivalent) sur l'hôte de messagerie.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Éliminez le démon `sendmail`.

```
# svcadm disable network/smtp:sendmail
```

À présent, `sendmail` n'effectue plus le traitement du répertoire de file d'attente.

3 Passez au répertoire `/var/spool`.

```
# cd /var/spool
```

4. **Déplacez le répertoire, mqueue, et son contenu vers le répertoire omqueue. Ensuite, créez un répertoire vide nommé mqueue.**

   ```
   # mv mqueue omqueue; mkdir mqueue
   ```

5. **Définissez les autorisations du répertoire en lecture/écriture/exécution par propriétaire, et en lecture/exécution par groupe. En outre, définissez le propriétaire et le groupe sur daemon.**

   ```
   # chmod 750 mqueue; chown root:bin mqueue
   ```

6. **Démarrez sendmail.**

   ```
   # svcadm enable network/smtp:sendmail
   ```

▼ Exécution de l'ancienne file d'attente de messages, /var/spool/omqueue

Pour exécuter une ancienne file d'attente de messages, suivez ces instructions.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Exécutez l'ancienne file d'attente de messages.**

   ```
   # /usr/lib/sendmail -oQ/var/spool/omqueue -q
   ```

   L'indicateur -oQ spécifie un autre répertoire de file d'attente. L'indicateur -q spécifie l'exécution de chaque tâche de la file d'attente. Utilisez l'indicateur -v si vous affichez la sortie détaillée à l'écran.

3. **Supprimez le répertoire vide.**

   ```
   # rmdir /var/spool/omqueue
   ```

Administration des fichiers .forward (liste des tâches)

Le tableau ci-dessous décrit les procédures d'administration des fichiers .forward. Pour plus d'informations, reportez-vous à la section "Fichier .forward" à la page 374 du Chapitre 14, "Services de messagerie (référence)".

Tâche	Description	Voir
Désactivation des fichiers .forward	Utilisez cette procédure si, par exemple, vous voulez empêcher le transfert automatique.	"Désactivation de fichiers .forward" à la page 332
Modification du chemin de recherche de fichier .forward	Utilisez cette procédure si, par exemple, vous souhaitez déplacer tous les fichiers .forward dans un répertoire commun.	"Modification du chemin de recherche de fichier .forward" à la page 333
Création et alimentation du fichier /etc/shells	Utilisez cette procédure pour permettre aux utilisateurs d'utiliser le fichier .forward pour le transfert du courrier vers un programme ou vers un fichier.	"Création et renseignement du fichier /etc/shells" à la page 334

Administration des fichiers .forward

Cette section contient plusieurs procédures qui sont liées à l'administration des fichiers .forward. Étant donné que ces fichiers peuvent être modifiés par les utilisateurs, des problèmes peuvent survenir. Pour plus d'informations, reportez-vous à la section "Fichier .forward" à la page 374 du Chapitre 14, "Services de messagerie (référence)".

Reportez-vous aux sections suivantes :

- "Désactivation de fichiers .forward" à la page 332
- "Modification du chemin de recherche de fichier .forward" à la page 333
- "Création et renseignement du fichier /etc/shells" à la page 334

▼ Désactivation de fichiers .forward

Cette procédure, qui empêche le transfert automatique, désactive le fichier .forward pour un hôte particulier.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Créez une copie du fichier /etc/mail/cf/domain/solaris-generic.m4 ou du fichier m4 de domaine spécifique à votre site.

```
# cd /etc/mail/cf/domain
# cp solaris-generic.m4 mydomain.m4
```

mydomain Utilisez le nom de fichier de votre choix.

3 **Ajoutez la ligne suivante au fichier que vous venez de créer.**

```
define('confFORWARD_PATH','')dnl
```

Si une valeur pour confFORWARD_PATH existe déjà dans le fichier m4, remplacez-la par cette valeur nulle.

4 **Créez et installez un fichier de configuration.**

Si vous avez besoin d'aide pour procéder à cette étape, reportez-vous à la section "Création d'un fichier sendmail.cf" à la page 306.

Remarque – Lorsque vous modifiez le fichier .mc, n'oubliez pas de changer DOMAIN('solaris-generic') en DOMAIN('*mydomain* ').

▼ Modification du chemin de recherche de fichier .forward

Si, par exemple, vous voulez placer tous les fichiers .forward dans un répertoire commun, suivez ces instructions.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Créez une copie du fichier /etc/mail/cf/domain/solaris-generic.m4 ou du fichier m4 de domaine spécifique à votre site.**

```
# cd /etc/mail/cf/domain
# cp solaris-generic.m4 mydomain.m4
```

mydomain Utilisez le nom de fichier de votre choix.

3 **Ajoutez la ligne suivante au fichier que vous venez de créer.**

```
define('confFORWARD_PATH','$z/.forward:/var/forward/$u')dnl
```

Si une valeur pour confFORWARD_PATH existe déjà dans le fichier m4, remplacez-la par cette nouvelle valeur.

4 **Créez et installez un fichier de configuration.**

Si vous avez besoin d'aide pour procéder à cette étape, reportez-vous à la section "Création d'un fichier sendmail.cf" à la page 306.

Remarque – Lorsque vous modifiez le fichier `.mc`, n'oubliez pas de changer `DOMAIN(‘solaris-generic’)` en `DOMAIN(‘`*mydomain*`’)`.

▼ Création et renseignement du fichier `/etc/shells`

Ce fichier n'est pas inclus dans la version standard. Vous devez l'ajouter si vous souhaitez autoriser les utilisateurs à utiliser des fichiers `.forward` pour le transfert de messages vers un programme ou un fichier. Vous pouvez créer ce fichier manuellement en utilisant `grep` pour identifier tous les shells qui sont répertoriés dans le fichier de mot de passe et ainsi entrer les shells dans le fichier. Cependant, la procédure suivante, qui utilise un script téléchargeable, est plus facile à utiliser.

1. **Téléchargez le script.**

   `http://www.sendmail.org/vendor/sun/gen-etc-shells.html`

2. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

3. **Pour générer une liste de shells, exécutez le script `gen-etc-shells`.**

   ```
   # ./gen-etc-shells.sh > /tmp/shells
   ```

   Ce script utilise la commande `getent` pour collecter les noms des shells qui sont inclus dans les sources de fichier de mot de passe répertoriées dans `/etc/nsswitch.conf`.

4. **Examinez et modifiez la liste des shells dans `/tmp/shells`.**

   Avec l'éditeur de votre choix, supprimez les shells que vous ne souhaitez pas inclure.

5. **Déplacez le fichier vers `/etc/shells`.**

   ```
   # mv /tmp/shells /etc/shells
   ```

Procédures de dépannage et conseils pour les services de messagerie (liste des tâches)

Le tableau ci-dessous décrit les procédures de dépannage et des conseils pour les services de messagerie.

Tâche	Description	Voir
Test de la configuration de la messagerie	Étapes de test des modifications apportées au fichier de configuration `sendmail`	"Test de la configuration de la messagerie" à la page 335
Vérification des alias de messagerie	Étape pour confirmer que le courrier peut ou non être distribué au destinataire indiqué	"Vérification d'alias de messagerie" à la page 336
Test des ensembles de règles	Étapes de vérification de l'entrée et des retours des ensembles de règles `sendmail`	"Test des ensembles de règles `sendmail`" à la page 337
Vérification des connexions à d'autres systèmes	Conseils de vérification des connexions à d'autres systèmes	"Vérification des connexions à d'autres systèmes" à la page 338
Consignation de messages à l'aide du programme `syslogd`	Conseils pour la collecte d'informations relatives au message d'erreur	"Consignation des messages d'erreur" à la page 338
Vérification d'autres sources pour obtenir des informations de diagnostic	Conseils pour l'obtention d'informations de diagnostic auprès d'autres sources	"Autres sources d'informations de diagnostic pour la messagerie" à la page 339

Procédures de dépannage et conseils pour les services de messagerie

Cette section fournit des procédures et des conseils que vous pouvez utiliser pour le dépannage des problèmes de services de messagerie.

▼ Test de la configuration de la messagerie

Pour tester les modifications que vous apportez au fichier de configuration, suivez ces instructions.

1 **Redémarrez `sendmail` sur n'importe quel système qui dispose d'un fichier de configuration révisé.**

```
# svcadm refresh network/smtp:sendmail
```

2 **Envoyez des messages de test à partir de chaque système.**

```
# /usr/lib/sendmail -v names </dev/null
```

names Spécifiez l'adresse e-mail d'un destinataire.

Cette commande envoie un message null au destinataire indiqué et affiche l'activité liée au message sur votre écran.

3 **Envoyez un message à vous-même ou à d'autres personnes sur le système local en adressant le message à un nom d'utilisateur standard.**

4. **(Facultatif) Si vous êtes connecté à un réseau, envoyez un message tridirectionnel à une personne d'un autre système.**

   - Du système principal vers un système client
   - D'un système client vers le système principal
   - D'un système client vers un autre système client

5. **(Facultatif) Si vous disposez d'une passerelle de messagerie, envoyez un message à partir de l'hôte de messagerie vers un autre domaine pour vous assurer que le logiciel de messagerie relais et l'hôte sont correctement configurés.**

6. **(Facultatif) Si vous avez configuré sur votre ligne téléphonique une connexion UUCP à un autre hôte, envoyez un message à une personne située sur cet hôte. Demandez à cette personne de vous renvoyer un message ou de vous appeler lorsque le message est reçu.**

7. **Demandez à une personne de vous envoyer un message par le biais de la connexion UUCP.**

   Le programme `sendmail` ne peut pas détecter si le message est distribué dans la mesure où il le transmet à UUCP pour qu'il le distribue.

8. **À partir de différents systèmes, envoyez un message à `postmaster` et assurez-vous que le message est transmis à la boîte à lettres de votre administrateur du courrier.**

Vérification d'alias de messagerie

L'exemple suivant vous montre comment vérifier un alias.

```
% mconnect
connecting to host localhost (127.0.0.1), port 25
connection open
220 your.domain.com ESMTP Sendmail 8.13.6+Sun/8.13.6; Tue, 12 Sep 2004 13:34:13 -0800 (PST)
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
221 2.0.0 your.domain.com closing connection
%
```

Dans cet exemple, le programme `mconnect` a ouvert une connexion vers un serveur de courrier sur un hôte local et vous a permis de tester cette connexion. Le programme s'exécute en mode interactif, de sorte que vous pouvez émettre différentes commandes de diagnostic. Pour une description complète, reportez-vous à la page de manuel `mconnect(1)`. L'entrée, `expn sandy`, a fourni l'adresse complète, `sandy@phoenix.example.com`. Par conséquent, vous avez vérifié que le courrier peut être distribué lorsque l'alias `sandy` est utilisé.

Pensez à éviter les boucles et bases de données incohérentes lorsque des alias locaux et à l'échelle du domaine sont utilisés. Veillez particulièrement à éviter la création de boucles d'alias lorsque vous déplacez un utilisateur d'un système à un autre.

▼ Test des ensembles de règles `sendmail`

Pour vérifier l'entrée et les retours des ensembles de règles `sendmail`, suivez ces instructions.

1 Passez en mode test d'adresse.

```
# /usr/lib/sendmail -bt
```

2 Testez une adresse e-mail.

Fournissez l'adresse et les numéros suivants à la dernière invite (>).

> **3,0** *mail-sraddress*

mail-address Utilisez l'adresse e-mail que vous testez.

3 Mettez fin à la session.

Appuyez sur Ctrl-d.

Exemple 13–6 Sortie en mode test d'adresse

Voici un exemple de sortie en mode test d'adresse.

```
% /usr/lib/sendmail -bt
ADDRESS TEST MODE (ruleset 3 NOT automatically invoked)
Enter <ruleset> <address>
> 3,0 sandy@phoenix
canonify           input: sandy @ phoenix
Canonify2          input: sandy < @ phoenix >
Canonify2        returns: sandy < @ phoenix . example . com . >
canonify         returns: sandy < @ phoenix . example . com . >
parse              input: sandy < @ phoenix . example . com . >
Parse0             input: sandy < @ phoenix . example . com . >
Parse0           returns: sandy < @ phoenix . example . com . >
ParseLocal         input: sandy < @ phoenix . example . com . >
ParseLocal       returns: sandy < @ phoenix . example . com . >
Parse1             input: sandy < @ phoenix . example . com . >
MailerToTriple     input: < mailhost . phoenix . example . com >
     sandy < @ phoenix . example . com . >
MailerToTriple   returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
Parse1           returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
parse            returns: $# relay $@ mailhost . phoenix . example . com
     $: sandy < @ phoenix . example . com . >
```

Vérification des connexions à d'autres systèmes

Le programme `mconnect` ouvre une connexion vers un serveur de courrier sur un hôte que vous spécifiez et vous permet de tester cette connexion. Le programme s'exécute en mode interactif, de sorte que vous pouvez émettre différentes commandes de diagnostic. Reportez-vous à la page de manuel `mconnect(1)` pour une description complète. L'exemple suivant vérifie que le courrier envoyé au nom d'utilisateur `sandy` est livrable.

```
% mconnect phoenix

connecting to host phoenix (172.31.255.255), port 25
connection open
220 phoenix.example.com ESMTP Sendmail 8.13.1+Sun/8.13.1; Sat, 4 Sep 2004 3:52:56 -0700
expn sandy
250 2.1.5 <sandy@phoenix.example.com>
quit
```

Si vous ne pouvez pas utiliser `mconnect` pour vous connecter à un port `SMTP`, vérifiez ces conditions.

- La charge du système est-elle trop élevée ?
- Le démon `sendmail` est-il en cours d'exécution ?
- Le système est-il doté du fichier `/etc/mail/sendmail.cf` approprié ?
- Le port 25 est-il celui utilisé par `sendmail` ?

Consignation des messages d'erreur

Votre service de messagerie consigne la plupart des messages d'erreurs en utilisant le programme `syslogd`. Par défaut, le programme `syslogd` envoie ces messages à un système appelé `loghost`, qui est spécifié dans le fichier `/etc/hosts`. Vous pouvez définir `loghost` pour qu'il contienne tous les journaux de l'ensemble d'un domaine NIS. Si aucun `loghost` n'est spécifié, les messages d'erreur de `syslogd` ne sont pas signalés.

Le fichier `/etc/syslog.conf` contrôle où le programme `syslogd` transfère les messages. Vous pouvez changer la configuration par défaut en modifiant le fichier `/etc/syslog.conf`. Vous devez redémarrer le démon `syslog` pour que les modifications deviennent actives. Pour collecter des informations sur le courrier, vous pouvez ajouter les sélections suivantes au fichier.

- `mail.alert` – Messages sur les conditions qui doivent être résolues immédiatement
- `mail.crit` – Messages critiques
- `mail.warning` – Messages d'avertissement
- `mail.notice` – Messages qui ne sont pas des erreurs, mais requièrent votre attention
- `mail.info` – Messages d'information
- `mail.debug` – Messages de débogage

L'entrée suivante du fichier `/etc/syslog.conf` envoie une copie de tous les messages critiques, d'information et de débogage vers `/var/log/syslog`.

```
mail.crit;mail.info;mail.debug              /var/log/syslog
```

Chaque ligne du journal système contient un horodatage, le nom du système qui a généré la ligne, et un message. Le fichier `syslog` peut consigner une grande quantité d'informations.

Le journal est organisé en plusieurs niveaux successifs. Au niveau le plus bas, seules les occurrences inhabituelles sont consignées. Au niveau le plus élevé, même les événements les plus courants et inintéressants sont enregistrés. Par convention, les niveaux de consignation inférieurs à 10 sont considérés utiles. Les niveaux de consignation supérieurs à 10 sont généralement utilisés pour le débogage. Reportez-vous à la section "Personnalisation de la journalisation des messages système" du *Guide d'administration système : Administration avancée* pour plus d'informations sur `loghost` et le programme `syslogd`.

Autres sources d'informations de diagnostic pour la messagerie

Pour obtenir d'autres informations de diagnostic, reportez-vous aux sources suivantes.

- Consultez les lignes `Received` dans l'en-tête du message. Ces lignes consignent l'itinéraire que le message a pris lorsqu'il a été relayé. N'oubliez pas de tenir compte des différences de fuseau horaire.
- Consultez les messages issus de `MAILER-DAEMON`. Ces messages signalent généralement des problèmes de distribution.
- Vérifiez le journal système qui consigne les problèmes de distribution de votre groupe de systèmes. Le programme `sendmail` consigne toujours ses activités dans le journal système. Vous pouvez souhaiter modifier le fichier `crontab` pour qu'il exécute un script shell pendant la nuit. Le script recherche dans le journal les messages `SYSERR` et envoie ceux qu'il trouve à l'administrateur du courrier.
- Utilisez le programme `mailstats` pour tester les types de message et déterminer le nombre de messages entrants et sortants.

Résolution des messages d'erreur

Cette section décrit comment résoudre certains messages d'erreur `sendmail`. Vous pouvez également vous reporter à `http://www.sendmail.org/faq`.

Les messages d'erreur suivants contiennent au moins deux types d'informations parmi les trois présentés ci-dessous.

- **Cause :** motif probable du message
- **Description :** activité de l'utilisateur lorsque le message d'erreur a été généré
- **Solution :** actions possibles pour résoudre le problème ou pour poursuivre votre travail

`451 timeout waiting for input during` *source*

Origine : Lorsque `sendmail` lit à partir d'une source susceptible d'arriver à expiration, telle qu'une connexion SMTP, le programme définit une horloge sur la valeur de différentes options `Timeout` avant que la lecture commence. Si la lecture n'est pas terminée avant la fin du délai d'exécution, ce message s'affiche et la lecture s'arrête. En général, cette situation se produit pendant l'exécution de la commande `RCPT`. Le message est alors mis en file d'attente pour une distribution ultérieure.

Solution : Si ce message s'affiche souvent, augmentez la valeur de diverses options `Timeout` dans le fichier `/etc/mail/sendmail.cf`. Si l'horloge est déjà définie sur une valeur élevée, recherchez les problèmes matériels, tels qu'un mauvais câblage réseau ou de mauvaises connexions réseau.

`550` *hostname*`... Host unknown`

Origine : Ce message `sendmail` indique que la machine hôte de destination, qui est spécifiée par la partie de l'adresse située après le signe arobase (@), n'a pas été trouvée au cours de la recherche du DNS (Domain Name System).

Solution : Utilisez la commande `nslookup` pour vérifier que l'hôte de destination existe dans ce domaine ou d'autres domaines, avec peut-être une orthographe légèrement différente. Sinon, contactez le destinataire visé et demandez la bonne adresse.

`550` *username*`... User unknown`

Origine : Ce message `sendmail` indique que le destinataire visé spécifié par la partie de l'adresse située avant le signe arobase (@), n'a pas pu être trouvé sur la machine hôte de destination.

Solution : Vérifiez l'adresse e-mail et essayez à nouveau, peut-être avec une orthographe légèrement différente. Si cette solution ne fonctionne pas, contactez le destinataire visé et demandez la bonne adresse.

`554` *hostname*`... Local configuration error`

Origine : Ce message `sendmail` indique généralement que l'hôte local tente d'envoyer un courrier à lui-même.

Solution : Vérifiez la valeur de la macro `$j` dans le fichier `/etc/mail/sendmail.cf` afin de vous assurer que cette valeur est un nom de domaine complet.

Description : Lorsque le système émetteur fournit son nom d'hôte au système récepteur dans la commande `HELO` SMTP, le système récepteur compare son nom à celui de l'expéditeur. Si

ces noms sont identiques, le système récepteur émet ce message d'erreur et ferme la connexion. Le nom fourni dans la commande `HELO` est la valeur de la macro `$j`.

Pour plus d'informations, reportez-vous à `http://www.sendmail.org/faq/section4#4.5`.

`config error: mail loops back to myself.`

Origine : Ce message d'erreur se produit si vous configurez un enregistrement MX et faites de l'hôte *bar* l'échangeur de messagerie (Mail eXchanger) pour le domaine *foo*. Par contre, vous ne parvenez pas à configurer l'hôte *bar* pour vérifier qu'il s'agit de l'échangeur de messagerie pour le domaine *foo* .

Il se peut également que les systèmes émetteur et récepteur soient identifiés comme étant de domaine identique.

Solution : Pour plus d'instructions, reportez-vous à `http://www.sendmail.org/faq/section4#4.5`.

`host name configuration error`

Description : Il s'agit d'un ancien message `sendmail`, qui a remplacé le message `I refuse to talk to myself` et est maintenant remplacé par le message `Local configuration error`.

Solution : Suivez les instructions qui ont été fournies pour résoudre ce message d'erreur, `554` *hostname* `... Local configuration error`.

`user unknown`

Origine : Lorsque vous essayez d'envoyer un message à un utilisateur, l'erreur `Username... user unknown` s'affiche. L'utilisateur se trouve sur le même système.

Solution : Vérifiez si une erreur typographique s'est glissée dans l'adresse e-mail saisie. Dans ce cas, l'alias de l'utilisateur peut être défini sur une adresse e-mail qui n'existe pas dans `/etc/mail/aliases` ou dans le fichier `.mailrc` de l'utilisateur. En outre, vérifiez les caractères majuscules dans le nom d'utilisateur. Il est préférable que les adresses e-mail ne soient pas sensibles à la casse.

Pour plus d'informations, reportez-vous à `http://www.sendmail.org/faq/section4#4.17`.

◆ ◆ ◆ CHAPITRE 14

Services de messagerie (référence)

Le programme `sendmail` est un agent d'acheminement du courrier. Le programme utilise un fichier de configuration pour fournir la définition d'alias, le transfert, l'acheminement automatique vers des passerelles réseau et une configuration flexible. Le système d'exploitation Solaris fournit des fichiers de configuration standard que la plupart des sites peuvent utiliser. Le Chapitre 12, “Services de messagerie (présentation)” constitue une introduction aux composants des services de messagerie et la description d'une configuration de services de messagerie typique. Le Chapitre 13, “Services de messagerie (tâches)” explique comment configurer et administrer un système de courrier électronique. Le présent chapitre donne des informations sur les sujets suivants.

Pour les détails qui ne sont pas traités dans ces chapitres, reportez-vous aux pages de manuel suivantes :

- `sendmail`(1M)
- `mail.local`(1M)
- `mailstats`(1)
- `makemap`(1M)
- `editmap`(1M)

Version Solaris de sendmail

Cette section, qui comprend les rubriques suivantes, décrit certaines des différences entre la version Solaris de sendmail et la version Berkeley générique.

Indicateurs utilisés et non utilisés pour compiler sendmail

À partir de la version Solaris 10, les indicateurs suivants sont utilisés pour compiler sendmail. Si votre configuration nécessite d'autres indicateurs, vous devez télécharger la source et recompiler le fichier binaire. Vous pouvez trouver des informations concernant ce processus à http://www.sendmail.org.

TABLEAU 14–1 Indicateurs sendmail généraux

Indicateur	Description
SOLARIS=21000	Prise en charge de la version Solaris 10.
MILTER	Prise en charge de l'API de filtre de courrier. Dans la version 8.13 de sendmail, cet indicateur est activé par défaut. Reportez-vous à la section "MILTER, API de filtre de courrier pour sendmail" à la page 345.
NETINET6	Prise en charge d'IPv6. Cet indicateur a été déplacé de conf.h vers Makefile.

TABLEAU 14–2 Cartes et types de base de données

Indicateur	Description
NDBM	Prise en charge des bases de données ndbm
NEWDB	Prise en charge des bases de données Berkeley DB
USERDB	Prise en charge de la base de données utilisateur
NIS	Prise en charge des bases de données nis
NISPLUS	Prise en charge des bases de données nisplus
LDAPMAP	Prise en charge des cartes LDAP
MAP_REGEX	Prise en charge des cartes d'expressions régulières

TABLEAU 14–3 Indicateurs de système d'exploitation

Indicateur	Description
SUN_EXTENSIONS	Prise en charge d'extensions incluses dans sun_compat.o.
SUN_INIT_DOMAIN	Pour des raisons de compatibilité ascendante, prise en charge de l'utilisation de noms de domaine NIS pour qualifier le nom de l'hôte local. Pour plus d'informations, recherchez les informations spécifiques à chaque fournisseur dans http://www.sendmail.org.
SUN_SIMPLIFIED_LDAP	Prise en charge d'un API LDAP simplifié, qui est spécifique à Sun. Pour plus d'informations, recherchez les informations spécifiques à chaque fournisseur dans http://www.sendmail.org.
VENDOR_DEFAULT=VENDOR_SUN	Sélectionne Sun en tant que fournisseur par défaut.

Le tableau suivant répertorie les indicateurs génériques qui ne sont pas utilisés pour compiler la version de sendmail qui est fournie avec Solaris 10.

TABLEAU 14–4 Indicateurs génériques non utilisés dans cette version de sendmail

Indicateur	Description
SASL	Simple Authentication and Security Layer (Couche de sécurité et d'authentification simple, RFC 2554)
STARTTLS	Transaction Level Security (Sécurité au niveau des transactions, RFC 2487)

Pour afficher la liste des indicateurs utilisés pour compiler sendmail, utilisez la commande suivante.

```
% /usr/lib/sendmail -bt -d0.10 < /dev/null
```

Remarque – La commande ci-dessus ne répertorie pas les indicateurs qui sont spécifiques à Sun.

MILTER, API de filtre de courrier pour sendmail

MILTER, l'API de filtre de courrier de sendmail, permet à des programmes tiers d'accéder aux messages en cours de traitement pour le filtrage des méta-informations et du contenu. Vous n'avez pas besoin de créer le filtre et de configurer sendmail pour l'utiliser. Cette API est activée par défaut dans la version 8.13 de sendmail.

Pour plus d'informations, reportez-vous aux sites suivants :

- http://www.sendmail.org
- https://www.milter.org/

Autres commande sendmail

La version Solaris n'inclut pas tous les synonymes de commandes fournis dans la version générique de sendmail.org. Ce tableau comprend une liste complète des alias de commandes. Le tableau indique également si les commandes sont incluses dans la version Solaris et comment générer le même comportement en utilisant sendmail.

TABLEAU 14–5 Autre commande sendmail

Nom alternatif	Dans cette version ?	Options avec sendmail
hoststat	Non	sendmail -bh
mailq	Oui	sendmail -bp
newaliases	Oui	sendmail -bi
purgestat	Non	sendmail -bH
smtpd	Non	sendmail -bd

Versions du fichier de configuration

À partir de la version Solaris 10, sendmail inclut une option de configuration permettant de définir la version du fichier sendmail.cf. Cette option permet l'utilisation d'anciens fichiers de configuration avec la version actuelle de sendmail. Vous pouvez définir le niveau de version sur des valeurs entre 0 et 10. Vous pouvez également définir le fournisseur. Berkeley ou Sun est une option de fournisseur valide. Si un niveau de version est spécifié, mais pas le fournisseur, Sun est utilisé en tant que fournisseur par défaut. Le tableau suivant répertorie certaines des options valides.

TABLEAU 14–6 Valeurs de version pour le fichier de configuration

Champ	Description
V7/Sun	Paramètre qui était utilisé pour la version 8.8 de sendmail.
V8/Sun	Paramètre qui était utilisé pour la version 8.9 de sendmail. Ce paramètre était inclus dans la version Solaris 8.
V9/Sun	Paramètre qui était utilisé pour les versions 8.10 et 8.11 de sendmail.

TABLEAU 14–6 Valeurs de version pour le fichier de configuration *(Suite)*

Champ	Description
`V10/Sun`	Paramètre qui était utilisé pour les versions 8.12 et 8.13 de `sendmail`. La version 8.12 est la valeur par défaut pour Solaris 9. À partir de Solaris 10, la version 8.13 est la version par défaut.

Remarque – Vous êtes invité à ne pas utiliser `V1/Sun`. Pour plus d'informations, reportez-vous à `http://www.sendmail.org/vendor/sun/differences.html#4`.

Pour plus d'informations sur les tâches, reportez-vous à la section "Modification de la configuration sendmail" à la page 305 du Chapitre 13, "Services de messagerie (tâches)".

Composants matériels et logiciels des services de messagerie

Cette section décrit les composants matériels et logiciels d'un système de messagerie.

Composants logiciels

Chaque service de messagerie inclut au moins un exemplaire de chacun des composants logiciels suivants.

Cette section décrit également les composants logiciels suivants.

Agent utilisateur de messagerie

L'*agent utilisateur de messagerie* est le programme qui sert d'interface entre l'utilisateur et l'agent de transfert de courrier. Le programme `sendmail` est un agent de transfert de courrier. Le système d'exploitation Solaris fournit les agents utilisateur de messagerie suivants.

- `/usr/bin/mail`

- `/usr/bin/mailx`
- `/usr/dt/bin/dtmail`

Agent de transfert de courrier

L'*agent de transfert de courrier* est responsable de l'acheminement des messages électroniques et de la résolution des adresses e-mail. Cet agent est également connu comme un agent d'*acheminement* du courrier. L'agent de transfert pour le système d'exploitation Solaris est `sendmail`. L'agent de transfert effectue les fonctions suivantes.

- Accepte des messages de l'agent utilisateur de messagerie.
- Résout les adresses de destination.
- Sélectionne un agent de distribution approprié pour remettre le courrier.
- Reçoit le courrier entrant provenant d'autres agents de transfert de courrier.

Agent de distribution locale

Un *agent de distribution locale* est un programme qui implémente un protocole de distribution du courrier. Les agents de distribution locale suivants sont fournis avec le système d'exploitation Solaris.

- L'agent de distribution locale UUCP, qui utilise la commande `uux` pour remettre le courrier
- L'agent de distribution locale, qui est `mail.local` dans la version standard de Solaris

La section "Modifications à partir de la version 8.12 de `sendmail`" à la page 392 fournit des informations sur ces sujets connexes.

- "Indicateurs d'agent de distribution supplémentaires à partir de la version 8.12 de `sendmail`" à la page 404
- "Conditions d'égalité supplémentaires pour les agents de distribution à partir de la version 8.12 de `sendmail`" à la page 405

Logiciels de messagerie et `sendmail`

Le *logiciel de messagerie* (mailer, en anglais) est un terme spécifique à `sendmail`. Un *logiciel de messagerie* est utilisé par `sendmail` afin d'identifier une instance spécifique d'un agent de distribution locale personnalisé ou d'un agent de transfert de courrier personnalisé. Vous devez spécifier au moins un logiciel de messagerie dans le fichier `sendmail.cf`. Pour plus d'informations sur les tâches, reportez-vous à la section "Modification de la configuration sendmail" à la page 305 du Chapitre 13, "Services de messagerie (tâches)". Cette section fournit une brève description des deux types de logiciel de messagerie.

- "Logiciel de messagerie SMTP (Simple Mail Transfer Protocol)" à la page 349
- "Logiciels de messagerie UUCP (UNIX-to-UNIX Copy Program)" à la page 349

Pour plus d'informations sur les logiciels de messagerie, reportez-vous au site `http://www.sendmail.org/m4/readme.html` ou `/etc/mail/cf/README`.

Logiciel de messagerie SMTP (Simple Mail Transfer Protocol)

SMTP est le protocole de messagerie standard utilisé sur Internet. Ce protocole définit ces logiciels de messagerie.

- `smtp` fournit des transferts SMTP normaux vers d'autres serveurs.
- `esmtp` fournit des transferts SMTP étendus vers d'autres serveurs.
- `smtp8` fournit des transferts SMTP vers d'autres serveurs sans conversion des données 8 bits au format MIME.
- `dsmtp` fournit la distribution à la demande en utilisant l'indicateur de logiciel de messagerie `F=%`. Reportez-vous aux sections "Modifications apportées à la déclaration `MAILER()` à partir de la version 8.12 de `sendmail`" à la page 403 et "Indicateurs d'agent de distribution supplémentaires à partir de la version 8.12 de `sendmail`" à la page 404.

Logiciels de messagerie UUCP (UNIX-to-UNIX Copy Program)

Si possible, évitez d'utiliser UUCP. Pour obtenir une explication, reportez-vous à la page Web `http://www.sendmail.org/m4/uucp_mailers.html` ou effectuez une recherche dans le fichier `/etc/mail/cf/README` sur cette chaîne : `USING UUCP MAILERS`.

UUCP définit ces logiciels de messagerie.

`uucp-old` Les noms contenus dans la classe `$=U` sont envoyés à `uucp-old`. `uucp` est le nom obsolète pour ce logiciel de messagerie. Le logiciel de messagerie `uucp-old` utilise une adresse à point d'exclamation dans les en-têtes.

`uucp-new` Les noms contenus dans la classe `$=Y` sont envoyés à `uucp-new`. Utilisez ce logiciel de messagerie lorsque vous savez que le logiciel de messagerie UUCP récepteur peut gérer plusieurs destinataires dans un seul transfert. `suucp` est le nom obsolète pour ce logiciel de messagerie. Le logiciel de messagerie `uucp-new` utilise une adresse à point d'exclamation dans les en-têtes.

Si `MAILER(smtp)` est également indiqué dans votre configuration, deux autres logiciels de messagerie sont définis.

`uucp-dom` Ce logiciel de messagerie utilise des adresses de type domaine et applique les règles de réécriture SMTP.

`uucp-uudom` Les noms contenus dans la classe `$=Z` sont envoyés à `uucp-uudom`. `uucp-uudom` et `uucp-dom` utilisent le même format d'adresse d'en-tête, des adresses de type domaine.

Remarque – Étant donné que le logiciel de messagerie `smtp` modifie le logiciel de messagerie UUCP, placez toujours `MAILER(smtp)` avant `MAILER(uucp)` dans votre fichier `.mc`.

Adresses e-mail

L'*adresse e-mail* contient le nom du destinataire et le système auquel est distribué le message électronique. Lorsque vous administrez un petit système de messagerie qui n'utilise pas de service de noms, l'adressage du courrier est facile. Les noms de connexion permettant d'identifier de manière unique les utilisateurs. La complexité apparaît si vous administrez un système de messagerie qui a plus d'un système doté de boîtes à lettres ou qui a un ou plusieurs domaines. Une complexité supplémentaire peut être générée si vous avez une connexion de messagerie UUCP (ou d'autres) vers des serveurs en dehors de votre réseau. Les informations contenues dans les sections suivantes peuvent vous aider à comprendre les composantes et les complexités d'une adresse e-mail.

- "Domaines et sous-domaines" à la page 350
- "Nom de domaine de service de noms et nom de domaine de messagerie" à la page 351
- "Format standard des adresses e-mail" à la page 351
- "Adresses e-mail à acheminement indépendant" à la page 352

Domaines et sous-domaines

L'adressage de courrier utilise les domaines. Un *domaine* est une structure de répertoires pour le nommage d'adresses réseau. Un domaine peut avoir un ou plusieurs *sous-domaines*. Le domaine et les sous-domaines d'une adresse peuvent être comparés à la hiérarchie d'un système de fichiers. Tout comme un sous-répertoire est considéré comme étant à l'intérieur du répertoire au-dessus de lui, chaque sous-domaine d'une adresse e-mail est considéré comme étant à l'intérieur de l'emplacement situé à sa droite.

Le tableau suivant montre quelques domaines supérieurs.

TABLEAU 14–7 Domaines supérieurs

Domaine	Description
`com`	Sites commerciaux
`edu`	Sites éducatifs
`gov`	Administration gouvernementale des États-Unis
`mil`	Administration militaire des États-Unis
`net`	Organisations en réseau
`org`	Autres organismes à but non lucratif

Les domaines sont sensibles à la casse. Vous pouvez utiliser sans risque d'erreur des lettres majuscules, minuscules ou majuscules et minuscules dans la partie domaine d'une adresse.

Nom de domaine de service de noms et nom de domaine de messagerie

Lorsque vous travaillez avec des noms de domaine de service de noms et des noms de domaine de messagerie, n'oubliez pas les points suivants.

- Par défaut, le programme `sendmail` supprime le premier composant du nom de domaine NIS ou NIS+ pour former le nom de domaine de messagerie. Par exemple, si un nom de domaine NIS+ est `bldg5.example.com`, son nom de domaine de messagerie est `example.com`.
- Bien que les adresses de domaine de messagerie ne soient pas sensibles à la casse, le nom de domaine NIS ou NIS+ l'est. Pour obtenir de meilleurs résultats, utilisez des caractères minuscules lors de la configuration de noms de domaine NIS ou NIS+.
- Le nom de domaine DNS et le nom de domaine de messagerie doivent être identiques.

Pour plus d'informations, reportez-vous à la section "Interactions de `sendmail` avec des services de noms" à la page 378.

Format standard des adresses e-mail

En règle générale, une adresse e-mail a le format suivant. Pour de plus amples détails, reportez-vous à la section "Adresses e-mail à acheminement indépendant" à la page 352.

user@subdomain. subdomain2.subdomain1.top-level-domain

La partie de l'adresse située à gauche du signe `@` est l'adresse locale. L'adresse locale peut contenir les éléments suivants.

- Des informations sur l'acheminement avec un autre transport de courrier (par exemple, `bob::vmsvax@gateway` ou `smallberries%mill.uucp@gateway`)
- Un alias (par exemple, `iggy.ignatz`)

Remarque – Le logiciel de messagerie récepteur est chargé de déterminer ce que signifie la partie locale de l'adresse. Pour plus d'informations sur les logiciels de messagerie, reportez-vous à la section "Logiciels de messagerie et `sendmail`" à la page 348.

La partie de l'adresse située à droite du signe `@` indique les niveaux de domaine où réside l'adresse locale. Un point sépare chaque sous-domaine. La partie domaine de l'adresse peut être une organisation, une zone physique ou une région géographique. En outre, l'ordre des informations sur le domaine est hiérarchique, de sorte que plus le sous-domaine est local, plus il est proche du signe `@`.

Adresses e-mail à acheminement indépendant

Les adresses e-mail peuvent être acheminées de manière indépendante. L'adressage à acheminement indépendant requiert de l'expéditeur d'un message électronique qu'il spécifie le nom du destinataire et la destination finale. Un réseau haute vitesse, tel qu'Internet, utilise des adresses à acheminement indépendant. Ces adresses peuvent présenter le format suivant.

user@*host*.*domain*

Les adresses à acheminement indépendant pour les connexions UUCP peuvent présenter le format d'adresse suivant.

host.*domain*!*user*

La popularité croissante du schéma de nommage de domaine hiérarchique pour les ordinateurs rend l'utilisation d'adresses à acheminement indépendant de plus en plus courante. En fait, l'adresse à acheminement indépendant la plus courante omet le nom d'hôte et s'appuie sur le service de noms de domaine pour identifier correctement la destination finale du message électronique.

user@*domain*

Les adresses à acheminement indépendant sont d'abord lues en recherchant le signe `@`. La hiérarchie de domaines est ensuite lue de la droite (le niveau le plus élevé) vers la gauche (la partie la plus spécifique de l'adresse située à droite du signe `@`).

Fichiers de boîte à lettres

Une *boîte à lettres* est un fichier qui est la destination finale des messages électroniques. Le nom de la boîte à lettres peut être le nom d'utilisateur ou l'identité d'une fonction spécifique, telle que l'administrateur du courrier. Les boîtes à lettres se trouvent dans le fichier `/var/mail/`*username*, qui peut exister sur le système local de l'utilisateur ou sur un serveur de courrier distant. Dans l'un ou l'autre cas, la boîte à lettres se trouve sur le système sur lequel le courrier est distribué.

Le courrier doit toujours être distribué à un système de fichiers local afin que l'agent utilisateur puisse extraire le courrier à partir d'un spool de messages et le stocker facilement dans la boîte à lettres locale. N'utilisez pas des systèmes de fichiers montés via NFS comme destination pour la boîte à lettres d'un utilisateur. Plus précisément, ne dirigez pas le courrier à un client de messagerie qui monte le système de fichiers `/var/mail` à partir d'un serveur distant. Le courrier de l'utilisateur, dans cet exemple, doit être adressé au serveur de courrier et non au nom d'hôte du client. Les systèmes de fichiers montés via NFS peuvent entraîner des problèmes de gestion et de distribution du courrier.

Le fichier `/etc/mail/aliases` et les services de noms, tels que NIS et NIS+, fournissent des mécanismes pour la création d'alias pour les adresses e-mail. Par conséquent, les utilisateurs n'ont pas besoin de connaître précisément le nom local de la boîte à lettres d'un utilisateur.

Le tableau suivant présente les conventions de nommage habituelles pour des boîtes à lettres spécialisées.

TABLEAU 14–8 Conventions pour le format des noms de boîtes à lettres

Format	Description
username	Les noms d'utilisateur sont souvent les mêmes que les noms de boîtes à lettres.
Firstname. *Lastname* *Firstname*_ *Lastname* *Firstinitial*. *Lastname* *Firstinitial*_ *Lastname*	Les noms d'utilisateur peuvent être identifiés en tant que noms complets avec un point (ou un trait de soulignement) qui sépare le nom et prénom. Vous pouvez aussi identifier les noms d'utilisateur par la première initiale avec un point (ou un trait de soulignement) qui sépare l'initiale et le nom.
`postmaster`	Les utilisateurs peuvent envoyer des questions et soumettre des problèmes avec le système de messagerie à la boîte à lettres du `postmaster`. Chaque site et domaine doivent avoir une boîte à lettres d'`postmaster`.
`MAILER-DAEMON`	`sendmail` achemine automatiquement les messages adressés au `MAILER-DÉMON` à l'administrateur du courrier.
aliasname`-request`	Les noms qui se terminent par `-request` sont des adresses administratives pour les listes de distribution. Ces adresses doivent rediriger les messages à la personne qui gère la liste de distribution en question.
`owner-`*aliasname*	Les noms qui commencent par `owner-` sont des adresses administratives pour les listes de distribution. Ces adresses doivent rediriger les messages à la personne qui gère les erreurs de messagerie.
`owner-owner`	Cet alias est utilisé lorsqu'aucun alias `owner-`*aliasname* de réception des erreurs n'existe. Ces adresses doivent rediriger les messages à la personne qui gère les erreurs de messagerie. Cette adresse doit également être définie sur n'importe quel système qui gère un grand nombre d'alias.
Locale`%`*Domaine*	Le signe de pourcentage (`%`) indique une adresse locale qui est étendue lorsque le message arrive à destination. La plupart des systèmes de messagerie interprètent les noms de boîtes à lettres comportant des caractères `%` comme des adresses e-mail complètes. Le signe `%` est remplacé par un `@`, et le message est redirigé en conséquence. Bien que de nombreuses personnes utilisent la convention `%`, cette convention n'est pas une norme officielle. Cette convention est désignée comme le “hack de pourcentage”. Cette fonction est souvent utilisée pour aider à déboguer les problèmes de messagerie.

À partir de `sendmail` version 8, l'expéditeur d'enveloppes pour le courrier qui est envoyé à un alias de groupe a été modifié pour l'adresse qui est développée à partir de l'alias du propriétaire, le cas échéant. Cette modification permet aux erreurs de messagerie d'être envoyées au propriétaire d'alias, plutôt que d'être renvoyées à l'expéditeur. Grâce à cette modification, les utilisateurs remarquent que le message qui a été envoyé à un alias semble provenir du propriétaire d'alias, une fois distribué. Le format d'alias suivant permet de résoudre certains des problèmes associés à cette modification.

```
mygroup: :include:/pathname/mygroup.list
owner-mygroup: mygroup-request
mygroup-request: sandys, ignatz
```

Dans cet exemple, l'alias `mygroup` est l'alias de messagerie pour le groupe. L'alias `owner-mygroup` reçoit les messages d'erreur. L'alias `mygroup-request` doit être utilisé pour les demandes

d'administration. Cette structure signifie que dans le courrier envoyé à l'alias `mygroup`, l'expéditeur d'enveloppes devient `mygroup-request`.

Alias de messagerie

Un *alias* est un nom alternatif. Pour le courrier, vous pouvez utiliser des alias pour assigner l'emplacement d'une boîte à lettres ou pour définir des listes de diffusion. Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)". Vous pouvez également vous reporter à la section "Fichiers d'alias de messagerie" à la page 371 de ce chapitre.

Pour les sites de grande taille, l'alias de messagerie définit généralement l'emplacement d'une boîte à lettres. Fournir un alias de messagerie revient à fournir un numéro de pièce en tant que partie de l'adresse d'une personne travaillant dans une grande société qui occupe plusieurs salles. Si vous ne donnez pas le numéro de la salle, le courrier est distribué à une adresse centrale et un effort supplémentaire est nécessaire pour déterminer dans quelle partie du bâtiment le courrier doit être distribué. Par conséquent, la possibilité d'erreur augmente. Par exemple, si deux personnes nommées Kevin Smith travaillent dans le même bâtiment, un seul d'entre eux risque de recevoir le courrier. Pour corriger le problème, chaque Kevin Smith doit avoir un numéro de pièce ajouté à son adresse.

Utilisez des domaines et des adresses indépendantes de l'emplacement autant que possible lorsque vous créez des listes de diffusion. Afin d'améliorer la portabilité et la flexibilité des fichiers d'alias, rendez les entrées d'alias des listes de diffusion aussi génériques et indépendantes du système que possible. Par exemple, s'il existe un utilisateur nommé `ignatz` sur le système `mars` du domaine `example.com`, créez l'alias `ignatz@example` au lieu de `ignatz@mars`. Si l'utilisateur `ignatz` change le nom de son système, mais demeure à l'intérieur du domaine `example`, il n'est pas nécessaire de mettre à jour les fichiers d'alias pour refléter le changement dans le nom du système.

Lorsque vous créez des entrées d'alias, entrez un alias par ligne. Vous devez n'avoir qu'une seule entrée qui contient le nom du système de l'utilisateur. Par exemple, vous pouvez créer les entrées suivantes pour l'utilisateur `ignatz`.

```
ignatz: iggy.ignatz
iggyi: iggy.ignatz
iggy.ignatz: ignatz@mars
```

Vous pouvez créer un alias pour les noms ou domaines locaux. Par exemple, l'utilisateur `fred`, qui a une boîte à lettres sur le système `mars` et se trouve dans le domaine `planets`, pourrait avoir une entrée d'alias dans la table d'alias NIS+.

```
fred: fred@planets
```

Lorsque vous créez des listes de diffusion incluant les utilisateurs en dehors de votre domaine, créez l'alias avec le nom d'utilisateur et le nom du domaine. Par exemple, si un utilisateur nommé `smallberries` sur le système `privet` du domaine `example.com`, créez l'alias

`smallberries@example.com`. L'adresse e-mail de l'expéditeur est maintenant automatiquement convertie en un nom de domaine complet lorsque le courrier sort du domaine de l'utilisateur.

La liste suivante décrit les méthodes de création et d'administration des fichiers d'alias de messagerie.

- Vous pouvez créer des alias de messagerie pour une utilisation globale dans la table `mail_aliases` NIS+, la carte `alias` NIS ou les fichiers `/etc/mail/aliases` locaux. Vous pouvez également créer et administrer des listes de diffusion qui utilisent les mêmes fichiers d'alias.
- En fonction de la configuration de vos services de messagerie, vous pouvez administrer les alias à l'aide du service de noms NIS ou NIS+ pour gérer une base de données `alias` globale. Sinon, vous pouvez mettre à jour tous les fichiers `/etc/mail/aliases` locaux afin d'assurer la synchronisation des alias.
- Les utilisateurs peuvent également créer et utiliser des alias. Les utilisateurs peuvent créer des alias dans leurs fichier `~/.mailrc` local, utilisable uniquement par l'utilisateur, ou dans leur fichier `/etc/mail/aliases` local, que tout le monde peut utiliser. Les utilisateurs ne peuvent pas normalement créer ou administrer des fichiers d'alias NIS ou NIS+.

Composants matériels

Vous pouvez fournir les trois éléments requis pour la configuration de la messagerie dans le même système ou demander aux différents systèmes d'apporter ces éléments.

- "Hôte de messagerie" à la page 355
- "Serveur de courrier" à la page 356
- "Client de messagerie" à la page 357

Lorsque les utilisateurs doivent communiquer avec des réseaux en dehors de votre domaine, vous devez également ajouter un quatrième élément, une passerelle de messagerie. Pour plus d'informations, reportez-vous à la section "Passerelle de messagerie" à la page 357. Les sections suivantes décrivent chaque composant matériel.

Hôte de messagerie

Un *hôte de messagerie* est la machine que vous désignez en tant que machine de messagerie principale sur votre réseau. Un hôte de messagerie correspond à la machine vers laquelle les autres systèmes du site transfèrent le courrier qui ne peut pas être distribué. Vous pouvez désigner un système en tant qu'hôte de messagerie dans la base de données `hosts` en ajoutant le mot `mailhost` à droite de l'adresse IP dans le fichier`/etc/hosts` local. Alternativement, vous pouvez ajouter de la même façon le mot `mailhost` au fichier d'hôtes dans le service de noms. Pour obtenir des informations détaillées sur les tâches, reportez-vous à la section "Configuration d'un hôte de messagerie" à la page 301 du Chapitre 13, "Services de messagerie (tâches)".

Un bon candidat pour un hôte de messagerie est un système qui est configuré en tant que routeur reliant votre réseau au réseau Internet mondial. Pour plus d'informations, reportez-vous au Chapitre 15, “Solaris PPP 4.0 (Présentation) ”, Chapitre 24, “UUCP (présentation)”, and “Configuration d’un routeur IPv4” du *Guide d’administration système : services IP*. Si aucun système de votre réseau local n'a de modem, désignez un système en tant qu'hôte de messagerie.

Certains sites utilisent des machines autonomes qui ne sont pas en réseau selon une configuration de partage du temps. Plus précisément, la machine indépendante sert des terminaux qui sont reliés à ses ports série. Vous pouvez paramétrer le courrier électronique pour cette configuration en désignant le système autonome en tant qu'hôte de messagerie d'un réseau à système unique. La section “Présentation des composants matériels” à la page 288 du Chapitre 12, “Services de messagerie (présentation)” fournit un chiffre qui montre une configuration de messagerie typique.

Serveur de courrier

Une *boîte à lettres* est un fichier unique contenant le courrier pour un utilisateur donné. Le courrier est distribué au système sur lequel la boîte à lettres de l'utilisateur réside, ce peut être sur une machine locale ou sur un serveur distant. Un *serveur de courrier* est un système qui gère les boîtes à lettres des utilisateurs dans leur répertoire `/var/mail`. Pour obtenir des informations sur les tâches, reportez-vous à la section “Configuration d'un serveur de courrier” à la page 297 du Chapitre 13, “Services de messagerie (tâches)”.

Le serveur de courrier achemine tous les messages provenant d'un client. Lorsqu'un client envoie un message, le serveur de courrier place ce message dans une file d'attente pour sa distribution. Une fois le message placé dans la file d'attente, un utilisateur peut redémarrer ou arrêter le client sans perdre ces messages. Lorsque le destinataire reçoit un courrier provenant d'un client, le chemin dans la ligne `From` du message contient le nom du serveur de courrier. Si le destinataire répond, la réponse est envoyée à la boîte à lettres de l'utilisateur. De bons candidats pour les serveurs de courrier sont des systèmes qui fournissent un répertoire personnel pour les utilisateurs ou les systèmes sauvegardés régulièrement.

Si le serveur de courrier n'est pas le système local de l'utilisateur, les utilisateurs présents dans des configurations utilisant le logiciel NFS peuvent monter le répertoire `/var/mail` en utilisant le fichier `/etc/vfstab`, s'ils bénéficient d'un accès `root`. Dans le cas contraire, les utilisateurs peuvent utiliser l'agent de montage automatique. Si la prise en charge de NFS n'est pas disponible, les utilisateurs peuvent se connecter au serveur pour lire leur courrier.

Si les utilisateurs de votre réseau envoient d'autres types de courrier, tels que des fichiers audio ou des fichiers issus de systèmes de publication assistée par ordinateur, vous devez allouer plus d'espace aux boîtes à lettres sur le serveur de courrier.

L'établissement d'un serveur de courrier pour toutes les boîtes à lettres simplifie votre processus de sauvegarde. Les sauvegardes peuvent être difficiles à effectuer lorsque le courrier est réparti sur de nombreux systèmes. L'inconvénient de stocker plusieurs boîtes à lettres sur un seul

serveur est que le serveur peut constituer un point d'échec unique pour de nombreux utilisateurs. Cependant, les avantages de l'apport de sauvegardes sûres justifient le risque.

Client de messagerie

Un client de messagerie est un utilisateur de services de messagerie doté d'une boîte à lettres sur un serveur de courrier. En outre, le client de messagerie possède un alias de messagerie dans le fichier `/etc/mail/aliases` qui pointe vers l'emplacement de la boîte à lettres. Pour obtenir des informations sur les tâches, reportez-vous à la section "Configuration d'un client de messagerie" à la page 299 du Chapitre 13, "Services de messagerie (tâches)".

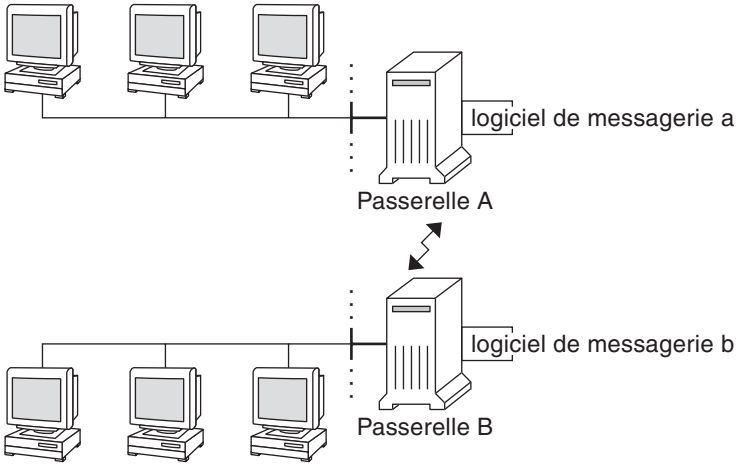
Passerelle de messagerie

La *passerelle de messagerie* est une machine qui gère les connexions entre des réseaux qui exécutent différents protocoles de communication ou les communications entre divers réseaux utilisant le même protocole. Par exemple, une passerelle de messagerie peut connecter un réseau TCP/IP à un réseau qui exécute une suite de protocoles SNA (Systems Network Architecture).

La passerelle de messagerie la plus simple à configurer est celle qui relie deux réseaux utilisant le même protocole ou logiciel de messagerie. Ce système gère le courrier portant une adresse dont `sendmail` ne parvient pas à trouver un destinataire dans votre domaine. Si une passerelle de messagerie existe, `sendmail` l'utilise pour envoyer et recevoir du courrier en dehors de votre domaine.

Vous pouvez configurer une passerelle de messagerie entre deux réseaux qui utilisent des logiciels de messagerie différents, comme le montre la figure suivante. Pour prendre en charge cette configuration, vous devez personnaliser le fichier `sendmail.cf` sur le système de passerelle de messagerie, qui peut s'avérer une tâche difficile et fastidieuse.

FIGURE 14–1 Passerelle entre différents protocoles de communication



Si vous disposez d'une machine qui fournit des connexions à Internet, vous pouvez la configurer en tant que passerelle de messagerie. Examinez attentivement les besoins en sécurité pour votre site avant de configurer une passerelle de messagerie. Vous devrez peut-être créer une passerelle pare-feu entre le réseau de votre entreprise et d'autres réseaux, et configurer cette passerelle en tant que passerelle de messagerie. Pour obtenir des informations sur les tâches, reportez-vous à la section "Configuration d'une passerelle de messagerie" à la page 303 du Chapitre 13, "Services de messagerie (tâches)".

Programmes et fichiers de service de messagerie

Les services de messagerie comprennent de nombreux programmes et démons qui interagissent. Cette section présente les fichiers, programmes, termes et concepts liés à l'administration des messages électroniques.

Amélioration de l'utilitaire `vacation`

À partir de la version Solaris 10, l'utilitaire `vacation` a été amélioré pour permettre à un utilisateur de spécifier les messages entrants qui reçoivent des réponses générées automatiquement. Grâce à cette amélioration, l'utilisateur peut éviter de partager des informations confidentielles ou des coordonnées avec des personnes inconnues. Les messages provenant d'expéditeurs de courrier indésirable ou de personnes inconnues ne reçoivent pas de réponse.

Le principe consiste à comparer l'adresse e-mail d'un émetteur de message entrant avec une liste de domaines ou d'adresses e-mail dans un fichier `.vacation.filter`. Ce fichier est créé par l'utilisateur et situé dans le répertoire personnel de l'utilisateur. Si une correspondance de domaine ou d'adresse e-mail est trouvée, une réponse est envoyée. Dans le cas contraire, aucune réponse n'est envoyée.

Le fichier `.vacation.filter` peut contenir des entrées telles que :

```
company.com
mydomain.com
onefriend@hisisp.com
anotherfriend@herisp.com
```

Notez que chaque ligne contient un domaine ou une adresse e-mail. Chaque entrée doit figurer sur une ligne séparée. Pour que l'adresse e-mail d'un expéditeur corresponde à une entrée d'adresse e-mail, la correspondance doit être exacte, à l'exception de la casse. Les lettres contenues dans l'adresse de l'expéditeur peuvent donc être en minuscules ou en majuscules. Pour que l'adresse e-mail de l'expéditeur corresponde à une entrée de domaine, l'adresse doit contenir le domaine répertorié. Par exemple, `somebody@dept.company.com` et `someone@company.com` est une correspondance pour une entrée de domaine de `company.com`.

Pour plus d'informations, reportez-vous à la page de manuel `vacation(1)`.

Contenu du répertoire `/usr/bin`

Le tableau ci-après présente le contenu du répertoire `/usr/bin`, qui est utilisé pour les services de messagerie.

Nom	Type	Description
`aliasadm`	Fichier	Programme qui manipule la carte d'alias NIS+.
`mail`	Fichier	Agent utilisateur.
`mailcompat`	Fichier	Filtre qui stocke le courrier au format de boîte à lettres SunOS 4.1.
`mailq`	Fichier	Programme qui répertorie le contenu de la file d'attente de messages.

Nom	Type	Description
`mailstats`	Fichier	Programme qui est utilisé pour lire les statistiques de courrier stockées dans le fichier `/etc/mail/statistics` (le cas échéant).
`mailx`	Fichier	Agent utilisateur.
`mconnect`	Fichier	Programme qui se connecte au logiciel de messagerie pour la vérification de l'adresse et le débogage.
`praliases`	Fichier	Une commande pour décompiler la base de données d'alias. Reportez-vous aux informations sur la décompilation fournies à la page de manuel pour `praliases(1)`.
`rmail`	Lien symbolique	Lien symbolique vers `/usr/bin/mail`. Commande qui est souvent utilisée pour autoriser uniquement l'envoi du courrier.
`vacation`	Fichier	Commande qui configure une réponse automatique au courrier.

Contenu du répertoire `/etc/mail`

Le tableau ci-après présente le contenu du répertoire `/etc/mail`.

Nom	Type	Description
`Mail.rc`	Fichier	Paramètres par défaut pour l'agent utilisateur `mailx`.
`aliases`	Fichier	Informations sur le transfert du courrier.
`aliases.db`	Fichier	Format binaire par défaut des informations sur le transfert du courrier qui sont créées en exécutant la commande `newaliases`.
`aliases.dir`	Fichier	Format binaire des informations sur le transfert du courrier qui sont créées en exécutant la commande `newaliases`. Peut toujours être utilisé, mais n'est plus utilisé par défaut à partir de la version Solaris 9.
`aliases.pag`	Fichier	Format binaire des informations sur le transfert du courrier qui sont créées en exécutant la commande `newaliases`. Peut toujours être utilisé, mais n'est plus utilisé par défaut à partir de la version Solaris 9.
`mailx.rc`	Fichier	Paramètres par défaut pour l'agent utilisateur `mailx`.
`main.cf`	Lien symbolique	Lien symbolique reliant cet exemple de fichier de configuration pour les principaux systèmes au fichier `sendmail.cf` qui est fourni à des fins de compatibilité ascendante. Ce fichier n'est pas nécessaire dans la version 8.13 de `sendmail`.
`relay-domains`	Fichier	Liste de tous les domaines pour lesquels le relais est autorisé. Par défaut, seul le domaine local est autorisé.

Nom	Type	Description
`sendmail.cf`	Fichier	Fichier de configuration pour l'acheminement du courrier.
`submit.cf`	Fichier	Nouveau fichier de configuration pour le programme d'envoi du courrier (MSP). Pour plus d'informations, reportez-vous à la section "Fichier de configuration `submit.cf` à partir de la version 8.12 de `sendmail`" à la page 393.
`local-host-names`	Fichier	Fichier facultatif que vous pouvez créer si le nombre d'alias pour l'hôte de messagerie est trop grand.
`helpfile`	Fichier	Fichier d'aide qui est utilisé par la commande `HELP` SMTP.
`sendmail.pid`	Fichier	Fichier qui indique le PID du démon d'écoute et qui se trouve maintenant dans `/var/run`.
`statistics`	Fichier	Fichier de statistiques `sendmail`. Si ce fichier est présent, `sendmail` enregistre la quantité de trafic passant par chaque logiciel de messagerie. Auparavant, ce fichier était appelé `sendmail.st`.
`subsidiary.cf`	Lien symbolique	Lien symbolique reliant cet exemple de fichier de configuration pour les systèmes subsidiaires au fichier `sendmail.cf` qui est fourni à des fins de compatibilité ascendante. Ce fichier n'est pas nécessaire dans la version 8.13 de `sendmail`.
`trusted-users`	Fichier	Fichier qui répertorie les utilisateurs (un seul utilisateur par ligne) qui peuvent être autorisés à effectuer certaines opérations de messagerie. Par défaut, seul l'utilisateur `root` est dans ce fichier. Certaines opérations de messagerie, dès lors qu'elles sont effectuées par des utilisateurs non autorisés, entraînent l'affichage de l'avertissement suivant : `X-Authentication-Warning: header being added to a message`.

Contenu du répertoire `/etc/mail/cf`

Au sein du répertoire `/etc/mail` se trouve un sous-répertoire, `cf`, qui contient tous les fichiers nécessaires pour créer un fichier `sendmail.cf`. Le contenu de `cf` est présenté dans le Tableau 14–9.

À partir de la version Solaris 10, pour la prise en charge du système de fichiers `/usr` en lecture seule, le contenu du répertoire `/usr/lib/mail` a été déplacé vers le répertoire `/etc/mail/cf`. Notez, toutefois, les exceptions suivantes : Les scripts de shell `/usr/lib/mail/sh/check-hostname` et `/usr/lib/mail/sh/check-permissions` se trouvent désormais dans le répertoire `/usr/sbin`. Reportez-vous à la section "Autres fichiers utilisés pour les services de messagerie" à la page 364. Pour garantir la compatibilité ascendante, des liens symboliques pointent vers le nouvel emplacement de chaque fichier.

TABLEAU 14–9 Contenu du répertoire `/etc/mail/cf` utilisé pour les services de messagerie

Nom	Type	Description
`README`	Fichier	Décrit les fichiers de configuration.
`cf/main.cf`	Lien symbolique	À partir de la version Solaris 10, le nom de ce fichier est lié à `cf/sendmail.cf`. Ce fichier était auparavant le fichier de configuration principal.
`cf/main.mc`	Lien symbolique	À partir de la version Solaris 10, le nom de ce fichier est lié à `cf/sendmail.mc`. Ce fichier était utilisé pour créer le fichier de configuration principal.
`cf/Makefile`	Fichier	Fournit des règles pour la création, de nouveaux fichiers de configuration.
`cf/submit.cf`	Fichier	Fichier de configuration pour le programme d'envoi du courrier (MSP), qui est utilisé pour envoyer des messages.
`cf/submit.mc`	Fichier	Fichier utilisé pour créer le fichier `submit.cf`. Le fichier définit des macros `m4` pour le programme d'envoi du courrier (MSP).
`cf/sendmail.cf`	Fichier	Fichier de configuration principal de sendmail.
`cf/sendmail.mc`	Fichier	Contient les macros `m4` qui sont utilisées pour générer le fichier `sendmail.cf`.
`cf/subsidiary.cf`	Lien symbolique	À partir de la version Solaris 10, le nom de ce fichier est lié à `cf/sendmail.cf`. Ce fichier était le fichier de configuration pour les hôtes qui montaient via NFS le fichier `/var/mail` à partir d'un autre hôte.
`cf/subsidiary.mc`	Lien symbolique	À partir de la version Solaris 10, le nom de ce fichier est lié à `cf/sendmail.mc`. Ce fichier contenait les macros `m4` qui généraient le fichier `subsidiary.cf`.
`domain`	Répertoire	Offre des descriptions de sous-domaines liés au site.
`domain/generic.m4`	Fichier	Fichier de domaine générique de Berkeley Software Distribution.

TABLEAU 14–9 Contenu du répertoire `/etc/mail/cf` utilisé pour les services de messagerie *(Suite)*

Nom	Type	Description
`domain/solaris-antispam.m4`	Fichier	Fichier de domaine contenant les modifications permettant à `sendmail` de fonctionner comme les précédentes versions de `sendmail`. Cependant, le relais est complètement désactivé, les adresses des expéditeurs sans nom d'hôte sont rejetées et les domaines impossibles à résoudre sont rejetés.
`domain/solaris-generic.m4`	Fichier	Fichier de domaine par défaut contenant les modifications permettant à `sendmail` de fonctionner comme les versions précédentes de `sendmail`.
`feature`	Répertoire	Contient les définitions de fonctions spécifiques à certains hôtes. Reportez-vous au fichier `README` pour une description complète des fonctions.
`m4`	Répertoire	Contient les fichiers d'inclusion indépendants du site.
`mailer`	Répertoire	Contient les définitions des logiciels de messagerie, qui incluent `local`, `smtp` et `uucp`.
`main-v7sun.mc`	Fichier	Obsolète : à partir de la version Solaris 10, le nom de ce fichier est renommé `cf/sendmail.mc`.
`ostype`	Répertoire	Décrit différents environnements de système d'exploitation.
`ostype/solaris2.m4`	Fichier	Définit le logiciel de messagerie local par défaut comme `mail.local`.
`ostype/solaris2.ml.m4`	Fichier	Définit le logiciel de messagerie local par défaut comme `mail.local`.
`ostype/solaris2.pre5.m4`	Fichier	Définit le logiciel de messagerie local comme `mail`.
`ostype/solaris8.m4`	Fichier	Définit le logiciel de messagerie local comme `mail.local` (en mode LMTP), active IPv6 et spécifie `/var/run` comme le répertoire du fichier `sendmail.pid`.
`subsidiary-v7sun.mc`	Fichier	Obsolète : à partir de la version Solaris 10, le nom de ce fichier est renommé `cf/sendmail.mc`.

Contenu du répertoire /usr/lib

Le tableau ci-après présente le contenu du répertoire /usr/lib, qui est utilisé pour les services de messagerie.

TABLEAU 14–10 Contenu du répertoire /usr/lib

Nom	Type	Description
mail.local	Fichier	Logiciel de messagerie qui distribue le courrier aux boîtes à lettres.
sendmail	Fichier	Programme de transfert, également connu comme l'agent de transfert de courrier.
smrsh	Fichier	Programme de shell (shell restreint de sendmail) qui utilise la syntaxe "|program" de sendmail pour restreindre les programmes que sendmail peut exécuter sur les programmes répertoriés dans le répertoire /var/adm/sm.bin. Reportez-vous à la page de manuel smrsh(1M) pour obtenir des recommandations concernant les éléments à inclure dans le fichier /var/adm/sm.bin. Pour l'activer, incluez la commande m4, FEATURE('smrsh'), dans votre fichier mc.
mail	lien symbolique	Lien symbolique pointant vers le répertoire /etc/mail/cf. Pour plus d'informations, reportez-vous à la section "Contenu du répertoire /etc/mail/cf" à la page 361.

Autres fichiers utilisés pour les services de messagerie

Plusieurs autres fichiers et répertoires sont utilisés pour les services de messagerie, comme présentés dans leTableau 14–11.

TABLEAU 14–11 Autres fichiers utilisés pour les services de messagerie

Nom	Type	Description
/etc/default/sendmail	Fichier	Répertorie les variables d'environnement pour le script de démarrage pour sendmail.
/etc/shells	Fichier	Répertorie les shells de connexion valides.
/etc/mail/cf/sh	Répertoire	Contient les scripts shell qui sont utilisés par les aides à la migration et à la création m4.
/usr/sbin/check-permissions	Fichier	Vérifie les autorisations valides des alias :include:, des fichiers .forward et de leur chemin d'accès au répertoire parent.
/usr/sbin/check-hostname	Fichier	Vérifie que sendmail est en mesure de déterminer le nom d'hôte complet.

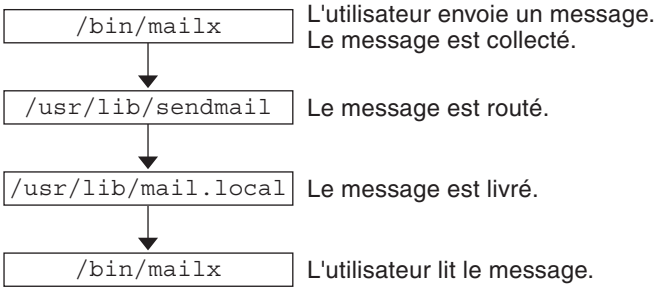
TABLEAU 14–11 Autres fichiers utilisés pour les services de messagerie *(Suite)*

Nom	Type	Description
`/usr/sbin/editmap`	Fichier	Interroge et modifie des enregistrements contenus dans les cartes de la base de données pour `sendmail`.
`/usr/sbin/in.comsat`	Fichier	Démon de notification par e-mail.
`/usr/sbin/makemap`	Fichier	Crée des formes binaires de cartes à clé.
`/usr/sbin/newaliases`	Lien symbolique	Lien symbolique vers `/usr/lib/sendmail`. Utilisé pour créer la forme binaire de la base de données d'alias. Auparavant placé dans le fichier `/usr/bin`.
`/usr/sbin/syslogd`	Fichier	Journal de messages d'erreur, utilisé par `sendmail`.
`/usr/sbin/etrn`	Fichier	Script perl pour le démarrage de la file d'attente de messages à distance côté client.
`/usr/dt/bin/dtmail`	Fichier	Agent utilisateur de messagerie CDE.
`/var/mail/`*mailbox1*, `/var/mail/`*mailbox2*	Fichier	Boîtes à lettres pour le courrier distribué.
`/var/spool/clientmqueue`	Répertoire	Stockage du courrier distribué par le démon client.
`/var/spool/mqueue`	Répertoire	Stockage du courrier distribué par le démon principal.
`/var/run/sendmail.pid`	Fichier	Fichier qui répertorie le PID du démon d'écoute.

Interactions des programmes de messagerie

Les services de messagerie sont fournis par une combinaison des programmes suivants, qui interagissent comme indiqué dans l'illustration simplifiée de la Figure 14–2.

FIGURE 14–2 Interactions des programmes de messagerie



Vous trouverez ci-dessous une description des interactions des programmes de messagerie.

1. Les utilisateurs envoient des messages en utilisant des programmes tels que `mailx`. Pour plus d'informations, reportez-vous à la page de manuel pour `mailx(1)`.
2. Le message est collecté par le programme qui l'a généré, puis le message est transmis au démon `sendmail`.
3. Le démon `sendmail` *analyse* les adresses (les divise en segments identifiables) du message. Le démon utilise les informations issues du fichier de configuration, `/etc/mail/sendmail.cf`, afin de déterminer la syntaxe du nom de réseau , les alias, les informations de transfert et la topologie réseau. En utilisant ces informations, `sendmail` détermine la route qu'un message doit suivre pour atteindre un destinataire.
4. Le démon `sendmail` transmet le message au système approprié.
5. Le programme `/usr/lib/mail.local` sur le système local distribue le courrier vers la boîte à lettres dans le répertoire `/var/mail/` *username* du destinataire du message.
6. Le destinataire est informé que le courrier est arrivé et récupère le courrier en utilisant `mail`, `mailx` ou un programme similaire.

Programme `sendmail`

La liste ci-après décrit certaines des fonctionnalités du programme `sendmail`.

- `sendmail` peut utiliser différents types de protocoles de communication, tels que TCP/IP et UUCP.
- `sendmail` met en place un serveur SMTP, la mise en file d'attente des messages et les listes de diffusion.
- `sendmail` contrôle l'interprétation des noms en utilisant un système de correspondance d'expression qui peut fonctionner avec les conventions de nommage suivantes.
  - Convention de nommage basé sur le domaine. La technique par domaine sépare les problèmes de nommage logique et physique. Pour plus d'informations sur les domaines, reportez-vous à la section "Adresses e-mail" à la page 350.

- Techniques improvisées, telles que celles fournissant des noms de réseaux qui sont en local sur des hôtes d'autres réseaux.
- Syntaxes de nommage arbitraires (plus anciennes).
- Différents schémas de nommage.

Le système d'exploitation Solaris utilise le programme `sendmail` comme routeur de messages. La liste suivante décrit certaines de ses fonctions.

- `sendmail` est responsable de la réception et transmission des messages électroniques à un agent de distribution locale, tel que `mail.local` ou `procmail`.
- `sendmail` est un agent de transfert de courrier qui accepte les messages provenant d'agents utilisateur, tels que `mailx` et Mozilla Mail, et qui achemine les messages par le biais d'Internet jusqu'à leur destination.
- `sendmail` contrôle les messages électroniques envoyés par des utilisateurs de la manière suivante.
  - en évaluant les adresses des destinataires ;
  - en choisissant un programme de distribution approprié ;
  - en réécrivant les adresses dans un format que l'agent de distribution prend en charge ;
  - en reformatant les en-têtes de courrier comme requis ;
  - puis en transmettant le message transformé au programme de messagerie pour qu'il soit distribué.

Pour plus d'informations sur le programme `sendmail`, reportez-vous aux sections suivantes.

- “`sendmail` et ses mécanismes de réacheminement” à la page 367
- “Fonctions de `sendmail`” à la page 369
- “Fichier de configuration `sendmail`” à la page 370

`sendmail` et ses mécanismes de réacheminement

Le programme `sendmail` prend en charge trois mécanismes de réacheminement du courrier. Le mécanisme choisi dépend du type de modification qui est impliqué :

- Un changement de serveur
- Un changement à l'échelle d'un domaine
- Un changement pour un utilisateur

En outre, le mécanisme de réacheminement que vous choisissez peut avoir une incidence sur le niveau d'administration requis. Prenez en compte les options suivantes.

1. Un mécanisme de réacheminement est la *définition d'alias*.

   La définition d'alias peut mettre en correspondance des noms à des adresses au niveau du serveur ou d'un service de noms, en fonction du type de fichier que vous utilisez.

Prenez en compte les avantages et inconvénients suivants relatifs à la définition d'alias de service de noms.

- L'utilisation d'un fichier d'alias de service de noms permet que les modifications de réacheminement du courrier soient administrées à partir d'une source unique. Cependant, la définition d'alias de service de noms peut créer un retard lorsque le réacheminement est propagé.
- L'administration du service de noms est généralement limitée à un groupe donné d'administrateurs système. Un utilisateur normal n'administre pas ce fichier.

Tenez compte des avantages et inconvénients suivants relatifs à l'utilisation d'un fichier d'alias de serveur.

- L'utilisation d'un fichier d'alias de serveur permet la gestion du réacheminement par quiconque pouvant devenir utilisateur `root` sur le serveur désigné.
- La définition d'alias doit créer peu ou pas de latence lorsque le réacheminement est propagé.
- La modification n'a d'incidence que sur le serveur local, ce qui peut être acceptable si la plupart du courrier est envoyé à un seul serveur. Toutefois, si vous avez besoin de propager la modification à de nombreux serveurs de courrier, utilisez un service de noms.
- Un utilisateur normal n'administre pas cette modification.

Pour plus d'informations, reportez-vous à la section "Fichiers d'alias de messagerie" à la page 371 de ce chapitre. Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

2. Le mécanisme suivant est *forwarding*.

   Ce mécanisme permet aux utilisateurs d'administrer le réacheminement du courrier. Les utilisateurs locaux peuvent réacheminer leur courrier entrant vers les emplacements suivants.

   - Une autre boîte à lettres
   - Un autre logiciel de messagerie
   - Un autre hôte de messagerie

   Ce mécanisme est pris en charge par l'utilisation de fichiers `.forward`. Pour plus d'informations sur ces fichiers, reportez-vous à la section "Fichier `.forward`" à la page 374 de ce chapitre. Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers `.forward` (liste des tâches)" à la page 331 du Chapitre 13, "Services de messagerie (tâches)".

3. Le dernier mécanisme de réacheminement est l'*inclusion*.

   Ce mécanisme permet aux utilisateurs de conserver les listes d'alias au lieu de demander l'accès en tant qu'utilisateur `root`. Pour offrir cette fonction, l'utilisateur `root` doit créer une entrée appropriée dans le fichier d'alias sur le serveur. Une fois l'entrée créée, l'utilisateur

peut réacheminer le courrier selon les besoins. Pour plus d'informations sur l'inclusion, reportez-vous à la section "Fichier /etc/mail/aliases" à la page 371 de ce chapitre. Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Remarque – Les programmes qui lisent le courrier, tels que `/usr/bin/mailx`, peuvent avoir leurs propres alias, qui sont développés avant que le message n'atteigne `sendmail`. Les alias de `sendmail` peuvent provenir d'un certain nombre de sources de service de noms, telles que les fichiers locaux, NIS ou NIS+. L'ordre de la recherche est déterminé par le fichier `nsswitch.conf`. Reportez-vous à la page de manuel `nsswitch.conf(4)`.

Fonctions de `sendmail`

Le programme `sendmail` fournit les caractéristiques suivantes.

- `sendmail` est fiable. Le programme est conçu pour distribuer correctement tous les messages. Aucun message ne doit se perdre complètement.
- `sendmail` utilise les logiciels existants pour la distribution chaque fois que cela est possible. Par exemple, l'utilisateur interagit avec un programme de création de courrier et un programme d'envoie de courrier. Lorsqu'un message est envoyé, le programme de création de courrier appelle `sendmail`, qui achemine le message vers les logiciels de messagerie adéquats. Étant donné que certains expéditeurs sont susceptibles d'être des serveurs réseau et certains logiciels de messagerie sont susceptibles d'être des clients réseau, `sendmail` peut être utilisé en tant que passerelle de messagerie via Internet. Pour obtenir une description plus détaillée du processus, reportez-vous à la section "Interactions des programmes de messagerie" à la page 365.
- `sendmail` peut être configuré pour gérer des environnements complexes, comprenant plusieurs réseaux. `sendmail` vérifie le contenu d'une adresse, ainsi que sa syntaxe pour déterminer le logiciel de messagerie à utiliser.
- `sendmail` utilise des fichiers de configuration pour contrôler la configuration de la messagerie au lieu d'exiger que les informations de configuration soient compilées dans le code.
- Les utilisateurs peuvent gérer leurs propres listes de diffusion. En outre, chaque individu peut spécifier son propre mécanisme de transfert sans qu'il soit nécessaire de modifier le fichier d'alias à l'échelle d'un domaine, généralement situé dans les alias à l'échelle du domaine qui sont mis à jour par NIS ou NIS+.
- Chaque utilisateur peut désigner un logiciel de messagerie personnalisé pour traiter le courrier entrant. Le logiciel de messagerie personnalisé peut fournir des fonctions telles que l'envoi d'un message de réponse qui dit : "Je suis en vacances". Pour plus d'informations, reportez-vous à la page de manuel `vacation(1)`.
- `sendmail` crée des lots d'adresses envoyées à un seul hôte afin de réduire le trafic réseau.

Fichier de configuration `sendmail`

Un *fichier de configuration* contrôle la façon dont `sendmail` effectue ses fonctions. Le fichier de configuration détermine le choix des agents de distribution, des règles de réécriture d'adresse et du format de l'en-tête de courrier. Le programme `sendmail` utilise les informations issues du fichier `/etc/mail/sendmail.cf` pour exécuter ses fonctions.

Le système d'exploitation Solaris fournit deux fichiers de configuration par défaut dans le répertoire `/etc/mail`.

1. `sendmail.cf`, fichier de configuration utilisé pour exécuter `sendmail` en mode démon.
2. `submit.cf`, fichier de configuration utilisé pour exécuter `sendmail` en mode programme d'envoi du courrier, au lieu du mode démon. Pour plus d'informations, reportez-vous à la section "Fichier de configuration `submit.cf` à partir de la version 8.12 de `sendmail`" à la page 393.

Lors de la configuration des clients de messagerie, serveurs de courrier, hôtes de messagerie ou passerelles de messagerie, prenez en compte les points suivants :

- Pour les clients de messagerie et les serveurs de courrier, vous n'avez rien à faire pour configurer ou modifier le fichier de configuration par défaut.
- Pour configurer un hôte de messagerie ou une passerelle de messagerie, vous devez définir les paramètres du logiciel de messagerie relais et de l'hôte de relais qui sont nécessaires pour votre configuration de messagerie. Pour plus d'informations sur les tâches, reportez-vous à la section "Configuration des services de messagerie (liste des tâches)" à la page 296 ou "Modification de la configuration sendmail" à la page 305 du Chapitre 13, "Services de messagerie (tâches)". Notez qu'avec `sendmail` version 8.13, vous n'avez plus besoin du fichier `main.cf`.

La liste suivante décrit certains paramètres de configuration que vous pouvez modifier, selon les exigences de votre site.

- Les valeurs temporelles, qui permettent de spécifier les informations suivantes.
  - Délais d'attente de lecture.
  - Durée pendant laquelle un message reste dans la file d'attente sans avoir été distribué avant qu'il ne soit renvoyé à l'expéditeur. Reportez-vous à la section "Fonctions de file d'attente supplémentaires à partir de la version 8.12 de `sendmail`" à la page 406. Pour obtenir la liste des tâches, reportez-vous à la section "Administration des répertoires de file d'attente (liste des tâches)" à la page 327.
- Modes de distribution, qui permettent de spécifier la vitesse de distribution du courrier.
- Limites de charge, qui permettent d'améliorer l'efficacité en périodes d'activité élevée. Ces paramètres empêcher `sendmail` d'essayer de distribuer les messages volumineux, les messages adressés à un trop grand nombre de destinataires et les messages vers des sites qui ont été arrêtés depuis longtemps.
- Niveau de consignation, qui indique les types de problème qui sont consignés.

Fichiers d'alias de messagerie

Vous pouvez utiliser quelconque des fichiers, cartes ou tables suivants pour tenir à jour les alias.

Votre méthode de mise à jour des alias dépend de l'utilisateur de l'alias et de la personne qui doit être en mesure de modifier l'alias. Chaque type d'alias possède ses propres exigences de format.

Si vous recherchez des informations sur les tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Alias `.mailrc`

Les alias qui sont répertoriés dans un fichier `.mailrc` sont accessibles uniquement par l'utilisateur qui détient le fichier. Cette restriction permet aux utilisateurs d'établir un fichier d'alias qu'ils contrôlent et qui est uniquement utilisable par son propriétaire. Les alias d'un fichier `.mailrc` respectent le format suivant.

`alias` *aliasname value value value* `...`

aliasname est le nom que l'utilisateur utilise lors de l'envoi de courrier et *value* est une adresse e-mail valide.

Si un utilisateur établit un alias personnel pour `scott` qui ne correspond pas à l'adresse e-mail pour `scott` dans le service de noms, une erreur se produit. Le courrier est acheminé à la personne erronée lorsque les gens essaient de répondre à un message généré par cet utilisateur. La seule solution consiste à utiliser l'un des autres mécanismes de définition d'alias.

Fichier `/etc/mail/aliases`

N'importe quel alias qui est établi dans le fichier `/etc/mail/aliases` peut être utilisé par tout utilisateur qui connaît le nom de l'alias et le nom d'hôte du système qui contient le fichier. Les listes de distribution d'un fichier `/etc/mail/aliases` respectent le format suivant.

aliasname: *value,value,value* `...`

aliasname est le nom que l'utilisateur utilise lors de l'envoi de courrier à cet alias et *value* est une adresse e-mail valide.

Si votre réseau n'exécute pas de service de noms, le fichier `/etc/mail/aliases` de chaque système doit contenir des entrées pour tous les clients de messagerie. Vous pouvez modifier le fichier sur chaque système ou modifier le fichier sur un système et le copier sur chacun des autres systèmes.

Les alias du fichier `/etc/mail/aliases` sont stockés sous forme de texte. Lorsque vous modifiez le fichier `/etc/mail/aliases`, vous avez besoin d'exécuter le programme `newaliases`. Ce programme recompile la base de données et rend les alias disponibles sous forme binaire pour le programme `sendmail`. Pour obtenir des informations sur les tâches, reportez-vous à la section "Configuration d'un fichier d'alias de messagerie locale" à la page 323 du Chapitre 13, "Services de messagerie (tâches)". Vous pouvez également utiliser la fonction de liste de diffusion dans la console de gestion Solaris pour administrer les alias de messagerie stockés dans les fichiers `/etc` locaux.

Vous pouvez créer des alias uniquement pour les noms locaux, tels qu'un nom d'hôte en cours ou aucun nom d'hôte. Par exemple, une entrée d'alias pour l'utilisateur `ignatz` qui possède une boîte à lettres sur le système `saturn` aurait l'entrée suivante dans le fichier `/etc/mail/aliases`.

```
ignatz: ignatz@saturn
```

Vous devez créer un compte d'administration pour chaque serveur de courrier. Vous créez un tel compte en affectant une boîte à lettres sur le serveur de courrier à l'utilisateur `root` et en ajoutant une entrée pour `root` au fichier `/etc/mail/aliases`. Par exemple, si le système `saturn` est un serveur de boîte à lettres, ajoutez l'entrée `root: sysadmin@saturn` au fichier `/etc/mail/aliases`.

Normalement, seul l'utilisateur `root` peut modifier ce fichier. Cependant, lorsque vous utilisez la console de gestion Solaris, tous les utilisateurs du groupe 14, qui est le groupe sysadmin, peuvent modifier le fichier local. Une autre option consiste à créer l'entrée suivante.

aliasname`: :include:`*/path/aliasfile*

aliasname est le nom que l'utilisateur utilise lors de l'envoi du courrier et */path/aliasfile* est le chemin d'accès complet au fichier qui contient la liste des alias. Le fichier d'alias doit inclure les entrées de messagerie, une entrée sur chaque ligne et aucune autre notation.

user1@host1
user2@host2

Vous pouvez définir d'autres fichiers de courrier dans `/etc/mail/aliases` pour enregistrer un journal ou une copie de sauvegarde. L'entrée suivante stocke tout le courrier qui est envoyé à *aliasname* dans *filename*.

aliasname`: /home/backup/`*filename*

Vous pouvez également acheminer le courrier vers un autre processus. L'exemple suivant stocke une copie du message e-mail dans *filename* et en imprime une copie.

aliasname`: "|tee -a /home/backup/`*filename*` |lp"`

Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Carte `aliases` NIS

Tous les utilisateurs d'un domaine local peuvent utiliser les entrées qui sont contenues dans la carte `aliases` NIS. La raison en est que le programme `sendmail` peut utiliser la carte `aliases` NIS au lieu des fichiers `/etc/mail/aliases` locaux pour déterminer les adresses de la liste de diffusion. Pour plus d'informations, reportez-vous à la page de manuel `nsswitch.conf(4)`.

Les alias de la carte `aliases` NIS respectent le format suivant.

aliasname: *value,value,value* ...

aliasname est le nom que l'utilisateur utilise lors de l'envoi de courrier et *value* est une adresse e-mail valide.

La carte `aliases` NIS doit contenir des entrées pour tous les clients de messagerie. En général, seul l'utilisateur root sur le maître NIS peut modifier ces entrées. Ce type d'alias n'est peut-être pas un bon choix pour les alias qui sont en constante évolution. Toutefois, ces alias peuvent être utiles s'ils pointent vers un autre fichier d'alias, comme dans l'exemple de syntaxe suivant.

aliasname: *aliasname@host*

aliasname est le nom que l'utilisateur utilise lors de l'envoi de courrier et *host* est le nom d'hôte du serveur qui contient un fichier `/etc/mail/alias`.

Pour obtenir des informations sur les tâches, reportez-vous à la section "Configuration d'une carte `mail.alias` NIS" à la page 322 du Chapitre 13, "Services de messagerie (tâches)".

Table `mail_aliases` NIS+

La table `mail_aliases` NIS+ contient les noms par lesquels un système ou une personne est connu(e) dans le domaine local. Le programme `sendmail` peut utiliser la table `mail_aliases` NIS+, au lieu des fichiers `/etc/mail/aliases` locaux, pour déterminer les adresses de la liste de diffusion. Pour plus d'informations, reportez-vous aux pages de manuel `aliasadm(1M)` et `nsswitch.conf(4)`.

Les alias de la table `mail_aliases` NIS+ respectent le format suivant.

alias: *expansion* `#` `[`"*options*" `#` "*comments*"`]`

Le Tableau 14–12 décrit les quatre colonnes qui se trouvent dans une table `mail_aliases` NIS+.

TABLEAU 14–12 Colonnes de la table `mail_aliases` NIS+

Colonne	Description
`alias`	Nom de l'alias
`expansion`	Valeur de l'alias ou liste d'alias tel qu'elle apparaîtrait dans un fichier `sendmail` `/etc/mail/aliases`

TABLEAU 14–12 Colonnes de la table `mail_aliases` NIS+ *(Suite)*

Colonne	Description
`options`	Colonne réservée pour une utilisation ultérieure
`comments`	Colonne des commentaires sur un alias particulier

La table `mail_aliases` NIS+ doit contenir des entrées pour tous les clients de messagerie. Vous pouvez répertorier, créer, modifier et supprimer des entrées dans la table `aliases` NIS+ avec la commande `aliasadm`. Pour utiliser la commande `aliasadm`, vous devez être membre du groupe NIS+ propriétaire de la table `aliases`. Pour plus d'informations sur les tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)". Alternativement, vous pouvez utiliser la console de gestion Solaris pour administrer les alias de messagerie NIS+.

Remarque – Si vous créez une nouvelle table `aliases` NIS+, vous devez initialiser la table avant de créer les entrées. Si la table existe, aucune initialisation n'est nécessaire.

Fichier `.forward`

Les utilisateurs peuvent créer un fichier `.forward` dans leurs répertoires personnels que `sendmail`, ainsi que d'autres programmes, peut utiliser pour rediriger le courrier ou l'envoyer. Reportez-vous aux sections ci-après.

Pour obtenir la liste des tâches, reportez-vous à la section "Administration des fichiers `.forward` (liste des tâches)" à la page 331 du Chapitre 13, "Services de messagerie (tâches)".

Situations à éviter

La liste suivante décrit certaines situations que vous pouvez éviter ou résoudre facilement.

- Si le courrier n'est pas distribué à l'adresse attendue, vérifiez le fichier `.forward` de l'utilisateur. L'utilisateur a peut-être mis le fichier `.forward` dans le répertoire personnel de `host1`, qui transfère le courrier à `user@host2`. Lorsque le message arrive à `host2`, `sendmail` vérifie la présence de `user` dans les alias NIS ou NIS+ et renvoie le message à `user@host1`. Cet acheminement forme une boucle et davantage de courrier retourné.
- Pour éviter les problèmes de sécurité, ne placez jamais les fichiers `.forward` dans les comptes `root` et `bin`. Si nécessaire, au lieu de ça, transférez le courrier à l'aide du fichier `aliases`.

Contrôles des fichiers `.forward`

Pour que les fichiers `.forward` constituent un élément efficace de la distribution du courrier, assurez-vous que les contrôles suivants (des paramètres des autorisations principalement) sont correctement appliqués.

- Le fichier `.forward` doit être accessible en écriture uniquement par le propriétaire du fichier. Cette restriction empêche les autres utilisateurs de rompre la sécurité.
- Les chemins qui conduisent au répertoire personnel doivent être possédés et accessibles en écriture par l'utilisateur `root` uniquement. Par exemple, si un fichier `.forward` se trouve dans `/export/home/terry`, les fichiers `/export` et `/export/home` doivent être possédés et accessibles en écriture par l'utilisateur `root` uniquement.
- Le répertoire personnel utilisé doit être accessible en écriture uniquement par l'utilisateur.
- Le fichier `.forward` ne peut pas être un lien symbolique, et ce fichier ne peut pas avoir plus d'un lien physique.

Fichier `.forward.`*hostname*

Vous pouvez créer un fichier `.forward.` *hostname* pour rediriger le courrier qui est envoyé à un hôte spécifique. Par exemple, si l'alias d'un utilisateur est passé de `sandy@phoenix.example.com` à `sandy@example.com`, placez un fichier `.forward.phoenix` dans le répertoire personnel pour `sandy`.

```
% cat .forward.phoenix
sandy@example.com
"|/usr/bin/vacation sandy"
% cat .vacation.msg
From: sandy@example.com (via the vacation program)
Subject: my alias has changed

My alias has changed to sandy@example.com.
Please use this alias in the future.
The mail that I just received from you
has been forwarded to my new address.

Sandy
```

Dans cet exemple, le courrier peut être transférer à la bonne place alors que l'expéditeur est informé du changement d'alias. Dans la mesure où le programme `vacation` permet un seul fichier de message, vous ne pouvez transférer qu'un message à la fois. Toutefois, si le message n'est pas spécifique à l'hôte, un fichier de message vacation peut être utilisé par des fichiers `.forward` pour de nombreux hôtes.

Fichier `.forward+`*détail*

Le fichier `.forward+`*detail* est une autre extension du mécanisme de transfert. La chaîne *detail* peut être n'importe quelle séquence de caractères à l'exception des caractères d'opérateur. Ces caractères sont `.:%&!^[]+`. L'utilisation de ce type de fichier permet de déterminer si quelqu'un

d'autre utilise votre adresse e-mail sans que vous le sachiez. Par exemple, si un utilisateur indique à quelqu'un d'utiliser l'adresse e-mail `sandy+test1@example.com`, l'utilisateur doit être en mesure d'identifier tous les futurs messages distribués à cet alias. Par défaut, tous les messages envoyés à l'alias `sandy+test1@example.com` sont comparés à l'alias et aux fichiers `.forward+`*detail*. Si aucune correspondance n'est établie, le message est replanifié pour être distribué à `sandy@example.com`, mais l'utilisateur est en mesure de voir un changement dans l'en-tête du message `To:`.

Fichier `/etc/default/sendmail`

Ce fichier est utilisé pour stocker les options de démarrage pour `sendmail` afin qu'elles ne soient pas supprimées lorsqu'un hôte est mis à niveau. Les variables ci-dessous peuvent être utilisées.

CLIENTOPTIONS="*string*"
: Permet de sélectionner des options supplémentaires à utiliser avec le démon client, qui effectue ses recherches dans la file d'attente du client uniquement (`/var/spool/clientmqueue`) et agit comme un programme d'exécution de la file d'attente client. Aucune vérification de la syntaxe n'est effectuée, soyez donc prudent lorsque vous apportez des modifications à cette variable.

CLIENTQUEUEINTERVAL=#
: De la même manière que l'option `QUEUEINTERVAL`, `CLIENTQUEUEINTERVAL` définit l'intervalle de temps avant l'exécution de la file d'attente de messages. Toutefois, l'option `CLIENTQUEUEINTERVAL` contrôle les fonctions du démon client, plutôt que celles du démon principal. En règle générale, le démon principal est en mesure de distribuer tous les messages au port SMTP. Toutefois, si la charge de messages est trop élevée ou si le démon principal n'est pas en cours d'exécution, les messages sont mis dans la file d'attente du client uniquement, `/var/spool/clientmqueue`. Le démon client, qui vérifie la file d'attente du client uniquement, agit ensuite comme un processeur de file d'attente client.

ETRN_HOSTS="*string*"
: Permet à un client et un serveur SMTP d'interagir immédiatement, sans attendre l'intervalle d'exécution de la file d'attente, qui est périodique. Le serveur peut immédiatement distribuer la partie de sa file d'attente destinée aux hôtes spécifiés. Pour plus d'informations, reportez-vous à la page de manuel `etrn`(1M).

MODE=-bd
: Sélectionne le mode pour démarrer `sendmail` avec. Utilisez l'option `-bd` ou laissez-la non définie.

OPTIONS=*string*
: Sélectionne des options supplémentaires à utiliser avec le démon principal. Aucune vérification de la syntaxe n'est effectuée, soyez donc prudent lorsque vous apportez des modifications à cette variable.

QUEUEINTERVAL=#
: Définit l'intervalle pour les exécutions de la file d'attente de messages sur le démon principal. # est un entier positif qui peut être suivi par `s` pour les secondes, `m` pour les minutes, `h` pour les heures, `d` pour les jours ou `w` pour les semaines. La syntaxe est vérifiée avant le démarrage de `sendmail`. Si l'intervalle est négatif ou si l'entrée ne termine pas par une lettre appropriée, l'intervalle est ignoré et `sendmail` commence par un intervalle de file d'attente de 15 minutes.

QUEUEOPTIONS=p
: Active un seul programme d'exécution de file d'attente persistante qui demeure en veille entre les intervalles d'exécution de la file d'attente, au lieu d'activer un nouveau programme d'exécution de file d'attente pour chaque intervalle d'exécution de la file d'attente. Vous pouvez définir cette option sur `p`, qui est le seul paramètre disponible. Dans le cas contraire, cette option n'est pas définie.

Adresses e-mail et acheminement du courrier

Le chemin emprunté par un message électronique lors de la distribution dépend de la configuration du système client et de la topologie du domaine de messagerie. Chaque niveau supplémentaire d'hôtes de messagerie ou de domaines de messagerie peut ajouter une autre résolution d'alias, mais le processus d'acheminement est essentiellement le même sur la plupart des hôtes.

Vous pouvez configurer un système client pour qu'il reçoive le courrier localement. La réception du courrier en local est connue comme étant l'exécution de `sendmail` en mode local. Ce mode est celui défini par défaut pour tous les serveurs de courrier et certains clients. Sur un serveur de courrier ou un client de messagerie exécuté en mode local, un message électronique est acheminé selon la procédure ci-dessous.

Remarque – L'exemple ci-après suppose que vous utilisez l'ensemble de règles par défaut du fichier `sendmail.cf`.

---

1. Développez l'alias de messagerie, si possible, et redémarrez le processus d'acheminement local.

   L'adresse e-mail est développée en recherchant l'alias de messagerie dans le service de noms et en remplaçant la nouvelle valeur, si une nouvelle valeur est trouvée. Ce nouvel alias est ensuite à nouveau vérifié.

2. Si le courrier est local, remettez-le à `/usr/lib/mail.local`.

   Le courrier est transmis à une boîte à lettres locale.

3. Si l'adresse e-mail inclut un hôte dans ce domaine de messagerie, distribuez le courrier à cet hôte.

4. Si l'adresse n'inclut pas d'hôte dans ce domaine, transférez le courrier à l'hôte de messagerie.

L'hôte de messagerie utilise le même processus d'acheminement que le serveur de courrier. Cependant, le serveur de courrier peut recevoir du courrier qui est adressé au nom du domaine, ainsi qu'au nom de l'hôte.

Interactions de sendmail avec des services de noms

Cette section décrit les noms de domaine tels qu'ils s'appliquent à sendmail et aux services de noms. En outre, cette section décrit les règles pour une utilisation efficace des services de noms et les interactions spécifiques de sendmail avec les services de noms. Pour plus d'informations, reportez-vous aux rubriques suivantes.

Si vous recherchez des informations sur les tâches en rapport, reportez-vous à la section "Utilisation de DNS avec sendmail" à la page 304 ou "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

sendmail.cf et domaines de messagerie

Le fichier sendmail.cf standard utilise des domaines de messagerie afin de déterminer si le courrier est distribué directement ou par le biais d'un hôte de messagerie. Le courrier intradomaine est livré par l'intermédiaire d'une connexion SMTP directe, alors que le courrier interdomaine est transférer à un hôte de messagerie.

Dans un réseau sécurisé, seuls quelques hôtes sélectionnés sont autorisés à générer les paquets qui sont destinés à des destinations extérieures. Même si un hôte dispose de l'adresse IP de l'hôte distant qui est externe au domaine de messagerie, l'établissement d'une connexion SMTP n'est pas garanti. Le fichier sendmail.cf standard suppose les conditions suivantes.

- L'hôte en cours n'est pas autorisé à envoyer des paquets directement à un hôte à l'extérieur du domaine de messagerie.
- L'hôte de messagerie est capable de transférer le courrier à un hôte autorisé qui peut transmettre les paquets directement à un hôte externe. En fait, l'hôte de messagerie peut être un hôte autorisé.

Selon ces suppositions, l'hôte de messagerie est responsable de la distribution ou du transfert du courrier interdomaine.

sendmail et les services de noms

sendmail impose diverses exigences pour les services de noms. Pour améliorer votre compréhension de ces exigences, cette section décrit d'abord la relation des domaines de messagerie avec les domaines de service de noms. La section décrit ensuite les différentes exigences. Reportez-vous aux sections suivantes.

- "Domaines de messagerie et domaines de service de noms" à la page 379
- "Configuration requise pour les services de noms" à la page 379
- Pages de manuel pour NIS+(1), nisaddent(1M) et nsswitch.conf(4)

Domaines de messagerie et domaines de service de noms

Le nom du domaine de messagerie doit être un suffixe du domaine de service de noms. Par exemple, si le nom de domaine du service de noms est A.B.C.D, le nom du domaine de messagerie peut être l'un des suivants.

- A.B.C.D
- B.C.D
- C.D
- D

Lorsqu'il est établi pour la première fois, le nom du domaine de messagerie est souvent identique au domaine de service de noms. Au fur et à mesure que le réseau s'étend, le domaine de service de noms peut être divisé en petites parties pour rendre le service de noms plus facile à gérer. Cependant, le domaine de messagerie demeure souvent entier pour assurer la cohérence de la définition d'alias.

Configuration requise pour les services de noms

Cette section décrit les exigences que sendmail impose pour les services de noms.

Une table ou une carte d'hôtes dans un service de noms doit être configurée pour prendre en charge trois types de requêtes gethostbyname().

- mailhost – Certaines configurations de service de noms satisfont automatiquement cette exigence.
- Nom d'hôte complet (par exemple, smith.admin.acme.com) – De nombreuses configurations de service de noms répondent à cette condition.
- Nom d'hôte court (par exemple, smith) – sendmail doit se connecter à l'hôte de messagerie afin de transférer le courrier externe. Pour déterminer si une adresse e-mail se trouve dans le domaine de messagerie en cours, la fonction gethostbyname() est appelée avec le nom d'hôte complet. Si l'entrée est trouvée, l'adresse est considérée comme interne.

  NIS, NIS+ et DNS prennent en charge gethostbyname() avec un nom d'hôte court comme argument, de sorte que cette condition est automatiquement remplie.

Deux règles supplémentaires relatives au service de noms d'hôte doivent être respectées pour établir des services sendmail efficaces au sein d'un service de noms.

- La fonction gethostbyname() avec un argument de nom d'hôte complet et un argument de nom d'hôte court doit obtenir des résultats cohérents. Par exemple, gethostbyname(smith.admin.acme.com) doit renvoyer le même résultat que gethostbyname(smith), si ces deux fonctions sont appelées à partir du domaine de messagerie admin.acme.com.
- Pour tous les domaines du service de noms placés sous un domaine de messagerie commun, gethostbyname() avec un nom d'hôte court doit donner le même résultat. Si, par exemple, le domaine de messagerie smith.admin.acme.com est donné, gethostbyname(smith) doit renvoyer le même résultat lorsque l'appel est effectué à partir du domaine ebb.admin.acme.com ou du domaine esg.admin.acme.com. Le nom de domaine de messagerie est généralement plus court que celui du domaine de service de noms, ce qui confère à cette exigence des conséquences particulières pour plusieurs services de noms.

Pour plus d'informations sur la fonction gethostbyname(), reportez-vous à la page de manuel gethostbyname(3NSL).

Interactions entre NIS et sendmail

La liste ci-dessous décrit les interactions entre sendmail et NIS et fournit quelques indications.

- **Nom de domaine de messagerie** – Si vous configurez NIS en tant que service de noms principal, sendmail supprime automatiquement le premier composant du nom de domaine NIS et utilise ce qu'il obtient en tant que nom de domaine de messagerie. Par exemple, ebs.admin.acme.com devient admin.acme.com.
- **Nom d'hôte de messagerie** – Vous devez disposer d'une entrée mailhost dans la carte d'hôtes NIS.
- **Noms d'hôte complets** – La configuration NIS normale ne “comprend” pas le nom d'hôte complet. Plutôt que de faire en sorte que NIS comprenne le nom d'hôte complet, désactivez cette exigence à l'aide de la commande sendmail en modifiant le fichier sendmail.cf et en remplaçant toutes les occurrences de %l par %y. Cette modification désactive la détection du courrier interdomaine de sendmail. Si l'hôte cible peut être résolu en une adresse IP, une distribution SMTP directe est tentée. Assurez-vous que votre carte d'hôtes NIS ne contient pas d'entrée d'hôte qui est externe au domaine de messagerie actuel. Sinon, vous devez personnaliser davantage le fichier sendmail.cf.
- **Correspondance des noms d'hôte complets et des noms d'hôte courts** – Suivez les instructions ci-dessus sur la manière de désactiver gethostbyname() pour un nom d'hôte complet.
- **Plusieurs domaines NIS dans un domaine de messagerie** – Toutes les cartes d'hôtes NIS sous un même domaine de messagerie doivent avoir le même ensemble d'entrées d'hôte. Par exemple, la carte d'hôtes dans le domaine ebs.admin.acme.com doit être identique à la carte

d'hôtes dans esg.admin.acme.com. Dans le cas contraire, une adresse peut fonctionner dans un domaine NIS, mais ne pas fonctionner dans l'autre domaine NIS.

Pour plus d'informations sur les tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Interactions de sendmail avec NIS et DNS

La liste ci-dessous décrit les interactions de sendmail avec NIS et DNS, et fournit quelques indications.

- **Nom de domaine de messagerie** – Si vous configurez NIS en tant que service de noms principal, sendmail supprime automatiquement le premier composant du nom de domaine NIS et utilise ce qu'il obtient en tant que nom de domaine de messagerie. Par exemple, ebs.admin.acme.com devient admin.acme.com.
- **Nom d'hôte de messagerie** – Lorsque la fonction de transfert DNS est activée, les requêtes non résolues par NIS sont transférées à DNS ; ainsi, vous n'avez pas besoin d'une entrée mailhost dans la carte d'hôtes NIS.
- **Noms d'hôte complets** – Même si NIS ne sait pas interpréter les noms d'hôte complets, DNS le sait. Cette condition est remplie lorsque vous suivez la procédure standard pour configurer NIS et DNS.
- **Correspondance des noms d'hôte complets et des noms d'hôte courts** – Pour chaque entrée d'hôte dans la table d'hôtes NIS, vous devez avoir une entrée d'hôte correspondante dans DNS.
- **Plusieurs domaines NIS dans un domaine de messagerie** – Toutes les cartes d'hôtes NIS sous un même domaine de messagerie doivent avoir le même ensemble d'entrées d'hôte. Par exemple, la carte d'hôtes dans le domaine ebs.admin.acme.com doit être identique à la carte d'hôtes dans esg.admin.acme.com. Dans le cas contraire, une adresse peut fonctionner dans un domaine NIS, mais ne pas fonctionner dans l'autre domaine NIS.

Pour plus d'informations sur les tâches, reportez-vous à la section "Utilisation de DNS avec sendmail" à la page 304 ou "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Interactions entre NIS+ et sendmail

La liste ci-dessous décrit les interactions entre sendmail et NIS+, et fournit quelques indications.

- **Nom de domaine de messagerie** – Si vous configurez NIS+ en tant que service de noms principal, `sendmail` peut vérifier le domaine de messagerie à partir de la table `sendmailvars` NIS+. Cette table NIS+ présente une colonne de clés et une colonne de valeurs. Pour configurer votre domaine de messagerie, vous devez ajouter une entrée à cette table. La colonne de clés de cette entrée doit être définie sur la chaîne littérale `maildomain` et la colonne de valeurs doit être définie sur votre nom de domaine de messagerie. C'est le cas, par exemple, de `admin.acme.com`. Bien que NIS+ permette la présence de n'importe quelle chaîne dans la table `sendmailvars`, la règle du suffixe s'applique toujours pour que le système de messagerie fonctionne correctement. Vous pouvez utiliser `nistbladm` pour ajouter l'entrée `maildomain` à la table `sendmailvars`. Remarquez, dans l'exemple ci-dessous, que le domaine de messagerie est un suffixe du domaine NIS+.

  ```
  nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
  ```
- **Nom d'hôte de messagerie** – Vous devez disposer d'une entrée `mailhost` dans la carte d'hôtes NIS+.
- **Noms d'hôte complets** – NIS+ sait interpréter le nom d'hôte complet. Suivez la procédure de configuration NIS+ habituelle pour satisfaire cette exigence.
- **Correspondance ces noms d'hôte complets et des noms d'hôte courts** – Pour satisfaire cette exigence, vous pouvez dupliquer les entrées de la table d'hôtes. Sinon, vous pouvez saisir toutes les entrées d'hôtes des domaines de service de noms d'utilisateur dans une table d'hôtes principale au niveau du domaine de messagerie.
- **Plusieurs domaines NIS dans un domaine de messagerie** – Pour satisfaire cette condition, vous pouvez dupliquer les entrées de toutes les tables d'hôtes. Sinon, vous pouvez saisir toutes les entrées d'hôtes des domaines de service de noms d'utilisateur dans une table d'hôtes principale au niveau du domaine de messagerie. En réalité, vous fusionnez plusieurs tables d'hôtes logiques ou physiques dans une seule table d'hôtes. Par conséquent, le même nom d'hôte ne peut pas être réutilisé dans le domaine de service de noms multiples qui partage un domaine de messagerie commun.

Pour plus d'informations sur les tâches, reportez-vous à la section "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 du Chapitre 13, "Services de messagerie (tâches)".

Interactions de `sendmail` avec NIS+ et DNS

La liste ci-dessous décrit les interactions de `sendmail` avec NIS+ et DNS, et fournit quelques indications.

- **Nom de domaine de messagerie** – Si vous configurez NIS+ en tant que service de noms principal, `sendmail` peut vérifier le domaine de messagerie à partir de la table `sendmailvars` NIS+. Cette table NIS+ présente une colonne de clés et une colonne de valeurs. Pour configurer votre domaine de messagerie, vous devez ajouter une entrée à cette table. La colonne de clés de cette entrée doit être définie sur la chaîne littérale `maildomain` et la colonne de valeurs doit être définie sur votre nom de domaine de messagerie. C'est le cas,

par exemple, de admin.acme.com. Bien que NIS+ permette la présence de n'importe quelle chaîne dans la table sendmailvars, la règle du suffixe s'applique toujours pour que le système de messagerie fonctionne correctement. Vous pouvez utiliser nistbladm pour ajouter l'entrée maildomain à la table sendmailvars. Remarquez, dans l'exemple ci-dessous, que le domaine de messagerie est un suffixe du domaine NIS+.

```
nistbladm -A key="maildomain" value=<mail domain> sendmailvars.org_dir.<NIS+ domain>
```

- **Nom d'hôte de messagerie** – Si votre réseau utilise NIS+ et DNS en tant que source pour la base de données d'hôtes, vous pouvez placer l'entrée mailhost dans l'une ou l'autre des tables d'hôtes NIS+ ou DNS. Assurez-vous que vos utilisateurs incluent NIS+ et DNS en tant que source de la base de données d'hôtes dans le fichier /etc/nsswitch.conf.
- **Noms d'hôte complets** – NIS+ et DNS savent interpréter les noms d'hôte complets. Suivez les procédures de configuration NIS+ et DNS habituelles pour satisfaire cette exigence.
- **Correspondance des noms d'hôte complets et des noms d'hôte courts** – Pour chaque entrée d'hôte dans la table d'hôtes NIS+, vous devez avoir une entrée d'hôte correspondante dans DNS.
- **Plusieurs domaines NIS dans un domaine de messagerie** – Pour satisfaire cette condition, vous pouvez dupliquer les entrées de toutes les tables d'hôtes. Vous pouvez également saisir toutes les entrées d'hôtes des domaines de service de noms d'utilisateur dans une table d'hôtes principale au niveau du domaine de messagerie.

Pour plus d'informations sur les tâches, reportez-vous aux sections "Administration des fichiers d'alias de messagerie (liste des tâches)" à la page 315 et "Utilisation de DNS avec sendmail" à la page 304 du Chapitre 13, "Services de messagerie (tâches)".

Modifications de la version 8.13 de sendmail

Bien que cette nouvelle version de sendmail propose de nombreuses nouveautés, l'option FallBackSmartHost constitue le nouvel élément le plus important. Grâce à cette option, il n'est plus nécessaire d'utiliser les fichiers main.cf et subsidiary.cf. Le fichier main.cf était utilisé dans des environnements qui prenaient en charge les enregistrements MX. Le fichier subsidiary.cf, quant à lui, était employé dans des environnements sans DNS entièrement opérationnel. Dans ce type d'environnement, un hôte intelligent était utilisé à la place des enregistrements MX. L'option FallBackSmartHost propose une configuration unifiée. Elle agit comme un enregistrement MX de la dernière préférence possible pour tous les environnements. Pour s'assurer que les messages ont été envoyés aux clients, cette option, lorsqu'elle est activée, fournit un hôte connecté de façon appropriée (ou intelligent), qui est utilisé en tant que sauvegarde (ou basculement) en cas de problème avec les enregistrements MX.

Pour plus d'informations sur la version 8.13, reportez-vous aux sections suivantes :

- “Options de ligne de commande supplémentaires dans la version 8.13 de sendmail” à la page 389
- “Options de fichier de configuration supplémentaires et révisées dans la version 8.13 de sendmail” à la page 390
- “Déclarations FEATURE() supplémentaires et révisées dans la version 8.13 de sendmail” à la page 391

En outre, à partir de la version Solaris 10 1/06, SMTP peut s'exécuter avec le protocole TLS (Transport Layer Security). Reportez-vous à la description ci-après.

Prise en charge de l'exécution de SMTP avec TLS dans la version 8.13 de sendmail

Les communications entre les serveurs et clients SMTP ne sont généralement pas contrôlées ni de confiance sur l'une ou l'autre extrémité. Ce manque de sécurité peut autoriser un tiers à surveiller et même modifier une communication entre un serveur et un client. À partir de la version Solaris 10 1/06, SMTP peut utiliser le protocole TLS (Transport Layer Security) dans la version 8.13 de sendmail pour résoudre ce problème. Ce service étendu aux serveurs et clients SMTP fournit les avantages suivants :

- Communications privées et authentifiées sur Internet
- Protection contre les écoutes électroniques et les pirates

Remarque – L'implémentation du protocole TLS est basée sur le protocole SSL (Secure Sockets Layer).

STARTTLS est le mot-clé SMTP qui lance une connexion SMTP sécurisée en utilisant TLS. Cette connexion sécurisée peut se située entre deux serveurs ou entre un serveur et un client. Une connexion sécurisée est définie comme suit :

- L'adresse e-mail source et l'adresse de destination sont chiffrées.
- Le contenu du message électronique est chiffré.

Lorsque le client émet la commande STARTTLS, le serveur répond avec l'un des messages suivants :

- `220 Ready to start TLS`
- `501 Syntax error (no parameters allowed)`
- `454 TLS not available due to temporary reason`

La réponse 220 nécessite que le client lancer la négociation TLS. La réponse 501 indique que le client a lancé la commande STARTTLS à tort. La commande STARTTLS est émise sans paramètres.

La réponse 454 nécessite que le client applique des valeurs d'ensemble de règles pour déterminer s'il doit accepter ou maintenir la connexion.

Notez que pour maintenir l'infrastructure SMTP Internet, les serveurs utilisés publiquement ne doivent pas exiger une négociation TLS. Toutefois, un serveur qui est utilisé de manière exclusive peut exiger que le client effectue une négociation TLS. Dans de tels cas, le serveur renvoie la réponse suivante :

```
530 Must issue a STARTTLS command first
```

La réponse 530 indique au client d'émettre la commande STARTTLS pour l'établissement d'une connexion.

Le serveur ou le client peut refuser une connexion si le niveau d'authentification et de confidentialité n'est pas satisfaisant. En outre, dans la mesure où la plupart des connexions SMTP ne sont pas sûres, le serveur et le client peuvent également conserver une connexion non sécurisée. Le maintien ou le refus d'une connexion est déterminé par la configuration du serveur et du client.

La prise en charge de l'exécution de SMTP avec TLS n'est pas activée par défaut. Le protocole TLS est activé lorsque le client SMTP émet la commande STARTTLS. Avant que le client SMTP puisse émettre cette commande, vous devez configurer les certificats permettant à sendmail d'utiliser TLS. Reportez-vous à la section "Configuration de SMTP pour utiliser le protocole TLS" à la page 309. Notez que cette procédure inclut la définition des options d'un nouveau fichier de configuration et la reconstruction de votre fichier sendmail.cf.

Options du fichier de configuration pour l'exécution de SMTP avec TLS

Le tableau ci-dessous décrit les options du fichier de configuration qui sont utilisées pour exécuter SMTP avec TLS. Si vous déclarez n'importe laquelle de ces options, utilisez l'une des syntaxes suivantes :

- O *OptionName*= *argument* # for the configuration file
- -O *OptionName*= *argument* # for the command line
- define(‘*m4Name*', *argument*) # for m4 configuration

TABLEAU 14–13 Options du fichier de configuration pour l'exécution de SMTP avec TLS

Option	Description
CACertFile	Nom de la commande m4 : confcacert Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient un certificat d'AC.

TABLEAU 14–13 Options du fichier de configuration pour l'exécution de SMTP avec TLS *(Suite)*

Option	Description
CACertPath	Nom de la commande m4 : confCACERT_PATH Argument : *path* Valeur par défaut : non définie Identifie le chemin d'accès au répertoire contenant les certificats d'AC.
ClientCertFile	Nom de la commande m4 : confCLIENT_CERT Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient le certificat du client. Notez que ce certificat est utilisé lorsque sendmail agit comme un client.
ClientKeyFile	Nom de la commande m4 : confCLIENT_KEY Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient la clé privée qui appartient au certificat client.
CRLFile	Nom de la commande m4 : confCRL Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient l'état de révocation de certificats, qui est utilisé pour l'authentification X.509v3.
DHParameters	Nom de la commande m4 : confDH_PARAMETERS Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient les paramètres Diffie-Hellman (DH).
RandFile	Nom de la commande m4 : confRAND_FILE Argument : file:*filename* ou egd:*UNIX socket* Valeur par défaut : non définie Utilise le préfixe file: pour identifier le fichier qui contient des données aléatoires ou utilise le préfixe egd: pour identifier le socket UNIX. Notez que dans la mesure où le système d'exploitation Solaris prend en charge le générateur de nombres random, cette option n'a pas besoin d'être spécifiée. Reportez-vous à la page de manuel random(7D).

TABLEAU 14–13 Options du fichier de configuration pour l'exécution de SMTP avec TLS *(Suite)*

Option	Description
ServerCertFile	Nom de la commande m4 : confSERVER_CERT Argument : *filename* Valeur par défaut : non définie Identifie le fichier qui contient le certificat du serveur. Ce certificat est utilisé lorsque sendmail agit comme un serveur.
Timeout.starttls	Nom de la commande m4 : confTO_STARTTLS Argument : *amount of time* Valeur par défaut : 1h Définit la durée pendant laquelle le client SMTP attend une réponse à la commande STARTTLS.
TLSSrvOptions	Nom de la commande m4 : confTLS_SRV_OPTIONS Argument : V Valeur par défaut : non définie Détermine si le serveur demande un certificat au client. Si cette option est définie sur V, aucune vérification du client n'est effectuée.

Pour que la commande sendmail prenne en charge l'utilisation de TLS par SMTP, les options suivantes doivent être définies :

- CACertPath
- CACertFile
- ServerCertFile
- ClientKeyFile

Les autres options ne sont pas nécessaires.

Macros pour l'exécution de SMTP avec TLS

Le tableau suivant décrit les macros qui sont utilisées par la commande STARTTLS.

TABLEAU 14–14 Macros pour l'exécution de SMTP avec TLS

Macro	Description
${cert_issuer}	Contient le nom distinctif (DN) de l'autorité de certification (AC), qui est l'émetteur du certificat.
${cert_subject}	Contient le nom distinctif (DN) de certificat qui est appelé l'**objet du certificat**.

TABLEAU 14–14 Macros pour l'exécution de SMTP avec TLS *(Suite)*

Macro	Description
`${cn_issuer}`	Contient le nom commun (CN) de l'autorité de certification, qui est l'**émetteur du certificat**.
`${cn_subject}`	Contient le nom commun du certificat qui est appelé l'**objet du certificat**.
`${tls_version}`	Contient la version du protocole TLS qui est utilisé pour la connexion.
`${cipher}`	Contient un ensemble d'algorithmes de chiffrement (appelé **suite de chiffrement**) qui est utilisé pour la connexion.
`${cipher_bits}`	Conserve, en bits, la longueur de la clé de l'algorithme de chiffrement symétrique qui est utilisé pour la connexion.
`${verify}`	Contient le résultat de la vérification du certificat qui a été présenté. Les valeurs possibles sont les suivantes : ■ `OK` – La vérification a réussi. ■ `NO` – Aucun certificat n'a été présenté. ■ `NOT` – Aucun certificat n'a été demandé. ■ `FAIL` – Le certificat qui a été présenté n'a pas pu être vérifié. ■ `NONE` – La commande `STARTTLS` n'a pas été exécutée. ■ `TEMP` – Une erreur momentanée s'est produite. ■ `PROTOCOL` – Une erreur SMTP s'est produite. ■ `SOFTWARE` – Le protocole de transfert `STARTTLS` a échoué.
`${server_name}`	Contient le nom du serveur qui fournit la connexion SMTP sortante.
`${server_addr}`	Contient l'adresse du serveur qui fournit la connexion SMTP sortante.

Ensembles de règles pour l'exécution de SMTP avec TLS

Le tableau suivant décrit les ensembles de règles qui déterminent si une connexion SMTP qui utilise TLS doit être acceptée, maintenue ou refusée.

TABLEAU 14–15 Ensembles de règles pour l'exécution de SMTP avec TLS

Ensemble de règles	Description
`tls_server`	Agissant en tant que client, `sendmail` utilise cet ensemble de règles pour déterminer si le serveur est actuellement pris en charge par TLS.
`tls_client`	Agissant en tant que serveur, `sendmail` utilise cet ensemble de règles pour déterminer si le client est actuellement pris en charge par TLS.
`tls_rcpt`	Cet ensemble de règles nécessite la vérification du MTA du destinataire. Cette restriction du destinataire rend les attaques, telles que l'usurpation DNS, impossibles.
`TLS_connection`	Cet ensemble de règles vérifie la condition qui est spécifiée par le membre droit de la carte d'accès par rapport aux paramètres de la connexion TLS actuelle.

TABLEAU 14–15 Ensembles de règles pour l'exécution de SMTP avec TLS *(Suite)*

Ensemble de règles	Description
try_tls	sendmail utilise cet ensemble de règles pour déterminer la faisabilité d'utiliser STARTTLS lors de l'établissement de la connexion à un autre agent MTA. Si l'agent MTA ne peut pas correctement implémenter la commande STARTTLS, STARTTLS n'est pas utilisée.

Pour plus d'informations, reportez-vous au site http://www.sendmail.org/m4/starttls.html.

Considérations de sécurité liées à l'exécution de SMTP avec TLS

En tant que protocole de messagerie standard qui définit les logiciels de messagerie qui s'exécute sur Internet, le protocole SMTP n'est pas un mécanisme complet. En raison de cette limitation, la sécurité TLS via SMTP n'inclut pas les agents utilisateur de messagerie. Les agents utilisateur de messagerie agissent comme une interface entre les utilisateurs et un agent de transfert de courrier comme sendmail.

En outre, le courrier peut être acheminé par le biais de plusieurs serveurs. Pour une sécurité SMTP complète, la totalité de la chaîne de connexions SMTP doit prendre en charge TLS.

Enfin, le niveau de confidentialité et d'authentification négociées entre chaque paire de serveurs ou entre une paire client/serveur doit être pris en compte. Pour plus d'informations, reportez-vous à la section "Authentication Services" du *System Administration Guide: Security Services*.

Options de ligne de commande supplémentaires dans la version 8.13 de sendmail

Le tableau ci-après décrit des options de ligne de commande supplémentaires qui sont disponibles dans la version 8.13 de sendmail. D'autres options de ligne de commande sont décrites dans la page de manuel sendmail(1M).

TABLEAU 14–16 Options de ligne de commande disponibles dans la version 8.13 de sendmail

Option	Description
-D *logfile*	Envoie le résultat du débogage au fichier *logfile* indiqué, au lieu d'inclure ces informations à la sortie standard.
-q[!]Q*substr*	Spécifie le traitement des tâches mises en quarantaine et présentant l'élément *substr* , qui est une sous-chaîne de la quarantaine *reason*. Reportez-vous à la description de l'option -Q*reason*. Si un point d'exclamation (!) est ajouté, cette option traite les tâches mises en quarantaine qui ne présentent pas l'élément *substr*.

TABLEAU 14–16 Options de ligne de commande disponibles dans la version 8.13 de sendmail *(Suite)*

Option	Description
-Q*reason*	Met en quarantaine un élément de file d'attente normale avec cette *reason*. Si aucune *reason* n'est donnée, l'élément est retiré de la quarantaine. Cette option fonctionne avec l'option -q[!]Q*substr*. *substr* est une partie (ou sous-chaîne) de la *reason*.

Options de fichier de configuration supplémentaires et révisées dans la version 8.13 de sendmail

Le tableau suivant décrit les options du fichier de configuration ajoutées et révisées. Si vous déclarez n'importe laquelle de ces options, utilisez l'une des syntaxes suivantes :

```
O OptionName=argument          # for the configuration file
-O OptionName=argument         # for the command line
define(‘m4Name’,argument)     # for m4 configuration
```

TABLEAU 14–17 Options de fichier de configuration disponibles dans la version 8.13 de sendmail

Option	Description
ConnectionRateWindowSize	Nom de la commande m4 : confCONNECTION_RATE_WINDOW_SIZE Argument : *number* Valeur par défaut : 60 Définit le nombre de secondes avant la maintenance des connexions entrantes.
FallBackSmartHost	Nom de la commande m4 : confFALLBACK_SMARTHOST Argument : *hostname* Pour s'assurer que les messages ont été envoyés aux clients, cette option fournit un hôte connecté de façon appropriée, qui est utilisé en tant que sauvegarde (ou basculement) en cas de problème avec les enregistrements MX.
InputMailFilters	Nom de la commande m4 : confINPUT_MAIL_FILTERS Argument : *filename* Répertorie les filtres de courrier entrant pour le démon sendmail.
PidFile	Nom de la commande m4 : confPID_FILE Argument : *filename* Valeur par défaut : /var/run/sendmail.pid De même que dans les versions précédentes, le nom de fichier est développé par macro avant l'ouverture du fichier. En outre, dans la version 8.13, le fichier est dissocié lorsque sendmail s'arrête.

TABLEAU 14–17 Options de fichier de configuration disponibles dans la version 8.13 de sendmail *(Suite)*

Option	Description
QueueSortOrder	Nom de la commande m4 : confQUEUE_SORT_ORDER Argument ajouté : none Dans la version 8.13, none est utilisé pour ne spécifier aucun ordre de tri.
RejectLogInterval	Nom de la commande m4 : confREJECT_LOG_INTERVAL Argument : *period-of-time* Valeur par défaut : 3h, qui représente trois heures. Lorsqu'une connexion du démon est refusée pour la *période-de-temps* spécifiée, l'information est consignée.
SuperSafe	Nom de la commande m4 : confSAFE_QUEUE Nom abrégé : s Argument ajouté : postmilter Valeur par défaut : true Si postmilter est défini, la commande sendmail diffère la synchronisation du fichier de file d'attente jusqu'à ce que tous les milters aient signalés l'acceptation du message. Pour que cet argument s'avère utile, sendmail doit être exécuté en tant que serveur SMTP. Sinon, postmilter fonctionne comme si vous utilisiez l'argument true.

Déclarations FEATURE() supplémentaires et révisées dans la version 8.13 de sendmail

Le tableau suivant décrit les déclarations FEATURE() ajoutées et révisées. Cette macro m4 utilise la syntaxe suivante.

FEATURE(‘*name*’, ‘*argument*’)

TABLEAU 14–18 Déclarations FEATURE() disponibles dans la version 8.13 de sendmail

Nom de FEATURE()	Description
conncontrol	Fonctionne avec l'ensemble de règles access_db pour vérifier le nombre de connexions SMTP entrantes. Pour plus de détails, reportez-vous au fichier /etc/mail/cf/README.
greet_pause	Ajoute l'ensemble de règles greet_pause, qui active le proxy ouvert et la protection contre le slamming via SMTP. Pour plus de détails, reportez-vous au fichier /etc/mail/cf/README.

TABLEAU 14–18 Déclarations FEATURE() disponibles dans la version 8.13 de sendmail *(Suite)*

Nom de FEATURE()	Description
local_lmtp	L'argument par défaut reste mail.local, qui est le logiciel de messagerie compatible LMTP dans cette version de Solaris. Cependant, dans la version 8.13, si un autre logiciel de messagerie compatible LMTP est utilisé, le nom du chemin d'accès peut être spécifié comme un deuxième paramètre et les arguments qui sont transmis au deuxième paramètre peuvent être spécifiés dans le troisième paramètre. Exemple : FEATURE('local_lmtp', '/usr/local/bin/lmtp', 'lmtp')
mtamark	Offre une prise en charge expérimentale pour le marquage des agents de transfert de courrier dans le DNS inverse avec des enregistrements de ressources TXT RR (MTAMark). Pour plus de détails, reportez-vous au fichier /etc/mail/cf/README.
ratecontrol	Fonctionne avec l'ensemble de règles access_db pour contrôler les débits de connexion pour les hôtes. Pour plus de détails, reportez-vous au fichier /etc/mail/cf/README.
use_client_ptr	Si cette FEATURE() est activée, l'ensemble de règles check_relay remplace son premier argument par cet argument, $&{client_ptr}.

Modifications à partir de la version 8.12 de sendmail

Cette section contient des informations sur les sujets suivants.

Prise en charge des wrappers TCP à partir de la version 8.12 de sendmail

Les wrappers TCP permettent d'implémenter des contrôles d'accès en vérifiant à l'aide d'une liste de contrôle d'accès (ACL) les adresses d'un hôte demandant un service réseau particulier. Les demandes sont accordées ou refusées en conséquence. Non seulement les wrappers TCP fournissent ce système de contrôle des accès mais ils consignent également les demandes hôte de services réseau, offrant ainsi une fonction de surveillance utile. Les services réseau pouvant être soumis à un contrôle des accès incluent par exemple `rlogind`, `telnetd` et `ftpd`.

À partir de la version 8.12, `sendmail` permet l'utilisation de wrappers TCP. Cette vérification n'élimine pas les autres mesures de sécurité. Avec l'activation des wrappers TCP dans `sendmail`, une nouvelle vérification permettant de valider la source d'une demande de service réseau avant tout accord à la demande a été ajoutée. Reportez-vous à la page de manuel `hosts_access`(4).

Remarque – La prise en charge des wrappers TCP dans `inetd`(1M) et `sshd`(1M) est incluse depuis la version de Solaris 9.

Pour plus d'informations sur les listes de contrôle d'accès (ACL), reportez-vous à la section "Using Access Control Lists to Protect UFS Files" du *System Administration Guide: Security Services*.

Fichier de configuration submit.cf à partir de la version 8.12 de sendmail

À partir de la version 8.12, `sendmail` comprend un fichier de configuration supplémentaire, `/etc/mail/submit.cf`. Ce fichier, `submit.cf`, est utilisé pour exécuter `sendmail` en mode programme d'envoi du courrier, au lieu du mode démon. Le mode programme d'envoi du courrier, contrairement au mode démon, ne nécessite pas les privilèges `root`, de sorte que ce nouveau paradigme assure une meilleure sécurité.

Reportez-vous à la liste suivante de fonctions pour `submit.cf` :

- La commande `sendmail` utilise `submit.cf` pour l'exécution en mode programme d'envoi du courrier (MSP), qui envoie des messages électroniques et peut être démarré par des programmes (tels que `mailx`), ainsi que par les utilisateurs. Reportez-vous à la description des options `-Ac` et `-Am` dans la page de manuel `sendmail(1M)`.
- `submit.cf` est utilisé dans les modes de fonctionnement suivants :
  - `-bm`, qui est le mode de fonctionnement par défaut ;
  - `-bs`, qui utilise l'entrée standard pour exécuter SMTP ;
  - `-bt`, qui est le mode test utilisé pour résoudre les adresses.
- `sendmail`, lorsque vous utilisez `submit.cf`, ne s'exécute pas comme un démon SMTP.
- `sendmail`, lorsque vous utilisez `submit.cf`, utilise `/var/spool/clientmqueue`, la file d'attente de messages client uniquement, qui contient les messages qui n'ont pas été distribués au démon `sendmail`. Les messages de cette file d'attente sont distribués par le démon client, qui agit vraiment en tant que programme d'exécution de file d'attente client.
- Par défaut, `sendmail` utilise `submmit.cf` régulièrement pour exécuter la file d'attente MSP (également appelée file d'attente client uniquement), `/var/spool/clientmqueue`.

```
/usr/lib/sendmail -Ac -q15m
```

Prenez note des remarques suivantes :

- À partir de la version Solaris 9, `submit.cf` est automatiquement inclus.
- `submit.cf` n'exige pas de planification ni de procédures préliminaires avant de procéder à l'installation de la version Solaris 9 ou d'une version plus récente.
- Sauf si vous spécifiez un fichier de configuration, `sendmail` utilise automatiquement `submit.cf` comme requis. En fait, `sendmail` sait quelles sont les tâches appropriées pour `submit.cf` et `sendmail.cf`.

Fonctions permettant de distinguer `sendmail.cf` de `submit.cf`

Le fichier de configuration `sendmail.cf` est destiné au mode démon. Lors de l'utilisation de ce fichier, `sendmail` agit comme un agent de transfert de courrier (MTA), qui est démarré par l'utilisateur `root`.

```
/usr/lib/sendmail -L sm-mta -bd -q1h
```

Reportez-vous à la liste suivante répertoriant d'autres fonctions de distinction pour `sendmail.cf` :

- Par défaut, `sendmail.cf` accepte les connexions SMTP sur les ports 25 et 587.
- Par défaut, `sendmail.cf` exécute la principale file d'attente, `/var/spool/mqueue`.

Modifications fonctionnelles à partir de la version 8.12 de sendmail

Avec l'ajout de submit.cf, les modifications fonctionnelles suivantes ont été effectuées :

- À partir de la version 8.12 de sendmail, seul root peut exécuter la file d'attente de messages. Pour plus d'informations, reportez-vous aux modifications qui sont décrites dans les pages de manuel mailq(1). Pour obtenir des informations sur les nouvelles tâches, reportez-vous à la section "Administration des répertoires de file d'attente (liste des tâches)" à la page 327.
- Le mode de programme d'envoi du courrier s'exécute sans privilège root, ce qui peut empêcher sendmail d'avoir accès à certains fichiers (tels que les fichiers .forward). Par conséquent, l'option -bv pour sendmail pourrait donner à l'utilisateur des résultats erronés. Il n'est pas possible de contourner ce problème.
- Avant sendmail version 8.12, si vous n'exécutiez pas sendmail en mode démon, vous empêchiez uniquement la distribution du courrier entrant. À partir de sendmail version 8.12, si vous n'exécutez pas le démon sendmail avec la configuration par défaut, vous empêchez également la distribution du courrier sortant. Le programme d'exécution de file d'attente client (également appelé programme d'envoi du courrier) doit être en mesure d'envoyer le courrier au démon sur le port SMTP local. Si ce programme d'exécution tente d'ouvrir une session SMTP avec l'hôte local et le démon n'écoute pas sur le port SMTP, le courrier reste dans la file d'attente. La configuration par défaut exécute un démon, de sorte que ce problème ne se produit pas si vous utilisez cette configuration. Cependant, si vous avez désactivé le démon, reportez-vous à la section "Gestion de la distribution du courrier à l'aide d'une autre configuration de sendmail.cf" à la page 314 pour découvrir un moyen de résoudre ce problème.

Options de ligne de commande supplémentaires ou abandonnées à partir de la version 8.12 de sendmail

Le tableau ci-dessous décrit les options de ligne de commande nouvelles ou abandonnées pour sendmail. D'autres options de ligne de commande sont décrites dans la page de manuel sendmail(1M).

TABLEAU 14–19 Options de ligne de commande supplémentaires ou abandonnées à partir de la version 8.12 de sendmail

Option	Description
-Ac	Indique que vous souhaitez utiliser le fichier de configuration, submit.cf, même si le mode de fonctionnement n'indique pas d'envoi de courrier initial. Pour plus d'informations sur les submit.cf, reportez-vous à la section "Fichier de configuration submit.cf à partir de la version 8.12 de sendmail" à la page 393.
-Am	Indique que vous souhaitez utiliser le fichier de configuration, sendmail.cf, même si le mode de fonctionnement indique l'envoi de courrier initial. Pour plus d'informations, reportez-vous à la section "Fichier de configuration submit.cf à partir de la version 8.12 de sendmail" à la page 393.

TABLEAU 14–19 Options de ligne de commande supplémentaires ou abandonnées à partir de la version 8.12 de sendmail *(Suite)*

Option	Description
-bP	Indique que vous imprimez le nombre d'entrées de chaque file d'attente.
-G	Indique que le message qui est envoyé à partir de la ligne de commande est destiné au relais, et non à un envoi initial. Le message est rejeté si les adresses ne sont pas complètes. Aucune mise en forme canonique n'est effectuée. Comme il est indiqué dans les notes de version qui font partie de la distribution sendmail sur ftp://ftp.sendmail.org, les messages mal formés peuvent être rejetés dans les versions à venir.
- L *tag*	Définit l'identificateur qui est utilisé pour les messages syslog sur la *tag* fournie.
- q[!]I *substring*	Traite uniquement les tâches qui contiennent cette *substring* de l'un des destinataires. Lorsque le caractère ! est ajouté, l'option traite uniquement les tâches qui ne disposent pas de cette *substring* de l'un des destinataires.
- q[!]R *substring*	Traite uniquement les tâches qui contiennent cette *substring* de l'ID de la file d'attente. Lorsque le caractère ! est ajouté, l'option traite uniquement les tâches qui ne disposent pas de cette *substring* de l'ID de la file d'attente.
- q[!]S *substring*	Traite uniquement les tâches qui contiennent cette *substring* du destinataire. Lorsque le caractère ! est ajouté, l'option traite uniquement les tâches qui ne disposent pas de cette *substring* du destinataire.
-qf	Traite les messages enregistrés dans la file d'attente une seule fois, sans l'aide de l'appel système fork, et exécute le processus en arrière-plan. Reportez-vous à la page de manuel fork(2).
- qG*name*	Traite uniquement les messages dans le groupe de files d'attente *name*.
- qp*time*	Traite les messages enregistrés dans la file d'attente à un intervalle de temps déterminé à l'aide d'un seul enfant qui est cloné pour chaque file d'attente. L'enfant demeure en veille entre chaque exécution de la file d'attente. Cette nouvelle option est similaire à l'instruction -q*time* , qui clone périodiquement un enfant pour le traitement de la file d'attente.
-U	Comme il est indiqué dans les notes de version qui font partie de la distribution sendmail sur ftp://ftp.sendmail.org, cette option n'est pas disponible à partir de la version 8.12. Les agents utilisateur de messagerie doivent utiliser l'argument -G.

Arguments supplémentaires pour les options PidFile et ProcessTitlePrefix à partir de la version 8.12 de sendmail

Le tableau ci-dessous décrit les arguments traités par macro supplémentaires pour les options PidFile et ProcessTitlePrefix. Pour plus d'informations sur ces options, reportez-vous à la page de manuel sendmail(1M).

TABLEAU 14–20 Arguments des options PidFile et ProcessTitlePrefix

Macro	Description
${daemon_addr}	Fournit l'adresse du démon (par exemple, 0.0.0.0).
${daemon_family}	Fournit la famille du démon (par exemple, inet et inet6)
${daemon_info}	Fournit des informations relatives au démon (par exemple, SMTP+queueing@00:30:00).
${daemon_name}	Fournit le nom du démon (par exemple, MSA).
${daemon_port}	Fournit le port du démon (par exemple, 25)
${queue_interval}	Fournit l'intervalle d'exécution de la file d'attente (par exemple, 00:30:00).

Macros définies supplémentaires à partir de la version 8.12 de sendmail

Le tableau suivant décrit les macros qui sont réservées à une utilisation par le programme sendmail. Les valeurs des macros sont attribuées en interne. Pour plus d'informations, reportez-vous à la page de manuel sendmail(1M).

TABLEAU 14–21 Macros définies supplémentaires pour sendmail

Macro	Description
${addr_type}	Identifie l'adresse actuelle en tant que l'expéditeur d'une enveloppe ou l'adresse d'un destinataire.
${client_resolve}	Contient le résultat de l'appel de résolution pour ${client_name} : OK, FAIL, FORGED ou TEMP.
${deliveryMode}	Spécifie le mode de distribution utilisé par sendmail, à la place de la valeur de l'option DeliveryMode.
${dsn_notify}, ${dsn_envid}, ${dsn_ret}	Contient les valeurs de paramètre DSN correspondantes.
${if_addr}	Fournit l'adresse de l'interface pour la connexion entrante si l'interface n'appartient pas au réseau loopback. Cette macro est particulièrement utile pour l'hébergement virtuel.

TABLEAU 14–21 Macros définies supplémentaires pour sendmail *(Suite)*

Macro	Description
${if_addr_out}, ${if_name_out}, ${if_family_out}	Permet d'éviter la réutilisation de ${if_addr}. Contient les valeurs suivantes respectivement : L'adresse de l'interface pour la connexion sortante Le nom d'hôte de l'interface pour la connexion sortante La famille de l'interface pour la connexion sortante
${if_name}	Fournit le nom d'hôte de l'interface pour la connexion entrante et s'avère particulièrement utile pour l'hébergement virtuel.
${load_avg}	Vérifie et indique le nombre moyen de tâches en cours dans la file d'attente d'exécution.
${msg_size}	Contient la valeur de la taille du message (SIZE=parameter) dans une boîte de dialogue ESMTP avant que le message soit collecté. Par la suite, la macro conserve la taille du message calculée par sendmail et est utilisée dans check_compat. Pour plus d'informations sur check_compat, reportez-vous au Tableau 14–25.
${nrcpts}	Contient le nombre de destinataires validées.
${ntries}	Contient le nombre de tentatives de distribution.
${rcpt_mailer}, ${rcpt_host}, ${rcpt_addr}, ${mail_mailer}, ${mail_host}, ${mail_addr}	Contient les résultats de l'analyse des arguments RCPT et MAIL, qui est constituée par les trois membres droits résolus (RHS) à partir de l'agent de distribution du courrier ($#*mailer*), l'hôte ($@*hôte*) et l'utilisateur ($:*addr*).

Macros supplémentaires à partir de la version 8.12 de sendmail

Cette section présente un tableau qui décrit d'autres macros qui sont utilisées pour créer le fichier de configuration sendmail.

TABLEAU 14–22 Macros supplémentaires utilisées pour créer le fichier de configuration sendmail

Macro	Description
LOCAL_MAILER_EOL	Remplace la chaîne de fin de ligne par défaut pour le logiciel de messagerie local.

TABLEAU 14–22 Macros supplémentaires utilisées pour créer le fichier de configuration sendmail *(Suite)*

Macro	Description
LOCAL_MAILER_FLAGS	Ajoute l'en-tête Return-Path: par défaut.
MAIL_SETTINGS_DIR	Contient le chemin d'accès (y compris la barre oblique de fin) pour le répertoire des paramètres de messagerie.
MODIFY_MAILER_FLAGS	Améliore la macro *_MAILER_FLAGS. Cette macro définit, ajoute ou supprime des indicateurs.
RELAY_MAILER_FLAGS	Définit des indicateurs supplémentaires pour le logiciel de messagerie relais.

Macros MAX supplémentaires à partir de la version 8.12 de sendmail

Utilise les macros suivantes pour configurer le nombre maximal de commandes qui peuvent être reçues avant que sendmail ralentisse sa distribution. Vous pouvez définir ces macros MAX au moment de la compilation. Les valeurs maximales dans le tableau suivant représentent les valeurs par défaut actuelles.

TABLEAU 14–23 Macros MAX supplémentaires

Macro	Valeur maximum	Commandes vérifiées par chaque macro
MAXBADCOMMANDS	25	Commandes inconnues
MAXNOOPCOMMANDS	20	NOOP, VERBE, ONEX, XUSR
MAXHELOCOMMANDS	3	HELO, EHLO
MAXVRFYCOMMANDS	6	VRFY, EXPN
MAXETRNCOMMANDS	8	ETRN

Remarque – Vous pouvez désactiver la vérification d'une macro en définissant sa valeur sur zéro.

Macros de configuration m4 supplémentaires et révisées à partir de la version 8.12 de sendmail

Cette section contient un tableau des macros de configuration m4 supplémentaires et révisées pour sendmail. Utilisez la syntaxe suivante pour déclarer ces macros.

symbolic-name(‘*value*’)

Si vous avez besoin de construire un fichier sendmail.cf, reportez-vous à la section “Modification de la configuration sendmail” à la page 305 du Chapitre 13, “Services de messagerie (tâches)”.

TABLEAU 14–24 Macros de configuration m4 supplémentaires et révisées pour sendmail

Macro m4	Description
FEATURE()	Pour plus de détails, reportez-vous à la section “Modifications apportées à la déclaration FEATURE() à partir de la version 8.12 de sendmail” à la page 400.
LOCAL_DOMAIN()	Cette macro ajoute des entrées à la classe w ($=w).
MASQUERADE_EXCEPTION()	Nouvelle macro qui définit les hôtes ou les sous-domaines pour lesquels le masquerading ne peut pas être appliqué.
macro()	Cette macro peut maintenant être utilisée pour les adresses entre crochets, comme par exemple user@[*host*].
VIRTUSER_DOMAIN() ou VIRTUSER_DOMAIN_FILE()	Lorsque ces macros sont utilisées, incluez ${VirtHost} dans $=R. Pour rappel, $=R est l'ensemble des noms d'hôte qui sont autorisés à effectuer le relais.

Modifications apportées à la déclaration FEATURE() à partir de la version 8.12 de sendmail

Reportez-vous aux tableaux suivants pour obtenir des informations sur les modifications spécifiques apportées aux déclarations FEATURE().

Pour utiliser des noms de FEATURE nouveaux et révisés, utilisez la syntaxe ci-dessous.

FEATURE(‘*name*’, ‘*argument*’)

Si vous avez besoin de créer un fichier sendmail.cf, reportez-vous à la section “Modification de la configuration sendmail” à la page 305 du Chapitre 13, “Services de messagerie (tâches)”.

TABLEAU 14–25 Déclarations FEATURE() supplémentaires et révisées

Nom de FEATURE()	Description
compat_check	Argument : reportez-vous à l'exemple du paragraphe suivant. Cette nouvelle FEATURE() vous permet de rechercher une clé dans la carte d'accès qui se compose de l'adresse de l'expéditeur et de l'adresse du destinataire. Cette FEATURE() est délimitée par la chaîne suivante : <@>. *sender*@ *sdomain*<@>*recipient* @*rdomain* (par exemple).
delay_checks	Argument : friend, qui entraîne un test spam-friend, ou hater, qui entraîne un test spam-hater. Nouvelle FEATURE() qui retarde toutes les vérifications. En utilisant FEATURE('delay_checks'), les ensembles de règles check_mail et check_relay ne sont pas appelés lorsqu'un client se connecte ou émet une commande MAIL respectivement. Au lieu de cela, ces ensembles de règles sont appelés par l'ensemble de règles check_rcpt. Pour plus de détails, reportez-vous au fichier /etc/mail/cf/README.
dnsbl	Argument : cette FEATURE() accepte un maximum de deux arguments : ■ Nom du serveur DNS ■ Message de rejet Nouvelle FEATURE() que vous pouvez inclure plusieurs fois pour vérifier les valeurs de retour des recherches DNS. Notez que cette FEATURE() vous permet de spécifier le comportement d'échecs de recherche temporaires.
enhdnsbl	Argument : nom du domaine. Nouvelle FEATURE() qui est une version améliorée de dnsbl, qui vous permet de vérifier les valeurs de retour des recherches DNS. Pour plus d'informations, reportez-vous au fichier /etc/mail/cf/README.
generics_entire_domain	Argument : aucun. Nouvelle FEATURE() que vous pouvez également utiliser pour appliquer genericstable aux sous-domaines de $=G.
ldap_routing	Argument : pour plus de détails, reportez-vous aux notes de version sur le site Web http://www.sendmail.org. Nouvelle FEATURE() qui implémente l'acheminement des adresses LDAP.
local_lmtp	Argument : nom du chemin d'accès d'un logiciel de messagerie compatible LMTP. La valeur par défaut est mail.local, qui est compatible LMTP dans cette version de Solaris. FEATURE() qui définit désormais le type de code de diagnostic pour la notification d'état de distribution (DSN) du logiciel de messagerie local sur la bonne valeur de SMTP.

TABLEAU 14–25 Déclarations FEATURE() supplémentaires et révisées *(Suite)*

Nom de FEATURE()	Description
local_no_masquerade	Argument : aucun. Nouvelle FEATURE() que vous pouvez utiliser pour éviter tout masquerading du logiciel de messagerie local.
lookupdotdomain	Argument : aucun. Nouvelle FEATURE() que vous pouvez également utiliser pour rechercher *.domain* dans la carte d'accès.
nocanonify	Argument : canonify_hosts ou rien. FEATURE() qui inclut désormais les fonctions suivantes. Permet à une liste de domaines, telle que spécifiée par CANONIFY_DOMAIN ou CANONIFY_DOMAIN_FILE, d'être transmise aux opérateurs $[et $] pour sa mise en forme canonique. Permet aux adresses qui ne disposent que d'un nom d'hôte, tel que <user@host>, d'êtres mises en forme canonique, si canonify_hosts est spécifié comme paramètre. Ajoute un point de fin aux adresses composées de plusieurs composants.
no_default_msa	Argument : aucun. Nouvelle FEATURE() qui désactive le paramètre par défaut de sendmail à partir des fichiers de configuration générés par m4 afin d'écouter, sur différents ports, une implémentation du document RFC 2476.
nouucp	Argument : reject, qui n'autorise pas le jeton !, ou nospecial, qui autorise le jeton !. FEATURE() qui détermine s'il faut autoriser le jeton ! dans la partie locale de l'adresse.
nullclient	Argument : aucun. FEATURE() qui offre désormais les ensembles de règles complets d'une configuration normale, permettant l'exécution des vérifications antispam.
preserve_local_plus_detail	Argument : aucun. Nouvelle FEATURE() qui vous permet de conserver la partie de l'adresse +detail lorsque sendmail transmet l'adresse à l'agent de distribution locale.
preserve_luser_host	Argument : aucun. Nouvelle FEATURE() qui vous permet de conserver le nom de l'hôte destinataire, si LUSER_RELAY est utilisé.
queuegroup	Argument : aucun. Nouvelle FEATURE() qui vous permet de sélectionner un groupe de files d'attente qui est basé sur l'adresse e-mail complète ou sur le domaine du destinataire.

TABLEAU 14–25 Déclarations FEATURE() supplémentaires et révisées *(Suite)*

Nom de FEATURE()	Description
relay_mail_from	Argument : le *domain* est un argument facultatif. Nouvelle FEATURE() qui autorise le relais si l'expéditeur du message est répertorié en tant que RELAY dans la carte d'accès et est marqué avec la ligne d'en-tête From:. Si l'argument *domain* facultatif est donné, la partie du domaine de l'expéditeur du message est également vérifiée.
virtuser_entire_domain	Argument : aucun. FEATURE() que vous pouvez désormais utiliser pour appliquer $={VirtHost}, une nouvelle classe pour la correspondance d'entrées virtusertable qui peuvent être renseignées par VIRTUSER_DOMAIN ou VIRTUSER_DOMAIN_FILE. FEATURE('virtuser_entire_domain') peut également appliquer la classe $={VirtHost} à des sous-domaines entiers.

Les déclarations FEATURE() suivantes ne sont plus prises en charge.

TABLEAU 14–26 Déclarations FEATURE() non prises en charge

Nom de FEATURE()	Remplacement
rbl	FEATURE('dnsbl') et FEATURE('enhdnsbl') remplacent cette FEATURE(), qui a été supprimée.
remote_mode	MASQUERADE_AS('$S') remplace FEATURE('remote_mode') dans /etc/mail/cf/subsidiary.mc. $S est la valeur SMART_HOST dans sendmail.cf.
sun_reverse_alias_files	FEATURE('genericstable').
sun_reverse_alias_nis	FEATURE('genericstable').
sun_reverse_alias_nisplus	FEATURE('genericstable').

Modifications apportées à la déclaration MAILER() à partir de la version 8.12 de sendmail

La déclaration MAILER() spécifie la prise en charge des agents de distribution. Pour déclarer un agent de distribution, utilisez la syntaxe ci-dessous.

MAILER('*symbolic-name*')

Veuillez noter les modifications suivantes :

- Dans cette nouvelle version de sendmail, la déclaration MAILER('smtp') inclut désormais une autre logiciel de messagerie, dsmtp, qui fournit la distribution à la demande en utilisant l'indicateur de messagerie F=%. La définition du logiciel de messagerie dsmtp utilise la nouvelle option DSMTP_MAILER_ARGS, qui est définie par défaut sur IPC $h.
- Les numéros pour les ensembles de règles qui sont utilisés par les MAILERs ont été supprimés. Vous n'avez à présent aucun ordre requis pour répertorier vos MAILERs excepté pour MAILER('uucp'), qui doit suivre MAILER('smtp') si uucp-dom et uucp-uudom sont utilisés.

Pour plus d'informations sur les logiciels de messagerie, reportez-vous à la section "Logiciels de messagerie et sendmail" à la page 348. Si vous avez besoin de construire un fichier sendmail.cf, reportez-vous à la section "Modification de la configuration sendmail" à la page 305 du Chapitre 13, "Services de messagerie (tâches)".

Indicateurs d'agent de distribution supplémentaires à partir de la version 8.12 de sendmail

Le tableau ci-dessous décrit des indicateurs d'agent de distribution supplémentaires, qui ne sont pas définis par défaut. Ces indicateurs à caractère unique sont booléens. Vous pouvez définir ou annuler la définition d'un indicateur en l'incluant ou en l'excluant dans l'instruction F= de votre fichier de configuration, comme indiqué dans l'exemple suivant.

```
Mlocal,    P=/usr/lib/mail.local, F=lsDFMAw5:/|@qSXfmnz9, S=10/30, R=20/40,
Mprog,     P=/bin/sh, F=lsDFMoqeu9, S=10/30, R=20/40, D=$z:/,
Msmtp,     P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990,
Mesmtp,    P=[IPC], F=mDFMuXa, S=11/31, R=21, E=\r\n, L=990,
Msmtp8,    P=[IPC], F=mDFMuX8, S=11/31, R=21, E=\r\n, L=990,
Mrelay,    P=[IPC], F=mDFMuXa8, S=11/31, R=61, E=\r\n, L=2040,
```

TABLEAU 14–27 Indicateurs de logiciel de messagerie supplémentaires

Indicateur	Description
%	Les logiciels de messagerie qui utilisent cet indicateur ne tentent pas la distribution d'un message à son destinataire initial ni la mise en file d'attente d'exécutions, à moins que le message en attente soit sélectionné à l'aide d'une requête ETRN ou de l'une des options suivantes : -qI, -qR ou -qS.
1	Cet indicateur désactive la possibilité pour le logiciel de messagerie d'envoyer des caractères null (par exemple, \0).
2	Cet indicateur désactive l'utilisation du protocole ESMTP et exige l'utilisation de SMTP à la place.
6	Cet indicateur permet aux logiciels de messagerie de réduire les en-têtes à 7 bits.

Conditions d'égalité supplémentaires pour les agents de distribution à partir de la version 8.12 de sendmail

Le tableau ci-dessous décrit des conditions d'égalité supplémentaires que vous pouvez utiliser avec la commande de définition d'agent de distribution M. La syntaxe suivante montre comment ajouter de nouvelles conditions d'égalité ou de nouveaux arguments à des égalités qui existent déjà dans le fichier de configuration.

```
Magent-name, equate, equate, ...
```

L'exemple suivant comprend la nouvelle égalité W=. Cette égalité spécifie le délai d'attente maximal pour le retour du logiciel de messagerie après l'envoi de toutes les données.

```
Msmtp, P=[IPC], F=mDFMuX, S=11/31, R=21, E=\r\n, L=990, W=2m
```

Lorsque vous modifiez la définition d'une valeur pour la configuration m4, utilisez la syntaxe qui est fournie dans l'exemple suivant.

```
define('SMTP_MAILER_MAXMSGS', '1000')
```

L'exemple précédent place une limite de 1 000 pour le nombre de messages distribués par connexion sur un logiciel de messagerie smtp.

Si vous avez besoin de construire un fichier sendmail.cf, reportez-vous à la section "Modification de la configuration sendmail" à la page 305 du Chapitre 13, "Services de messagerie (tâches)".

Remarque – En règle générale, vous modifiez les définitions des conditions d'égalité dans le répertoire mailer uniquement lorsque vous procédez à l'ajustement du programme.

TABLEAU 14–28 Conditions d'égalité supplémentaires pour les agents de distribution

Condition d'égalité	Description
/=	Argument : chemin d'accès à un répertoire. Indique un répertoire auquel appliquer chroot() avant l'exécution du logiciel de messagerie.
m=	Argument : l'une des valeurs m4 suivantes qui ont été définies auparavant avec la routine define(). SMTP_MAILER_MAXMSGS, pour le logiciel de messagerie smtp LOCAL_MAILER_MAXMSGS, pour le logiciel de messagerie local RELAY_MAILER_MAXMSGS, pour le logiciel de messagerie relay Limite le nombre de messages qui sont distribués par connexion sur un logiciel de messagerie smtp, local ou relay.

TABLEAU 14–28 Conditions d'égalité supplémentaires pour les agents de distribution *(Suite)*

Condition d'égalité	Description
W=	Argument : incrément de temps Spécifie le délai d'attente maximal pour le retour du logiciel de messagerie après l'envoi de toutes les données.

Fonctions de file d'attente supplémentaires à partir de la version 8.12 de sendmail

La liste ci-après fournit des détails sur les fonctions de file d'attente supplémentaires.

- Cette version prend en charge plusieurs répertoires de file d'attente. Pour utiliser plusieurs files d'attente, indiquez une valeur d'option QueueDirectory dans le fichier de configuration qui se termine par un astérisque (*), comme présenté dans l'exemple suivant.

  ```
  O QueueDirectory=/var/spool/mqueue/q*
  ```

  La valeur de l'option, /var/spool/mqueue/q*, utilise tous les répertoires (ou les liens symboliques vers ces répertoires) qui commencent par "q" comme répertoires de file d'attente. Ne modifiez pas la structure des répertoires de file d'attente lorsque sendmail est en cours d'exécution. Les exécutions de files d'attente créent un processus distinct pour l'exécution de chaque file d'attente, sauf si l'indicateur de détail (-v) est utilisé sur l'exécution d'une file d'attente non démon. Les nouveaux éléments sont attribués au hasard à une file d'attente.
- Le nouveau système de nommage de fichier de file d'attente utilise des noms de fichiers qui sont garantis d'être uniques pendant 60 ans. Ce système permet aux ID de file d'attente d'être attribués sans verrouillage de système de fichiers complexe et simplifie le déplacement des éléments en file d'attente entre les files d'attente.
- À partir de la version 8.12, seul l'utilisateur root peut exécuter la file d'attente de messages. Pour plus d'informations, reportez-vous aux modifications qui sont décrites dans les pages de manuel mailq(1). Pour obtenir des informations sur les nouvelles tâches, reportez-vous à la section "Administration des répertoires de file d'attente (liste des tâches)" à la page 327.
- Pour s'adapter au fractionnement d'enveloppes, les noms des fichiers de file d'attente sont désormais de 15 caractères, au lieu de 14 caractères. Les systèmes de fichiers avec une limite de 14 caractères pour les noms ne sont plus pris en charge.

Pour obtenir des informations, reportez-vous à la section "Administration des répertoires de file d'attente (liste des tâches)" à la page 327.

Modifications pour LDAP à partir de la version 8.12 de sendmail

La liste ci-dessous décrit les modifications apportées dans l'utilisation du protocole LDAP (Lightweight Directory Access Protocol) avec sendmail.

- LDAPROUTE_EQUIVALENT() et LDAPROUTE_EQUIVALENT_FILE() vous permettent de spécifier des noms d'hôte équivalents, qui sont remplacés par le nom de domaine issu du masquerading pour les recherches d'acheminement LDAP. Pour plus d'informations, reportez-vous au fichier /etc/mail/cf/README.
- Comme indiqué dans les notes de version qui font partie de la distribution sendmail sur ftp://ftp.sendmail.org, la carte LDAPX a été renommée LDAP. Utilisez la syntaxe suivante pour le protocole LDAP.

  ```
  Kldap ldap options
  ```

- Cette version prend en charge le retour de plusieurs valeurs pour une même recherche LDAP. Placez les valeurs à renvoyer, séparées par des virgules, dans une chaîne avec l'option -v, comme présenté.

  ```
  Kldap ldap -v"mail,more-mail"
  ```

- Si aucun attribut LDAP n'est spécifié dans une déclaration de carte LDAP, tous les attributs qui sont trouvés dans la correspondance sont renvoyés.
- Cette version de sendmail empêche que les virgules placées dans les chaînes de valeurs et de clés entre guillemets, dans les spécifications du fichier d'alias LDAP, divisent une seule entrée en plusieurs entrées.
- Cette version de sendmail dispose d'une nouvelle option pour les cartes LDAP. L'option -V*separator* vous permet de spécifier un séparateur, de sorte qu'une recherche puisse renvoyer un attribut et une valeur qui sont séparés par le *separator* adéquat.
- En plus d'utiliser le jeton %s pour l'analyse de la spécification d'un filtre LDAP, vous pouvez utiliser le nouveau jeton, %0, pour coder le tampon de clés. Le jeton %0 applique un sens littéral aux caractères spéciaux LDAP.

L'exemple suivant montre les variations de ces jetons pour une recherche “*”.

TABLEAU 14–29 Comparaison des jetons

Spécification de carte LDAP	Spécification équivalente	Résultat
-k"uid=%s"	-k"uid=*"	Correspond à n'importe quel enregistrement doté d'un attribut utilisateur.
-k"uid=%0"	-k"uid=\2A"	Correspond à un utilisateur portant le nom “*”.

Le tableau suivant décrit d'autres indicateurs de carte LDAP.

TABLEAU 14–30 Indicateurs de carte LDAP supplémentaires

Indicateur	Description
`-1`	Nécessite le renvoi d'une seule correspondance. Si plus d'une correspondance est renvoyée, les résultats sont équivalents à ceux affichés lorsqu'aucun enregistrement n'a été trouvé.
`-r never|always|search|find`	Définit l'option de déréférencement d'alias LDAP.
`-Z size`	Limite le nombre de correspondances à renvoyer.

Modifications apportées au logiciel de messagerie intégré à partir de la version 8.12 de `sendmail`

L'ancien logiciel de messagerie `[TCP]` intégré n'est pas disponible. Utilisez le logiciel de messagerie `P=[L'IPC]` intégré à la place. Le logiciel de messagerie intégré de communication interprocessus (`[IPC]`) permet désormais la distribution à un socket de domaine UNIX sur les systèmes qui le prennent en charge. Vous pouvez utiliser ce logiciel de messagerie avec des agents de distribution `LMTP` qui écoutent sur un socket nommé. Un logiciel de messagerie peut ressembler à l'exemple suivant.

```
Mexecmail, P=[IPC], F=lsDFMmnqSXzA5@/:|, E=\r\n,
S=10, R=20/40, T=DNS/RFC822/X-Unix, A=FILE /var/run/lmtpd
```

Une valeur légitime est désormais recherchée dans le premier argument du logiciel de messagerie `[IPC]`. Le tableau ci-dessous présente les valeurs possibles pour le premier argument du logiciel de messagerie.

TABLEAU 14–31 Valeurs possibles pour le premier argument du logiciel de messagerie

Valeur	Description
`A=FILE`	Utiliser pour la distribution de sockets de domaine UNIX.
`A=TCP`	Utiliser pour les connexions TCP/IP.
`A=IPC`	N'est plus disponible en tant que premier argument de logiciel de messagerie.

Ensembles de règles supplémentaires à partir de la version 8.12 de `sendmail`

Le tableau suivant répertorie les ensembles de règles supplémentaires et décrit ce que leurs rôles.

TABLEAU 14–32 Nouveaux ensembles de règles

Set	Description
check_eoh	Met en corrélation les informations recueillies entre les en-têtes et vérifie s'il manque des en-têtes. Cet ensemble de règles est utilisé avec la carte de stockage de macros et est appelé une fois que tous les en-têtes ont été collectés.
check_etrn	Utilise la commande ETRN (comme check_rcpt utilise RCPT).
check_expn	Utilise la commande EXPN (comme check_rcpt utilise RCPT).
check_vrfy	Utilise la commande VRFY (comme check_rcpt utilise RCPT).

La liste suivante décrit les autres fonctions des ensembles de règles.

- Les ensembles de règles portent également un nom, mais ils sont toujours accessibles avec leurs numéros.
- La commande du fichier de configuration d'en-têtes H permet la spécification d'un ensemble de règles par défaut pour les vérifications d'en-têtes. Cet ensemble de règles n'est appelé que si l'ensemble de règles de l'en-tête en question ne lui a pas été attribué.
- Les commentaires contenus dans les ensembles de règles (c'est-à-dire le texte figurant entre parenthèses) ne sont pas supprimés si la version du fichier de configuration utilisé est la neuvième ou plus. Par exemple, la règle suivante correspond à l'entrée `token (1)`, mais ne correspond pas à l'entrée `token`.

```
R$+ (1)         $@ 1
```

- `sendmail` accepte la commande RSET SMTP même lorsqu'il rejette des commandes en raison de wrappers TCP ou de l'ensemble de règles `check_relay`.
- Vous recevez un message d'avertissement si vous définissez plusieurs fois l'option `OperatorChars`. En outre, ne définissez pas `OperatorChars` après avoir défini les ensembles de règles.
- Le nom de l'ensemble de règles, ainsi que ses lignes, sont ignorés si un ensemble de règles invalide est déclaré. Les lignes de l'ensemble de règles ne sont pas ajoutées à `S0`.

Modifications apportées aux fichiers à partir de la version 8.12 de `sendmail`

Notez les modifications suivantes.

- À partir de la version Solaris 10, pour la prise en charge du système de fichiers `/usr` en lecture seule, le contenu du répertoire `/usr/lib/mail` a été déplacé vers le répertoire `/etc/mail/cf`. Pour plus d'informations, reportez-vous à la section "Contenu du répertoire /etc/mail/cf" à la page 361. Notez, toutefois, que les scripts shell `/usr/lib/mail/sh/check-hostname` et `/usr/lib/mail/sh/check-permissions` se

trouvent désormais dans le répertoire /usr/sbin. Reportez-vous à la section "Autres fichiers utilisés pour les services de messagerie" à la page 364. Pour garantir la compatibilité ascendante, des liens symboliques pointent vers le nouvel emplacement de chaque fichier.

- Le nouveau nom de /usr/lib/mail/cf/main-v7sun.mc est /etc/mail/cf/cf/main.mc.
- Le nouveau nom de /usr/lib/mail/cf/subsidiary-v7sun.mc est /etc/mail/cf/cf/subsidiary.mc.
- Le fichier helpfile se trouve désormais dans /etc/mail/helpfile. L'ancien nom (/etc/mail/sendmail.hf) a un lien symbolique pointant vers le nouveau nom.
- Le fichier trusted-users se trouve désormais dans /etc/mail/trusted-users. Au cours d'une mise à jour, si l'ancien nom (/etc/mail/sendmail.ct) est détecté, mais pas le nouveau nom, un lien physique allant de l'ancien nom vers le nouveau est créé. Sinon, aucune modification n'est effectuée. Le contenu par défaut est root.
- Le fichier local-host-names se trouve désormais dans /etc/mail/local-host-names. Au cours d'une mise à jour, si l'ancien nom (/etc/mail/sendmail.cw) est détecté, mais pas le nouveau nom, un lien physique allant de l'ancien nom vers le nouveau est créé. Sinon, aucune modification n'est effectuée. Le contenu par défaut est la longueur nulle.

Version 8.12 de sendmail et adresses IPv6 dans la configuration

À partir de la version 8.12 de sendmail, les adresses IPv6 qui sont utilisées dans la configuration doivent être précédées de la balise IPv6: pour permettre leur identification adéquate. Si vous n'identifiez pas une adresse IPv6, aucune balise de préfixe n'est utilisée.

PARTIE V

Sujets relatifs à la mise en réseau série

Cette section relative à la mise en réseau série fournit une présentation, des listes de tâches et des informations de référence sur PPP et UUCP.

◆ ◆ ◆ CHAPITRE 15

Solaris PPP 4.0 (Présentation)

Cette section est consacrée à la mise en réseau série. La mise en réseau série fait référence à l'utilisation d'une interface série (un port RS-232 ou V.35, par exemple) pour relier deux ordinateurs ou plus dans le cadre du transfert de données. Contrairement aux interfaces LAN, telles qu'Ethernet, ces interfaces série permettent de connecter des systèmes très éloignés. Pour mettre en œuvre la mise en réseau série, vous disposez des technologies PPP (Point-to-Point Protocol) et UUCP (UNIX-to-UNIX CoPy). Lorsqu'une interface série est configurée pour la mise en réseau, elle devient disponible à plusieurs utilisateurs, tout comme n'importe quelle autre interface réseau, notamment Ethernet.

Ce chapitre présente Solaris PPP 4.0. Cette version de PPP permet à deux ordinateurs situés à différents emplacements physiques de communiquer en utilisant PPP sur une large gamme de supports. Depuis la version Solaris 9, Solaris PPP 4.0 est inclus dans l'installation de base.

Les sujets suivants sont abordés :

Notions de base de Solaris PPP 4.0

Solaris PPP 4.0 met en œuvre le protocole de liaison de données PPP (Point-to-Point Protocol) qui fait partie de la suite de protocoles TCP/IP. PPP décrit la façon dont les données sont transmises entre deux machines, au moyen de supports de communication tels que des lignes téléphoniques.

Depuis le début des années 1990, PPP est un standard Internet fréquemment utilisé pour l'envoi de datagrammes par la biais d'une liaison de communication. Le standard PPP est décrit dans le document RFC 1661 par le groupe de travail du Protocole Point à Point de l'IETF (Internet

Engineering Task Force). PPP est couramment utilisé lorsque des ordinateurs distants appellent un fournisseur de service Internet (FAI) ou un serveur d'entreprise configuré pour recevoir des appels entrants.

Solaris PPP 4.0 est basé sur l'ANU (Australian National University) PPP–2.4 public et met en œuvre le standard PPP. Les liaisons PPP synchrones et asynchrones sont toutes deux prises en charge.

Compatibilité avec Solaris PPP 4.0

Diverses versions du standard PPP sont disponibles et couramment utilisées par la communauté Internet. ANU PPP-2.4 est plébiscité pour Linux, Tru64 UNIX et les trois principales variantes de BSD :

- FreeBSD
- OpenBSD
- NetBSD

Solaris PPP 4.0 apporte les fonctions hautement configurables d'ANU PPP-2.4 aux machines qui exécutent le système d'exploitation Solaris. Les machines exécutant Solaris PPP 4.0 peuvent configurer facilement des liaisons PPP à toutes les machines exécutant une mise en œuvre du standard PPP.

Parmi les implémentations PPP non basées sur l'ANU qui interopèrent avec Solaris PPP 4.0, citons :

- Solaris PPP, également appelée `asppp`, disponible avec les versions Solaris 2.4 à 8
- Solstice PPP 3.0.1
- Microsoft Windows 98 DUN
- Cisco IOS 12.0 (synchrone)

Quelle version de Solaris PPP utiliser

Solaris PPP 4.0 est l'implémentation PPP prise en charge. Les versions Solaris 9 et ultérieures n'incluent pas le logiciel Asynchronous Solaris PPP (`asppp`) antérieur. Pour plus d'informations, reportez-vous à la documentation suivante :

- Chapitre 23, “Migration de Solaris PPP asynchrone à Solaris PPP 4.0 (tâches) ”
- Solaris System Administrator Collection sur le site Web http://docs.sun.com

Pourquoi utiliser Solaris PPP 4.0 ?

Si vous utilisez actuellement `asppp`, envisagez de migrer vers Solaris PPP 4.0. Notez les différences entre les deux technologies Solaris PPP :

- **Modes de transfert**

  `asppp` prend en charge les communications asynchrones uniquement. Solaris PPP 4.0 prend en charge les communications asynchrones et les communications synchrones.

- **Processus de configuration**

  La configuration de `asppp` requiert la configuration du fichier de configuration `asppp.cf` , de trois fichiers UUCP et de la commande `ifconfig`. En outre, vous devez préconfigurer les interfaces de tous les utilisateurs susceptibles de se connecter à une machine.

  La configuration de Solaris PPP 4.0 requiert de définir des options pour les fichiers de configuration PPP ou d'exécuter la commande `pppd` avec des options. Vous pouvez également utiliser à la fois le fichier de configuration et la ligne de commande. Solaris PPP crée et supprime des interfaces de manière dynamique. Il n'est pas nécessaire de configurer directement les interfaces PPP de chaque utilisateur.

- **Fonctionnalités de Solaris PPP 4.0 non disponibles à partir de asppp**
  - Authentification MS-CHAPv1 et MS-CHAPv2
  - PPPoE (PPP over Ethernet) pour la prise en charge des ponts ADSL
  - Authentification PAM
  - Modules de plug-in
  - Adressage IPv6
  - Compression de données utilisant l'algorithme BSD ou Deflate
  - Prise en charge de la fonction de rappel côté client de Microsoft

Chemin de mise à niveau de Solaris PPP 4.0

Si vous convertissez une configuration `asppp` à Solaris PPP 4.0, vous pouvez utiliser le script de conversion fourni avec cette version. La section "Conversion de `asppp` à Solaris PPP 4.0" à la page 558 contient les instructions complètes à ce sujet.

Sources d'informations sur PPP

De nombreuses ressources sur PPP sont disponibles en ligne et sous forme de documentation imprimée. Les sous-sections suivantes offrent quelques suggestions.

Ouvrages de référence professionnelle à propos de PPP

Pour plus d'informations sur les implémentations PPP courantes, notamment ANU PPP, reportez-vous aux ouvrages suivants :

- Carlson, James. *PPP Design, Implementation, and Debugging*. 2è éd. Addison-Wesley, 2000.
- Sun, Andrew. *Using and Managing PPP*. O'Reilly & Associates, 1999.

Sites Web sur PPP

Consultez les sites Web suivants pour obtenir des informations générales à propos de PPP :

- La ressource des administrateurs système http://www.sun.com/bigadmin/home/index.html contient des informations techniques, des FAQ, des discussions sur l'administration du système Solaris et des versions précédentes de PPP.
- Sur le site Web Web Project Management & Software Development de Stokely Consulting http://www.stokely.com/unix.serial.port.resources/ppp.slip.html, vous trouverez la configuration de modem et des conseils sur les diverses implémentations de PPP.

Documents RFC sur PPP

Voici quelques documents RFC utiles sur PPP :

- 1661 et 1662 décrivent les caractéristiques principales de PPP
- 1334 décrit les protocoles d'authentification, tels que PAP (Password Authentication Protocol) et CHAP (Challenge-Handshake Authentication Protocol)
- 1332 est un RFC international qui décrit PPPoE (PPP over Ethernet)

Pour obtenir des copies des RFC PPP, spécifiez le numéro du document sur la page Web IETF RFC http://www.ietf.org/rfc.html .

Pages de manuel sur PPP

Pour des détails techniques sur la mise en œuvre de Solaris PPP 4.0, reportez-vous aux pages de manuel suivantes :

- `pppd`(1M)
- `chat`(1M)
- `pppstats`(1M)
- `pppoec`(1M)
- `pppoed`(1M)
- `sppptun`(1M)
- `snoop`(1M)

Consultez en outre la page de manuel de `pppdump`(1M). Vous trouverez les pages de manuel sur PPP à l'aide de la commande `man`.

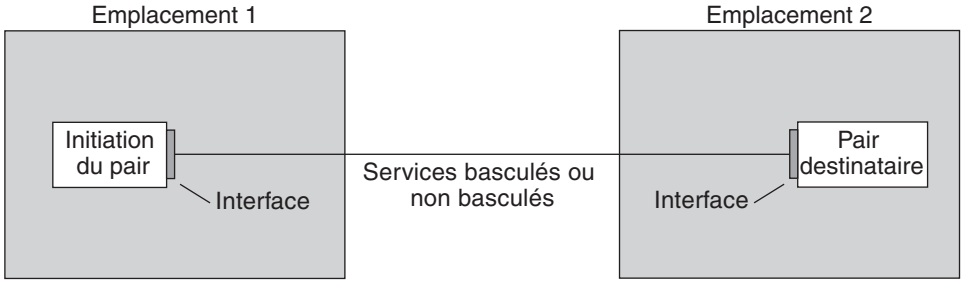
Configurations et terminologie PPP

Cette section présente les configurations PPP. Elle définit également les termes utilisés dans ce guide.

Solaris PPP 4.0 prend en charge différentes configurations.

- Configurations commutées ou à accès *commuté*
- Configurations câblées ou de *ligne spécialisée*

FIGURE 15–1 Composants de la liaison PPP



La figure précédente illustre une liaison PPP de base. La liaison est constituée des composants suivants :

- Deux machines, situées habituellement à des emplacements physiques distincts, appelées *pairs*. Un pair peut être un ordinateur personnel, une station de travail d'ingénierie, un serveur de grande taille ou même un routeur commercial, selon les exigences du site.
- Interface série sur chaque pair. Sur des machines Solaris, cette interface peut être `cua`, `hihp` ou une autre interface, selon que vous configurez une liaison PPP synchrone ou asynchrone.
- Liaison physique, telle qu'un câble série, une connexion modem ou une ligne spécialisée d'un fournisseur réseau (ligne T1 ou T3, par exemple).

Présentation de la liaison commutée PPP

La configuration PPP la plus fréquente est la *liaison commutée*. Dans une liaison commutée, le pair local *appelle* le pair distant pour établir la connexion et exécuter PPP. Au cours du processus de commutation, le pair local compose le numéro de téléphone du pair distant afin d'initialiser la liaison.

Un ordinateur domestique qui appelle un pair situé chez un FAI, configuré pour recevoir des appels entrants, constitue un scénario de commutation courant. Un autre scénario est un site d'entreprise où une machine locale transmet des données via une liaison PPP à un pair situé dans un autre bâtiment.

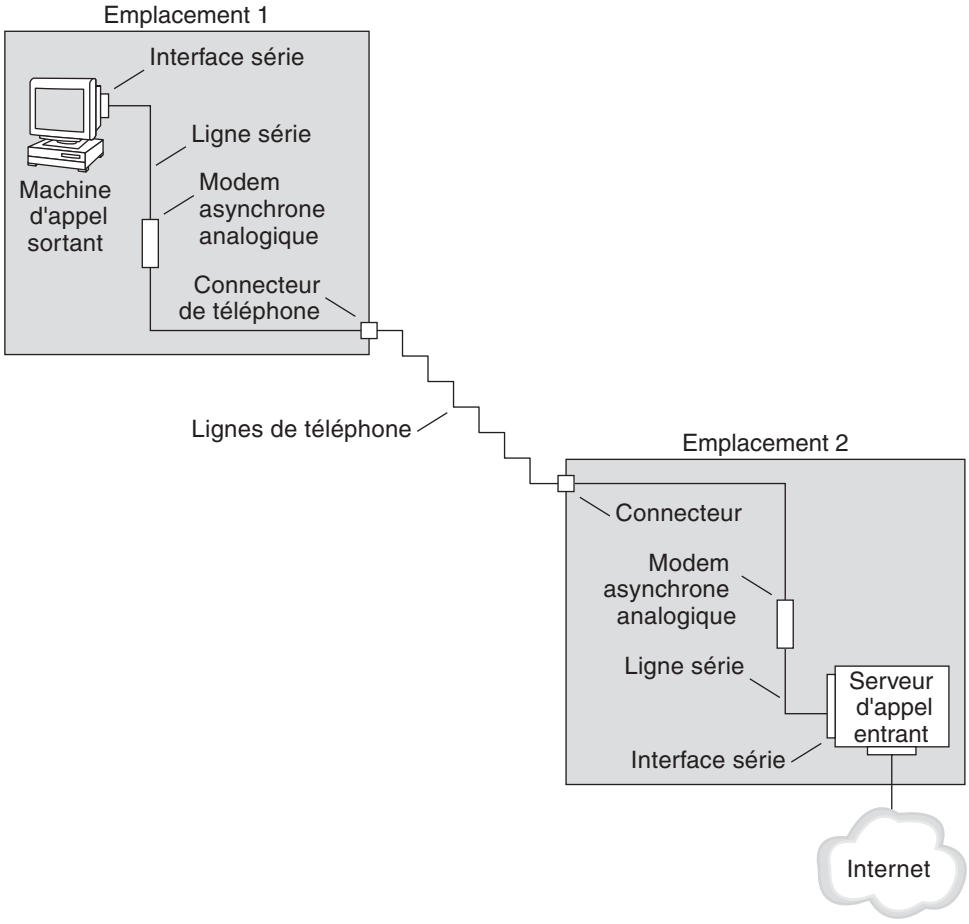
Dans ce guide, le pair local qui initialise la connexion commutée est appelé la *machine d'appel sortant*. Le pair qui reçoit l'appel entrant est désigné comme le *serveur d'appel entrant*. Cette machine est en réalité le pair cible de la machine d'appel sortant et n'est pas nécessairement un vrai serveur.

PPP n'est pas un protocole client-serveur. Certains documents PPP emploient les termes "client" et "serveur" dans le contexte de l'établissement d'un appel téléphonique. Un serveur d'appel entrant n'est pas un vrai serveur, comme un serveur de fichiers ou un serveur de noms. Le terme "serveur d'appel entrant" est répandu parce que les machines d'appel entrant "servent" plusieurs machines d'appel sortant auxquelles elles offrent l'accès au réseau. Néanmoins, le serveur d'appel entrant représente le pair cible de la machine d'appel sortant.

Composants de la liaison PPP commutée

Reportez-vous à la figure suivante.

FIGURE 15–2 Liaison PPP commutée analogique de base



La configuration de l'emplacement 1 (côté appel sortant de la liaison) se compose des éléments suivants :

- Machine d'appel sortant, généralement un ordinateur personnel ou une station de travail au domicile d'un utilisateur.
- Interface série sur la machine d'appel sortant. L'interface `/dev/cua/a` ou `/dev/cua/b` est l'interface série standard pour les appels sortants sur des machines exécutant le logiciel Solaris.
- Modem asynchrone ou adaptateur de terminal RNIS connecté à une prise téléphonique.
- Lignes et services téléphoniques d'un opérateur de téléphonie.

La configuration de l'emplacement 2 (côté appel entrant de la liaison) se compose des éléments suivants :

- Prise téléphonique (ou connecteur similaire) connectée au réseau téléphonique.
- Modem asynchrone ou adaptateur de terminal RNIS
- Interface série sur le serveur d'appel entrant, `ttya` ou `ttyb` pour les appels entrants
- Serveur d'appel entrant connecté à un réseau, tel qu'un intranet d'entreprise, ou dans le cas d'un FAI, Internet

Utilisation d'adaptateurs de terminal RNIS avec une machine d'appel sortant

Les adaptateurs de terminal RNIS externes sont plus rapides que les modems, mais ils se configurent plus ou moins de la même manière. La principale différence dans la configuration d'un adaptateur de terminal RNIS réside dans le script de discussion, qui requiert les commandes spécifiques du fabricant de l'adaptateur. La section "Script de discussion pour adaptateur de terminal RNIS externe" à la page 532 contient des informations sur les scripts de discussion pour les adaptateurs de terminal.

Description des communications commutées

Les fichiers de configuration PPP à la fois sur les pairs entrants et sortants contiennent les instructions pour la configuration de la liaison. Le processus suivant s'effectue lors de l'initialisation de la liaison commutée.

1. L'utilisateur ou le processus sur la machine d'appel sortant exécute la commande `pppd` pour démarrer la liaison.
2. La machine d'appel sortant lit les fichiers de configuration PPP. La machine d'appel sortant envoie ensuite des instructions via la ligne série à son modem, y compris le numéro de téléphone du serveur d'appel entrant.
3. Le modem compose le numéro de téléphone pour établir une connexion téléphonique avec le modem du serveur d'appel entrant.

   La série de chaînes de texte que la machine d'appel sortant envoie au modem et au serveur d'appel entrant est contenue dans un fichier appelé *script de discussion*. Si nécessaire, la machine d'appel sortant envoie des commandes au serveur d'appel entrant pour appeler PPP sur le serveur.
4. Le modem connecté au serveur d'appel entrant entame la négociation de liaison avec le modem connecté à la machine d'appel sortant.
5. À l'issue de la négociation entre les modems, le modem connecté à la machine d'appel sortant indique "CONNECT".
6. La liaison PPP sur les deux pairs entre dans la phase *Establish* où le protocole LCP (Link Control Protocol) négocie les paramètres de liaison de base et l'utilisation de l'authentification.

7. Si nécessaire, les pairs s'authentifient mutuellement.
8. Les NCP (Network Control Protocol) de PPP négocient l'utilisation de protocoles réseau, tels que IPv4 ou IPv6.

La machine d'appel sortant peut alors exécuter `telnet` ou une commande similaire au niveau d'un hôte accessible via le serveur d'appel entrant.

Présentation de la liaison PPP de ligne spécialisée

Une configuration PPP câblée de *ligne spécialisée* implique deux pairs reliés par le biais d'une liaison. Cette liaison constitue un service numérique commuté ou non commuté, loué auprès d'un fournisseur. Solaris PPP 4.0 fonctionne sur tous les supports de ligne spécialisée point à point et duplex intégral. En règle générale, une société loue une liaison câblée auprès d'un fournisseur réseau pour se connecter à un fournisseur d'accès Internet ou à un autre site distant.

Comparaison des liaisons commutées et des liaisons de ligne spécialisées

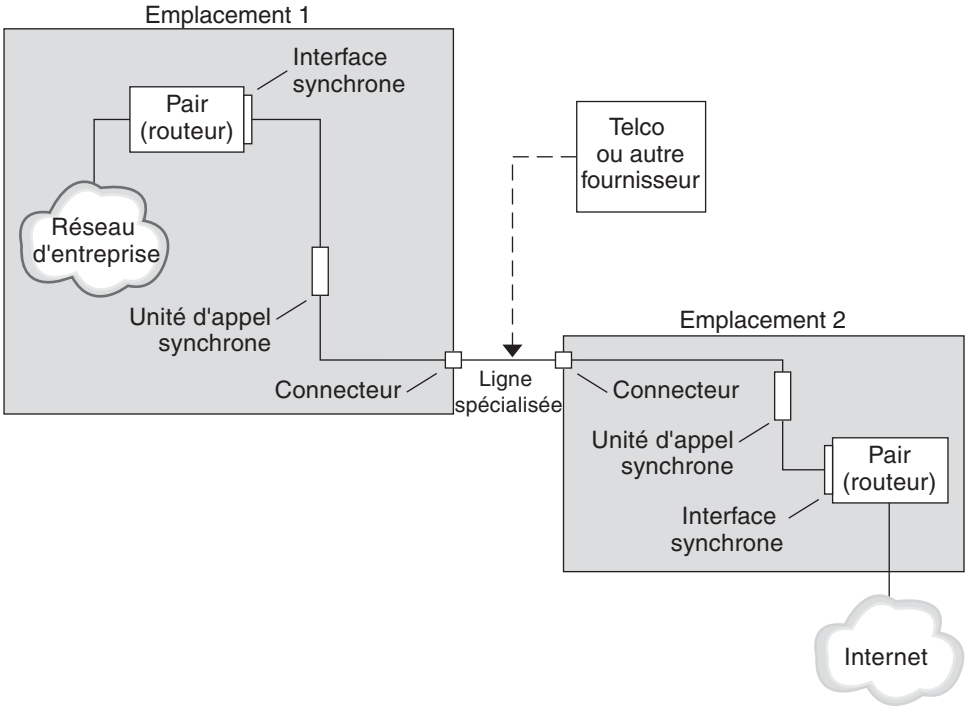
Les deux types de liaison, commutée et spécialisée, impliquent deux pairs connectés par un support de communication. Le tableau suivant récapitule les différences entre les types de liaison.

Ligne spécialisée	Ligne commutée
Toujours connectée, à moins qu'un administrateur système ou une coupure d'alimentation ne l'interrompe.	Lancée sur demande, lorsqu'un utilisateur tente d'appeler un pair distant.
Utilise les communications synchrones et asynchrones. Un modem longue distance est souvent utilisé pour les communications asynchrones.	Utilise les communications asynchrones.
Louée auprès d'un fournisseur.	Utilise des lignes téléphoniques existantes.
Requiert des unités synchrones.	Utilise des modems moins coûteux.
Nécessite des ports synchrones, courants sur la plupart des systèmes SPARC. Cependant, les ports synchrones ne sont pas fréquents sur les systèmes x86 et les systèmes SPARC plus récents.	Utilise les interfaces série standard incluses sur la plupart des ordinateurs.

Composants de la liaison PPP de ligne spécialisée

Reportez-vous à la figure suivante.

FIGURE 15–3 Configuration de la ligne spécialisée de base



La liaison de ligne spécialisée est constituée des composants suivants :

- **Deux pairs**, chacun situé à l'une des extrémités de la liaison. Les pairs peuvent être une station de travail ou un serveur. Le pair fonctionne souvent comme un routeur entre son réseau, ou Internet, et le pair opposé.
- **Une interface synchrone sur chaque pair**. Certaines machines exécutant le logiciel Solaris exigent l'acquisition d'une carte d'interface synchrone, telle que HSI/P, pour la connexion à une ligne spécialisée. D'autres machines, comme les stations de travail UltraSPARC , intègrent des interfaces synchrones.
- **Une unité numérique synchrone CSU/DSU sur chaque pair**, qui relie le port synchrone à la ligne spécialisée.

  En fonction de votre environnement linguistique, une CSU peut être intégrée à la DSU, être louée auprès d'un fournisseur ou vous appartenir. La DSU offre une interface série synchrone standard à la machine Solaris. Avec Frame Relay, le périphérique FRAD (Frame Relay Access Device) réalise l'adaptation de l'interface série.
- **Une ligne spécialisée**, offrant des services numériques commutés ou non commutés. C'est le cas de SONET/SDH, Frame Relay PVC et T1.

Description des communications de ligne spécialisée

Sur la plupart des types de lignes spécialisées, les pairs ne s'appellent pas. Une société acquiert plutôt un service de ligne spécialisée pour connecter explicitement deux emplacements fixes. Il arrive que les deux pairs à chaque extrémité de la ligne spécialisée soient situés à différents emplacements physiques de la même société. Une société qui définit un routeur sur une ligne spécialisée connectée à un FAI constitue un autre scénario.

Les lignes spécialisées sont moins courantes que les liaisons commutées, bien qu'elles soient plus faciles à configurer. Elles ne nécessitent pas de scripts de discussion. L'authentification n'est généralement pas utilisée, car les deux pairs se connaissent lorsqu'une ligne est louée. Une fois initialisée par les deux pairs, la liaison PPP reste active. Une liaison de ligne spécialisée reste active, sauf en cas de panne de la ligne ou si l'un des pairs met explicitement fin à la liaison.

Les pairs de ligne spécialisée exécutant Solaris PPP 4.0 utilisent la plupart des fichiers de configuration qui définissent une liaison commutée.

Le processus suivant a lieu pour lancer la communication sur la ligne spécialisée :

1. Chaque pair exécute la commande `pppd` dans le cadre du processus d'initialisation ou d'un autre script d'administration.
2. Les pairs lisent leurs fichiers de configuration PPP.
3. Les pairs négocient les paramètres de communication.
4. Une liaison IP est établie.

Authentification PPP

L'authentification est le processus qui permet de vérifier qu'un utilisateur est bien celui qu'il dit être. La séquence de connexion UNIX est une forme simple d'authentification :

1. La commande `login` invite l'utilisateur à spécifier un nom et un mot de passe.
2. `login` tente alors d'authentifier l'utilisateur en recherchant le nom d'utilisateur et le mot de passe entrés dans la base de données de mots de passe.
3. Si la base de données contient le nom d'utilisateur et le mot de passe en question, l'utilisateur est *authentifié* et se voit autoriser à accéder au système. Si la base de données ne contient pas le nom d'utilisateur et le mot de passe, l'accès au système est refusé à l'utilisateur.

Par défaut, Solaris PPP 4.0 n'exige pas l'authentification sur les machines qui ne disposent pas d'une route par défaut spécifiée. Par conséquent, une machine locale sans route par défaut n'authentifie pas les appelants distants. A l'inverse, si elle possède une route par défaut définie, la machine authentifie toujours les appelants distants.

Vous pouvez utiliser les protocoles d'authentification PPP pour vérifier l'identité des appelants qui tentent de configurer une liaison PPP sur votre machine. À l'inverse, vous devez configurer des informations d'authentification PPP, si votre machine locale doit appeler des pairs qui authentifient des appelants.

Authentificateurs et authentifiés

Sur une liaison PPP, la machine à l'origine de l'appel est considérée comme l'*authentifié*, car elle doit prouver son identité au pair distant. Le pair est considéré comme l'*authentificateur*. L'authentificateur recherche l'identité de l'appelant dans les fichiers PPP correspondant au protocole de sécurité et authentifie ou non l'appelant.

Généralement, vous configurez une authentification PPP pour une liaison commutée. Au début de l'appel, la machine d'appel sortant est l'authentifié. Le serveur d'appel sortant est l'authentificateur. Le serveur possède une base de données sous forme de fichier de *secrets*. Ce fichier répertorie tous les utilisateurs autorisés à configurer une liaison PPP vers le serveur. Considérez ces utilisateurs comme des *appelants de confiance*.

Certaines machines d'appel sortant demandent aux pairs distants de fournir des informations d'authentification lorsqu'ils répondent à leurs appels. Leurs rôles sont ensuite inversés : le pair distant devient l'authentifié et la machine d'appel sortant l'authentificateur.

Remarque – Bien que PPP 4.0 n'empêche pas l'authentification par les pairs de ligne spécialisée, l'authentification n'est pas fréquente dans ce type de liaison. La nature des contrats de lignes spécialisées implique généralement que les deux participants à chaque extrémité de la ligne se connaissent. Il s'agit souvent de participants de confiance. Toutefois, étant donné que l'authentification PPP n'est pas très difficile à gérer, vous devriez sérieusement envisager de mettre en œuvre l'authentification pour les lignes spécialisées.

Protocoles d'authentification PPP

Les protocoles d'authentification PPP sont les protocoles PAP (Password Authentication Protocol) et CHAP (Challenge-Handshake Authentication Protocol). Chaque protocole utilise une base de données de *secrets* qui contient des informations d'identification, ou *informations d'identification de sécurité*, pour chaque appelant autorisé à se connecter à la machine locale. Pour une explication détaillée de PAP, voir "Protocole d'authentification par mot de passe (PAP)" à la page 536. Pour une explication de CHAP, voir "Protocole CHAP (Challenge-Handshake Authentication Protocol)" à la page 539.

Raisons de l'utilisation de l'authentification PPP

Fournir l'authentification sur une liaison PPP est facultatif. En outre, bien que l'authentification vérifie qu'un pair est digne de confiance, l'authentification PPP ne garantit pas la confidentialité des données. Pour des raisons de confidentialité, utilisez des logiciels de chiffrement, comme IPsec, PGP, SSL, Kerberos et Solaris Secure Shell.

Remarque – Solaris PPP 4.0 ne met pas en œuvre le protocole ECP (Encryption Control Protocol) PPP, décrit dans le document RFC 1968.

Envisagez la mise en œuvre de l'authentification PPP dans les situations suivantes :

- Votre société accepte les appels entrants provenant d'utilisateurs sur le réseau téléphonique commuté public.
- La stratégie de sécurité de votre entreprise exige que les utilisateurs distants fournissent des informations d'authentification lorsqu'ils accèdent à votre réseau à travers un pare-feu d'entreprise ou lorsqu'ils se livrent à des transactions sécurisées.
- Vous voulez authentifier les appelants par rapport à une base de données de mots de passe UNIX standard, telle que `/etc/passwd`, NIS, NIS+, LDAP ou PAM. Utilisez une authentification PAP pour ce scénario.
- Les serveurs d'appel entrant de votre société fournissent également la connexion Internet du réseau. Utilisez une authentification PAP pour ce scénario.
- La ligne série est moins sûre que la base de données de mots de passe sur la machine ou les réseaux à chaque extrémité de la liaison. Utilisez une authentification CHAP pour ce scénario.

Prise en charge des utilisateurs DSL via PPPoE

De nombreux fournisseurs réseau et utilisateurs qui travaillent à domicile ont recours à la technologie DSL (Digital Subscriber Line, ligne d'abonné numérique) pour accélérer l'accès au réseau. Pour prendre en charge les utilisateurs DSL, Solaris PPP 4.0 intègre la fonction PPPoE (PPP over Ethernet). La technologie PPPoE permet à plusieurs hôtes d'exécuter des sessions PPP sur une liaison Ethernet vers une ou plusieurs destinations.

Si l'un des facteurs suivants s'applique à votre situation, vous devez utiliser le protocole PPPoE :

- Vous prenez en charge les utilisateurs DSL, y compris éventuellement vous-même. Votre fournisseur de services DSL peut demander aux utilisateurs de configurer un tunnel PPPoE pour recevoir des services sur la ligne DSL.
- Votre site est un FAI qui envisage de proposer PPPoE à ses clients.

Cette section présente les termes associés à la technologie PPPoE et une vue d'ensemble d'une topologie PPPoE de base.

Présentation PPPoE

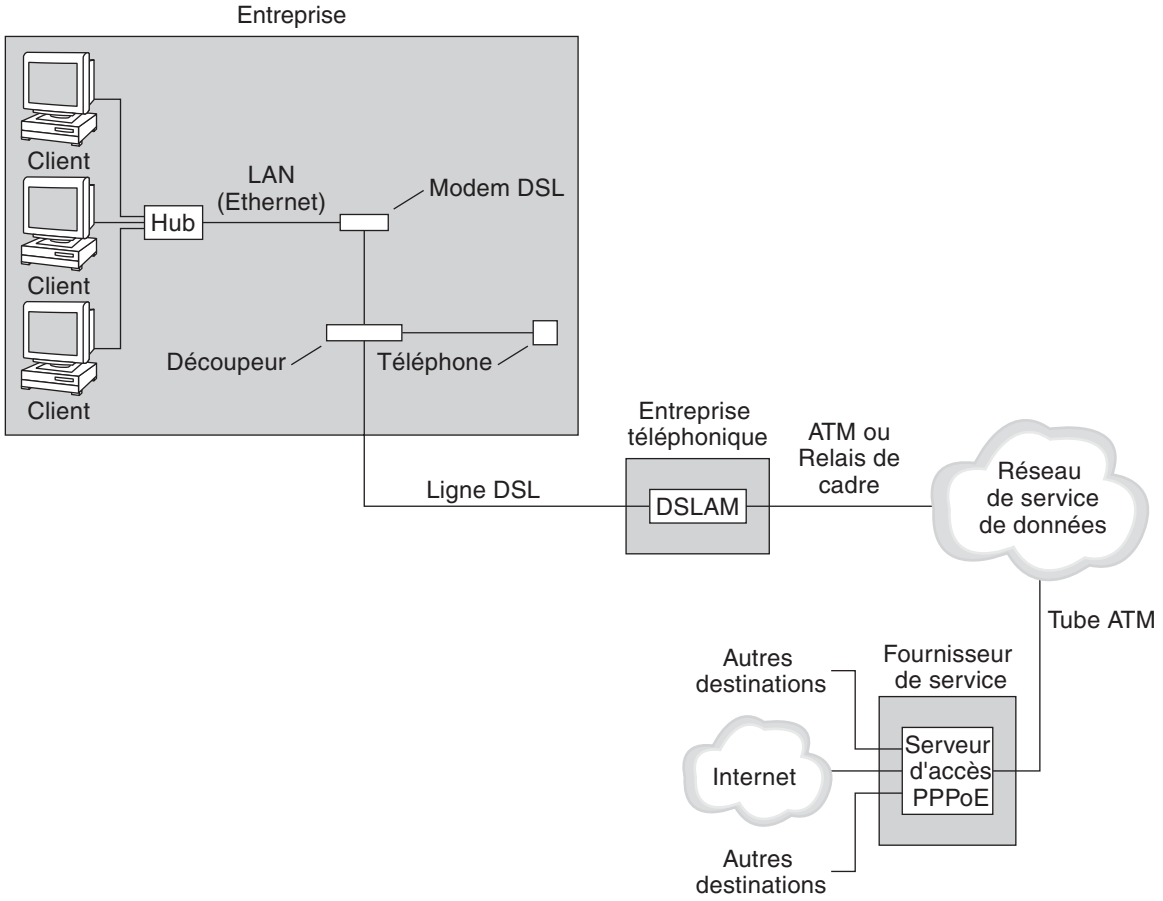
PPPoE est un protocole propriétaire de RedBack Networks. Plus qu'une autre version du protocole PPP standard, PPPoE est un protocole de découverte. Dans un scénario PPPoE, une machine qui lance des communications PPP doit d'abord repérer, ou *découvrir* , un pair qui exécute PPPoE. Le protocole PPPoE utilise des paquets de diffusion Ethernet pour localiser le pair.

Une fois le processus de détection terminé, PPPoE configure un tunnel Ethernet reliant l'hôte initiateur (*client PPPoE*) au pair (*serveur d'accès PPPoE*). La *mise en tunnel* consiste à exécuter un protocole sur un autre. À l'aide du protocole PPPoE, Solaris PPP 4.0 met en tunnel PPP sur Ethernet IEEE 802.2, deux protocoles de liaison de données. La connexion PPP obtenue se comporte comme une liaison dédiée entre le client PPPoE et le serveur d'accès. Pour des informations détaillées sur PPPoE, voir “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 544.

Composants d'une configuration PPPoE

Trois participants sont impliqués dans une configuration PPPoE : un consommateur, un opérateur de téléphonie et un fournisseur de service, comme illustré dans la figure suivante.

FIGURE 15–4 Participants à un tunnel PPPoE



Consommateurs PPPoE

En tant qu'administrateur système, vous pouvez aider les consommateurs à réaliser leur configuration PPPoE. Une personne ayant besoin d'exécuter PPPoE sur une ligne DSL est un consommateur PPPoE typique. Un autre consommateur PPPoE est une société qui acquiert une ligne DSL par le biais de laquelle ses employés peuvent exécuter des tunnels PPPoE, comme illustré dans la figure précédente.

Offrir des communications PPP par le biais d'un périphérique DSL haut débit à un nombre d'hôtes est la principale raison qui incite un consommateur professionnel à utiliser PPPoE. Souvent, un client PPPoE possède son propre *modem DSL*. Plusieurs clients sur un hub peuvent aussi partager un modem DSL également connecté au hub par une ligne Ethernet.

Remarque – Techniquement, les périphériques DSL sont des ponts, pas des modems. Cependant, ces périphériques étant couramment appelés des modems, ce guide utilise le terme "modem DSL".

PPPoE exécute PPP via un tunnel sur la ligne Ethernet connectée au modem DSL. Cette ligne est connectée à un séparateur, qui à son tour se connecte à une ligne téléphonique.

PPPoE côté opérateur de téléphonie

L'entreprise téléphonique correspond à la couche intermédiaire du scénario PPPoE. Il divise le signal reçu via la ligne téléphonique à l'aide d'un périphérique appelé *multiplexeur DSLAM (Digital Subscriber Line Access Multiplexer, multiplexeur d'accès de ligne d'abonné numérique)*. Le multiplexeur DSLAM décompose les signaux analogiques sur différents câbles, câbles analogiques pour le service téléphonique et câbles numériques pour PPPoE. Depuis le multiplexeur DSLAM, les câbles numériques prolongent le tunnel sur un réseau de données ATM jusqu'au FAI.

PPPoE côté fournisseur de service

Le FAI reçoit la transmission PPPoE du réseau de données ATM via un pont. Au niveau du fournisseur d'accès Internet, un serveur d'accès exécutant PPPoE fonctionne tout comme le pair de la liaison PPP. Le serveur d'accès fonctionne de manière très similaire au serveur d'appel entrant présenté à la Figure 15–2, à ceci près que le serveur n'utilise pas de modems. Le serveur d'accès convertit chaque session PPPoE en trafic IP régulier, un accès à Internet par exemple.

Si vous êtes l'administrateur système d'un fournisseur d'accès Internet, vous pouvez être chargé de la configuration et de la gestion d'un serveur d'accès.

Sécurité d'un tunnel PPPoE

Le tunnel PPPoE est par nature non sécurisé. Vous pouvez utiliser PAP ou CHAP afin de fournir l'authentification de l'utilisateur pour la liaison PPP en cours d'exécution sur le tunnel.

◆ ◆ ◆ CHAPITRE 16

Planification de la liaison PPP (tâches)

Définir une liaison PPP implique un ensemble de tâches distinctes, qui inclut la planification et d'autres activités qui ne sont pas liées à PPP. Ce chapitre explique comment planifier les liaisons PPP les plus courantes, l'authentification et PPPoE.

Les chapitres qui suivent le Chapitre 16, “Planification de la liaison PPP (tâches) ” utilisent des exemples de configuration pour illustrer comment configurer une liaison donnée. Ces exemples de configuration sont présentés dans ce chapitre.

Voici la liste des sujets abordés :

Planification PPP générale (liste des tâches)

PPP requiert des tâches de planification avant que la liaison puisse être configurée. En outre, si vous souhaitez utiliser la mise en tunnel PPPoE, vous devez d'abord configurer la liaison PPP, puis assurer la mise en tunnel. La liste des tâches suivante répertorie les principales tâches de planification abordées dans ce chapitre. Il se peut que la tâche générale suffise à configurer votre type de liaison. Il se peut aussi que les tâches de liaison, authentification et peut-être PPPoE soient nécessaires.

TABLEAU 16–1 Liste des tâches de planification PPP

Tâche	Description	Voir
Planification d'une liaison PPP commutée	Rassemblez les informations nécessaires à la configuration d'une machine d'appel sortant ou d'un serveur d'appel entrant.	“Planification d'une liaison PPP commutée” à la page 430

TABLEAU 16–1 Liste des tâches de planification PPP *(Suite)*

Tâche	Description	Voir
Planification d'une liaison de ligne spécialisée	Rassemblez les informations nécessaires à la configuration d'un client sur une ligne spécialisée.	"Planification d'une liaison de ligne spécialisée" à la page 434
Planification de l'authentification sur une liaison PPP	Rassemblez les informations nécessaires à la configuration de l'authentification PAP ou CHAP sur la liaison PPP.	"Planification de l'authentification sur une liaison" à la page 437
Planification d'un tunnel PPPoE	Rassemblez les informations nécessaires à la configuration d'un tunnel PPPoE sur lequel une liaison PPP peut s'exécuter.	"Planification de la prise en charge DSL sur un tunnel PPPoE" à la page 442

Planification d'une liaison PPP commutée

Parmi les liaisons PPP, les liaisons commutées sont les plus courantes. Cette section contient les informations suivantes :

- Informations de planification d'une liaison commutée
- Explication de l'exemple de liaison à utiliser au Chapitre 17, "Configuration d'une liaison PPP commutée (tâches)"

En général, vous configurez uniquement la machine située à l'une des extrémités de la liaison PPP commutée : la machine d'appel sortant ou le serveur d'appel entrant. Pour une présentation de la liaison PPP commutée, voir "Présentation de la liaison commutée PPP " à la page 417.

Avant de configurer la machine d'appel sortant

Avant de configurer une machine d'appel sortant, rassemblez les informations répertoriées dans le tableau ci-dessous.

Remarque – Les informations de planification contenues dans cette section n'incluent pas les informations à rassembler sur l'authentification ou PPPoE. Pour plus d'informations sur la planification de l'authentification, voir "Planification de l'authentification sur une liaison" à la page 437. Pour la planification PPPoE, voir "Planification de la prise en charge DSL sur un tunnel PPPoE" à la page 442.

TABLEAU 16–2 Informations pour une machine d'appel sortant

Informations	Action
Vitesse maximale du modem	Reportez-vous à la documentation fournie par le fabricant du modem.

TABLEAU 16–2 Informations pour une machine d'appel sortant *(Suite)*

Informations	Action
Commandes de connexion du modem (commandes AT)	Reportez-vous à la documentation fournie par le fabricant du modem.
Nom à attribuer au serveur d'appel entrant situé à l'autre extrémité de la liaison	Créez un nom vous permettant d'identifier le serveur d'appel entrant.
Séquence de connexion requise par le serveur d'appel entrant	Contactez l'administrateur du serveur d'appel entrant ou consultez la documentation du FAI si le serveur d'appel entrant se trouve chez le FAI.

Avant de configurer le serveur d'appel entrant

Avant de configurer un serveur d'appel entrant, rassemblez les informations répertoriées dans le tableau ci-dessous.

Remarque – Les informations de planification contenues dans cette section n'incluent pas les informations à rassembler sur l'authentification ou PPPoE. Pour plus d'informations sur la planification de l'authentification, voir "Planification de l'authentification sur une liaison" à la page 437. Pour la planification PPPoE, voir "Planification de la prise en charge DSL sur un tunnel PPPoE" à la page 442.

TABLEAU 16–3 Informations pour un serveur d'appel entrant

Informations	Action
Vitesse maximale du modem	Reportez-vous à la documentation fournie par le fabricant du modem.
Noms des utilisateurs autorisés à appeler le serveur d'appel entrant	Obtenez le nom des utilisateurs potentiels avant de configurer leurs répertoires personnels, comme indiqué à la section "Configuration des utilisateurs du serveur d'appel entrant " à la page 458.
Adresse IP dédiée aux communications PPP	Obtenez l'adresse de la personne responsable au sein de votre société de la délégation des adresses IP.

Exemple de configuration d'une liaison PPP commutée

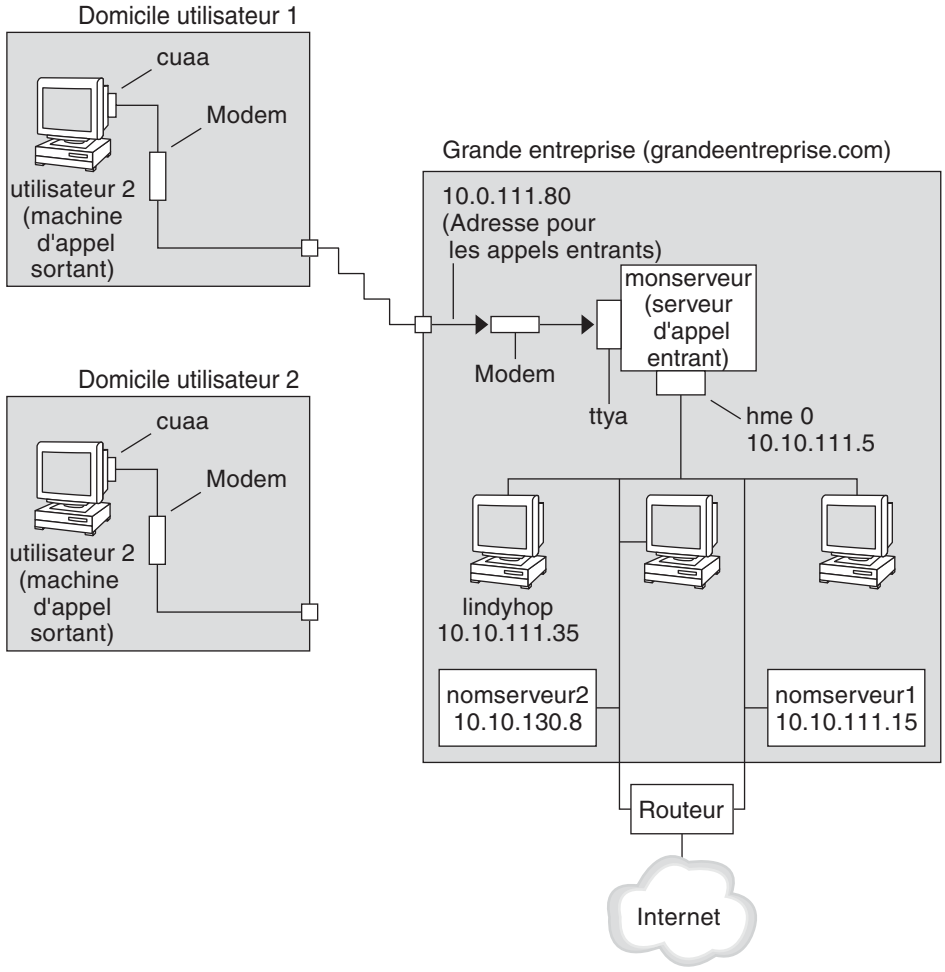
Les tâches présentées au Chapitre 17, "Configuration d'une liaison PPP commutée (tâches)" permettent de répondre aux besoins d'une petite société qui autorise ses employés à travailler de chez eux quelques jours par semaine. Le SE Solaris doit être installé sur l'ordinateur que les employés utilisent chez eux. Ceux-ci doivent également se connecter à distance à leur machine de travail sur l'intranet de l'entreprise.

Les tâches permettent de configurer une liaison commutée de base aux caractéristiques suivantes :

- Les machines *d'appel sortant* sont situées chez les employés qui doivent appeler l'intranet de l'entreprise.
- Le serveur *d'appel entrant* est une machine située sur l'intranet de l'entreprise, configurée pour recevoir les appels entrants des employés.
- Une connexion de type UNIX est utilisée pour authentifier la machine d'appel sortant. Des méthodes d'authentification Solaris PPP 4.0 plus strictes ne sont pas requises par la politique de sécurité de l'entreprise.

La figure suivante illustre la liaison configurée au Chapitre 17, “Configuration d'une liaison PPP commutée (tâches)”.

FIGURE 16–1 Exemple de liaison commutée



Dans cette figure, un hôte distant lance un appel sortant par le biais de son modem via les lignes téléphoniques à l'intranet de Big Company. Un autre hôte est configuré pour pouvoir établir une connexion à Big Company mais est actuellement inactif. Les appels provenant d'utilisateurs distants sont traités dans l'ordre selon lequel ils sont reçus par le modem connecté au serveur d'appel entrant au sein de Big Company Une connexion PPP est établie entre les pairs. La machine d'appel sortant peut ensuite se connecter à distance à une machine hôte sur l'intranet.

Sources d'informations sur la liaison PPP commutée

Reportez-vous aux sections suivantes :

- Pour configurer une machine d'appel sortant, voir Tableau 17–2.
- Pour configurer une machine d'appel entrant, voir Tableau 17–3.
- Pour obtenir un aperçu des liaisons commutées, voir “Présentation de la liaison commutée PPP ” à la page 417.
- Pour obtenir des informations détaillées sur les commandes et fichiers PPP, voir “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 513.

Planification d'une liaison de ligne spécialisée

Configurer une liaison de ligne spécialisée consiste à configurer le pair situé à une extrémité d'un service commuté ou non commuté, loué à un fournisseur.

Cette section contient les informations suivantes :

- Informations de planification d'une ligne spécialisée
- Explication de l'exemple de liaison illustré à la Figure 16–2

Pour une présentation des liaisons de ligne spécialisée, reportez-vous à la section “Présentation de la liaison PPP de ligne spécialisée” à la page 421. Pour connaître les tâches de configuration d'une ligne spécialisée, voir le Chapitre 18, “Configuration d'une liaison PPP de ligne spécialisée (tâches) ”.

Avant de configurer une liaison de ligne spécialisée

Lorsque votre société loue une liaison de ligne spécialisée à un fournisseur réseau, vous ne configurez généralement que le système à votre extrémité de la liaison. Le pair situé à l'autre extrémité de la liaison est géré par un autre administrateur. Il peut s'agir d'un administrateur système situé à un emplacement distant au sein de votre société ou d'un administrateur système chez le fournisseur d'accès Internet.

Matériel nécessaire à une liaison de ligne spécialisée

Outre le support de la liaison, votre extrémité de la liaison nécessite le matériel suivant :

- Interface synchrone pour votre système
- Unité synchrone (CSU/DSU)
- Votre système

L'équipement des locaux d'abonné (CPE, customer premises equipment) de certains fournisseurs de services réseau inclut un routeur, une interface synchrone et une CSU/DSU.

Cependant, l'équipement nécessaire varie en fonction du fournisseur et des restrictions gouvernementales liées à votre environnement linguistique. Le fournisseur réseau peut vous fournir des informations sur l'unité nécessaire, si cet équipement n'est pas fourni avec la ligne spécialisée.

Informations à rassembler pour la liaison de ligne spécialisée

Avant de configurer le pair local, il vous faudra peut-être rassembler les éléments répertoriés dans le tableau suivant.

TABLEAU 16–4 Planification d'une liaison de ligne spécialisée

Informations	Action
Nom de périphérique de l'interface	Reportez-vous à la documentation de la carte d'interface.
Instructions de configuration de la carte d'interface synchrone	Reportez-vous à la documentation de la carte d'interface. Vous avez besoin de ces informations pour configurer l'interface HSI/P. Il n'est peut-être pas nécessaire de configurer d'autres types de cartes d'interface.
(Facultatif) Adresse IP du pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant. Ces informations sont nécessaires uniquement si l'adresse IP n'est pas négociée entre les deux pairs.
(Facultatif) Nom du pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.
(Facultatif) Vitesse de la liaison	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.
(Facultatif) Compression utilisée par le pair distant	Reportez-vous à la documentation du fournisseur de service. Vous pouvez également contacter l'administrateur système du pair distant.

Exemple de configuration d'une liaison de ligne spécialisée

Les tâches décrites au Chapitre 18, “Configuration d'une liaison PPP de ligne spécialisée (tâches) ” illustrent comment une entreprise de taille moyenne (LocalCorp) atteint son objectif de fournir un accès Internet à ses employés. À présent, les ordinateurs des employés sont connectés au réseau privé de l'entreprise (intranet).

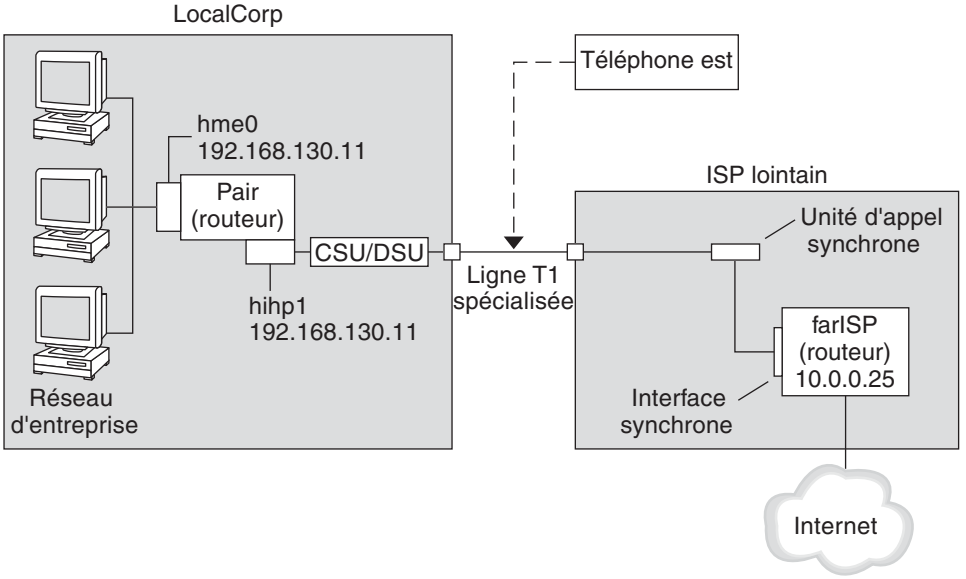
LocalCorp a besoin d'accélérer les transactions et l'accès aux nombreuses ressources disponibles sur Internet. La société signe un contrat avec le fournisseur d'accès Internet Far, ce qui lui

permet de définir sa propre ligne spécialisée avec Far. Ensuite, LocalCorp loue une ligne T1 à Phone East, un opérateur de téléphonie. Phone East installe la ligne spécialisée entre LocalCorp et le FAI Far. Phone East fournit ensuite une CSU/DSU déjà configurée à LocalCorp.

Les tâches permettent de configurer une liaison de ligne spécialisée dotée des caractéristiques suivantes :

- LocalCorp a configuré un système sous forme de routeur de passerelle, qui transmet les paquets à des hôtes sur Internet via la ligne spécialisée.
- Le FAI Far a également défini un pair comme routeur auquel des lignes spécialisées de clients sont connectées.

FIGURE 16–2 Exemple d'une configuration de ligne spécialisée



Dans la figure, un routeur est configuré pour PPP au sein de LocalCorp. Le routeur se connecte à l'intranet de l'entreprise par l'intermédiaire de son interface `hme0`. La deuxième connexion relie l'interface HSI/P (hihp1) de la machine à l'unité numérique CSU/DSU. La CSU/DSU se connecte alors à la ligne spécialisée installée. L'administrateur de LocalCorp configure l'interface HSI/P et fichiers PPP. L'administrateur tape ensuite `/etc/init.d/pppd` pour initialiser la liaison entre LocalCorp et le FAI Far.

Sources d'informations sur les lignes spécialisées

Reportez-vous aux sections suivantes :

- Chapitre 18, “Configuration d'une liaison PPP de ligne spécialisée (tâches) ”
- “Présentation de la liaison PPP de ligne spécialisée” à la page 421

Planification de l'authentification sur une liaison

Cette section contient les informations de planification pour fournir l'authentification sur la liaison PPP. Le Chapitre 19, “Paramétrage de l'authentification PPP (tâches)” contient les tâches permettant de mettre en œuvre l'authentification PPP sur votre site.

PPP offre deux types d'authentification : PAP, qui est décrite en détail à la section “Protocole d'authentification par mot de passe (PAP)” à la page 536 et CHAP, qui est décrite à la section “Protocole CHAP (Challenge-Handshake Authentication Protocol)” à la page 539.

Avant de configurer l'authentification sur une liaison, vous devez choisir le protocole d'authentification qui répond le mieux à la stratégie de sécurité de votre site. Ensuite, vous configurez le fichier des secrets et les fichiers de configuration PPP pour les machines d'appel entrant ou les machines d'appel sortant des appelants, ou les deux types de machines. Pour plus d'informations sur le choix du protocole d'authentification qui convient à votre site, reportez-vous à la section “Raisons de l'utilisation de l'authentification PPP” à la page 425.

Cette section contient les informations suivantes :

- Informations de planification pour les authentifications PAP et CHAP
- Explications des exemples de scénario d'authentification présentés aux Figure 16–3 et Figure 16–4

Pour une description des tâches de configuration de l'authentification, reportez-vous au Chapitre 19, “Paramétrage de l'authentification PPP (tâches)”.

Avant de configurer l'authentification PPP

La configuration de l'authentification sur votre site doit faire partie intégrante de votre stratégie PPP générale. Avant de mettre en œuvre l'authentification, vous devez monter le matériel, configurer le logiciel et tester la liaison.

TABLEAU 16–5 Prérequis à la configuration de l'authentification

Informations	Voir
Tâches de configuration d'une liaison commutée	Chapitre 17, “Configuration d'une liaison PPP commutée (tâches)”.

TABLEAU 16–5 Prérequis à la configuration de l'authentification *(Suite)*

Informations	Voir
Tâches relatives au test de la liaison	Chapitre 21, “Résolution des problèmes PPP courants (tâches) ”.
Exigences en matière de sécurité pour votre site	Stratégie de sécurité de votre entreprise. Si vous ne disposez pas d'une stratégie de sécurité, la configuration de l'authentification PPP vous offre l'occasion d'en créer une.
Suggestions à propos de l'utilisation du protocole PAP ou CHAP sur votre site	“Raisons de l'utilisation de l'authentification PPP” à la page 425. Pour obtenir des informations plus détaillées sur ces protocoles, voir “Authentification des appelants sur une liaison” à la page 536

Exemples de configuration d'authentification PPP

Cette section contient des exemples de scénarios d'authentification à utiliser dans les procédures décrites au Chapitre 19, “Paramétrage de l'authentification PPP (tâches)”.

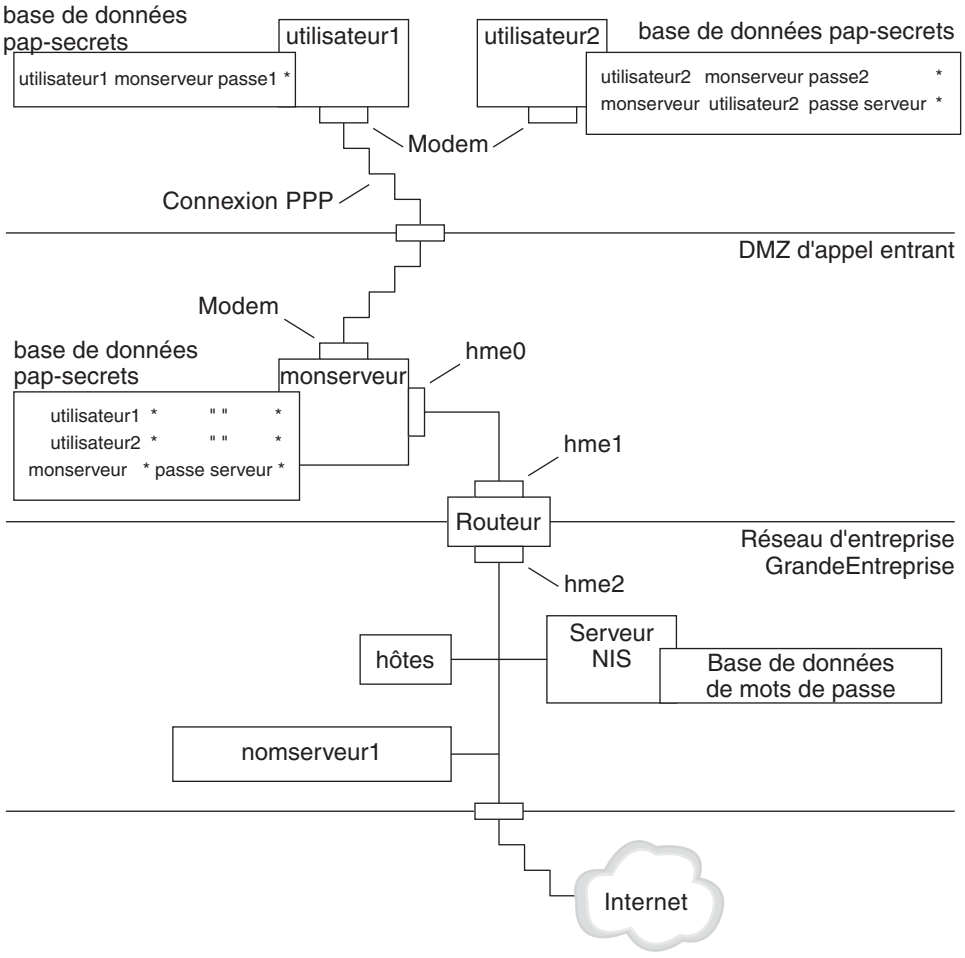
- “Exemple de configuration utilisant une authentification PAP ” à la page 438
- “Exemple de configuration utilisant l'authentification CHAP” à la page 440

Exemple de configuration utilisant une authentification PAP

Les tâches décrites à la section “Configuration de l'authentification PAP” à la page 470 montrent comment configurer une authentification PAP sur la liaison PPP. Les procédures utilisent comme exemple un scénario PAP créé pour la société fictive Big Company dans l'“Exemple de configuration d'une liaison PPP commutée” à la page 431.

Big Company veut permettre à ses utilisateurs de travailler à domicile. Les administrateurs système veulent une solution sûre pour les lignes série reliées au serveur d'appel entrant. La connexion de type UNIX qui fait appel aux bases de données de mots de passe NIS a convenu au réseau de Big Company par le passé. Les administrateurs système veulent un modèle d'authentification UNIX pour les appels entrant sur le réseau via la liaison PPP. Par conséquent, ils peuvent appliquer le scénario suivant qui a recours à l'authentification PAP.

FIGURE 16–3 Exemple d'un scénario d'authentification PAP (travail à domicile)



Le administrateurs système créent une DMZ d'appel entrant dédiée et séparée du reste du réseau d'entreprise par un routeur. L'acronyme DMZ provient du terme militaire anglais “demilitarized zone” (zone démilitarisée). La DMZ est un réseau isolé, configuré pour des raisons de sécurité. La DMZ contient généralement les ressources qu'une société offre au public, telles que des serveurs Web, des serveurs FTP anonymes, des bases de données et des serveurs modem. Les concepteurs de réseaux placent souvent la DMZ entre un pare-feu et une connexion Internet de l'entreprise.

Les seuls occupants de la DMZ décrite à la Figure 16–3 sont le serveur d'appel entrant `myserver` et le routeur. Le serveur d'appel entrant exige des appelants qu'ils fournissent leurs informations d'identification PAP, notamment leurs nom d'utilisateur et mot de passe, lors de la configuration de la liaison. En outre, le serveur d'appel entrant utilise l'option `login` de PAP.

Ainsi, les noms d'utilisateur et mots de passe PAP des appelants doivent correspondre exactement à leurs noms d'utilisateur et mots de passe UNIX dans la base de données de mots de passe du serveur d'appel entrant.

Une fois la liaison PPP établie, les paquets de l'appelant sont transmis au routeur. Le routeur fait suivre la transmission à sa destination sur le réseau de l'entreprise ou sur Internet.

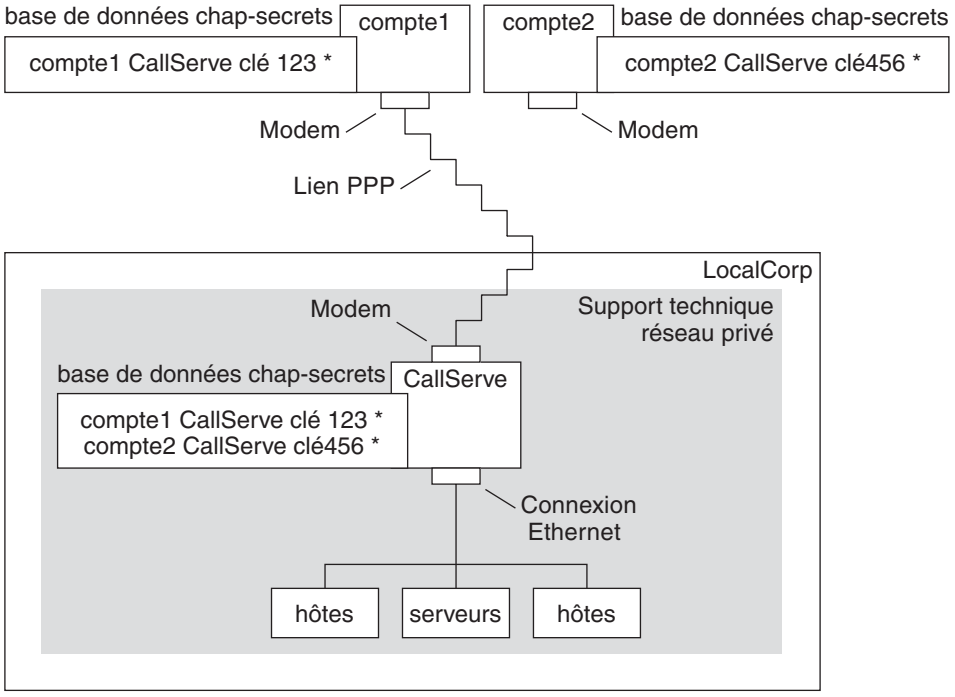
Exemple de configuration utilisant l'authentification CHAP

Les tâches décrites à la section "Configuration de l'authentification CHAP" à la page 478 montrent comment configurer l'authentification CHAP. Les procédures utilisent comme exemple un scénario CHAP à créer pour la société fictive LocalCorp présentée à l'"Exemple de configuration d'une liaison de ligne spécialisée" à la page 435.

LocalCorp fournit la connexion à Internet via une ligne spécialisée à un FAI. Le service d'assistance technique de LocalCorp génère un trafic réseau important. Par conséquent, il a besoin d'un réseau privé isolé. Les techniciens du service voyagent beaucoup et ont besoin d'accéder à distance au réseau de l'assistance technique pour obtenir des informations leur permettant de résoudre des problèmes. Pour protéger les informations confidentielles contenues dans la base de données du réseau privé, les appelants distants doivent être authentifiés avant d'être autorisés à se connecter.

Par conséquent, les administrateurs système mettent en œuvre le scénario d'authentification CHAP suivant pour une configuration PPP commutée.

FIGURE 16–4 Exemple d'un scénario d'authentification CHAP (appel d'un réseau privé)



Le seul lien entre le réseau de l'assistance technique et le monde extérieur est la ligne série vers l'extrémité du serveur d'appel entrant de la liaison. Les administrateurs système configurent l'ordinateur portable de chaque représentant du service pour une liaison PPP dotée de la sécurité CHAP, comprenant un secret CHAP. La base de données des secrets CHAP située sur le serveur d'appel entrant contient les informations d'identification CHAP pour toutes les machines qui sont autorisées à appeler le réseau de l'assistance technique.

Sources d'informations sur l'authentification

Vous disposez des ressources suivantes :

- Voir "Configuration de l'authentification PAP" à la page 470.
- Voir "Configuration de l'authentification CHAP" à la page 478.
- Voir "Authentification des appelants sur une liaison" à la page 536 et la page de manuel `pppd`(1M).

Planification de la prise en charge DSL sur un tunnel PPPoE

Certains fournisseurs DSL vous demandent de configurer la mise en tunnel PPPoE de votre site pour exécuter PPP sur leurs réseaux numériques haut débit et lignes DSL. Pour une présentation de PPPoE, voir “Prise en charge des utilisateurs DSL via PPPoE ” à la page 425.

Un tunnel PPPoE implique trois participants : un consommateur, un opérateur de téléphonie et un fournisseur d'accès Internet. Vous configurez PPPoE pour des consommateurs (des clients PPPoE au sein de votre entreprise ou des particuliers à domicile, par exemple) ou sur un serveur auprès d'un fournisseur d'accès Internet.

Cette section contient les informations de planification pour l'exécution PPPoE sur les clients et les serveurs d'accès. Il aborde les sujets suivants :

- Informations de planification pour le serveur d'accès et l'hôte PPPoE
- Explication du scénario PPPoE présenté à la section “Exemple de configuration d'un tunnel PPPoE ” à la page 444

Le Chapitre 20, “Configuration d'un tunnel PPPoE (tâches)” décrit les tâches de configuration d'un tunnel PPPoE.

Avant de configurer un tunnel PPPoE

Les activités précédant la configuration varient en fonction du côté du tunnel que vous configurez, client ou serveur. Dans les deux cas, vous ou votre entreprise devez conclure un contrat avec un opérateur de téléphonie. Celui-ci fournit les lignes DSL aux clients, ainsi qu'une passerelle et éventuellement un tube ATM aux serveurs d'accès. La plupart des contrats stipulent qu'il incombe à l'opérateur de téléphonie de monter son équipement sur votre site.

Avant de configurer un client PPPoE

Généralement, l'implémentation du client PPPoE inclut l'équipement suivant :

- Ordinateur personnel ou autre système utilisé par un particulier ;
- Modem DSL généralement installé par l'opérateur de téléphonie ou le fournisseur d'accès Internet ;
- (Facultatif) Hub, si plusieurs clients sont impliqués, ce qui est le cas des consommateurs DSL d'entreprises ;
- (Facultatif) Séparateur, généralement installé par le fournisseur.

De nombreuses configurations DSL sont possibles, en fonction des besoins de l'utilisateur ou de la société, ainsi que des services proposés par le fournisseur.

TABLEAU 16–6 Planification pour les clients PPPoE

Informations	Action
Si vous configurez un client PPPoE à domicile pour un particulier ou pour vous-même, rassemblez les informations de configuration figurant hors du champ d'application de PPPoE.	Demandez les procédures de configuration requises à l'opérateur de téléphonie ou au fournisseur d'accès Internet (FAI).
Si vous configurez des clients PPPoE au niveau d'un site d'entreprise, rassemblez le nom des utilisateurs auxquels sont affectés les systèmes client PPPoE. Si vous configurez des clients PPPoE distants, la responsabilité de fournir aux utilisateurs des informations relatives à l'ajout d'équipements DSL à domicile peut vous incomber.	Demandez une liste des utilisateurs autorisés à la direction de votre entreprise.
Recherchez les interfaces disponibles sur le client PPPoE.	Exécutez la commande `ifconfig -a` sur chaque machine pour connaître le nom des interfaces.
(Facultatif) Obtenez le mot de passe du client PPPoE.	Demandez aux utilisateurs les mots de passe qu'ils préfèrent. Ou affectez des mots de passe aux utilisateurs. Notez que ce mot de passe est utilisé pour l'authentification de liaison, non pour la connexion UNIX.

Avant de configurer un serveur PPPoE

La planification d'un serveur d'accès PPPoE implique une collaboration avec l'opérateur de téléphonie qui vous fournit la connexion à son réseau de service de données. L'opérateur de téléphonie installe ses lignes, souvent des tubes ATM, sur votre site, et fournit une passerelle à votre serveur d'accès. Vous devez configurer les interfaces Ethernet qui ont accès aux services offerts par votre société. Par exemple, vous devez configurer des interfaces pour l'accès à Internet, ainsi que les interfaces Ethernet du pont de l'opérateur de téléphonie

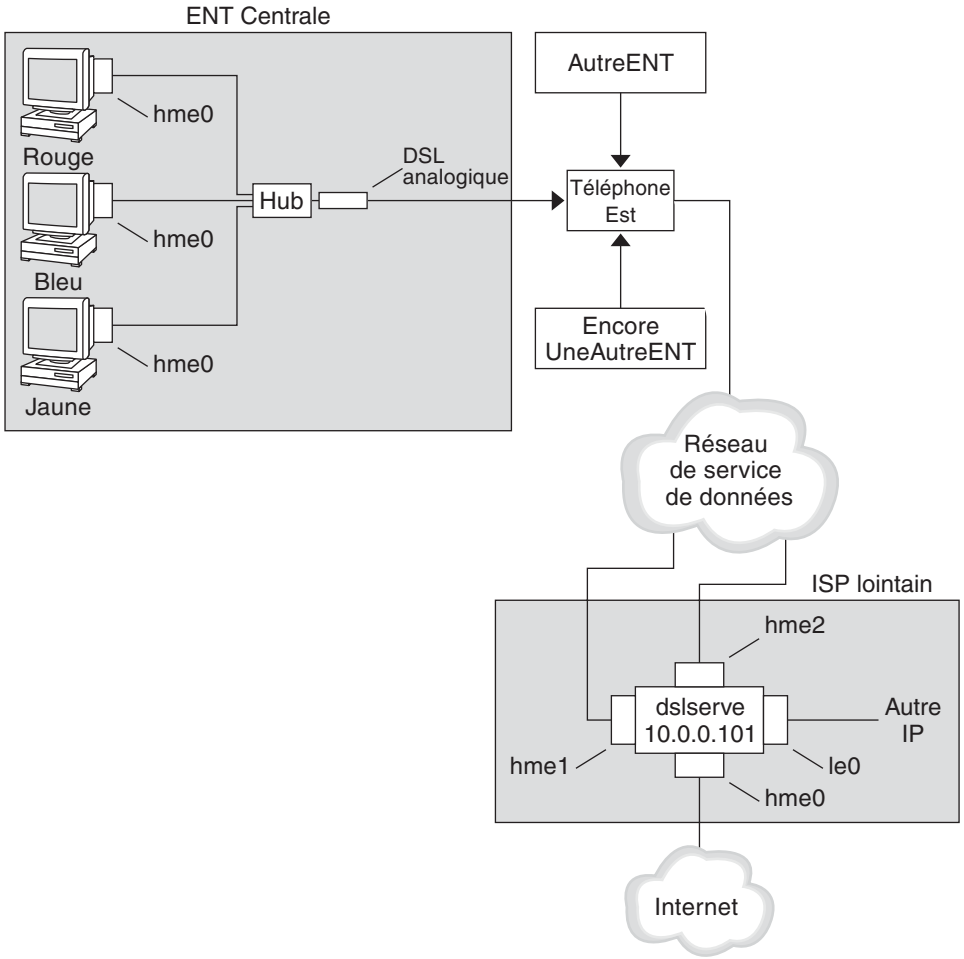
TABLEAU 16–7 Planification d'un serveur d'accès PPPoE

Informations	Action
Interfaces utilisées pour les lignes du réseau de service de données	Exécutez la commande `ifconfig -a` pour identifier les interfaces.
Types de services à fournir à partir du serveur PPPoE	Demandez à la direction et aux planificateurs de réseau qu'ils vous fournissent leurs exigences et suggestions.
(Facultatif) Types de services à fournir aux consommateurs	Demandez à la direction et aux planificateurs de réseau qu'ils vous fournissent leurs exigences et suggestions.
(Facultatif) Noms d'hôte et mots de passe des clients distants	Demandez aux planificateurs de réseau et aux autres personnes responsables sur votre site de la négociation des contrats. Les noms d'hôte et mots de passe sont utilisés pour l'authentification PAP ou CHAP, non pour la connexion UNIX.

Exemple de configuration d'un tunnel PPPoE

Cette section contient un exemple de tunnel PPPoE qui sert d'illustration des tâches décrites au Chapitre 20, “Configuration d'un tunnel PPPoE (tâches)”. Bien que l'illustration indique tous les participants au tunnel, vous administrez uniquement une extrémité, le côté client ou le côté serveur.

FIGURE 16–5 Exemple de tunnel PPPoE



Dans l'exemple, MiddleCo souhaite fournir un accès Internet haut débit à ses employés. MiddleCo acquiert un package DSL auprès de Phone East, qui, à son tour, passe un contrat avec

le fournisseur d'accès Internet (FAI) Far. Le FAI Far offre un accès Internet et d'autres services IP aux clients qui achètent un package DSL à Phone East.

Exemple de configuration client PPPoE

MiddleCo acquiert un package auprès de Phone East qui fournit une ligne DSL au site. L'offre comprend une connexion authentifiée dédiée au FAI pour les clients PPPoE de MiddleCo. L'administrateur système connecte les clients PPPoE potentiels à un hub. Les techniciens de Phone East connecte le hub à leur équipement DSL.

Exemple de configuration d'un serveur PPPoE

Dans le cadre de l'application de l'accord commercial entre le FAI Far et Phone East, l'administrateur système du FAI configure le serveur d'accès `dslserve`. Ce serveur possède quatre interfaces :

- `eri0` : interface du réseau principal qui se connecte au réseau local
- `hme0` : interface par la biais de laquelle le FAI Far fournit un service Internet à ses clients
- `hme1` : interface contractée par MiddleCo pour les tunnels PPPoE authentifiés
- `hme2` : interface contractée par d'autres clients pour leur tunnel PPPoE

Sources d'informations sur PPPoE

Vous disposez des ressources suivantes :

- Voir “Configuration du client PPPoE” à la page 486.
- Voir “Configuration d'un serveur d'accès PPPoE” à la page 489.
- Reportez-vous à la section “Création de tunnels PPPoE pour la prise en charge DSL ” à la page 544 et aux pages de manuel `pppoed`(1M), `pppoec`(1M) et `sppptun`(1M).

◆ ◆ ◆ CHAPITRE 17

Configuration d'une liaison PPP commutée (tâches)

Ce chapitre explique les tâches de la configuration de la liaison PPP la plus courante, la liaison commutée. Les sections principales sont les suivantes :

Tâches principales de la configuration de la liaison PPP commutée (liste des tâches)

Pour configurer la liaison PPP commutée, vous devez configurer des modems, modifier des fichiers de base de données et modifier les fichiers de configuration PPP décrits dans le Tableau 22–1.

Le tableau suivant répertorie les principales tâches de la configuration des deux côtés d'une liaison PPP commutée. En général, vous configurez une seule extrémité de la liaison, c'est-à-dire la machine d'appel sortant ou le serveur d'appel entrant.

TABLEAU 17–1 Liste des tâches de la configuration de la liaison PPP commutée

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	"Planification d'une liaison PPP commutée" à la page 430
2. Configuration de la machine d'appel sortant	Configurez le protocole PPP sur la machine qui effectue l'appel via la liaison.	Tableau 17–2

TABLEAU 17–1 Liste des tâches de la configuration de la liaison PPP commutée *(Suite)*

Tâche	Description	Voir
3. Configuration du serveur d'appel entrant	Configurez le protocole PPP sur la machine qui reçoit les appels entrants.	Tableau 17–3
4. Appel du serveur d'appel entrant	Tapez la commande `pppd` pour initialiser les communications.	"Appel du serveur d'appel entrant" à la page 461

Configuration de la machine d'appel sortant

Les tâches de cette section expliquent comment configurer une machine d'appel sortant. Le scénario d'appel entrant à partir du domicile présenté à la Figure 16–1 sert d'exemple. Vous pouvez effectuer les tâches dans votre société avant de remettre la machine à un utilisateur potentiel. Vous pouvez également indiquer aux utilisateurs expérimentés comment configurer leur machine chez eux. Pour configurer une machine d'appel sortant, il est impératif de posséder l'autorisation racine sur cette machine.

Tâches de configuration de la machine d'appel sortant (liste des tâches)

TABLEAU 17–2 Liste des tâches de la configuration de la machine d'appel sortant

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	"Planification d'une liaison PPP commutée" à la page 430
2. Configuration du modem et du port série	Configurez le modem et le port série.	"Configuration du modem et du port série (machine d'appel sortant)" à la page 450
3. Configuration de la communication via la ligne série	Configurez les caractéristiques de la transmission via la ligne série.	"Définition des communications sur la ligne série " à la page 451
4. Définition de la conversation entre la machine d'appel sortant et le pair	Rassemblez les données de communication à utiliser lorsque vous créez le script de discussion.	"Création des instructions pour l'appel d'un pair" à la page 452
5. Configuration des informations concernant un pair particulier	Configurez les options PPP pour l'appel d'un serveur d'appel entrant donné.	"Définition de la connexion à un pair donné" à la page 453

TABLEAU 17–2 Liste des tâches de la configuration de la machine d'appel sortant *(Suite)*

Tâche	Description	Voir
6. Appel du pair	Tapez la commande `pppd` pour initialiser les communications.	"Appel du serveur d'appel entrant" à la page 461

Fichiers modèles de liaison PPP commutée

Solaris PPP 4.0 fournit des fichiers modèles. Chaque modèle contient des options courantes pour un fichier de configuration PPP particulier. Le tableau suivant répertorie les exemples de modèles qui peuvent être utilisés pour la configuration d'une liaison commutée et leurs fichiers Solaris PPP 4.0 équivalents.

Fichier modèle	Fichier de configuration PPP	Voir
`/etc/ppp/options.tmpl`	`/etc/ppp/options`	"Modèle `/etc/ppp/options.tmpl`" à la page 518
`/etc/ppp/options.ttya.tmpl`	`/etc/ppp/options.`*ttyname*	"Fichier modèle `options.ttya.tmpl`" à la page 520
`/etc/ppp/myisp-chat.tmpl`	Fichier portant le nom de votre choix pour contenir le script de discussion	"Modèle de script de discussion `/etc/ppp/myisp-chat.tmpl`" à la page 528
`/etc/ppp/peers/myisp.tmpl`	`/etc/ppp/peers/`*peer-name*	"Fichier modèle `/etc/ppp/peers/myisp.tmpl`" à la page 524

Si vous décidez d'utiliser l'un des fichiers modèles, veillez à le renommer comme le fichier de configuration PPP équivalent. La seule exception est le fichier de discussion modèle `/etc/ppp/myisp-chat.tmpl`. Vous pouvez nommer le script de discussion à votre convenance.

Configuration des périphériques sur la machine d'appel sortant

La première tâche du processus de configuration d'une machine PPP d'appel sortant consiste à configurer les périphériques sur la ligne série, c'est-à-dire le modem et le port série.

Remarque – Les tâches qui s'appliquent à un modem s'appliquent généralement à un adaptateur de terminal RNIS.

Avant d'effectuer la procédure ci-dessous, vous devez avoir effectué les opérations suivantes :

- Installation de la version de Solaris sur la machine d'appel sortant
- Identification de la vitesse optimale du modem
- Choix du port série à utiliser sur la machine d'appel sortant
- Obtention du mot de passe root pour la machine d'appel sortant

Le Tableau 16–2 contient des informations de planification.

▼ Configuration du modem et du port série (machine d'appel sortant)

1 **Programmez le modem.**

Bien qu'il existe une grande variété de types de modems, la plupart est livrée avec les paramètres appropriés pour Solaris PPP 4.0. La liste suivante présente les paramètres de base pour les modems qui utilisent Solaris PPP 4.0.

- **DCD :** suivre les instructions de la porteuse
- **DTR :** définir sur un niveau faible pour que le modem raccroche et accrocher le modem
- **Contrôle de flux :** définir sur RTS/CTS pour un contrôle de flux matériel duplex intégral
- **Séquences Attention :** désactiver

Si vous rencontrez des problèmes pour configurer la liaison et pensez que le modem est défectueux, consultez d'abord la documentation du fabricant du modem. En outre, un certain nombre de sites Web se proposent de vous aider à programmer votre modem. Enfin, vous pouvez trouver des suggestions permettant de résoudre des problème liés au modem à la section “Diagnostic des problèmes de modem ” à la page 503.

2 **Branchez les câbles du modem au port série de la machine d'appel sortant et à la prise de téléphone.**

3 **Connectez-vous en tant que superutilisateur (ou équivalent) à la machine d'appel sortant.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

4 **Exécutez la commande `/usr/smap/bin/smc`, comme expliqué à la section “Configuration des terminaux et modems avec l'outil Ports série (présentation)” du *Guide d'administration système : Administration avancée*. Cette commande ouvre la console de gestion Solaris.**

Utilisez la console de gestion Solaris pour effectuer les opérations suivantes :

a. **Sélectionnez le port auquel le modem est connecté.**

b. Définissez la direction du modem pour les appels sortants uniquement.

Vous êtes libre de configurer le modem dans les deux directions. Toutefois, le définir en appel sortant uniquement permet de se protéger d'éventuels intrus.

Remarque – Vous pouvez définir la vitesse de transmission et le délai d'attente à partir de `/usr/smap/bin/smc` . Toutefois, le démon `pppd` ne tient pas compte de ces paramètres.

---

5 Cliquez sur OK pour que vos modifications entrent en vigueur.

Configuration des communications sur la machine d'appel sortant

Les procédures décrites dans cette section expliquent comment configurer les communications transitant par la ligne série de la machine d'appel sortant. Avant de pouvoir appliquer ces procédures, vous devez configurer le modem et le port série, comme décrit à la section "Configuration du modem et du port série (machine d'appel sortant)" à la page 450.

Les tâches suivantes indiquent comment activer la machine d'appel sortant pour établir les communications avec le serveur d'appel entrant. L'amorce des communications est définie par les options contenues dans les fichiers de configuration PPP. Vous devez créer les fichiers suivants :

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- Script de discussion
- `/etc/ppp/peers/`*peer-name*

Solaris PPP 4.0 fournit des modèles pour les fichiers de configuration PPP, que vous pouvez ensuite adapter à vos besoins. Pour des informations détaillées sur ces fichiers, reportez-vous à la section "Fichiers modèles de liaison PPP commutée " à la page 449.

▼ Définition des communications sur la ligne série

1 Connectez-vous en tant que superutilisateur (ou équivalent) à la machine d'appel sortant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Créez un fichier appelé `/etc/ppp/options` avec l'entrée suivante :

```
lock
```

Le fichier `/etc/ppp/options` permet de définir les paramètres généraux qui s'appliquent à toutes les communications sur la machine locale. L'option `lock` permet le verrouillage de type UUCP de la forme `/var/spool/locks/LC.xxx.yyy.zzz` .

Remarque – Si la machine d'appel sortant ne dispose pas d'un fichier `/etc/ppp/options`, seul le superutilisateur peut exécuter la commande `pppd`. Toutefois, le fichier `/etc/ppp/options` peut être vide.

Pour une description complète de `/etc/ppp/options`, reportez-vous à "Fichier de configuration `/etc/ppp/options`" à la page 518.

3 **(Facultatif) Créez un fichier appelé `/etc/ppp/options.`*ttyname* pour définir la manière dont les communications doivent être lancées à partir d'un port série spécifique.**

L'exemple suivant illustre un fichier `/etc/ppp/options.` *ttyname* pour le port dont le nom de périphérique est `/dev/cua/un` .

```
# cat /etc/ppp/options.cua.a
crtscts
```

L'option PPP `crtscts` indique au démon `pppd` d'activer le contrôle de flux matériel du port série a.

Pour plus d'informations sur le fichier `/etc/ppp/options.ttyname`, reportez-vous à la section "Fichier de configuration `/etc/ppp/options.` *ttyname*" à la page 519.

4 **Définissez la vitesse du modem, comme décrit à la section "Définition de la vitesse du modem " à la page 457.**

▼ Création des instructions pour l'appel d'un pair

Avant que la machine d'appel sortant puisse initialiser une liaison PPP, vous devez rassembler les informations concernant le serveur d'appel entrant qui doit devenir le pair. Elles vous permettent de créer le script de discussion, qui décrit la conversation réelle entre la machine d'appel sortant et le pair.

1 **Déterminez la vitesse à laquelle le modem de la machine d'appel sortant doit s'exécuter.**

Pour plus d'informations, reportez-vous à la section "Configuration de la vitesse du modem pour une liaison commutée " à la page 525.

2 **Recherchez les informations suivantes sur le site du serveur d'appel entrant :**

- Numéro de téléphone du serveur ;
- Protocole d'authentification utilisé, le cas échéant ;
- Séquence de connexion requise par le pair pour le script de discussion.

3 **Recherchez les nom et adresse IP des serveurs de noms sur le site du serveur d'appel entrant.**

4 **Dans un script de discussion, fournissez les instructions permettant d'initialiser des appels vers un pair donné.**

Par exemple, vous pouvez être amené à créer le script de discussion suivant, `/etc/ppp/mychat`, pour appeler le serveur d'appel entrant `myserver`.

```
SAY "Calling the peer\n"
        TIMEOUT 10
        ABORT BUSY
        ABORT 'NO CARRIER'
        ABORT ERROR
        REPORT CONNECT
        "" AT&F1&M5S2=255
        TIMEOUT 60
        OK ATDT1-123-555-1234
        CONNECT \c
        SAY "Connected; logging in.\n"
        TIMEOUT 5
        ogin:--ogin: pppuser
        TIMEOUT 20
        ABORT 'ogin incorrect'
        ssword: \qmypassword
        "% " \c
        SAY "Logged in.  Starting PPP on peer system.\n"
        ABORT 'not found'
        "" "exec pppd"
        ~ \c
```

Le script contient des instructions pour appeler un serveur d'appel entrant Solaris nécessitant une séquence de connexion. Vous trouverez la description de chaque instruction à la section "Script de discussion de base amélioré pour une connexion de type UNIX " à la page 530. Pour plus de détails sur la création d'un script de discussion, reportez-vous à la section "Définition de la conversation sur la liaison commutée " à la page 526.

Remarque – Vous n'appelez pas le script de discussion directement. Vous utilisez plutôt le nom de fichier du script de discussion en tant qu'argument de la commande `chat`, qui appelle le script.

Si un pair exécute Solaris ou un système d'exploitation similaire, envisagez d'utiliser le script de discussion précédent comme modèle pour les machines d'appel sortant.

▼ Définition de la connexion à un pair donné

1 **Connectez-vous en tant que superutilisateur (ou équivalent) à la machine d'appel sortant.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Mettez à jour les bases de données DNS en créant le fichier `/etc/resolv.conf` suivant :

```
domain bigcompany.com
nameserver 10.10.111.15
nameserver 10.10.130.8
```

`domain bigcompany.com`
Indique que le domaine DNS du pair est `bigcompany.com`.

`nameserver 10.10.111.15` et **`nameserver 10.10.130.8`**
Dresse la liste des adresses IP des serveurs de noms dans `bigcompany.com` .

3 Modifiez le fichier `/etc/nsswitch.conf` pour que la recherche de la base de données DNS porte d'abord sur les informations hôtes.

```
hosts:      dns [NOTFOUND=return] files
```

4 Créez un fichier pour le pair.

Par exemple, vous devez créer le fichier suivant pour définir le serveur d'appel entrant `myserver` :

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
noauth
connect "chat -U ’mypassword’ -T 1-123-555-1213 -f /etc/ppp/mychat"
```

/dev/cua/a
Spécifie que le périphérique `/dev/cua/`un doit être utilisé en tant qu'interface série des appels vers `myserver`.

57600
Définit la vitesse de la liaison.

noipdefault
Spécifie que pour les transactions avec le pair `myserver` , la machine d'appel sortant possède au départ l'adresse IP 0.0.0.0. `myserver` affecte une adresse IP à la machine d'appel sortant pour chaque session commutée.

idle 120
Indique que la liaison doit expirer après une période d'inactivité de 120 secondes.

noauth
Spécifie qu'il n'est pas nécessaire que le pair `myserver` fournisse des informations d'authentification lorsqu'il négocie la connexion avec la machine d'appel sortant.

connect "chat -U 'mypassword' -T 1-123-555-1213 -f /etc/ppp/mychat"
Spécifie l'option `connect` et ses arguments, y compris le numéro de téléphone du pair, et le script de discussion `/etc/ppp/mychat` avec les instructions d'appel.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour configurer une autre machine d'appel sortant, reportez-vous à la section “Configuration du modem et du port série (machine d'appel sortant)” à la page 450.
- Pour tester la connectivité modem par appel sortant vers une autre machine, reportez-vous aux pages de manuel `cu(1C)` et `tip(1)`. Ces utilitaires peuvent vous aider à vérifier que votre modem est configuré correctement. Ils vous permettent également de vérifier que vous pouvez établir une connexion à une autre machine.
- Pour en savoir plus sur les fichiers de configuration et les options, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 513.
- Pour configurer un serveur d'appel entrant, reportez-vous à la section “Configuration des périphériques sur le serveur d'appel entrant ” à la page 456.

Configuration du serveur d'appel entrant

Les tâches décrites dans cette section permettent de configurer le serveur d'appel entrant. Le serveur d'appel entrant est un pair qui reçoit l'appel de la machine d'appel sortant via la liaison PPP. Ces tâches indiquent comment configurer le serveur d'appel entrant `myserver` présenté à la Figure 16–1.

Tâches de configuration du serveur d'appel entrant (liste des tâches)

TABLEAU 17–3 Liste des tâches de la configuration du serveur d'appel entrant

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison : noms d'hôte des pairs, numéros de téléphone cible et vitesse des modems.	“Planification d'une liaison PPP commutée” à la page 430
2. Configuration du modem et du port série	Configurez le modem et le port série.	“Configuration du modem et du port série (serveur d'appel entrant)” à la page 456
3. Configuration des informations d'appel du pair	Configurez les environnements utilisateur et les options PPP pour toutes les machines d'appel sortant autorisées à appeler le serveur d'appel entrant.	“Configuration des utilisateurs du serveur d'appel entrant ” à la page 458
4. Configuration de la communication en ligne série	Configurez les caractéristiques de la transmission via la ligne série.	“Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 459

Configuration des périphériques sur le serveur d'appel entrant

La procédure suivante explique comment configurer le modem et le port série sur le serveur d'appel entrant.

Avant d'effectuer la procédure suivante, vous devez effectuer les activités suivantes sur le serveur d'appel entrant pair :

- Installation de la version Solaris
- Identification de la vitesse optimale du modem
- Choix du port série à utiliser

▼ Configuration du modem et du port série (serveur d'appel entrant)

1. **Programmez le modem, comme indiqué dans la documentation du fabricant.**

   Pour d'autres suggestions, reportez-vous à la section "Configuration du modem et du port série (machine d'appel sortant)" à la page 450.

2. **Branchez le modem au port série sur le serveur d'appel entrant.**

3. **Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

4. **Configurez le port série à l'aide de la commande `/usr/smap/bin/smc` pour la console de gestion Solaris, comme décrit à la section "Configuration des terminaux et modems avec l'outil Ports série (présentation)" du *Guide d'administration système : Administration avancée*.**

   Utilisez la console de gestion Solaris pour effectuer les opérations suivantes :

   a. **Sélectionnez le port série auquel le modem est connecté.**

   b. **Définissez la direction du modem pour les appels entrants uniquement.**

      Remarque – Solaris 4.0 prend effectivement en charge les communications bidirectionnelles du modem.

   c. **Cliquez sur OK pour que vos modifications entrent en vigueur.**

▼ Définition de la vitesse du modem

La procédure suivante explique comment définir la vitesse du modem pour un serveur d'appel entrant. La section “Configuration de la vitesse du modem pour une liaison commutée ” à la page 525 contient des suggestions à propos des vitesses à utiliser avec les ordinateurs Sun Microsystems.

1. **Connectez-vous au serveur d'appel entrant.**
2. **Utilisez la commande `tip` pour atteindre le modem.**

   Vous trouverez des instructions d'utilisation de la commande `tip` pour définir la vitesse du modem à la page de manuel `tip` (1).
3. **Configurez le modem pour une vitesse DTE fixe.**
4. **Verrouillez le port série pour cette vitesse à l'aide de `ttymon` ou `/usr/smap/bin/smc`, comme indiqué à la section “Configuration des terminaux et modems avec l'outil Ports série (présentation)” du *Guide d'administration système : Administration avancée*.**

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Configuration du modem et du port série (serveur d'appel entrant)” à la page 456
- “Configuration des utilisateurs du serveur d'appel entrant ” à la page 458

Configuration des utilisateurs du serveur d'appel entrant

Le processus de configuration d'un serveur d'appel entrant consiste en partie à configurer des informations sur chaque appelant distant connu.

Avant de commencer les procédures décrites dans cette section, vous devez effectuer les opérations suivantes :

- Obtention des noms d'utilisateur UNIX pour tous les utilisateurs qui sont autorisés à se connecter à partir de machines distantes d'appel sortant
- Configuration du modem et de la ligne série, comme décrit dans la section “Configuration du modem et du port série (serveur d'appel entrant)” à la page 456.
- Définition d'une adresse IP dédiée à affecter aux appels entrants provenant d'utilisateurs distants. Envisagez de créer une adresse IP entrante dédiée si le nombre d'appelants potentiels dépasse le nombre de modems et de ports série sur le serveur d'appel entrant. Pour obtenir des informations complètes sur la création d'adresses IP dédiées, reportez-vous à la section “Création d'un schéma d'adressage IP pour appelants ” à la page 542.

▼ Configuration des utilisateurs du serveur d'appel entrant

1 Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Créez un compte sur le serveur d'appel entrant pour chaque utilisateur PPP distant.

Vous pouvez utiliser la console de gestion Solaris pour créer un utilisateur. La commande `/usr/smap/bin/smc` ouvre la console de gestion Solaris. Pour obtenir des instructions sur la création d'un utilisateur à l'aide de la console de gestion Solaris, reportez-vous à la section "Configuration des comptes utilisateur (liste des tâches) " du *Guide d'administration système : administration de base*.

3 Utilisez la console de gestion Solaris pour affecter des paramètres au nouvel utilisateur.

Par exemple, le tableau suivant indique les paramètres du compte appelé `pppuser` de l'utilisateur `user1` sur la machine d'appel sortant `myhome`.

Paramètre	Valeur	Définition
User Name (Nom d'utilisateur)	`pppuser`	Nom du compte utilisateur de l'utilisateur distant. Ce nom de compte doit correspondre à celui donné dans la séquence de connexion du script de discussion. Par exemple, `pppuser` est le nom de compte trouvé dans le script de discussion à la section "Création des instructions pour l'appel d'un pair" à la page 452.
Login Shell (Shell de connexion)	`/usr/bin/pppd`	Shell de connexion par défaut de l'utilisateur distant. Le shell de connexion `/usr/bin/pppd` restreint au départ l'appelant à un environnement PPP dédié.
Create Home Dir Path (Créer le chemin d'accès au répertoire personnel)	`/export/home/pppuser`	Le répertoire personnel `/export/Home/pppuser` est défini lorsque l'appelant se connecte au serveur d'appel entrant.

4 Pour chaque appelant, créez un fichier `$HOME/.pprc` qui contient diverses options spécifiques à la session PPP de l'utilisateur.

Par exemple, vous pouvez créer le fichier `.ppprc` suivant pour `pppuser`.

```
# cat /export/home/pppuser/.ppprc
noccp
```

L'option `noccp` désactive le contrôle de compression sur la liaison.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- “Configuration des utilisateurs du serveur d'appel entrant ” à la page 458.
- “Définition des communications sur la ligne série (serveur d'appel entrant) ” à la page 459.

Configuration de la communication sur le serveur d'appel entrant

La tâche suivante indique comment activer le serveur d'appel entrant pour ouvrir les communications avec toutes les machines d'appel sortant. Les options définies dans les fichiers de configuration PPP suivants déterminent la manière dont les communications sont établies.

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*

Pour obtenir des informations détaillées sur ces fichiers, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 513.

Avant de continuer, vous devez effectuer les opérations suivantes :

- Configuration du port série et du modem sur le serveur d'appel entrant, comme décrit à la section “Configuration du modem et du port série (serveur d'appel entrant)” à la page 456
- Configuration des informations sur les utilisateurs potentiels du serveur d'appel entrant, comme décrit à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 458

▼ Définition des communications sur la ligne série (serveur d'appel entrant)

1 Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2 Créez le fichier `/etc/ppp/options` avec l'entrée suivante.

```
nodefaultroute
```

`nodefaultroute` indique qu'aucune session `pppd` sur le système local peut établir une route par défaut sans privilèges `root`.

Remarque – Si le serveur d'appel entrant ne dispose pas d'un fichier `/etc/ppp/options`, seul le superutilisateur peut exécuter la commande `pppd`. Toutefois, le fichier `/etc/ppp/options` peut être vide.

3 Créez le fichier `/etc/options.` *ttyname* pour définir la façon dont les appels reçus via le port série *ttyname* doivent être traités.

Le fichier `/etc/options.ttya` suivant définit la façon dont le port série `/dev/ttya` du serveur d'appel entrant doit traiter les appels entrants.

```
:10.0.0.80
xonxoff
```

`:10.0.0.80` Affecte l'adresse IP 10.0.0.80 à tous les pairs qui appellent via le port série `ttya`.

`xonxoff` Autorise la ligne série à traiter les communications en provenance des modems avec le contrôle de flux logiciel activé.

Voir aussi Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison commutée. La liste ci-après fournit les références à des informations connexes.

- Pour tester la connectivité modem par appel sortant vers une autre machine, reportez-vous aux pages de manuel `cu(1C)` et `tip(1)`. Ces utilitaires peuvent vous aider à vérifier que votre modem est configuré correctement. Ils vous permettent également de vérifier que vous pouvez établir une connexion à une autre machine.
- Pour configurer des options supplémentaires pour le serveur d'appel entrant, reportez-vous à la section “Configuration du serveur d'appel entrant” à la page 455.
- Pour configurer plusieurs machines d'appel sortant, reportez-vous à la section “Configuration de la machine d'appel sortant” à la page 448.
- Pour que l'ordinateur distant appelle le serveur d'appel entrant, reportez-vous à la section “Appel du serveur d'appel entrant ” à la page 460.

Appel du serveur d'appel entrant

Pour établir une liaison PPP commutée, il suffit que la machine d'appel sortant appelle le serveur d'appel entrant. Vous pouvez demander à la machine d'appel sortant d'appeler le serveur en spécifiant l'option `demand` dans les fichiers de configuration PPP locaux. Cependant, la méthode la plus courante pour établir la liaison est que l'utilisateur exécute la commande `pppd` sur la machine d'appel sortant.

Avant de passer à la tâche suivante, vous devez effectuer l'une des opérations suivantes ou les deux :

- Configuration de la machine d'appel sortant, comme décrit à la section "Configuration de la machine d'appel sortant" à la page 448
- Configuration du serveur d'appel entrant, comme décrit à la section "Configuration du serveur d'appel entrant" à la page 455

▼ Appel du serveur d'appel entrant

1 Connectez-vous à la machine d'appel sortant à l'aide de votre compte utilisateur standard, pas `root`.

2 Appelez le serveur d'appel entrant en exécutant la commande `pppd`.

Par exemple, la commande suivante établit une liaison entre la machine d'appel sortant et le serveur d'appel entrant `myserver` :

```
% pppd 57600 call myserver
```

`pppd`	Démarre l'appel en appelant le démon `pppd`
`57600`	Définit la vitesse de la ligne entre l'hôte et le modem
`call myserver`	Appelle l'option `call` de la commande `pppd`. `pppd` puis lit les options dans le fichier `/etc/ppp/peers/myserver`, créé à la section "Définition de la connexion à un pair donné" à la page 453

3 Contactez un hôte sur le réseau du serveur, par exemple, l'hôte `lindyhop` illustré à la Figure 16–1 :

```
ping lindyhop
```

Si la liaison ne fonctionne pas correctement, reportez-vous au Chapitre 21, "Résolution des problèmes PPP courants (tâches) ".

4 Mettez fin à la session PPP :

```
% pkill -x pppd
```

Voir aussi Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison commutée. La liste ci-après fournit les références à des informations connexes.

- Pour que tous les utilisateurs commencent à travailler sur leur machine d'appel sortant, reportez-vous à la section "Appel du serveur d'appel entrant" à la page 461.
- Pour résoudre les problèmes de liaison, reportez-vous au Chapitre 21, "Résolution des problèmes PPP courants (tâches) ".

- Pour en savoir plus sur les fichiers et les options utilisés dans ce chapitre, reportez-vous à la section “Utilisation des options PPP dans les fichiers et sur la ligne de commande ” à la page 513.

◆ ◆ ◆ CHAPITRE 18

Configuration d'une liaison PPP de ligne spécialisée (tâches)

Ce chapitre explique comment configurer une liaison PPP entre pairs par le biais d'une ligne spécialisée. Les sections principales sont les suivantes :

Configuration d'une ligne spécialisée (liste des tâches)

Les liaisons de lignes spécialisées sont relativement faciles à configurer par rapport aux liaisons commutées. Dans la plupart des cas, il n'est pas nécessaire de configurer la CSU/DSU, les services ni l'authentification. Si vous devez configurer la CSU/DSU, reportez-vous à la documentation fournie par le fabricant pour obtenir de l'aide sur cette tâche complexe.

La liste des tâches répertoriées dans le tableau suivant décrit toutes les tâches que comporte la configuration d'une liaison de base par le biais d'une ligne spécialisée.

Remarque – Certains types de lignes spécialisées requièrent que la CSU/DSU “appelle” l'adresse du pair opposé. Par exemple, Frame Relay utilise le service SVC (Switched Virtual Circuits, circuits virtuels commutés) ou Switched 56.

TABLEAU 18–1 Liste des tâches de la configuration de la liaison de ligne spécialisée

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les données qui sont nécessaires avant de procéder à la configuration de la liaison.	Tableau 16–4
2. Configuration du matériel de la ligne spécialisée	Assemblez la CSU/DSU et la carte d'interface synchrone.	“Configuration de périphériques synchrones ” à la page 464

TABLEAU 18–1 Liste des tâches de la configuration de la liaison de ligne spécialisée *(Suite)*

Tâche	Description	Voir
3. Configuration de la carte d'interface, si nécessaire	Configurez le script d'interface à utiliser à l'initialisation de la ligne spécialisée.	"Configuration de périphériques synchrones " à la page 464
4. Configuration des informations relatives au pair distant	Définissez le mode de fonctionnement des communications entre la machine locale et le pair distant.	"Configuration d'une machine sur une ligne spécialisée " à la page 466
5. Initialisation de la ligne spécialisée	Configurez votre machine pour que la liaison PPP démarre sur la ligne spécialisée dans le cadre du processus d'initialisation.	"Configuration d'une machine sur une ligne spécialisée " à la page 466

Configuration des périphériques synchrones sur la ligne spécialisée

La tâche décrite dans cette section consiste à configurer l'équipement requis par la topologie de ligne spécialisée présentée à la section "Exemple de configuration d'une liaison de ligne spécialisée" à la page 435. Les périphériques synchrones qui doivent se connecter à la ligne spécialisée incluent l'interface et le modem.

Prérequis à la configuration des périphériques synchrones

Avant d'effectuer la procédure suivante, vous devez disposer des éléments suivants :

- Ligne spécialisée en fonctionnement, installée sur votre site par le fournisseur
- Unité synchrone (CSU/DSU)
- Version de Solaris installée sur votre système
- Carte d'interface synchrone du type requis par votre système

▼ Configuration de périphériques synchrones

1 **Installez physiquement la carte d'interface dans la machine locale, si nécessaire.**

Suivez les instructions décrites dans la documentation du fabricant.

2 **Connectez les câbles reliant la CSU/DSU à l'interface.**

Au besoin, branchez les câbles de la CSU/DSU au connecteur de la ligne spécialisée ou à un connecteur similaire.

3 **Configurez la CSU/DSU, comme indiqué dans la documentation fournie par le fabricant ou fournisseur réseau.**

Remarque – Le fournisseur auquel vous avez loué la ligne spécialisée peut fournir et configurer la CSU/DSU pour votre liaison.

---

4 **Configurez la carte d'interface, si nécessaire, comme indiqué dans la documentation de l'interface.**

La configuration de la carte d'interface implique la création d'un script de démarrage pour l'interface. Le routeur de LocalCorp dans la configuration de la ligne spécialisée, illustrée à la Figure 16–2, utilise une carte d'interface HSI/P.

Le script suivant, `hsi conf-`, lance l'interface HSI/P.

```
#!/bin/ksh
/opt/SUNWconn/bin/hsip_init hihp1 speed=1536000 mode=fdx loopback=no \
nrzi=no txc=txc rxc=rxc txd=txd rxd=rxd signal=no 2>&1 > /dev/null
```

`hihp1`	Indique que HSI/P est le port synchrone utilisé
`speed=1536000`	Indique la vitesse de la CSU/DSU

Voir aussi Pour configurer la machine locale sur la ligne spécialisée, reportez-vous à la section "Configuration d'une machine sur une ligne spécialisée " à la page 466.

Configuration d'une machine sur la ligne spécialisée

La procédure décrite dans cette section explique comment configurer un routeur en tant que pair local situé à votre extrémité de la ligne spécialisée. La tâche utilise la ligne spécialisée présentée à la section "Exemple de configuration d'une liaison de ligne spécialisée" à la page 435.

Prérequis à la configuration de la machine locale sur une ligne spécialisée

Avant d'effectuer la procédure ci-dessous, vous devez réaliser les opérations suivantes :

- Définition et configuration des périphériques synchrones de la liaison, comme décrit à la section "Configuration des périphériques synchrones sur la ligne spécialisée" à la page 464
- Obtention du mot de passe root de la machine locale sur la ligne spécialisée
- Configuration de la machine locale en tant que routeur sur le ou les réseaux afin d'utiliser les services du fournisseur de la ligne spécialisée

▼ Configuration d'une machine sur une ligne spécialisée

1 **Connectez-vous en tant que superutilisateur (ou équivalent) à la machine locale (routeur).**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez une entrée pour le pair distant dans le fichier `/etc/hosts` du routeur.**

```
# cat /etc/hosts
#
# Internet host table
#
127.0.0.1       localhost
192.168.130.10  local2-peer        loghost
192.168.130.11  local1-net
10.0.0.25       farISP
```

L'exemple de fichier `/etc/hosts` est pour le routeur local de la société fictive LocalCorp. Notez l'adresse IP et le nom d'hôte pour le pair distant `farISP` du fournisseur de service.

3 **Créez le fichier `/etc/ppp/peers/`*peer-name* pour stocker les informations relatives au pair du fournisseur.**

Pour cet exemple de liaison de ligne spécialisée, créez le fichier `/etc/ppp/peers/farISP`.

```
# cat /etc/ppp/peers/farISP
init '/etc/ppp/conf_hsi'
local
/dev/hihp1
sync
noauth
192.168.130.10:10.0.0.25
passive
persist
noccp
nopcomp
novj
noaccomp
```

Le tableau suivant décrit les options et les paramètres utilisés dans le fichier `/etc/ppp/peers/farISP`.

Option	Définition
`init '/etc/ppp/conf_hsi'`	Initialise la liaison. `init` configure ensuite les interfaces HSI à l'aide des paramètres du script `/etc/ppp/conf_hsi` .
`local`	Indique au démon `pppd` de ne pas modifier l'état du signal DTR (Data Terminal Ready). Indique également à `pppd` d'ignorer le signal d'entrée DCD (Data Carrier Detect).

Option	Définition
`/dev/hihp1`	Donne le nom de périphérique de l'interface synchrone.
`sync`	Établit le codage synchrone de la liaison.
`noauth`	Établit que le système local n'a pas besoin d'exiger du pair qu'il s'authentifie. Cependant, le pair peut toujours exiger l'authentification.
`192.168.130.10:10.0.0.25`	Définit les adresses IP du pair local et du pair distant, séparées par un signe deux-points.
`passive`	Indique au démon `pppd` résidant sur la machine locale de s'interrompre et d'attendre le démarrage du pair, après avoir établi le nombre maximal de demandes de configuration LCP.
`persist`	Indique au démon `pppd` d'essayer de réinitier la liaison après l'arrêt d'une connexion.
`noccp, nopcomp, novj, noaccomp`	Désactive CCP (Compression Control Protocol), la compression du champ protocole, la compression Van Jacobson et la compression de champ adresse et contrôle, respectivement. Ces formes de compression accélèrent les transmissions sur une liaison commutée mais peuvent ralentir une ligne spécialisée.

4 Créez un script d'initialisation appelé `demand`, qui crée la liaison PPP dans le cadre du processus de démarrage.

```
# cat /etc/ppp/demand
#!/bin/sh
if [ -f /var/run/ppp-demand.pid ] &&
   /usr/bin/kill -s 0 ‘/bin/cat /var/run/ppp-demand.pid‘
then
        :
else
        /usr/bin/pppd call farISP
fi
```

Le script `demand` contient la commande `pppd` permettant d'établir une liaison de ligne spécialisée. Le tableau suivant décrit le contenu de `$PPPDIR/demand`.

Exemple de code	Explication
`if [ -f /var/run/ppp-demand.pid ] && /usr/bin/kill -s 0 ‘/bin/cat /var/run/ppp-demand.pid‘`	Ces lignes vérifient l'exécution de la commande `pppd`. Si `pppd` est en cours d'exécution, il n'est pas nécessaire de la démarrer.
`/usr/bin/pppd call farISP`	Cette ligne lance `pppd`. `pppd` lit les options de `/etc/ppp/options`. L'option `call farISP` sur la ligne de commande entraîne la lecture de `/etc/ppp/peers/farISP` , également.

Le script de démarrage Solaris PPP 4.0 `/etc/rc2.d/S47pppd` appelle le script `demand` dans le cadre du processus d'initialisation. Les lignes suivantes dans `/etc/rc2.dS47pppd` recherchent la présence d'un fichier appelé `$PPPDIR/demand`.

```
if [ -f $PPPDIR/demand ]; then
            . $PPPDIR/demand
    fi
```

S'il est trouvé, `$PPPDIR/demand` est exécuté. Au cours de l'exécution de `$PPPDIR/demand`, la liaison est établie.

Remarque – Pour atteindre les machines résidant en dehors du réseau local, demandez aux utilisateurs d'exécuter `telnet`, `ftp`, `rsh` ou des commandes similaires.

Voir aussi Si vous avez suivi l'ensemble des procédures décrites dans ce chapitre, vous avez terminé la configuration de la liaison de ligne spécialisée. La liste ci-après fournit les références à des informations connexes.

- Pour obtenir des informations sur le dépannage, voir "Correction des problèmes des lignes spécialisées " à la page 510.
- Pour en savoir plus sur les fichiers et les options utilisés dans ce chapitre, voir "Utilisation des options PPP dans les fichiers et sur la ligne de commande " à la page 513.

◆ ◆ ◆ CHAPITRE 19

Paramétrage de l'authentification PPP (tâches)

Ce chapitre contient les tâches de la configuration de l'authentification PPP. Voici la liste des sujets abordés :

- “Configuration de l'authentification PAP” à la page 470
- “Configuration de l'authentification CHAP” à la page 478

Les procédures décrivent la mise en œuvre de l'authentification sur une liaison commutée, car les liaisons commutées sont plus susceptibles d'être configurées pour l'authentification que les lignes spécialisées. Vous pouvez configurer l'authentification sur des lignes spécialisées, si la stratégie de sécurité de votre entreprise l'exige. Pour mettre en œuvre l'authentification sur des lignes spécialisées, utilisez les tâches de ce chapitre comme directives.

Si vous souhaitez utiliser l'authentification PPP, mais que vous ne savez pas quel protocole utiliser, consultez la section “Raisons de l'utilisation de l'authentification PPP” à la page 425. Vous trouverez des informations plus détaillées sur l'authentification PPP dans la page de manuel `pppd(1M)` et à la section “Authentification des appelants sur une liaison” à la page 536.

Configuration de l'authentification PPP (liste des tâches)

Cette section contient la liste des tâches qui vous permettront d'accéder rapidement aux procédures de l'authentification PPP.

TABLEAU 19–1 Liste des tâches de l'authentification PPP générale

Tâche	Description	Voir
Configuration de l'authentification PAP	Utilisez ces procédures pour activer l'authentification PAP sur un serveur d'accès entrant et une machine d'appel sortant.	“Configuration de l'authentification PAP (liste des tâches) ” à la page 470

TABLEAU 19–1 Liste des tâches de l'authentification PPP générale *(Suite)*

Tâche	Description	Voir
Configuration de l'authentification CHAP	Utilisez ces procédures pour activer l'authentification CHAP sur un serveur d'accès entrant et une machine d'appel sortant.	"Configuration de l'authentification CHAP (liste des tâches) " à la page 478

Configuration de l'authentification PAP

Les tâches décrites dans cette section expliquent comment mettre en œuvre l'authentification sur une liaison PPP à l'aide du protocole PAP (Password Authentication Protocol, protocole d'authentification par mot de passe). Les tâches utilisent l'exemple de la section "Exemples de configuration d'authentification PPP " à la page 438 afin d'illustrer un scénario PAP qui fonctionne pour une liaison commutée. Utilisez les instructions comme base pour la mise en œuvre de l'authentification PAP sur votre site.

Avant de réaliser les procédures suivantes, vous devez effectuer les opérations ci-dessous :

- Définissez et testez la liaison commutée entre le serveur d'appel entrant et les machines d'appel sortant appartenant à des appelants de confiance.
- Dans l'idéal, pour l'authentification du serveur d'appel entrant, obtenez l'autorisation de superutilisateur pour la machine gérant la base de données de mots de passe réseau, par exemple, dans les fichiers locaux, LDAP ou NIS.
- Obtenez les droits de superutilisateur pour la machine locale, qu'il s'agisse du serveur d'appel entrant ou de la machine d'appel sortant.

Configuration de l'authentification PAP (liste des tâches)

Utilisez la liste des tâches suivante pour accéder rapidement aux tâches relatives à PAP pour le serveur d'appel entrant et les appelants de confiance sur les machines d'appel sortant.

TABLEAU 19–2 Liste des tâches de l'authentification PAP (serveur d'appel entrant)

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les noms d'utilisateur et autres données nécessaires à l'authentification.	"Planification de l'authentification sur une liaison" à la page 437
2. Mise à jour de la base de données de mots de passe, si nécessaire	Assurez-vous que tous les appelants figurent dans la base de données de mots de passe du serveur.	"Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) " à la page 471

TABLEAU 19–2 Liste des tâches de l'authentification PAP (serveur d'appel entrant) *(Suite)*

Tâche	Description	Voir
3. Création de la base de données PAP	Créez des informations d'identification de sécurité pour tous les appelants potentiels dans `/etc/ppp/pap-secrets` .	"Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) " à la page 471
4. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à PAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	"Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)" à la page 473

TABLEAU 19–3 Liste des tâches pour l'authentification PAP (machine d'appel sortant)

Tâche	Description	Voir
1. Collecte des informations de préconfiguration.	Rassemblez les noms d'utilisateur et autres données nécessaires à l'authentification.	"Planification de l'authentification sur une liaison" à la page 437
2. Création de la base de données PAP pour la machine de l'appelant de confiance	Créez les informations d'identification de sécurité pour l'appelant de confiance et, si nécessaire, pour les autres utilisateurs qui appellent la machine d'appel sortant, dans `/etc/ppp/pap-secrets`.	"Configuration des informations d'authentification PAP pour les appelants de confiance " à la page 475
3. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à PAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	"Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)" à la page 476

Configuration de l'authentification PAP sur le serveur d'appel entrant

Pour configurer l'authentification PAP, vous devez effectuer les opérations suivantes :

- Création d'une base de données d'informations d'identification PAP
- Modification des fichiers de configuration PPP pour la prise en charge PAP

▼ Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant)

Cette procédure modifie le fichier `/etc/ppp/pap-secrets`, qui contient les informations d'identification de sécurité PAP permettant d'authentifier les appelants sur la liaison. Le fichier `/etc/ppp/pap-secrets` doit exister sur les deux machines sur une liaison PPP.

L'exemple de configuration PAP présenté à la Figure 16–3 utilise l'option `login` de PAP. Si vous envisagez d'utiliser cette option, vous devrez peut-être mettre à jour la base de données de mots de passe de votre réseau. Pour plus d'informations sur l'option `login`, reportez-vous à la section "Utilisation de l'option `login` avec `/etc/ppp/pap-secrets`" à la page 539.

1. **Dressez la liste des éventuels appelants de confiance. Les appelants de confiance sont des utilisateurs auxquels vous accordez l'autorisation d'appeler le serveur d'appel entrant à partir de leur machine distante.**

2. **Vérifiez que chaque appelant de confiance possède déjà un nom d'utilisateur et un mot de passe UNIX dans la base de données des mots de passe du serveur d'appel entrant.**

   Remarque – La vérification est particulièrement importante pour l'exemple de configuration PAP, qui utilise l'option `login` de PAP pour authentifier les appelants. Si vous choisissez de ne pas appliquer l'option `login` pour PAP, les noms d'utilisateur PAP des appelants ne doivent pas forcément correspondre à leurs noms d'utilisateur UNIX. Pour plus d'informations sur le fichier `/etc/ppp/pap-secrets` standard, reportez-vous à "Fichier `/etc/ppp/pap-secrets`" à la page 536.

   Effectuez les opérations suivantes si un appelant de confiance potentiel ne possède pas un mot de passe et un nom d'utilisateur UNIX.

   a. **Confirmez avec leurs responsables que les appelants que vous ne connaissez pas personnellement sont autorisés à accéder au serveur d'appel entrant.**

   b. **Créez des noms d'utilisateur et mots de passe UNIX pour ces appelants, en conformité avec la stratégie de sécurité de votre entreprise.**

3. **Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

4. **Modifiez le fichier `/etc/ppp/pap-secrets`.**

   Cette version fournit un fichier `pap-secrets` dans `/etc/ppp` qui contient des commentaires relatifs à l'utilisation de l'authentification PAP mais pas d'options. Vous pouvez ajouter les options suivantes à la fin des commentaires.

   ```
   user1      myserver        ""          *
   user2      myserver        ""          *
   myserver   user2           serverpass  *
   ```

   Pour utiliser l'option `login` de `/etc/ppp/pap-secrets`, vous devez taper le nom d'utilisateur UNIX de chaque appelant de confiance. Lorsqu'un jeu de guillemets doubles (“”) s'affiche dans le troisième champ, le mot de passe pour l'appelant est recherché dans la base de données des mots de passe du serveur.

   L'entrée `myserver * serverpass *` contient le nom d'utilisateur et le mot de passe PAP pour le serveur d'appel entrant. Dans la Figure 16–3, l'appelant de confiance `user2` requiert l'authentification de pairs distants. Par conséquent, le fichier de `myserver`, `/etc/ppp/pap-secrets`, contient les informations d'identification PAP à utiliser lorsqu'une liaison est établie avec `user2`.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- "Modification des fichiers de configuration PPP pour PAP (serveur d'appel entrant)" à la page 473
- "Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)" à la page 474

Modification des fichiers de configuration PPP pour PAP (serveur d'appel entrant)

Les tâches décrites dans cette section expliquent comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification PAP sur le serveur d'appel entrant.

▼ Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)

La procédure utilise comme exemples les fichiers de configuration PPP présentés à la section "Définition des communications sur la ligne série (serveur d'appel entrant) " à la page 459.

1 Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez des options d'authentification dans le fichier `/etc/ppp/options`.

Par exemple, ajoutez les options en gras dans un fichier `/etc/ppp/options` pour mettre en œuvre l'authentification PAP :

```
lock
auth
login
nodefaultroute
proxyarp
ms-dns 10.0.0.1
idle 120
```

`auth`	Spécifie que le serveur doit authentifier les appelants avant d'établir la liaison.
`login`	Spécifie que l'appelant distant doit être authentifié à l'aide des services d'authentification d'utilisateur UNIX standard.
`nodefaultroute`	Indique qu'aucune session `pppd` sur le système local ne peut établir une route par défaut sans privilèges `root`.

`proxyarp`	Ajoute une entrée dans la table ARP (Address Resolution Protocol, protocole de résolution d'adresse) du système, qui indique l'adresse IP du pair et l'adresse Ethernet du système. Avec cette option, le pair semble se trouver sur le réseau Ethernet local aux autres systèmes.
`ms-dns 10.0.0.1`	Active `pppd` pour fournir l'adresse DNS (Domain Name Server) `10.0.0.1` au client
`idle 120`	Spécifie que les utilisateurs inactifs sont déconnectés après deux minutes.

3 **Dans le fichier `/etc/ppp/options.cua.a`, ajoutez l'adresse suivante pour l'utilisateur `cua/a`.**

```
:10.0.0.2
```

4 **Dans le fichier `/etc/ppp/options.cua.b`, ajoutez l'adresse suivante pour l'utilisateur `cua/b`.**

```
:10.0.0.3
```

5 **Dans le fichier `/etc/ppp/pap-secrets`, ajoutez l'entrée suivante.**

```
*     *          ""      *
```

Remarque – L'option `login`, comme décrit précédemment, fournit l'authentification utilisateur nécessaire. Cette entrée dans le fichier `/etc/ppp/pap-secrets` constitue la méthode normale d'activer PAP avec l'option `login`.

Voir aussi Pour configurer les informations d'authentification PAP des appelants de confiance du serveur d'appel entrant, reportez-vous à la section "Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)" à la page 474.

Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)

Cette section présente les tâches de configuration de l'authentification PAP sur les machines d'appel sortant des appelants de confiance. En tant qu'administrateur système, vous pouvez configurer l'authentification PAP sur les systèmes avant leur distribution aux appelants potentiels. Vous pouvez également affecter les tâches de cette section aux appelants distants, s'ils disposent déjà de leur machine.

La configuration PAP pour les appelants de confiance implique deux tâches :

- Configuration des informations d'identification de sécurité PAP des appelants
- Configuration des machines d'appel sortant des appelants pour prendre en charge l'authentification PAP

▼ Configuration des informations d'authentification PAP pour les appelants de confiance

Cette procédure indique comment configurer les informations d'identification PAP pour deux appelants de confiance, dont l'un requiert les informations d'authentification des pairs distants. Elle implique que vous, l'administrateur système, créez les informations d'identification PAP sur les machines d'appel sortant des appelants de confiance.

1 Connectez-vous en tant que superutilisateur (ou équivalent) à une machine d'appel sortant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

Utilisez l'exemple de configuration PAP présenté à la Figure 16–3 et partez du principe que la machine d'appel sortant appartient à l'utilisateur `user1`.

2 Modifiez la base de données des secrets PAP pour l'appelant.

Cette version fournit un fichier `/etc/ppp/pap-secrets` qui contient des commentaires utiles mais aucune option. Vous pouvez ajouter les options suivantes à ce fichier `/etc/ppp/pap-secrets`.

```
user1    myserver  pass1    *
```

Notez que le mot de passe `pass1` de l'utilisateur `user1` est transmis au format ASCII lisible par la liaison. `myserver` est le nom de l'appelant `user1` pour le pair.

3 Connectez-vous en tant que superutilisateur (ou équivalent) à une autre machine d'appel sortant.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

Utilisez l'exemple d'authentification PAP et supposez que cette machine d'appel sortant appartient à l'appelant `user2`.

4 Modifiez la base de données des secrets PAP pour l'appelant.

Vous pouvez ajouter les options suivantes à la fin du fichier `/etc/ppp/pap-secrets`.

```
user2     myserver   pass2       *
myserver  user2      serverpass  *
```

Dans cet exemple, `/etc/ppp/pap-secrets` comporte deux entrées. La première entrée contient les informations d'identification de sécurité PAP que `user2` transmet au serveur d'appel entrant `myserver` pour l'authentification.

`user2` exige les informations d'identification PAP du serveur d'appel entrant dans le cadre de la négociation de la liaison. Par conséquent, le fichier `/etc/ppp/pap-secrets` contient également les informations d'identification PAP attendues de `myserver` sur la deuxième ligne.

Remarque – Dans la mesure où la plupart des FAI ne fournissent pas d'informations d'authentification, le scénario précédent peut manquer de réalisme en ce qui concerne les communications avec un FAI.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- "Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) " à la page 471
- "Configuration des informations d'authentification PAP pour les appelants de confiance " à la page 475

Modification des fichiers de configuration PPP pour PAP (machine d'appel sortant)

Les tâches suivantes expliquent comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification PAP sur les machines d'appel sortant des appelants de confiance.

La procédure utilise les paramètres suivants pour configurer l'authentification PAP sur la machine d'appel sortant qui appartient à `user2`, présenté à la Figure 16–3. L'utilisateur `user2` exige des appelants entrants de s'authentifier, appels de `myserver` compris.

▼ Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)

Cette procédure utilise comme exemples les fichiers de configuration PPP présentés à la section "Définition des communications sur la ligne série " à la page 451. Elle permet de configurer la machine d'appel sortant qui appartient à `user2`, comme indiqué à la Figure 16–3.

1 Connectez-vous en tant que superutilisateur à la machine d'appel sortant.

2 Modifiez le fichier `/etc/ppp/options`.

Le fichier `/etc/ppp/options` suivant contient des options pour la prise en charge PAP, indiquées en gras.

```
# cat /etc/ppp/options
lock
```

```
name user2
auth
require-pap
```

name user2 — Définit `user2` comme nom PAP de l'utilisateur de la machine locale. Si l'option `login` est utilisée, le nom PAP doit être le même que celui de l'utilisateur UNIX dans la base de données de mots de passe.

auth — Indique que la machine d'appel sortant doit authentifier les appelants avant d'établir la liaison.

Remarque – Cette machine d'appel sortant exige l'authentification de ses pairs, bien que la plupart des machines d'appel sortant n'aient pas cette exigence. Les deux cas sont acceptables.

---

require-pap — Exige les informations d'identification PAP du pair.

3 Créez un fichier `/etc/ppp/peers/`*peer-name* pour la machine distante `myserver`.

L'exemple suivant indique comment ajouter la prise en charge PAP au fichier `/etc/ppp/peers/myserver` créé à la section "Définition de la connexion à un pair donné" à la page 453.

```
# cat /etc/ppp/peers/myserver
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user user2
remotename myserver
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

Les nouvelles options en gras ajoutent les exigences PAP pour le pair `myserver`.

user user2 — Définit `user2` comme le nom d'utilisateur de la machine locale.

remotename myserver — Définit `myserver` comme un pair qui requiert les informations d'authentification de la machine locale.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour tester la configuration de l'authentification PAP en appelant le serveur d'appel entrant, reportez-vous à la section "Appel du serveur d'appel entrant" à la page 461.
- Pour en savoir plus sur l'authentification PAP, reportez-vous à la section "Protocole d'authentification par mot de passe (PAP)" à la page 536.

Configuration de l'authentification CHAP

Les tâches décrites dans cette section expliquent comment mettre en œuvre l'authentification sur une liaison PPP à l'aide du protocole CHAP (Challenge-Handshake Authentication Protocol, protocole d'authentification par défi-réponse). Les tâches utilisent l'exemple de la Figure 16–4 afin d'illustrer un scénario CHAP qui fonctionne pour une liaison commutée sur un réseau privé. Utilisez les instructions comme base pour la mise en œuvre de l'authentification CHAP sur votre site.

Avant d'effectuer les procédures ci-dessous, vous devez réaliser les opérations suivantes :

- Définissez et testez la liaison commutée entre le serveur d'appel entrant et les machines d'appel sortant appartenant à des appelants de confiance.
- Obtenez les droits de superutilisateur pour la machine locale, qu'il s'agisse du serveur d'appel entrant ou de la machine d'appel sortant.

Configuration de l'authentification CHAP (liste des tâches)

TABLEAU 19–4 Liste des tâches de l'authentification CHAP (serveur d'appel entrant)

Tâche	Description	Voir
1. Affectation des secrets CHAP à tous les appelants de confiance	Créez les secrets CHAP des appelants ou demandez aux appelants qu'ils les créent.	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 479
2. Création de la base de données chap-secrets	Ajoutez les informations d'identification de sécurité pour tous les appelants de confiance dans le fichier `/etc/ppp/chap-secrets` .	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 479
3. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à CHAP dans les fichiers `/etc/ppp/options` et `/etc/ppp/peers/`*peer-name*.	“Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)” à la page 480

TABLEAU 19–5 Liste des tâches pour l'authentification CHAP (machine d'appel sortant)

Tâche	Description	Voir
1. Création de la base de données CHAP pour la machine de l'appelant de confiance	Créez les informations d'identification de sécurité pour l'appelant de confiance et, si nécessaire, pour les autres utilisateurs qui appellent la machine d'appel sortant, dans `/etc/ppp/chap-secrets`.	“Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)” à la page 479

TABLEAU 19–5 Liste des tâches pour l'authentification CHAP (machine d'appel sortant) *(Suite)*

Tâche	Description	Voir
2. Modification des fichiers de configuration PPP	Ajoutez des options spécifiques à CHAP dans le fichier `/etc/ppp/options`.	"Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)" à la page 483

Configuration de l'authentification CHAP sur le serveur d'appel entrant

La première tâche de la configuration de l'authentification CHAP consiste à modifier le fichier `/etc/ppp/chap-secrets`. Ce fichier contient le informations d'identification de sécurité CHAP utilisées pour authentifier les appelants sur la liaison.

Remarque – Les mécanismes d'authentification PAM ou UNIX ne fonctionnent pas avec CHAP. Par exemple, vous ne pouvez pas utiliser l'option `login` PPP comme décrit dans la section "Création d'une base de données d'informations d'identification PAP (serveur d'appel entrant) " à la page 471. Si votre scénario d'authentification nécessite l'authentification de type UNIX ou PAM, choisissez plutôt PAP.

La procédure suivante met en œuvre l'authentification CHAP pour un serveur d'appel entrant dans un réseau privé. La liaison PPP est la seule connexion au monde extérieur. Seuls les appelants autorisés par les gestionnaires du réseau (y compris l'administrateur système, éventuellement) peuvent accéder au réseau.

▼ Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)

1 Dressez la liste des noms d'utilisateur de tous les appelants de confiance.

Les appelants de confiance incluent tous les utilisateurs auxquels les droits d'appel sur le réseau privé ont été accordés.

2 Affectez un secret CHAP à chaque utilisateur.

Remarque – Assurez-vous de choisir un secret CHAP difficile à deviner. Aucune autre restriction n'est appliquée sur le contenu du secret CHAP.

La méthode d'attribution des secrets CHAP dépend de la stratégie de sécurité de votre site. Soit vous avez la responsabilité de créer les secrets, soit les appelants doivent créer leurs secrets eux-mêmes. Si vous n'êtes pas responsable de l'affectation des secrets CHAP, veillez à vous procurer les secrets CHAP qui ont été créés par, ou pour, chaque appelant de confiance.

3 **Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'appel entrant.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

4 **Modifiez le fichier `/etc/ppp/chap-secrets`.**

Cette version inclut un fichier `/etc/ppp/chap-secrets` qui contient des commentaires utiles, mais aucune option. Vous pouvez ajouter les options suivantes pour le serveur `CallServe` à la fin du fichier `/etc/ppp/chap-secrets`.

```
account1  CallServe   key123   *
account2  CallServe   key456   *
```

`key123` est le secret CHAP pour l'appelant de confiance `account1`.

`key456` est le secret CHAP pour l'appelant de confiance `account2`.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- "Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)" à la page 479
- "Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)" à la page 480
- "Configuration de l'authentification CHAP pour les appelants de confiance (machines d'appel sortant)" à la page 481

Modification des fichiers de configuration PPP pour CHAP (serveur d'appel entrant)

La tâche décrite dans cette section explique comment mettre à jour les fichiers de configuration PPP existants pour la prise en charge de l'authentification CHAP sur le serveur d'appel entrant.

▼ Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)

1 **Connectez-vous en tant que superutilisateur au serveur d'appel entrant.**

2 **Modifiez le fichier `/etc/ppp/options`.**

Ajoutez les options indiquées en caractères gras pour la prise en charge CHAP.

```
# cat /etc/ppp/options
lock
nodefaultroute
name CallServe
auth
```

`name` *CallServe*	Définit *CallServe* comme le nom CHAP de l'utilisateur de la machine locale, dans ce cas le serveur d'appel entrant.
`auth`	Demande à la machine locale d'authentifier les appelants avant d'établir la liaison.

3 **Créez les fichiers de configuration PPP restants pour la prise en charge des appelants de confiance.**

Reportez-vous aux sections "Configuration des utilisateurs du serveur d'appel entrant " à la page 458 et "Définition des communications sur la ligne série (serveur d'appel entrant) " à la page 459.

Voir aussi Pour configurer les informations d'authentification CHAP des appelants de confiance, reportez-vous à la section "Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)" à la page 479.

Configuration de l'authentification CHAP pour les appelants de confiance (machines d'appel sortant)

Cette section contient les tâches pour la configuration de l'authentification CHAP sur les machines d'appel sortant des appelants de confiance. En fonction de la stratégie de sécurité de votre site, vous ou les appelants de confiance pouvez être responsables de la configuration de l'authentification CHAP.

Pour que les appelants distants configurent l'authentification CHAP, assurez-vous que les secrets CHAP locaux des appelants correspondent aux secrets CHAP équivalents des appelants dans le fichier `/etc/ppp/chap-secrets` du serveur d'appel entrant. Ensuite, attribuez aux appelants les tâches de configuration CHAP décrites dans cette section.

La configuration CHAP pour les appelants de confiance implique deux tâches :

- Création des informations d'identification de sécurité CHAP des appelants
- Configuration des machines d'appel sortant des appelants pour prendre en charge l'authentification CHAP

▼ Configuration des informations d'authentification CHAP pour les appelants de confiance

Cette procédure indique comment configurer les informations d'identification CHAP de deux appelants de confiance. Elle implique que vous, l'administrateur système, créez les informations d'identification CHAP sur les machines d'appel sortant des appelants de confiance.

1. **Connectez-vous en tant que superutilisateur (ou équivalent) à une machine d'appel sortant.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

   Utilisez l'exemple de configuration CHAP présenté à la section "Exemple de configuration utilisant l'authentification CHAP" à la page 440 et partez du principe que la machine d'appel sortant appartient à l'appelant de confiance `account1`.

2. **Modifiez la base de données chap-secrets de l'appelant `account1`.**

   Cette version inclut un fichier `/etc/ppp/chap-secrets` qui contient des commentaires utiles mais aucune option. Vous pouvez ajouter les options suivantes au fichier `/etc/ppp/chap-secrets`.

   ```
   account1  CallServe   key123   *
   ```

   `CallServe` correspond au nom du pair que `account1` tente d'atteindre. `key123` est le secret CHAP à utiliser pour les liaisons entre `account1` et `CallServer`.

3. **Connectez-vous en tant que superutilisateur (ou équivalent) à une autre machine d'appel sortant.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

   Supposons que cette machine appartient à l'appelant `account2`.

4. **Modifiez la base de données `/etc/ppp/chap-secrets` pour l'appelant account2.**

   ```
   account2  CallServe   key456   *
   ```

   À présent, le secret `key456` correspond aux informations d'identification que l'appelant `account2` utilise pour communiquer avec le pair `CallServe` via la liaison.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- "Création d'une base de données d'informations d'identification CHAP (serveur d'appel entrant)" à la page 479
- "Configuration des informations d'authentification CHAP pour les appelants de confiance " à la page 481

Ajout de l'authentification CHAP dans les fichiers de configuration (machine d'appel sortant)

Pour en savoir plus sur l'authentification CHAP, reportez-vous à la section "Protocole CHAP (Challenge-Handshake Authentication Protocol)" à la page 539. La tâche suivante permet de configurer la machine d'appel sortant qui appartient à l'appelant `account1`, présenté à la section "Exemple de configuration utilisant l'authentification CHAP" à la page 440.

▼ Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)

1 **Connectez-vous en tant que superutilisateur à la machine d'appel sortant.**

2 **Assurez-vous que le fichier `/etc/ppp/options` possède les options suivantes.**

```
# cat /etc/ppp/options
lock
nodefaultroute
```

3 **Créez un fichier `/etc/ppp/peers/`** *peer-name* **pour la machine distante `CallServe`.**

```
# cat /etc/ppp/peers/CallServe
/dev/cua/a
57600
noipdefault
defaultroute
idle 120
user account1
connect "chat -U 'mypassword' -f /etc/ppp/mychat"
```

L'option `user account1` définit `account1` comme le nom d'utilisateur CHAP à attribuer à `CallServe`. Pour obtenir une description des autres options du fichier précédent, reportez-vous au fichier similaire `/etc/ppp/peers/myserver` décrit à la section "Définition de la connexion à un pair donné" à la page 453.

Voir aussi Pour tester l'authentification CHAP en appelant le serveur d'appel entrant, reportez-vous à la section "Appel du serveur d'appel entrant" à la page 461.

◆ ◆ ◆ CHAPITRE 20

Configuration d'un tunnel PPPoE (tâches)

Ce chapitre décrit les tâches de la configuration des participants situés à chaque extrémité du tunnel PPPoE : le client PPPoE et le serveur d'accès PPPoE. Voici la liste des sujets abordés :

- “Tâches principales de la configuration d'un tunnel PPPoE (liste des tâches) ” à la page 485
- “Configuration du client PPPoE” à la page 486
- “Configuration d'un serveur d'accès PPPoE” à la page 489

Le scénario présenté dans la section “Planification de la prise en charge DSL sur un tunnel PPPoE” à la page 442 sert d'exemple pour la description des tâches. Pour obtenir une présentation de PPPoE, reportez-vous à la section “Prise en charge des utilisateurs DSL via PPPoE ” à la page 425.

Tâches principales de la configuration d'un tunnel PPPoE (liste des tâches)

Les tableaux suivants répertorient les tâches principales de la configuration des clients PPPoE et du serveur d'accès PPPoE. Pour mettre en œuvre PPPoE sur votre site, il vous suffit de configurer votre extrémité du tunnel PPPoE : le côté client ou le côté serveur d'accès.

TABLEAU 20–1 Liste des tâches de configuration d'un client PPPoE

Tâche	Description	Voir
1. Configuration d'une interface PPPoE	Définissez l'interface Ethernet à utiliser pour le tunnel PPPoE.	“Configuration d'une interface pour un client PPPoE ” à la page 487
2. Configuration des informations concernant le serveur d'accès PPPoE	Définissez les paramètres du serveur d'accès à l'extrémité du tunnel PPPoE où se trouve le fournisseur de services.	“Définition d'un pair de serveur d'accès PPPoE” à la page 487
3. Configuration des fichiers de configuration PPP	Définissez les fichiers de configuration PPP pour le client, si ce n'est déjà fait.	“Définition des communications sur la ligne série ” à la page 451

TABLEAU 20–1 Liste des tâches de configuration d'un client PPPoE *(Suite)*

Tâche	Description	Voir
4. Création du tunnel	Appelez le serveur d'accès.	"Définition d'un pair de serveur d'accès PPPoE" à la page 487

TABLEAU 20–2 Liste des tâches de la configuration d'un serveur d'accès PPPoE

Tâche	Description	Voir
1. Configuration d'un serveur d'accès PPPoE	Définissez l'interface Ethernet à utiliser pour le tunnel PPPoE et les services offerts par le serveur d'accès.	"Configuration d'un serveur d'accès PPPoE" à la page 489
2. Configuration des fichiers de configuration PPP	Définissez les fichiers de configuration PPP pour le client, si ce n'est déjà fait.	"Configuration de la communication sur le serveur d'appel entrant " à la page 459
3. (Facultatif) Restriction de l'utilisation d'une interface	Utilisez les options PPPoE et l'authentification PAP afin de limiter pour certains clients l'utilisation d'une interface Ethernet donnée.	"Limitation de l'utilisation d'une interface à des clients spécifiques " à la page 491

Configuration du client PPPoE

Pour fournir PPP aux systèmes client via DSL, vous devez d'abord configurer PPPoE sur l'interface connectée au modem ou au hub. Vous devez ensuite modifier les fichiers de configuration PPP pour définir le serveur d'accès à l'extrémité opposée du protocole PPPoE.

Prérequis pour la configuration du client PPPoE

Avant de configurer le client PPPoE, vous devez effectuer les opérations suivantes :

- Installez la version Solaris sur les machines client qui doivent utiliser le tunnel PPPoE.
- Contactez le fournisseur de services pour plus d'informations sur son serveur d'accès PPPoE.
- Demandez à l'opérateur téléphonique ou au fournisseur de services de monter les périphériques utilisés par les machines client. Ces périphériques incluent, par exemple, le modem DSL et le séparateur, qu'il incombe à l'opérateur téléphonique de monter.

Configuration d'une interface pour un client PPPoE

Suivez cette procédure pour définir l'interface Ethernet à utiliser pour le tunnel PPPoE.

1. **Connectez-vous en tant que superutilisateur (ou équivalent) sur le client PPPoE.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Ajoutez le nom de l'interface Ethernet dotée de la connexion DSL au fichier `/etc/ppp/pppoe.if`.**

   Par exemple, vous pouvez ajouter l'entrée suivante à `/etc/ppp/pppoe.if` pour un client PPPoE qui utilise `hme0` comme l'interface réseau qui est connectée au modem DSL.

   ```
   hme0
   ```

   Pour plus d'informations sur `/etc/ppp/pppoe.if`, reportez-vous à la section "Fichier `/etc/ppp/pppoe.if`" à la page 545.

3. **Configurez l'interface pour une utilisation de PPPoE.**

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

4. **(Facultatif) Vérifiez que l'interface est maintenant montée pour PPPoE.**

   ```
   # /usr/sbin/sppptun query
   hme0:pppoe
   hme0:pppoed
   ```

   Vous pouvez également utiliser la commande `/usr/sbin/sppptun` pour monter manuellement les interfaces PPPoE. Pour plus d'instructions, reportez-vous à la section "Commande `/usr/sbin/sppptun`" à la page 546.

Définition d'un pair de serveur d'accès PPPoE

Vous définissez le serveur d'accès dans le fichier `/etc/ppp/peers/` *peer-name*. De nombreuses options utilisées pour le serveur d'accès permettent également de définir le serveur d'appel entrant dans le cadre d'un scénario de commutation. Pour obtenir une explication détaillée de `/etc/ppp/peers.` *peer-name*, reportez-vous à la section "Fichier `/etc/ppp/peers/` *peer-name*" à la page 523.

1. **Connectez-vous en tant que superutilisateur (ou équivalent) sur le client PPPoE.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Définissez le serveur d'accès PPPoE du fournisseur de services dans le fichier `/etc/ppp/peers/`*peer-name*.**

Par exemple, le fichier suivant, `/etc/ppp/peers/dslserve`, définit le serveur d'accès `dslserve` au niveau du FAI Far, présenté à la section "Exemple de configuration d'un tunnel PPPoE " à la page 444.

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

La section "Fichier `/etc/ppp/peers/` *peer-name* de définition d'un pair de serveur d'accès" à la page 553 définit les options contenues dans ce fichier.

3 **Modifiez les autres fichiers de configuration PPP sur le client PPPoE.**

a. **Configurez `/etc/ppp/options` comme décrit dans les instructions de configuration d'une machine d'appel sortant à la section "Configuration de la machine d'appel sortant" à la page 448.**

b. **Créez un fichier `/etc/ppp/options.sppptun`. `/etc/ppp/options.sppptun` définit les options PPP pour le port série auquel l'interface montée pour PPPoE est connectée.**

Vous pouvez utiliser toutes les options disponibles pour le fichier `/etc/ppp/options.`*ttyname* décrit dans "Fichier de configuration `/etc/ppp/options.`*ttyname*" à la page 519. Vous devez nommer le fichier `/etc/ppp/options.sppptun`, car `sppptun` est le nom de périphérique spécifié dans la configuration `pppd`.

4 **Assurez-vous que tous les utilisateurs peuvent démarrer PPP sur le client.**

```
# touch /etc/ppp/options
```

5 **Vérifiez que PPP peut s'exécuter sur une ligne DSL.**

```
% pppd debug updetach call dslserve
```

`dslserve` est le nom attribué au serveur d'accès au niveau du FAI illustré à la section "Exemple de configuration d'un tunnel PPPoE " à la page 444. L'option `debug updetach` entraîne l'affichage des informations de débogage dans la fenêtre de terminal.

Si PPP fonctionne correctement, la sortie du terminal indique l'activation de la liaison. Si PPP n'est toujours pas exécuté, essayez d'utiliser la commande ci-dessous pour voir si les serveurs fonctionnent correctement :

```
# /usr/lib/inet/pppoec -i hme0
```

Remarque – Les utilisateurs de clients PPPoE configurés peuvent lancer l'exécution de PPP sur une ligne DSL à l'aide de la commande suivante :

```
% pppd call ISP-server-name
```

Les utilisateurs peuvent alors exécuter une application ou un service.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Voir "Configuration du client PPPoE" à la page 486.
- Voir "Création de tunnels PPPoE pour la prise en charge DSL " à la page 544.
- Voir Chapitre 21, "Résolution des problèmes PPP courants (tâches) ".
- Voir "Configuration d'un serveur d'accès PPPoE" à la page 489.

Configuration d'un serveur d'accès PPPoE

Si votre société est un fournisseur de services, vous pouvez offrir des services, notamment Internet, aux clients qui accèdent à votre site par le biais d'une connexion DSL. La procédure consiste à déterminer les interfaces du serveur à impliquer dans le tunnel PPPoE et à définir les services mis à la disposition des utilisateurs.

▼ Configuration d'un serveur d'accès PPPoE

Cette procédure permet de définir l'interface Ethernet à utiliser pour le tunnel PPPoE et de configurer les services offerts par le serveur d'accès.

1 **Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'accès.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez le nom des interfaces Ethernet qui sont destinées aux tunnels PPPoE dans le fichier `/etc/ppp/pppoe.if`.**

Par exemple, utilisez le fichier `/etc/ppp/pppoe.if` pour le serveur d'accès `dslserve` décrit à la section "Exemple de configuration d'un tunnel PPPoE " à la page 444.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
```

3 **Définissez les services globaux fournis par le serveur d'accès dans le fichier `/etc/ppp/pppoe`.**

Le fichier `/etc/ppp/pppoe` suivant répertorie les services fournis par le serveur d'accès `dslserve` illustré à la Figure 16–5.

```
device hme1,hme2
service internet
    pppd "proxyarp 192.168.1.1:"
service debugging
    pppd "debug proxyarp 192.168.1.1:"
```

Dans le fichier exemple, le service Internet est annoncé pour les interfaces Ethernet `hme1` et `hme2` de `dslserve`. Le débogage est activé pour les liaisons PPP sur les interfaces Ethernet.

4 **Configurez les fichiers de configuration PPP de la même façon que pour un serveur d'appel entrant.**

Pour plus d'informations, voir "Création d'un schéma d'adressage IP pour appelants " à la page 542.

5 **Démarrez le démon `pppoed`.**

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

`pppd` monte également les interfaces qui sont répertoriées dans `/etc/ppp/pppoe.if`.

6 **(Facultatif) Vérifiez que les interfaces sur le serveur sont montées pour PPPoE.**

```
# /usr/sbin/sppptun query
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

L'exemple précédent indique que les interfaces `hme1` et `hme2` sont montées pour PPPoE. Vous pouvez également monter manuellement les interfaces pour PPPoE à l'aide de la commande `/usr/sbin/sppptun` . Pour plus d'instructions, reportez-vous à la section "Commande `/usr/sbin/sppptun`" à la page 546.

▼ Modification d'un fichier `/etc/ppp/pppoe`

1 **Connectez-vous en tant que superutilisateur (ou équivalent) sur le serveur d'accès.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez `/etc/ppp/pppoe`, selon vos besoins.**

3 **Faites en sorte que le démon `pppoed` reconnaisse les nouveaux services.**

```
# pkill -HUP pppoed
```

▼ Limitation de l'utilisation d'une interface à des clients spécifiques

La procédure suivante indique comment limiter une interface à un groupe de clients PPPoE. Avant d'effectuer cette tâche, vous devez vous procurer les vraies adresses MAC Ethernet des clients que vous affectez à l'interface.

Remarque – Certains systèmes permettent de modifier l'adresse MAC sur l'interface Ethernet. Cette possibilité doit être pour vous une commodité, non une mesure de sécurité.

Si vous utilisez l'exemple illustré à la section "Exemple de configuration d'un tunnel PPPoE " à la page 444, ces étapes indiquent comment réserver une interface de `dslserve`, `hme1`, aux clients MiddleCo.

1 **Configurez les interfaces du serveur d'accès et définissez les services, comme indiqué à la section "Configuration d'un serveur d'accès PPPoE" à la page 489.**

2 **Créez des entrées pour les clients dans la base de données `/etc/ethers` du serveur.**

Voici un exemple d'entrée pour les clients Red, Blue et Yellow.

```
8:0:20:1:40:30 redether
8:0:20:1:40:10 yellowether
8:0:20:1:40:25 blueether
```

Dans cet exemple, les noms symboliques `redether`, `yellowether` et `blueether` sont affectés aux adresses Ethernet des clients Red, Yellow et Blue. L'affectation de noms symboliques aux adresses MAC est facultative.

3 **Pour limiter les services fournis sur une interface donnée, définissez les informations suivantes dans le fichier `/etc/ppp/pppoe.`*device*.**

Dans ce fichier, *device* est le nom du périphérique à définir.

```
# cat /etc/ppp/pppoe.hme1
service internet
     pppd "name dslserve-hme1"
     clients redether,yellowether,blueether
```

`dslserve-hme1` est le nom du serveur d'accès utilisé dans les entrées correspondantes dans le fichier `pap-secrets`. L'option `clients` limite l'utilisation de l'interface `hme1` aux clients portant les noms Ethernet symboliques `redether`, `yellowether` et `blueether`.

Si vous n'avez pas défini de noms symboliques pour les adresses MAC du client dans la base de données `/etc/ethers`, vous pouvez utiliser les adresses numériques sous forme d'arguments de l'option `clients`. Les caractères génériques sont autorisés.

Vous pouvez, par exemple, spécifier l'adresse numérique `clients 8:0:20:*:*:*`. Grâce aux caractères génériques, toutes les adresses correspondantes dans la base de données `/etc/ethers` sont acceptées.

4 Créez le fichier `/etc/ppp/pap-secrets` pour le serveur d'accès.

```
Red         dslserve-hme1   redpasswd     *
Blue        dslserve-hme1   bluepasswd    *
Yellow      dslserve-hme1   yellowpassd   *
```

Les entrées sont les noms et mots de passe PAP des clients autorisés à exécuter PPP sur l'interface `hme1` de `dslserve`.

Pour plus d'informations sur l'authentification PAP, voir "Configuration de l'authentification PAP" à la page 470.

Voir aussi La liste ci-après fournit les références à des informations connexes.

- Pour en savoir plus à propos de PPPoE, voir "Création de tunnels PPPoE pour la prise en charge DSL " à la page 544.
- Pour résoudre les problèmes liés à PPPoE et PPP, reportez-vous à la section "Résolution des problèmes liés à PPP et PPPoE" à la page 497.
- Pour configurer un client PPPoE, voir "Configuration du client PPPoE" à la page 486.
- Pour configurer une authentification PAP pour un client, reportez-vous à la section "Configuration de l'authentification PAP pour les appelants de confiance (machines d'appel sortant)" à la page 474.
- Pour configurer une authentification PAP sur un serveur, voir "Configuration de l'authentification PAP sur le serveur d'appel entrant " à la page 471.

◆ ◆ ◆ CHAPITRE 21

Résolution des problèmes PPP courants (tâches)

Ce chapitre contient des informations de dépannage des problèmes courants qui se produisent avec Solaris PPP 4.0. Il aborde les sujets suivants :

- “Outils de dépannage de PPP ” à la page 494
- “Résolution des problèmes liés à PPP et PPPoE” à la page 497
- “Correction des problèmes des lignes spécialisées ” à la page 510
- “Diagnostic et résolution des problèmes d'authentification” à la page 511

Le livre intitulé *PPP Design, Implementation, and Debugging* de James Carlson et le site Web de l'Australian National University proposent également des conseils détaillés pour la résolution des problèmes liés à PPP. Pour plus d'informations, reportez-vous aux sections “Ouvrages de référence professionnelle à propos de PPP ” à la page 416 et “Sites Web sur PPP ” à la page 416.

Résolution des problèmes liés à PPP (liste des tâches)

Utilisez la liste des tâches suivante pour accéder facilement à des conseils et des solutions relatifs aux problèmes liés à PPP.

TABLEAU 21–1 Liste des tâches de résolution des problèmes liés à PPP

Tâche	Définition	Voir
Obtention d'informations de diagnostic sur la liaison PPP	Utilisez les outils de diagnostic PPP afin d'obtenir la sortie pour la résolution des problèmes.	“Obtention des informations de diagnostic à l'aide de pppd ” à la page 495
Obtention des informations de débogage pour la liaison PPP	Utilisez la commande `pppd debug` afin de générer une sortie pour la résolution de problèmes.	“Activation du débogage de PPP” à la page 496

TABLEAU 21–1 Liste des tâches de résolution des problèmes liés à PPP *(Suite)*

Tâche	Définition	Voir
Résolution des problèmes généraux avec la couche réseau	Identifiez et corrigez les problèmes liés à PPP qui sont relatifs au réseau en effectuant une série de vérifications.	“Diagnostic des problèmes réseau ” à la page 498
Résolution de problèmes de communication généraux	Identifiez et corrigez les problèmes de communication qui affectent la liaison PPP.	“Diagnostic et résolution des problèmes de communication ” à la page 500
Résolution des problèmes de configuration	Identifiez et corrigez les problèmes dans les fichiers de configuration PPP.	“Diagnostic des problèmes liés à la configuration PPP” à la page 502
Résolution des problèmes liés au modem	Identifiez et corrigez les problèmes de modem.	“Diagnostic des problèmes de modem ” à la page 503
Résolution des problèmes liés aux scripts de discussion	Identifiez et corrigez les problèmes de script de discussion sur l'ordinateur des appels sortants.	“Obtention des informations de débogage pour les scripts de discussion” à la page 504
Résolution des problèmes de débit de la ligne série	Identifiez et corrigez les problèmes de débit de ligne sur le serveur des appels entrants.	“Diagnostic et résolution des problèmes de débit de ligne série” à la page 507
Résolution des problèmes courants pour les lignes spécialisées	Identifiez et corrigez les problèmes de performances sur une ligne spécialisée.	“Correction des problèmes des lignes spécialisées ” à la page 510
Résolution des problèmes liés à l'authentification	Identifiez et corrigez les problèmes liés aux bases de données d'authentification.	“Diagnostic et résolution des problèmes d'authentification” à la page 511
Dépannage des zones à problème pour PPPoE	Utilisez les outils de diagnostic PPP afin d'obtenir la sortie pour l'identification et la résolution des problèmes liés à PPPoE.	“Obtention des informations de diagnostic pour PPPoE ” à la page 508

Outils de dépannage de PPP

Les liaisons PPP présentent généralement trois zones principales d'échec :

- échec de création du lien ;
- dégradation des performances du lien pendant l'utilisation normale ;
- problèmes pouvant être dus aux réseaux de l'un ou l'autre côté du lien.

La manière la plus simple de savoir si PPP fonctionne est d'exécuter une commande sur le lien. Exécutez une commande telle que `ping` ou `traceroute` sur un hôte du réseau du pair. Ensuite,

observez les résultats. Cependant, vous devez utiliser les outils de débogage PPP et UNIX pour contrôler les performances d'un lien établi ou pour résoudre les problèmes posés par un lien.

Cette section explique comment obtenir les informations de diagnostic de `pppd` et les fichiers journaux associés. Les autres sections de ce chapitre décrivent les problèmes couramment posés par PPP que vous pouvez détecter et corriger à l'aide des outils de dépannage PPP.

▼ Obtention des informations de diagnostic à l'aide de pppd

La procédure suivante montre comment visualiser le fonctionnement en cours d'un lien sur la machine locale.

1 Connectez-vous en tant que superutilisateur sur la machine local ou assumez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Exécutez `pppd` avec le périphérique série configuré pour PPP en tant qu'argument :

```
# pppd cua/b debug updetach
```

Les exemples suivants présentent les sorties obtenues pour une liaison commutée et une liaison de ligne spécialisée lorsque `pppd` s'exécute en arrière-plan. Si vous exécutez `pppd debug` en arrière-plan, la sortie produite est envoyée dans le fichier `/etc/ppp/connect-errors`.

Exemple 21–1 Sortie d'une liaison commutée fonctionnant correctement

```
# pppd /dev/cua/b debug updetach
have route to 0.0.0.0/0.0.0.0 via 172.21.0.4
serial speed set to 230400 bps
Using interface sppp0
Connect: sppp0 <--> /dev/cua/b
sent [LCP ConfReq id=0x7b <asyncmap 0x0> <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP Ident id=0x79 magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6
    2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
    rcvd [LCP ConfRej id=0x7b <asyncmap 0x0>]
sent [LCP Ident id=0x7c magic=0x0 "ppp-2.4.0b1 (Sun Microsystems, Inc., Sep 15
    2004 09:38:33)"
sent [LCP ConfReq id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x7d <magic 0x73e981c8> <pcomp> <accomp>]
rcvd [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP ConfAck id=0x78 <magic 0xdd4ad820> <pcomp> <accomp>]
sent [LCP Ident id=0x7e magic=0x73e981c8 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
    Sep 15 2004 09:38:33)"]
sent [IPCP ConfReq id=0x3d <addr 0.0.0.0> <compress VJ 0f 01>]
rcvd [LCP Ident id=0x7a magic=0xdd4ad820 "ppp-2.4.0b1 (Sun Microsystems, Inc.,
```

```
    Oct  6 2004 09:36:22)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct  6 2004 09:36:22)
rcvd [IPCP ConfReq id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
sent [IPCP ConfAck id=0x92 <addr 10.0.0.1> <compress VJ 0f 01>
rcvd [IPCP ConfNak id=0x3d <addr 10.0.0.2>]]
sent [IPCP ConfReq id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
rcvd [IPCP ConfAck id=0x3e <addr 10.0.0.2> <compress VJ 0f 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

Exemple 21–2 Sortie d'une liaison de ligne spécialisée fonctionnant correctement

```
# pppd /dev/se_hdlc1 default-asyncmap debug updetach
pppd 2.4.0b1 (Sun Microsystems, Inc., Oct 24 2004 07:13:18) started by root, uid 0
synchronous speed appears to be 0 bps
init option: '/etc/ppp/peers/syncinit.sh' started (pid 105122)
Serial port initialized.
synchronous speed appears to be 64000 bps
Using interface sppp0
Connect: sppp0 <--> /dev/se_hdlc1
sent [LCP ConfReq id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfAck id=0xe9 <magic 0x474283c6><pcomp> <accomp>]
rcvd [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP ConfReq id=0x22 <magic 0x8e3a53ff><pcomp> <accomp>]
sent [LCP Ident id=0xea magic=0x474283c6 "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
sent [IPCP ConfReq id=0xf7 <addr 0.0.0.0> <compress VJ 0f o1>]]
sent [CCP ConfReq id=0x3f <deflate 15> <deflate(old#) 15> <bsd v1 15>]
rcvd [LCP Ident id=0x23 magic=0x8e3a53ff "ppp-2.4.0b1 (Sun Microsystems, Inc., Oct
    22 2004 14:31:44)"]
Peer Identification: ppp-2.4.0b1 (Sun Microsystems, Inc., Oct 22 2004 14:31:44)
rcvd [IPCP ConfReq id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
sent [IPCP ConfAck id=0x25 <addr 10.0.0.1> <compress VJ Of 01>]
rcvd [CCP ConfReq id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
sent [CCP ConfAck id=0x3 <deflate 15> <deflate(old#) 15 <bsd v1 15>]
rcvd [IPCP ConfNak id=0xf8 <addr 10.0.0.2>]
rcvd [IPCP ConfReq id=0xf7 <addr 10.0.0.2> <compress VJ Of 01>]
rcvd [CCP ConfAck id=0x3f <deflate 15> <deflate(old#) 15 <bsd v1 15>]
Deflate (15) compression enabled
rcvd [IPCP ConfAck id=0xf8 <addr 10.0.0.2> <compress VJ Of 01>]
local  IP address 10.0.0.2
remote IP address 10.0.0.1
```

▼ Activation du débogage de PPP

La tâche suivante présente l'utilisation de la commande `pppd` pour obtenir des informations de débogage.

Remarque – Vous n'avez besoin d'exécuter les étapes 1 à 3 qu'une fois pour chaque hôte. Par la suite, vous pouvez passer à l'étape 4 pour activer le débogage pour l'hôte.

---

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez un fichier journal pour enregistrer la sortie de `pppd`.**

   ```
   # touch /var/log/pppdebug
   ```

3. **Ajoutez les fonctions `syslog` suivantes pour `pppd` dans `/etc/syslog.conf`.**

   ```
   daemon.debug;local2.debug       /var/log/pppdebug
   ```

4. **Redémarrez `syslogd`.**

   ```
   # pkill -HUP -x syslogd
   ```

5. **Activez le débogage pour les appels à un pair particulier à l'aide de la syntaxe suivante de `pppd`.**

   ```
   # pppd debug call peer-name
   ```

   peer-name doit être le nom d'un fichier dans le répertoire `/etc/ppp/peers`.

6. **Affichez le contenu du fichier journal.**

   ```
   # tail -f /var/log/pppdebug
   ```

   Pour obtenir un exemple de fichier journal, reportez-vous à l'Étape 3.

Résolution des problèmes liés à PPP et PPPoE

Reportez-vous aux sections suivantes pour plus d'informations sur la façon de résoudre les problèmes liés à PPP et PPPoE.

Diagnostic des problèmes réseau

Si la liaison PPP devient active mais que peu d'hôtes du réseau distant sont accessibles, cela indique peut-être un problème de réseau. La procédure suivante vous indique comment isoler et résoudre les problèmes réseau ayant une incidence sur une liaison PPP.

1. **Connectez-vous en tant que superutilisateur sur la machine local ou assumez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Arrêtez le lien qui pose problème.**

3. **Désactivez les protocoles facultatifs dans les fichiers de configuration en ajoutant les options suivantes à votre configuration de PPP :**

   ```
   noccp novj nopcomp noaccomp default-asyncmap
   ```

   Ces options offrent le PPP non compressé le plus simple qui existe. Essayez d'appeler ces options en tant qu'arguments associés à `pppd` sur la ligne de commande. Si vous pouvez atteindre les hôtes précédemment inaccessibles, ajoutez les options dans l'un ou l'autre des emplacements ci-dessous.

   - `/etc/ppp/peers/`*peer-name*, après l'option `appel`
   - `/etc/ppp/options`, en vous assurant que les options s'appliquent de manière globale.

4. **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

   ```
   % pppd debug call peer-name
   ```

5. **Obtenez les journaux détaillés du programme de messagerie instantanée en utilisant l'option `-v` de `chat`.**

   Par exemple, utilisez le format suivant dans n'importe quel fichier de configuration PPP :

   ```
   connect 'chat -v -f /etc/ppp/chatfile'
   ```

   /etc/ppp/chatfile représente le nom de votre fichier de messagerie instantanée.

6. **Essayez de recréer le problème en utilisant Telnet ou d'autres applications pour atteindre les hôtes distants.**

   Étudiez les journaux de débogage. Si vous ne pouvez toujours pas atteindre les hôtes distants, le problème PPP peut être lié au réseau.

7. **Vérifiez que les adresses IP des hôtes distants sont des adresses Internet enregistrées.**

   Certaines organisations assignent des adresses IP internes qui sont connues au sein du réseau local mais ne sont pas routables sur Internet. Si les hôtes distants se trouvent au sein de votre

entreprise, vous devez définir un serveur de conversion de nom en adresse ou un serveur proxy pour accéder à Internet. Si les hôtes distants ne sont pas au sein de votre entreprise, vous devez signaler le problème à l'organisation distante.

8 Examinez les tables de routage.

a. Vérifiez les tables de routage sur la machine locale et le pair.

b. Vérifiez les tables de routage pour les routeurs qui sont dans le chemin d'accès du pair vers le système distant. Vérifiez également les tables de routage pour les routeurs du chemin d'accès de retour au pair.

Assurez-vous que les routeurs intermédiaires n'ont pas été configurés de manière incorrecte. Souvent, le problème peut être trouvé dans le chemin de retour au pair.

9 (Facultatif) Si la machine est un routeur, vérifiez les fonctionnalités facultatives.

```
# ndd -set /dev/ip ip_forwarding 1
```

Pour plus d'informations sur `ndd`, reportez-vous à la page de manuel `ndd(1M)`.

Dans Solaris 10, vous pouvez utilisez `routeadm(1M)`, au lieu de `ndd(1M)`.

```
# routeadm -e ipv4-forwarding -u
```

Remarque – La commande `ndd` n'est pas persistante. Les valeurs définies à l'aide de cette commande sont perdues lors de la réinitialisation du système. La commande `routeadm` est persistante. Les valeurs définies avec cette commande sont conservées après la réinitialisation du système.

---

10 Vérifiez les statistiques qui sont obtenues à l'aide de `netstat -s` et des outils similaires.

Pour plus d'informations sur `netstat`, reportez-vous à la page de manuel `netstat(1M)`.

a. Exécutez les statistiques sur la machine locale.

b. Appelez le pair.

c. Observez les nouvelles statistiques générées par `netstat -s`. Pour plus d'informations, reportez-vous à la section "Problèmes réseau courants affectant PPP " à la page 500.

11 Vérifiez la configuration DNS.

Une configuration de service de noms incorrecte entraîne l'échec des applications car les adresses IP ne peuvent pas être résolues.

Problèmes réseau courants affectant PPP

Vous pouvez utiliser les messages qui sont générés par `netstat -s` pour corriger les problèmes de réseau qui sont présentés dans le tableau suivant. Pour des informations sur les procédures associées, reportez-vous à la section "Diagnostic des problèmes réseau " à la page 498.

TABLEAU 21–2 Problèmes réseau courants affectant PPP

Message	Problème	Solution
`IP packets not forwardable` (Paquets IP non transmissibles)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.
`ICMP input destination unreachable` (Destination d'entrée ICMP inaccessible)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.
`ICMP time exceeded` (Temps ICMP dépassé)	Deux routeurs se transfèrent la même adresse de destination, ce qui entraîne le rebondissement du paquet jusqu'à ce que la valeur de durée de vie soit dépassée.	Utilisez `traceroute` pour trouver l'origine de la boucle de routage, puis contactez l'administrateur du routeur concerné. Pour plus d'informations sur `traceroute`, reportez-vous à la page de manuel `traceroute(1M)`.
`IP packets not forwardable` (Paquets IP non transmissibles)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante à la table de routage de l'hôte local.
`ICMP input destination unreachable` (Destination d'entrée ICMP inaccessible)	Une route est manquante pour l'hôte local.	Ajoutez la route manquante aux tables de routage de l'hôte local.

▼ Diagnostic et résolution des problèmes de communication

Les problèmes de communication surviennent lorsque les deux pairs ne parviennent pas à un établir une liaison. Il arrive parfois que ces problèmes soient en fait des problèmes de négociation causés par une configuration incorrecte des scripts de discussion. La procédure suivante vous indique comment supprimer les problèmes de communication. Pour supprimer les problèmes de négociation dus à des scripts de discussion erronés, reportez-vous au Tableau 21–5.

1 Connectez-vous en tant que superutilisateur sur la machine local ou assumez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Appelez le pair.

3 **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

```
% pppd debug call peer-name
```

Vous devrez peut-être obtenir des informations de débogage du pair afin de résoudre certains problèmes de communication.

4 **Vérifiez les journaux obtenus pour connaître les problèmes de communication. Pour plus d'informations, reportez-vous à la section "Problèmes de communication généraux affectant PPP " à la page 501.**

Problèmes de communication généraux affectant PPP

Le tableau suivant présente les symptômes associés à la sortie de journal de la procédure "Diagnostic et résolution des problèmes de communication " à la page 500.

TABLEAU 21–3 Problèmes de communication généraux affectant PPP

Symptôme	Problème	Solution
`too many Configure-Requests` (Demandes de configuration trop nombreuses)	Un pair ne peut pas entendre l'autre pair.	Vérifiez les problèmes suivants : ■ Le câblage de l'ordinateur ou du modem est peut-être défectueux. ■ Les paramètres binaires de la configuration du modem sont peut-être incorrects. Il se peut également que le contrôle de flux de la configuration soit interrompu. ■ Le script de discussion a peut-être subi un échec. Dans cette situation, reportez-vous au Tableau 21–5.
La sortie `pppd debug` montre que LCP démarre, mais que les protocoles de niveau supérieur échouent ou affichent des erreurs CRC.	La table des caractères de contrôle asynchrone (ACCM) n'est pas correctement définie.	Utilisez l'option `default-async` afin de définir l'ACCM sur la valeur par défaut de FFFFFFFF. Tout d'abord, essayez d'utiliser `default-async` en tant qu'option de `pppd` sur la ligne de commande. Si le problème disparaît, ajoutez ensuite `default-async` à `/etc/ppp/options` ou `/etc/ppp/peers/`*peer-name* après l'appel.
La sortie de `pppd debug` montre qu'IPCP démarre mais s'arrête immédiatement.	Les adresses IP sont peut-être configurées de façon incorrecte.	1. Vérifiez le script de discussion afin de vérifier si le script contient des adresses IP incorrectes. 2. Si le script de discussion est correct, demandez les journaux de débogage du pair, et vérifiez-y les adresses IP.
Les performances du lien sont médiocres.	Le modem est peut-être mal configuré (erreurs de configuration du contrôle de flux, erreurs de configuration du modem et débits DTE configurés de façon incorrecte).	Vérifiez la configuration du modem. Modifiez la configuration, le cas échéant.

▼ Diagnostic des problèmes liés à la configuration PPP

Certains problèmes liés à PPP sont dus aux problèmes contenus dans les fichiers de configuration PPP. La procédure suivante vous indique comment identifier et résoudre les problèmes de configuration généraux.

1 **Connectez-vous en tant que superutilisateur sur la machine local ou assumez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Appelez le pair distant. Ensuite, activez les fonctions de débogage.**

```
% pppd debug call peer-name
```

3 **Vérifiez le journal qui en résulte à la recherche de problèmes de configuration. Pour plus d'informations, reportez-vous à la section "Problèmes courants de configuration de PPP " à la page 502.**

Problèmes courants de configuration de PPP

Le tableau suivant décrit les symptômes liés à la sortie de journal de la procédure "Diagnostic des problèmes liés à la configuration PPP" à la page 502.

TABLEAU 21–4 Problèmes courants de configuration de PPP

Symptôme	Problème	Solution
La sortie de `pppd debug` contient le message d'erreur `Could not determine remote IP address` (Impossible de déterminer l'adresse IP distante).	Le fichier `/etc/ppp/peers/`*peer-name* ne contient pas d'adresse IP pour le pair. Le pair ne fournit pas d'adresse IP pendant la négociation de lien.	Fournissez une adresse IP pour le pair sur la ligne de commande pppd ou dans `/etc/ppp/peers/`*peer-name* en utilisant le format suivant : :10.0.0.10
La sortie de `pppd debug` indique que la compression de données CCP a échoué. La sortie indique également que le lien a été supprimé.	Les configurations de compression PPP du pair sont peut-être en conflit.	Désactivez la compression CCP en ajoutant l'option `noccp` à `/etc/ppp/options` sur l'un des pairs.

Diagnostic des problèmes de modem

Les modems peuvent être des sources de problèmes majeures pour les liaisons commutées. L'indicateur le plus commun des problèmes liés à la configuration du modem est l'absence de réponse du pair. Cependant, il se peut que vous ayez des difficultés à déterminer si un problème de lien est effectivement le résultat des problèmes de configuration du modem.

Pour obtenir des suggestions de base sur le dépannage du modem, reportez-vous à la section "Résolution des problèmes liés aux terminaux et aux modems" du *Guide d'administration système : Administration avancée*. La documentation et les sites Web des fabricants de modems contiennent des solutions aux problèmes rencontrés avec leurs équipements. La procédure ci-après permet de déterminer si une configuration de modem incorrecte entraîne des problèmes de liens.

1. **Une fois le débogage activé, appelez le pair, comme expliqué dans la section "Activation du débogage de PPP" à la page 496.**

2. **Affichez le journal `/var/log/pppdebug` obtenu pour vérifier si la configuration du modem est incorrecte.**

3. **Utilisez `ping` pour envoyer des paquets de tailles diverses sur le lien.**

   Pour plus d'informations sur `ping`, reportez-vous à la page de manuel `ping(1M)`.

   Si les petits paquets sont reçus mais que les paquets plus volumineux sont supprimés, il existe des problèmes au niveau du modem.

4. **Vérifiez la présence d'erreurs sur l'interface `sppp0` :**

```
% netstat -ni
Name  Mtu  Net/Dest   Address      Ipkts    Ierrs Opkts    Oerrs Collis Queue
lo0   8232 127.0.0.0  127.0.0.1    826808   0     826808   0     0      0
hme0  1500 172.21.0.0 172.21.3.228 13800032 0     1648464  0     0      0
sppp0 1500 10.0.0.2   10.0.0.1     210      0     128      0     0      0
```

   Si les erreurs d'interface augmentent au fil du temps, il existe peut-être des problèmes au niveau de la configuration du modem.

Erreurs fréquentes

Lorsque vous affichez le journal `/var/log/pppdebug` obtenu, les symptômes suivants dans la sortie peuvent indiquer une configuration de modem incorrecte. La machine locale peut entendre le pair, mais ce dernier ne peut entendre la machine locale.

- Aucun message `recvd` n'a été émis par le pair.
- La sortie contient les messages LCP du pair, mais le lien échoue avec les messages `too many LCP Configure Requests` (Demandes de configuration LCP trop nombreuses) envoyés par la machine locale.
- Le lien se termine avec un signal SIGHUP.

▼ Obtention des informations de débogage pour les scripts de discussion

La procédure suivante permet d'obtenir des informations de débogage à l'aide de `chat`, ainsi que des suggestions pour la résolution des problèmes courants. Pour plus d'informations, reportez-vous à la section "Problèmes de scripts de discussion courants" à la page 504.

1 **Connectez-vous en tant que superutilisateur (ou équivalent) à la machine d'appel sortant.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez le fichier `/etc/ppp/peers/` *peer-name* pour le pair à appeler.**

3 **Ajoutez `-v` en tant qu'argument à la commande `chat` qui est spécifiée dans l'option `connect`.**

```
connect "/usr/bin/chat -v -f /etc/ppp/chat-script-name"
```

4 **Prenez connaissance des erreurs de script de discussion dans le fichier `/etc/ppp/connect-errors`.**

L'erreur suivante est la principale erreur qui se produit avec `chat`.

```
Oct 31 08:57:13 deino chat[107294]: [ID 702911 local2.info] expect (CONNECT)
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] alarm
Oct 31 08:57:58 deino chat[107294]: [ID 702911 local2.info] Failed
```

L'exemple montre le délai d'attente lors de l'attente d'une chaîne `(CONNECT)`. En cas d'échec de `chat`, vous obtenez le message suivant de `pppd` :

```
Connect script failed
```

Problèmes de scripts de discussion courants

Les scripts de discussion sont des sources de problèmes pour les liaisons commutées. Le tableau suivant énumère les erreurs courantes de script de discussion et donne des suggestions pour résoudre les erreurs. Pour des informations sur les procédures à suivre, reportez-vous à la section "Obtention des informations de débogage pour les scripts de discussion" à la page 504.

TABLEAU 21–5 Problèmes de scripts de discussion courants

Symptôme	Problème	Solution
La sortie de `pppd debug` contient `Connect script failed` (Échec du script de connexion)	Votre script de discussion fournit un nom d'utilisateur et un mot de passe. `ogin:` *user-name* `ssword:` *password* Cependant, le pair auquel vous aviez l'intention de vous connecter n'invite pas fournir ces informations.	1. Supprimez l'identification et le mot de passe du script de discussion. 2. Essayez d'appeler le pair une nouvelle fois. 3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.

Le journal `/usr/bin/chat -v` contient `"expect (login:)" alarm read timed out`	Votre script de discussion fournit un nom d'utilisateur et un mot de passe.
	`ogin: pppuser`
	`ssword: \q\U`
	Cependant, le pair auquel vous essayez de vous connecter n'invite pas à fournir ces informations.
		1. Supprimez l'identification et le mot de passe du script de discussion.
		2. Essayez d'appeler le pair une nouvelle fois.
		3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.

La sortie de `pppd debug` contient `possibly looped-back`	La machine locale ou son pair se bloque au niveau de la ligne de commande et n'exécute pas PPP. Le script de discussion contient un nom de connexion et un mot de passe configurés de manière incorrecte.	1. Supprimez l'identification et le mot de passe du script de discussion. 2. Essayez d'appeler le pair une nouvelle fois. 3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez la séquence de connexion correcte.
La sortie de `pppd debug` indique que le protocole LCP s'active, mais que la liaison s'arrête rapidement après.	Le mot de passe contenu dans le script de discussion est peut-être incorrect.	1. Assurez-vous que vous avez le mot de passe correct pour la machine locale. 2. Vérifiez le mot de passe dans le script de discussion. Corrigez le mot de passe, le cas échéant. 3. Essayez d'appeler le pair une nouvelle fois. 4. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez-lui la séquence de connexion correcte.

TABLEAU 21–5 Problèmes de scripts de discussion courants *(Suite)*

Symptôme	Problème	Solution

Le texte du pair commence par un tilde (~).	Votre script de discussion fournit un nom d'utilisateur et un mot de passe.
	`ogin: pppuser`
	`ssword: \q\U`
	Cependant, le pair auquel vous essayez de vous connecter n'invite pas à fournir ces informations.
		1. Supprimez l'identification et le mot de passe du script de discussion.
		2. Essayez d'appeler le pair une nouvelle fois.
		3. Si vous obtenez encore le message, appelez le fournisseur d'accès Internet. Demandez la séquence de connexion correcte.

Le modem se bloque.	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `LCP: timeout sending Config-Requests`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `Serial link is not 8-bit clean`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `Loopback detected` (Loopback détecté)	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.
La sortie de `pppd debug` contient `SIGHUP`	Votre script de discussion contient la ligne suivante pour forcer la machine locale à attendre le message `CONNECT` du pair : `CONNECT ”`	Utilisez la ligne suivante lorsque vous souhaitez que le script de discussion attende le message CONNECT du pair : `CONNECT \c` Terminez le script de discussion avec ~ `\c`.

Diagnostic et résolution des problèmes de débit de ligne série

Les serveurs des appels entrants peuvent rencontrer des problèmes en raison de conflits au niveau des paramètres de débit. La procédure suivante vous permet d'identifier la cause du problème de lien liée aux conflits de débits de ligne série.

Les comportements suivants causent des problèmes de débit :

- Vous avez appelé PPP par l'intermédiaire d'un programme tel que `/bin/login` et indiqué le débit de la ligne.
- Vous avez démarré PPP à partir de `mgetty` et fourni accidentellement le débit binaire.

pppd modifie le débit qui a été défini à l'origine pour la ligne au profit du débit défini par `/bin/login` ou `mgetty`. En conséquence, la ligne échoue.

1. **Connectez-vous au serveur d'appel entrant. Le débogage étant activé, appelez le pair.**

   Si vous avez besoin d'instructions, reportez-vous à la section "Activation du débogage de PPP" à la page 496.

2. **Affichez le journal `/var/log/pppdebug` obtenu.**

   Vérifiez la sortie pour le message suivant :

   ```
   LCP too many configure requests
   ```

   Ce message indique que le débit des lignes série qui ont été configurées pour PPP peut potentiellement être en conflit.

3. **Vérifiez si PPP est appelé par le biais d'un programme tel que `/bin/login` et le débit de ligne qui a été défini.**

   Dans une telle situation, `pppd` modifie le débit de ligne initialement configuré au profit du débit spécifié dans `/bin/login`.

4. **Vérifiez si un utilisateur a démarré PPP à l'aide de la commande `mgetty` et accidentellement spécifié un débit binaire.**

   Cette action entraîne également des conflits entre les débits de ligne série.

5. **Résolvez ce problème de conflit comme suit :**

   a. **Verrouillez le débit ETTD sur le modem.**

   b. **N'utilisez pas autobaud.**

   c. **Ne modifiez pas le débit de ligne après la configuration.**

▼ Obtention des informations de diagnostic pour PPPoE

Vous pouvez utiliser PPP et les utilitaires UNIX standard pour identifier les problèmes liés à PPPoE. Lorsque vous avez des raisons de croire que PPPoE est la cause des problèmes se produisant sur un lien, utilisez les outils de diagnostic suivants pour obtenir des informations sur le dépannage.

1. **Connectez-vous en tant que superutilisateur sur l'ordinateur qui exécute le tunnel PPPoE, le client PPPoE ou le serveur d'accès PPPoE.**

2. **Activez le débogage en suivant la procédure présentée dans la section "Activation du débogage de PPP" à la page 496.**

3. **Affichez le contenu du fichier journal `/var/log/pppdebug`.**

   L'exemple ci-dessous montre une partie d'un fichier journal qui a été généré pour un lien avec un tunnel PPPoE.

```
Sep  6 16:28:45 enyo pppd[100563]: [ID 702911 daemon.info] Plugin
  pppoe.so loaded.
Sep  6 16:28:45 enyo pppd[100563]: [ID 860527 daemon.notice] pppd
  2.4.0b1 (Sun Microsystems, Inc.,
Sep  5 2001 10:42:05) started by troot, uid 0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] connect option:
   '/usr/lib/inet/pppoec
-v hme0' started (pid 100564)
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Serial connection established.
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.info] Using interface sppp0
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.notice] Connect: sppp0
   <--> /dev/sppptun
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/pap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] /etc/ppp/chap-secrets
  is apparently empty
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] sent
  [LCP ConfReq id=0xef <mru 1492>
asyncmap 0x0 <magic 0x77d3e953><pcomp><acomp>
Sep  6 16:28:46 enyo pppd[100563]: [ID 702911 daemon.debug] rcvd
  [LCP ConfReq id=0x2a <mru 1402>
asyncmap 0x0 <magic 0x9985f048><pcomp><acomp
```

   Si la sortie de débogage ne vous permet pas d'identifier le problème, passez à la procédure suivante.

4. **Obtenez les messages de diagnostic pour PPPoE.**

   ```
   # pppd connect "/usr/lib/inet/pppoec -v interface-name"
   ```

   `pppoec` envoie les informations de diagnostic dans le fichier `stderr`. Si vous exécutez `pppd` au premier plan, la sortie s'affiche à l'écran. Si `pppd` s'exécute en arrière-plan, la sortie est envoyé dans `/etc/ppp/connect-errors`.

L'exemple suivant présente les messages qui sont générés lors de la négociation du tunnel PPPoE.

```
Connect option: '/usr/lib/inet/pppoec -v hme0' started (pid 100564)
/usr/lib/inet/pppoec: PPPoE Event Open (1) in state Dead (0): action SendPADI (2)
/usr/lib/inet/pppoec: Sending PADI to ff:ff:ff:ff:ff:ff: 18 bytes
/usr/lib/inet/pppoec: PPPoE State change Dead (0) -> InitSent (1)
/usr/lib/inet/pppoec: Received Active Discovery Offer from 8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADO+ (5) in state InitSent (1): action SendPADR+ (5)
/usr/lib/inet/pppoec: Sending PADR to 8:0:20:cd:c1:2: 22 bytes
/usr/lib/inet/pppoec: PPPoE State change InitSent (1) -> ReqSent (3)
/usr/lib/inet/pppoec: Received Active Discovery Session-confirmation from
   8:0:20:cd:c1:2/hme0:pppoed
/usr/lib/inet/pppoec: PPPoE Event rPADS (7) in state ReqSent (3): action Open (7)
/usr/lib/inet/pppoec: Connection open; session 0002 on hme0:pppoe
/usr/lib/inet/pppoec: PPPoE State change ReqSent (3) -> Convers (4)
/usr/lib/inet/pppoec: connected
```

Si les messages de diagnostic ne vous permettent pas d'identifier le problème, passez à la procédure suivante.

5 Exécutez snoop. Enregistrez ensuite le suivi dans un fichier.

Pour plus d'informations sur `snoop`, reportez-vous à la page de manuel `snoop(1M)`.

```
# snoop -o pppoe-trace-file
```

6 Affichez le fichier de suivi snoop.

```
# snoop -i pppoe-trace-file -v pppoe

ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 1 arrived at 6:35:2.77
ETHER: Packet size = 32 bytes
ETHER: Destination = ff:ff:ff:ff:ff:ff, (broadcast)
ETHER: Source      = 8:0:20:78:f3:7c, Sun
ETHER: Ethertype = 8863 (PPPoE Discovery)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 9 (Active Discovery Initiation)
PPPoE: Session Id = 0
PPPoE: Length = 12 bytes
PPPoE:
PPPoE: ----- Service-Name -----
PPPoE: Tag Type = 257
PPPoE: Tag Length = 0 bytes
PPPoE:
PPPoE: ----- Host-Uniq -----
PPPoE: Tag Type = 259
PPPoE: Tag Length = 4 bytes
PPPoE: Data = Ox00000002
PPPoE:
.
```

```
.
.
ETHER: ----- Ether Header -----
ETHER:
ETHER: Packet 5 arrived at 6:35:2.87
ETHER: Packet size = 60 bytes
ETHER: Destination = 8:0:20:78:f3:7c, Sun)
ETHER: Source      = 0:2:fd:39:7f:7,
ETHER: Ethertype = 8864 (PPPoE Session)
ETHER:
PPPoE: ----- PPP Over Ethernet -----
PPPoE:
PPPoE: Version = 1
PPPoE: Type = 1
PPPoE: Code = 0 (PPPoE Session)
PPPoE: Session Id = 24383
PPPoE: Length = 20 bytes
PPPoE:
PPP: ----- Point-to-Point Protocol -----
PPP:
PPP-LCP: ----- Link Control Protocol -----
PPP-LCP:
PPP-LCP: Code = 1 (Configure Request)
PPP-LCP: Identifier = 80
PPP-LCP: Length = 18
```

Correction des problèmes des lignes spécialisées

Les problèmes les plus couramment rencontrés avec les lignes spécialisées sont des performances médiocres. Dans la plupart des cas, vous pouvez résoudre le problème en collaboration avec l'opérateur téléphonique.

TABLEAU 21–6 Problèmes courants liés aux lignes spécialisées

Symptôme	Problème	Solution
Le lien ne démarre pas.	Cela peut être dû à des violations de bipolarité CSU. Une extrémité du lien est configurée pour les lignes AMI. L'autre extrémité est configurée pour le remplacement de huit zéros par un bit ESF (B8ZS).	Si vous êtes aux États-Unis ou au Canada, vous pouvez corriger ce problème directement à partir du menu du CSU/DSU. Vérifiez la documentation du fabricant du CSU/DSU pour plus de détails. Dans d'autres pays, le fournisseur peut être responsable de la correction des violations de bipolarité CSU.

TABLEAU 21–6 Problèmes courants liés aux lignes spécialisées *(Suite)*

Symptôme	Problème	Solution
Le lien présente des performances médiocres.	La sortie `pppd debug` indique des erreurs CRC lorsque le trafic est soutenu sur le lien. Votre ligne présente peut-être un problème de synchronisation, dû à des erreurs de configuration entre la compagnie de téléphone et votre réseau.	Contactez l'opérateur téléphonique pour vous assurer que l'option de synchronisation en boucle (loop clocking) est activée. Sur certaines lignes spécialisées non structurées, vous pouvez être amené à mettre en place la synchronisation. Les utilisateurs nord-américains doivent utiliser la synchronisation en boucle.

Diagnostic et résolution des problèmes d'authentification

Le tableau suivant décrit les solutions aux problèmes d'authentification généraux.

TABLEAU 21–7 Problèmes d'authentification généraux

Symptôme	Problème	Solution
La sortie de `pppd debug` indique le message `Peer is not authorized to use remote address` (Pair non autorisé à utiliser l'adresse à distance) *address*.	Vous utilisez l'authentification PAP, et l'adresse IP du pair distant ne se trouve pas dans le fichier `/etc/ppp/pap-secrets`.	Ajoutez un astérisque (*) après l'entrée pour le pair dans le fichier `/etc/ppp/pap-secrets`.
La sortie de `pppd debug` montre que LCP démarre mais s'arrête peu après.	Le mot de passe est peut-être incorrect dans la base de données pour le protocole de sécurité utilisé.	Vérifiez le mot de passe pour le pair dans le fichier `/etc/ppp/pap-secrets` ou `/etc/ppp/chap-secrets`.

◆ ◆ ◆ CHAPITRE 22

Solaris PPP 4.0 (Référence)

Ce chapitre fournit des informations détaillées sur les concepts de Solaris PPP 4.0. Les sujets abordés sont les suivants :

Utilisation des options PPP dans les fichiers et sur la ligne de commande

Solaris PPP 4.0 contient un grand nombre d'options permettant de définir votre configuration PPP. Vous pouvez utiliser ces options dans les fichiers de configuration PPP ou sur la ligne de commande, ou à l'aide à la fois des fichiers et des options de ligne de commande. Cette section contient des informations détaillées sur l'utilisation des options PPP dans les fichiers de configuration et sous forme d'arguments de commandes PPP.

Où définir les options PPP

La configuration de Solaris PPP 4.0 est très souple. Vous pouvez définir les options PPP aux endroits suivants :

- dans les fichiers de configuration PPP ;
- à l'aide des commandes PPP exécutées sur la ligne de commande ;

- à la fois dans ces fichiers et à l'aide de ces commandes.

Le tableau suivant répertorie les fichiers de configuration et les commandes PPP.

TABLEAU 22–1 Récapitulatif des fichiers de configuration et des commandes PPP

Fichier ou commande	Définition	Référence
`/etc/ppp/options`	Fichier contenant les caractéristiques appliquées par défaut à toutes les liaisons PPP du système (si la machine exige des pairs qu'ils s'authentifient, par exemple). En cas d'absence de ce fichier, un utilisateur sans rôle root n'est pas autorisé à utiliser PPP.	"Fichier de configuration `/etc/ppp/options`" à la page 518
`/etc/ppp/options.`*ttyname*	Fichier qui décrit les caractéristiques de toutes les communications transitant par le port série *ttyname*.	"Fichier de configuration `/etc/ppp/options.` *ttyname*" à la page 519
`/etc/ppp/peers`	Répertoire contenant généralement des informations sur les pairs auxquels une machine d'appel sortant se connecte. Les fichiers de ce répertoire sont utilisés avec l'option `call` de la commande `pppd`.	"Spécification des informations relatives à la communication avec le serveur d'appel entrant " à la page 522
`/etc/ppp/peers/`*peer-name*	Fichier contenant les caractéristiques du pair distant *peer-name* . Les caractéristiques habituelles comprennent le numéro de téléphone et le script de discussion du pair distant pour la négociation de la liaison avec le pair.	"Fichier `/etc/ppp/peers/` *peer-name*" à la page 523
`/etc/ppp/pap-secrets`	Fichier contenant les informations d'identification de sécurité nécessaires à l'authentification PAP (Password Authentication Protocol, protocole d'authentification par mot de passe).	"Fichier `/etc/ppp/pap-secrets`" à la page 536
`/etc/ppp/chap-secrets`	Fichier contenant les informations d'identification de sécurité nécessaires à l'authentification CHAP (Challenge-Handshake Authentication Protocol, protocole d'authentification par stimulation-réponse).	"Fichier `/etc/ppp/chap-secrets`" à la page 540
`~/.ppprc`	Fichier résidant dans le répertoire personnel de l'utilisateur PPP, plus souvent utilisé avec les serveurs d'appel entrant. Ce fichier contient des informations spécifiques sur la configuration de chaque utilisateur.	"Configuration de `$HOME/.ppprc` sur un serveur d'appel entrant" à la page 521
`pppd` *options*	Commande et options d'amorce d'une liaison PPP et de description de ses caractéristiques.	"Traitement des options PPP" à la page 515

Pour plus d'informations sur les fichiers PPP, voir la page de manuel pppd(1M). pppd (1M) comprend également les descriptions complètes de toutes les options disponibles pour la commande pppd. Vous trouverez des exemples de modèles pour tous les fichiers de configuration PPP dans /etc/ppp.

Traitement des options PPP

1. Le démon pppd réalise l'analyse suivante :

   Toutes les opérations Solaris PPP 4.0 sont traitées par le démon pppd, qui démarre lorsqu'un utilisateur exécute la commande pppd. Lorsqu'un utilisateur appelle un pair distant, les événements suivants se produisent :

   - /etc/ppp/options
   - $HOME/.ppprc
   - Tous les fichiers ouverts par l'option file ou call dans /etc/ppp/options et $HOME/.ppprc

2. pppd examine la ligne de commande afin de déterminer le périphérique en cours d'utilisation. Le démon n'interprète pas encore les options rencontrées.
3. pppd tente de détecter le périphérique série à utiliser en fonction des critères suivants :
   - Si un périphérique série est indiqué sur la ligne de commande, ou dans un fichier de configuration déjà traité, pppd utilise le nom de ce périphérique.
   - Si aucun périphérique série n'est nommé, pppd recherche l'option notty, pty ou socket sur la ligne de commande. Si l'une de ces options est spécifiée, pppd suppose qu'aucun nom de périphérique n'existe.
   - Dans le cas contraire, si pppd découvre que l'entrée standard est connectée à un tty, le nom du tty est utilisé.
   - Si pppd ne trouve toujours pas de périphérique série, pppd met fin à la connexion et émet un message d'erreur.
4. pppd vérifie alors l'existence du fichier /etc/ppp/options.*ttyname*. Si le fichier est trouvé, pppd l'analyse.
5. pppd traite toutes les options sur la ligne de commande.
6. pppd négocie le protocole LCP (Link Control Protocol) pour configurer la liaison.
7. (Facultatif) Si l'authentification est requise, pppd lit /etc/ppp/pap-secrets ou /etc/ppp/chap-secrets afin d'authentifier le pair opposé.

Le fichier /etc/ppp/peers/*peer-name* est lu lorsque le démon pppd rencontre l'option call *peer-name* sur la ligne de commande ou dans les autres fichiers de configuration.

Fonctionnement des privilèges du fichier de configuration PPP

La configuration Solaris PPP 4.0 inclut le concept de *privilège*. Les privilèges déterminent l'ordre de priorité des options de configuration, en particulier lorsque la même option est appelée à plusieurs emplacements. Toute option appelée d'une source privilégiée est prioritaire sur la même option appelée d'une source non privilégiée.

Privilèges d'utilisateur

Le seul utilisateur privilégié est le superutilisateur (`root`), dont l'ID utilisateur est zéro. Tous les autres utilisateurs ne sont pas privilégiés.

Privilèges de fichier

Les fichiers de configuration suivants sont privilégiés, indépendamment de leur propriété :

- `/etc/ppp/options`
- `/etc/ppp/options.`*ttyname*
- `/etc/ppp/peers/`*peer-name*

Le fichier `$HOME/.ppprc` appartient à l'utilisateur. Les options lues à partir de `$HOME/.ppprc` et de la ligne de commande sont privilégiées si l'utilisateur à l'origine de l'appel de `pppd` est `root` et uniquement à cette condition.

Les arguments qui suivent l'option `file` sont privilégiés.

Effets des privilèges d'option

Certaines options ne fonctionnent que si l'utilisateur ou la source à l'origine de l'appel est privilégié. Les options appelées sur la ligne de commande se voient affecter les privilèges de l'utilisateur qui exécute la commande `pppd`. Ces options ne sont pas privilégiées à moins que l'utilisateur qui appelle la commande `pppd` soit `root`.

Option	Statut	Explication
`domain`	Privilégiée	Privilèges requis pour l'utiliser
`linkname`	Privilégiée	Privilèges requis pour l'utiliser
`noauth`	Privilégiée	Privilèges requis pour l'utiliser
`nopam`	Privilégiée	Privilèges requis pour l'utiliser
`pam`	Privilégiée	Privilèges requis pour l'utiliser
`plugin`	Privilégiée	Privilèges requis pour l'utiliser

Option	Statut	Explication
`privgroup`	Privilégiée	Privilèges requis pour l'utiliser
`allow-ip` *addresses*	Privilégiée	Privilèges requis pour l'utiliser
`name` *hostname*	Privilégiée	Privilèges requis pour l'utiliser
`plink`	Privilégiée	Privilèges requis pour l'utiliser
`noplink`	Privilégiée	Privilèges requis pour l'utiliser
`plumbed`	Privilégiée	Privilèges requis pour l'utiliser
`proxyarp`	Devient privilégiée si `noproxyarp` a été spécifiée	Ne peut pas être ignorée par une utilisation sans privilèges
`defaultroute`	Privilégiée si `nodefaultroute` est définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`disconnect`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`bsdcomp`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	L'utilisateur sans privilège ne peut pas spécifier une taille de code plus grande que celle spécifiée par l'utilisateur privilégié
`deflate`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	L'utilisateur sans privilège ne peut pas spécifier une taille de code plus grande que celle spécifiée par l'utilisateur privilégié
`connect`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`init`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`pty`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
`welcome`	Privilégiée si définie dans un fichier privilégié ou par un utilisateur privilégié	Ne peut pas être ignorée par un utilisateur sans privilège
ttyname	Privilégiée si définie dans un fichier privilégié	Ouverte avec des permissions root quel que soit l'utilisateur qui appelle `pppd`
	Non privilégiée si définie dans un fichier sans privilège	Ouverte avec les privilèges de l'utilisateur qui appelle `pppd`

Fichier de configuration /etc/ppp/options

Le fichier /etc/ppp/options permet de définir des options s'appliquant à l'ensemble des communications PPP sur la machine locale. Le fichier /etc/ppp/options est privilégié. /etc/ppp/options doit appartenir à l'utilisateur root, bien que pppd n'impose pas cette règle. Les options que vous définissez dans /etc/ppp/options sont prioritaires sur les définitions des mêmes options dans tous les autres fichiers et sur la ligne de commande.

Les options classiques que vous pouvez être amené à utiliser dans /etc/ppp/options incluent les suivantes :

- **lock** : permet le verrouillage de fichier de type UUCP.
- **noauth** : indique que la machine n'authentifie pas les appelants.

Remarque – Le logiciel Solaris PPP 4.0 ne comprend aucun fichier /etc/ppp/options par défaut. La commande pppd peut fonctionner sans le fichier /etc/ppp/options . Si une machine ne dispose pas d'un fichier /etc/ppp/options , seul l'utilisateur root peut exécuter la commande pppd sur cette machine.

Vous devez créer le fichier /etc/ppp/options à l'aide d'un éditeur de texte, comme illustré dans la section "Définition des communications sur la ligne série " à la page 451. Si une machine ne nécessite pas d'options globales, créez un fichier /etc/ppp/options vide. Ensuite, l'utilisateur root et les utilisateurs standard peuvent exécuter pppd sur la machine locale.

Modèle /etc/ppp/options.tmpl

Le fichier modèle /etc/ppp/options.tmpl contient des commentaires utiles sur le fichier /etc/ppp/options et trois options courantes du fichier /etc/ppp/options global.

```
lock
nodefaultroute
noproxyarp
```

Option	Définition
lock	Active le verrouillage de fichier de type UUCP
nodefaultroute	Spécifie qu'aucune route par défaut n'est définie
noproxyarp	Rejette proxyarp

Pour utiliser /etc/ppp/options.tmpl en tant que fichier d'options globales, renommez /etc/ppp/options.tmpl en /etc/ppp/options . Ensuite, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/options`

Les sections suivantes contiennent des exemples du fichier `/etc/ppp/options` :

- Pour une machine d'appel sortant, voir "Définition des communications sur la ligne série " à la page 451
- Pour un serveur d'appel entrant, voir "Définition des communications sur la ligne série (serveur d'appel entrant) " à la page 459
- Pour la prise en charge PAP sur un serveur d'appel entrant, voir "Ajout de la prise en charge PAP dans les fichiers de configuration PPP (serveur d'appel entrant)" à la page 473
- Pour la prise en charge PAP sur une machine d'appel sortant, voir "Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)" à la page 476
- Pour la prise en charge CHAP sur un serveur d'appel entrant, reportez-vous à la section "Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (serveur d'appel entrant)" à la page 480.

Fichier de configuration `/etc/ppp/options.` *ttyname*

Vous pouvez configurer les caractéristiques des communications sur la ligne série dans le fichier `/etc/ppp/options.`*ttyname*. `/etc/ppp/options.`*ttyname* est un fichier privilégié, lu par la commande `pppd` après l'analyse des fichiers `/etc/ppp/options` et `$HOME/.pprc` existants. Dans le cas contraire, `pppd` lit `/etc/ppp/options.`*ttyname* après l'analyse `/etc/ppp/options`.

ttyname est utilisé dans le cadre des liaisons de ligne spécialisées et commutées. *ttyname* représente un port série particulier sur une machine, comme `cua/a` ou `cua/b`, à laquelle un modem ou un adaptateur de terminal RNIS peut être connecté.

Au moment d'attribuer un nom au fichier `/etc/ppp/options.`*ttyname*, remplacez la barre oblique (/) dans le nom de périphérique par un point (.). Par exemple, le fichier `options` du périphérique `cua/b` doit être nommé `/etc/ppp/options.cua.b.`.

Remarque – Solaris PPP 4.0 peut fonctionner sans le fichier `/etc/ppp/options.` *ttyname*. Votre serveur peut avoir une seule ligne série dédiée à PPP. En outre, le serveur nécessite peu d'options. Dans ce cas, vous pouvez spécifier les options requises dans un autre fichier de configuration ou sur la ligne de commande.

Utilisation de `/etc/ppp/options.` *ttyname* sur un serveur d'appels entrants

Pour une liaison commutée, vous pouvez choisir de créer des fichiers `/etc/ppp/options.`*ttyname* individuels pour chaque port série sur un serveur d'appels entrants avec modem. Des options standard sont répertoriées ci-dessous :

- Adresse IP requise par le serveur d'appel entrant

  Définissez cette option si vous demandez aux appelants sur le port série *ttyname* d'utiliser une adresse IP particulière. Il est possible que votre espace d'adresse ait un nombre limité d'adresses IP disponibles pour PPP, par rapport au nombre d'appelants éventuels. Dans ce cas, envisagez d'assigner une adresse IP à chaque interface série utilisée pour PPP sur le serveur d'appel entrant. Cette affectation applique l'adressage dynamique pour PPP.

- `asyncmap` *map-value*

  L'option `asyncmap` configure les caractères de contrôle que le modem ou adaptateur de terminal RNIS spécifique ne peut pas recevoir par le biais de la ligne série. Lorsque l'option `xonxoff` est utilisée, `pppd` définit automatiquement l'option asyncmap sur 0xa0000.

  map-value indique, au format hexadécimal, les caractères de contrôle problématiques.

- `init "chat -U -f /etc/ppp/mychat"`

  L'option `init` indique au modem d'initialiser les communications sur la ligne série à l'aide des informations contenues dans la commande `chat -U`. Le modem utilise la chaîne de discussion dans le fichier `/etc/ppp/mychat`.

- Les paramètres de sécurité répertoriés dans la page de manuel `pppd`(1m)

Utilisation de `/etc/ppp/options.` *ttyname* sur une machine sortante.

Dans le cadre d'un système d'appel sortant, vous pouvez soit créer un fichier `/etc/ppp/options.` *ttyname* pour le port série connecté au modem, soit décider de ne pas utiliser `/etc/ppp/options.`*ttyname*.

Remarque – Solaris PPP 4.0 peut fonctionner sans le fichier `/etc/ppp/options.` *ttyname*. Une machine d'appel sortant peut avoir une seule ligne série pour PPP. En outre, la machine d'appel sortant peut nécessiter peu d'options. Vous pouvez spécifier les options requises dans un autre fichier de configuration ou sur la ligne de commande.

Fichier modèle `options.ttya.tmpl`

Le fichier `/etc/ppp/options.ttya.tmpl` contient des commentaires utiles concernant le fichier `/etc/ppp/options.`*tty-name*. Le modèle contient trois options courantes pour le fichier `/etc/ppp/options.` *tty-name*.

```
38400
asyncmap 0xa0000
:192.168.1.1
```

Option	Définition
`38400`	Utilisez ce débit en bauds pour le port ttya.
`asyncmap 0xa0000`	Affectez à asyncmap la valeur 0xa0000 de telle sorte que la machine locale puisse communiquer avec les pairs interrompus.
`:192.168.1.1`	Affectez l'adresse IP 192.168.1.1 à tous les pairs qui lancent un appel sur la liaison.

Pour utiliser `/etc/ppp/options.ttya.tmpl` sur votre site, renommez `/etc/ppp/options.tmpl` en `/etc/ppp/options.` *ttya-name*. Remplacez *ttya-name* par le nom du port série connecté au modem. Puis, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/options.`*ttyname*

Les sections suivantes contiennent des exemples de fichiers `/etc/ppp/options`*ttyname* :

- Pour une machine d'appel sortant, reportez-vous à la section "Définition des communications sur la ligne série " à la page 451.
- Pour un serveur d'appel entrant, voir "Définition des communications sur la ligne série (serveur d'appel entrant) " à la page 459

Configuration des options spécifiques à l'utilisateur

Cette section contient des informations détaillées à propos de la configuration des utilisateurs sur le serveur d'appel entrant.

Configuration de `$HOME/.pprc` sur un serveur d'appel entrant

Le fichier `$HOME/.pprc` est destiné aux utilisateurs qui configurent des options PPP préférées. En tant qu'administrateur, vous pouvez également configurer `$HOME/.pprc` pour les utilisateurs.

Les options de `$HOME/.pprc` sont privilégiées lorsque l'utilisateur qui appelle le fichier est lui-même privilégié, et à cette seule condition.

Lorsqu'un appelant utilise la commande `pppd` pour lancer un appel, `.pprc` est le deuxième fichier que le démon `pppd` vérifie.

La section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 457 contient des instructions sur la configuration de `$HOME/.ppprc` sur le serveur d'appel entrant.

Configuration de `$HOME/.ppprc` sur une machine d'appel sortant

Le fichier `$HOME/.ppprc` n'est pas nécessaire sur la machine d'appel sortant pour que Solaris PPP 4.0 fonctionne correctement. En outre, une machine d'appel sortant ne nécessite pas un fichier `$HOME/.ppprc`, sauf dans des cas particuliers. Créez un ou plusieurs fichiers `.ppprc` si vous effectuez les opérations suivantes :

- Vous autorisez plusieurs utilisateurs ayant des besoins différents en matière de communication à appeler des pairs distants à partir de la même machine. Dans ce cas, créez des fichiers `.ppprc` distincts dans les répertoires personnels de chaque utilisateur devant effectuer un appel sortant.
- Vous devez spécifier des options qui gèrent les problèmes spécifiques à votre liaison, comme la désactivation de la compression Van Jacobson. L'ouvrage *PPP Design, Implementation, and Debugging* de James Carlson et la page de manuel `pppd(1M)` vous aideront à résoudre les problèmes de liaison.

Dans la mesure où le fichier `.ppprc` est plus souvent utilisé dans le cadre de la configuration d'un serveur d'appel entrant, reportez-vous à la section “Configuration des utilisateurs du serveur d'appel entrant ” à la page 458 pour obtenir les instructions de configuration de `.ppprc`.

Spécification des informations relatives à la communication avec le serveur d'appel entrant

Pour communiquer avec un serveur d'appel entrant, vous devez rassembler des informations le concernant. Modifiez ensuite un petit nombre de fichiers. Plus concrètement, vous devez configurer les exigences en matière de communication de tous les serveurs d'appel entrant que la machine d'appel sortant doit appeler. Vous pouvez spécifier des options sur un serveur d'appel entrant, tel que le numéro de téléphone du FAI, dans le fichier `/etc/ppp/options.`*ttyname*. Cependant, le meilleur emplacement pour configurer les informations de pair est le fichier `/etc/ppp/peers/`*peer-name*.

Fichier `/etc/ppp/peers/` *peer-name*

Remarque – Le fichier `/etc/ppp/peers/`*peer-name* n'est pas nécessaire sur la machine d'appel sortant pour que Solaris PPP 4.0 fonctionne correctement.

Utilisez le fichier `/etc/ppp/peers/`*peer-name* pour fournir des informations relatives à la communication avec un pair particulier. Le fichier `/etc/ppp/peers/` *peer-name* autorise les utilisateurs ordinaires à appeler des options privilégiées présélectionnées qu'ils ne sont pas autorisés à définir.

Par exemple, un utilisateur sans privilège ne peut pas ignorer l'option `noauth` si `noauth` est spécifiée dans le fichier `/etc/ppp/peers/` *peer-name*. Supposons que l'utilisateur souhaite configurer une liaison à `peerB`, qui ne fournit pas d'informations d'authentification. En tant que superutilisateur, vous pouvez créer un fichier `/etc/ppp/peers/peerB` qui comprend l'option `noauth`. L'option `noauth` indique que la machine locale n'authentifie pas les appels de `peerB`.

Le démon `pppd` lit le fichier `/etc/ppp/peers/` *peer-name* lorsque `pppd` rencontre l'option suivante :

`call` *peer-name*

Vous pouvez créer un fichier `/etc/ppp/peers/`*peer-name* pour chaque pair cible avec lequel la machine d'appel sortant doit communiquer. Cette pratique est particulièrement utile pour autoriser les utilisateurs ordinaires à appeler les liaisons d'appel sortant spécifiques sans avoir besoin des privilèges root.

Les options standard que vous spécifiez dans le fichier `/etc/ppp/peers/`*peer-name* sont les suivantes :

- `user` *user-name*

  Fournissez *user-name* au serveur d'appel entrant comme nom de connexion à la machine d'appel sortant, lors de l'authentification avec PAP ou CHAP.

- `remotename` *peer-name*

  Utilisez *peer-name* comme nom de la machine d'appel entrant. L'option `remotename` est utilisée avec l'authentification PAP ou CHAP lors de l'analyse des fichiers `/etc/ppp/pap-secrets` ou `/etc/ppp/chap-secrets`.

- `connect "chat` *chat_script* `..."`

  Ouvrez la communication vers le serveur d'appel entrant à l'aide des instructions fournies dans le script de discussion.

- `noauth`

  N'authentifiez pas le pair *peer-name* lors de l'initialisation des communications.

- `noipdefault`

Définissez la première adresse IP utilisée dans la négociation avec le pair sur 0.0.0.0. Utilisez `noipdefault` lors de la configuration d'une liaison vers la plupart des fournisseurs d'accès Internet pour faciliter la négociation IPCP entre les pairs.

- `defaultroute`

  Installez une route IPv4 par défaut lorsque l'adresse IP est établie sur la liaison.

La page de manuel pppd(1M) contient plus d'options qui peuvent s'appliquer à un pair cible spécifique.

Fichier modèle `/etc/ppp/peers/myisp.tmpl`

Le fichier `/etc/ppp/peers/myisp.tmpl` contient des commentaires utiles concernant le fichier `/etc/ppp/peers/`*peer-name*. Le modèle se termine par des options courantes que vous pouvez utiliser pour un fichier `/etc/ppp/peers/`*peer-name* :

```
connect "/usr/bin/chat -f /etc/ppp/myisp-chat"
user myname
remotename myisp
noauth
noipdefault
defaultroute
updetach
noccp
```

Option	Définition
`connect "/usr/bin/chat -f /etc/ppp/myisp-chat"`	Appelez le pair à l'aide du script de discussion `/etc/ppp/myisp-chat`.
`user myname`	Utilisez ce nom de compte pour la machine locale. `myname` est le nom de cette machine dans le fichier `/etc/ppp/pap-secrets` du pair.
`remotename myisp`	Reconnaissez `myisp` comme le nom du pair dans le fichier `/etc/ppp/pap-secrets` de la machine locale.
`noauth`	N'exigez pas des pairs qui effectuent des appels qu'ils fournissent des informations d'authentification.
`noipdefault`	N'utilisez pas une adresse IP par défaut pour la machine locale.
`defaultroute`	Utilisez la route par défaut qui est affectée à la machine locale.
`updetach`	Consignez les erreurs dans les fichiers journaux PPP, plutôt que sur la sortie standard.
`noccp`	N'utilisez pas la compression CCP.

Pour utiliser `/etc/ppp/peers/myisp.tmpl` sur votre site, renommez `/etc/ppp/peers/myisp.tmpl` en `/etc/ppp/peers/`. Remplacez *peer-name* par le nom du pair à appeler. Puis, modifiez le contenu du fichier en fonction des besoins de votre site.

Où trouver des exemples des fichiers `/etc/ppp/peers/`*peer-name*

Les sections suivantes contiennent des exemples des fichiers `/etc/ppp/peers/`*peer-name* :

- Pour une machine d'appel sortant, voir "Définition de la connexion à un pair donné" à la page 453.
- Pour une machine locale sur une ligne spécialisée, voir "Configuration d'une machine sur une ligne spécialisée " à la page 466.
- Pour la prise en charge de l'authentification PAP sur une machine d'appel sortant, voir "Ajout de la prise en charge PAP dans les fichiers de configuration PPP (machine d'appel sortant)" à la page 476
- Pour la prise en charge de l'authentification CHAP sur une machine d'appel sortant, voir "Ajout de la prise en charge CHAP dans les fichiers de configuration PPP (machine d'appel sortant)" à la page 483
- Pour la prise en charge du protocole PPPoE sur un système client, voir "Configuration du client PPPoE" à la page 486.

Configuration de la vitesse du modem pour une liaison commutée

Le problème principal posé par la configuration du modem est de désigner la vitesse à laquelle le modem doit fonctionner. Les recommandations suivantes s'appliquent aux modems utilisés avec les ordinateurs Sun Microsystems :

- Anciens systèmes SPARC : vérifiez la documentation du matériel qui accompagne le système. De nombreuses machines SPARCstation exigent que la vitesse du modem soit inférieure à 38 400 bps.
- Machines UltraSPARC : définissez la vitesse du modem sur 115 200 bps, ce qui s'avère utile avec les modems modernes et suffisamment rapide pour une liaison commutée. Si vous prévoyez d'utiliser un adaptateur de terminal RNIS à double canal avec compression, il vous faudra augmenter la vitesse du modem. La limite sur les machines UltraSPARC est de 460 800 bps pour une liaison asynchrone.

Pour une *machine d'appel sortant*, définissez la vitesse du modem dans les fichiers de configuration PPP, tels que `/etc/ppp/peers/` *peer-name* ou spécifiez la vitesse en tant qu'option de la commande `pppd`.

Pour un *serveur d'appel entrant*, vous devez définir la vitesse à l'aide de l'utilitaire `ttymon` ou de la console de gestion Solaris, comme décrit dans la section "Configuration des périphériques sur le serveur d'appel entrant " à la page 456.

Définition de la conversation sur la liaison commutée

La machine d'appel sortant et son pair distant communiquent via la liaison PPP, par négociation et échange de diverses instructions. Lors de la configuration d'une machine d'appel sortant, vous devez déterminer les instructions requises par les modems locaux et distants. Ensuite, vous créez un fichier appelé un script de discussion, qui contient ces instructions. Cette section contient des informations relatives à la configuration des modems et à la création des scripts de discussion.

Contenu du script de discussion

Chaque pair distant auquel la machine d'appel sortant doit se connecter a probablement besoin de son propre script de discussion.

Remarque – Les scripts de discussion sont habituellement utilisés sur les liaisons commutées uniquement. Les liaisons de ligne spécialisées n'utilisent pas les scripts de discussion à moins qu'elles ne comportent une interface asynchrone qui nécessite une configuration de démarrage.

Le contenu du script de discussion est déterminé par les exigences de votre modem ou adaptateur de terminal RNIS et le pair distant. Ce contenu s'affiche sous la forme d'un jeu de chaînes expect-send. La machine d'appel sortant et ses pairs distants échangent ces chaînes dans le cadre du processus d'initialisation des communications.

Une chaîne *expect* contient des caractères que la machine hôte d'appel sortant attend de recevoir du pair distant pour amorcer le dialogue. Une chaîne *send* contient des caractères que la machine d'appel sortant envoie au pair distant après la réception de la chaîne expect.

Le script de discussion contient habituellement les informations suivantes :

- Des commandes de modem, souvent appelées *commandes AT*, qui permettent au modem de transmettre des données par téléphone
- Le numéro de téléphone du pair cible

  Ce numéro de téléphone peut être le numéro requis par votre fournisseur d'accès à Internet, un serveur d'appel entrant sur un site d'entreprise ou une machine spécifique.
- Le délai d'expiration, si nécessaire
- La séquence de connexion attendue du pair distant

- La séquence de connexion envoyée par la machine d'appel sortant

Exemples de scripts de discussion

Cette section contient des scripts de discussion que vous pouvez utiliser comme référence pour créer vos propres scripts de discussion. Le manuel du fabricant de votre modem et les informations fournies par votre fournisseur d'accès Internet et d'autres hôtes cible contiennent les exigences du modem et de vos pairs cible en matière de discussion. En outre, de nombreux sites Web PPP proposent des exemples de scripts de discussion.

Script de discussion de modem de base

Le script de discussion de base ci-après peut vous servir de modèle lorsque vous créerez vos propres scripts de discussion.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myserver\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
ogin: pppuser
ssword: \q\U
% pppd
```

Le tableau suivant décrit le contenu du script de discussion.

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem signale `ABORT 'NO CARRIER'` lors de la numérotation. L'échec de la numérotation ou de la négociation du modem génère généralement ce message.
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`"" AT&F1M0&M5S2=255`	`M0` : désactivation du haut-parleur pendant la connexion. `&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES “+++”
`SAY "Calling myserver\n"`	Affichage du message `Calling myserver` sur la machine locale.

Contenu du script	Explication
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`ogin: pppuser`	Connexion au pair à l'aide d'une connexion de type UNIX Indiquer le nom d'utilisateur `pppuser`.
`ssword: \q\U`	`\q` : ne pas se connecter si le débogage est effectué avec l'option `-v`. `\U` : insérer à cet emplacement le contenu de la chaîne qui suit `-U`, spécifié sur la ligne de commande. Généralement, la chaîne contient le mot de passe.
`% pppd`	Attendre l'invite shell % et exécuter la commande `pppd`.

Modèle de script de discussion `/etc/ppp/myisp-chat.tmpl`

Cette version inclut le modèle `/etc/ppp/myisp-chat.tmpl`, que vous pouvez modifier pour l'utiliser sur votre site. Le modèle `/etc/ppp/myisp-chat.tmpl` ressemble au script de discussion de modem de base, à ceci près qu'il n'inclut pas une séquence de connexion.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
""      "AT&F1"
OK      "AT&C1&D2"
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
```

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER`	Abandon de la transmission si le modem signale `ABORT 'NO CARRIER'` lors de la numérotation. L'échec de la numérotation ou de la négociation du modem génère généralement ce message.
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`"" "AT&F1"`	Rétablissement des valeurs par défaut du modem.

Contenu du script	Explication
`OK "AT&C1&D2"`	Réinitialisation du modem afin que, pour &C1, le DCD du modem suive la porteuse. Si le côté distant raccroche le téléphone pour une raison quelconque, le DCD diminue. Pour &D2, la transition DTR décroissante fait raccrocher le modem.
`SAY "Calling myisp\n"`	Affichage du message “Calling myisp” sur la machine locale.
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.

Script de discussion du modem pour appeler le fournisseur d'accès Internet

Utilisez le script de discussion suivant comme modèle pour appeler un fournisseur d'accès à Internet (FAI) à partir d'une machine d'appel sortant équipée d'un modem U.S. Robotics Courier.

```
ABORT   BUSY
ABORT   'NO CARRIER'
REPORT  CONNECT
TIMEOUT 10
"" AT&F1M0&M5S2=255
SAY     "Calling myisp\n"
TIMEOUT 60
OK      "ATDT1-123-555-1212"
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

Le tableau ci-dessous décrit le contenu du script de discussion.

Contenu du script	Explication
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.

Contenu du script	Explication
`"" AT&F1M0M0M0M0&M5S2=255`	`M0` : désactivation du haut-parleur pendant la connexion. `&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES “+++”
`SAY "Calling myisp\n"`	Affichage du message `Calling myisp` sur la machine locale.
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK "ATDT1-123-555-1212"`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.
`\r \d\c`	Patienter jusqu'à la fin du message `CONNECT`.
SAY “Connected; running PPP\n”	Affichage du message d'informations `Connected; running PPP` sur la machine locale.

Script de discussion de base amélioré pour une connexion de type UNIX

Le script de discussion suivant est un script de base amélioré pour appeler un pair Solaris distant ou un autre pair de type UNIX. Ce script de discussion est utilisé à la section “Création des instructions pour l'appel d'un pair” à la page 452.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&F1&M5S2=255
TIMEOUT 60
OK ATDT1-123-555-1234
CONNECT \c
SAY "Connected; logging in.\n"
TIMEOUT 5
ogin:--ogin: pppuser
TIMEOUT 20
ABORT 'ogin incorrect'
ssword: \qmypassword
"% " \c
SAY "Logged in.  Starting PPP on peer system.\n"
ABORT 'not found'
"" "exec pppd"
~ \c
```

Le tableau ci-dessous décrit les paramètres du script de discussion.

Contenu du script	Explication
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes. La réponse du modem doit être immédiate.
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT ERROR`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`"" AT&F1&M5S2=255`	`&M5` : le modem requiert le contrôle d'erreur. `S2=255` : désactivation de la séquence d'interruption TIES "+++"
`TIMEOUT 60`	Réinitialisation du délai d'attente de 60 secondes pour laisser plus de temps à la négociation de liaison.
`OK ATDT1-123-555-1234`	Appel du pair distant à l'aide du numéro de téléphone 123-555-1212.
`CONNECT \c`	Attendre que le modem du pair opposé envoie le message `CONNECT`.
`SAY "Connected; logging in.\n"`	Affichage du message d'informations `Connected; logging in` sur l'état de l'utilisateur.
`TIMEOUT 5`	Modification du délai d'expiration pour activer l'affichage rapide de l'invite de connexion.
`ogin:--ogin: pppuser`	Attendre l'invite de connexion. Si l'invite n'est pas reçue, envoyer un RETURN et attendre. Envoyer ensuite le nom d'utilisateur `pppuser` au pair. La séquence qui suit est désignée par la plupart des FAI en tant que connexion PAP. Cependant, la connexion PAP n'est pas liée de quelque façon que ce soit à l'authentification PAP.
`TIMEOUT 20`	Remplacer la valeur du délai d'expiration par 20 secondes pour permettre une vérification lente du mot de passe.
`ssword: \qmysecrethere`	Attendre l'invite de mot de passe du pair. À la réception de l'invite, envoyer le mot de passe `\qmysecrethere`. L'option `\q` empêche l'écriture du mot de passe sur les fichiers journaux du système.
`"% " \c`	Attendre l'invite shell du pair. Le script de discussion utilise le shell C. Modifier cette valeur si l'utilisateur préfère se connecter avec un shell différent.
`SAY "Logged in. Starting PPP on peer system.\n"`	Affichage du message d'informations `Logged in. Starting PPP on peer system` pour donner l'état de l'utilisateur.

Contenu du script	Explication
`ABORT 'not found'`	Abandon de la transmission si le shell rencontre des erreurs.
`"" "exec pppd"`	Démarrage de `pppd` sur le pair.
`~ \c`	Attendre que PPP démarre sur le pair.

Le démarrage PPP juste après `CONNECT \c` est souvent appelé *connexion PAP* par les fournisseurs d'accès Internet (FAI) bien que la connexion PAP ne fasse pas partie de l'authentification PAP.

L'expression `ogin:--ogin: pppuser` indique au modem d'envoyer le nom d'utilisateur `pppuser` en réponse à l'invite de connexion du serveur d'appel entrant. `pppuser` est un nom de compte utilisateur PPP créé spécialement pour l'utilisateur distant `user1` sur le serveur d'appel entrant. Pour obtenir des instructions sur la création de comptes utilisateur PPP sur les serveurs d'appel entrant, reportez-vous à la section "Configuration des utilisateurs du serveur d'appel entrant " à la page 458.

Script de discussion pour adaptateur de terminal RNIS externe

Le script de discussion suivant sert à effectuer un appel à partir d'une machine d'appel sortant équipée d'un adaptateur de terminal RNIS ZyXEL omni.net.

```
SAY "Calling the peer\n"
TIMEOUT 10
ABORT BUSY
ABORT 'NO CARRIER'
ABORT ERROR
REPORT CONNECT
"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255
OK ATDI18882638234
CONNECT \c
\r \d\c
SAY "Connected; running PPP\n"
```

Le tableau ci-dessous décrit les paramètres du script de discussion.

Contenu du script	Explication
`SAY "Calling the peer"`	Affichage de ce message sur l'écran de la machine d'appel sortant.
`TIMEOUT 10`	Définition du délai d'attente initial sur 10 secondes.
`ABORT BUSY`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`ABORT 'NO CARRIER'`	Abandon de la transmission si le modem reçoit ce message du pair opposé

Contenu du script	Explication
`ABORT ERROR`	Abandon de la transmission si le modem reçoit ce message du pair opposé
`REPORT CONNECT`	Récupération de la chaîne `CONNECT` à partir du modem. Impression de la chaîne.
`"" AT&FB40S83.7=1&K44&J3X7S61.3=1S0=0S2=255`	Les lettres dans cette ligne ont la signification suivante : ■ `&F` : utiliser les valeurs d'usine ■ `B40` : effectuer une conversion PPP asynchrone ■ `S83.7=1` : utiliser les données sur support vocal ■ `&45` : activer la compression CCP ■ `&J3` : activer MP ■ `X7` : signaler les vitesses côté DCE ■ `S61.3=1` : utiliser la fragmentation des paquets ■ `S0=0` : aucune réponse automatique ■ `S2=255` : désactiver l'échappement TIES
`OK ATDI18882638234`	Réalisation d'un appel RNIS. Pour les liaisons multiples, le deuxième appel est passé au même numéro de téléphone, ce que la plupart des FAI requièrent habituellement. Si le pair distant requiert un deuxième numéro de téléphone différent, ajoutez "+ *nnnn*.". *nnnn* représente le deuxième numéro de téléphone.
`CONNECT \c`	Patientez jusqu'à ce que le message `CONNECT` du modem du pair opposé s'affiche.
`\r \d\c`	Patienter jusqu'à la fin du message `CONNECT`.
`SAY "Connected; running PPP\n"`	Affichage de ce message sur l'écran de la machine d'appel sortant.

Pour obtenir la description des options et d'autres informations détaillées sur le script de discussion, reportez-vous à la page de manuel `chat(1M)`. Pour obtenir une explication sur les chaînes expect-send, reportez-vous à la section "Champ Chat-Script du fichier `/etc/uucp/Systems`" à la page 581.

Pour d'autres exemples de scripts de discussion

Certains sites web offrent des exemples et leur assistance pour vous permettre de créer vos scripts de discussion. Visitez, par exemple, .http://ppp.samba.org/ppp/index.html .

Appel du script de discussion

Pour appeler un script de discussion, utilisez l'option `connect`. Vous pouvez utiliser `connect "chat ..."` dans tous les fichiers de configuration PPP ou sur la ligne de commande.

Les scripts de discussion ne sont pas exécutables, mais le programme appelé par `connect` doit l'être. L'utilitaire de discussion peut servir de programme devant être appelé par `connect`. Dans cet exemple, si vous stockez le script de discussion dans un fichier externe à l'aide de l'option `-f`, votre fichier de script de discussion n'est pas exécutable.

Le programme `chat` décrit dans `chat`(1m) exécute le script de discussion réel. Le démon `pppd` appelle le programme `chat` chaque fois que `pppd` rencontre l'option `connect "chat ..."`.

Remarque – Vous pouvez utiliser n'importe quel programme externe, tel que `Perl` ou `Tcl`, afin de créer des scripts de discussion perfectionnés. L'utilitaire `chat` est fourni pour votre convenance.

▼ Appel d'un script de discussion (tâche)

1 **Créez le script de discussion sous forme de fichier ASCII.**

2 **Appelez le script de discussion dans un fichier de configuration PPP à l'aide de la syntaxe suivante :**

```
connect 'chat  -f /etc/ppp/chatfile'
```

L'indicateur `-f` indique qu'un nom de fichier doit suivre. */etc/ppp/chatfile* représente le nom du fichier de discussion.

3 **Accordez l'autorisation de lecture du fichier de discussion externe à l'utilisateur qui exécute la commande `pppd`.**

Attention – Le programme de discussion est toujours exécuté avec les privilèges de l'utilisateur, même si l'option `connect 'chat ...'` est appelée à partir d'une source privilégiée. Par conséquent, un autre fichier de discussion lu avec l'option `-f` doit être lisible par l'utilisateur à l'origine de l'appel. Ce privilège risque de poser un problème de sécurité si le script de discussion contient des mots de passe ou d'autres informations confidentielles.

Exemple 22–1 Script de discussion en ligne

Vous pouvez placer l'intégralité de la conversation du script de discussion sur une seule ligne, comme dans l'exemple suivant :

```
connect 'chat "" "AT&F1" OK ATDT5551212 CONNECT "\c"'
```

Le script de discussion complet suit le mot-clé `chat`. Le script se termine par `"\c"'`. Vous utilisez cette forme dans tous les fichiers de configuration PPP ou sur la ligne de commande en tant qu'argument de `pppd` .

Informations supplémentaires

Script de discussion dans un fichier externe

Si le script de discussion nécessaire à un pair donné est long ou complexe, vous pouvez envisager de le créer sous forme de fichier séparé. Les fichiers de discussion externes sont faciles à gérer et à documenter. Vous pouvez ajouter des commentaires au fichier de discussion en les faisant précéder du signe dièse (#).

La section "Création des instructions pour l'appel d'un pair" à la page 452 présente la procédure d'utilisation d'un script de discussion contenu dans un fichier externe.

Création d'un fichier de discussion exécutable

Vous pouvez créer un fichier de discussion à exécuter automatiquement à l'initialisation de la liaison commutée. Ainsi, vous pouvez exécuter des commandes supplémentaires au cours de l'initialisation de la liaison, comme `stty` pour les paramètres de parité, outre les commandes contenues dans un script de discussion classique.

Ce script de discussion exécutable se connecte à un système UNIX de type ancien qui nécessite 7 bits de même parité. Le système passe alors à 8 bits sans parité lors de l'exécution de PPP.

```
#!/bin/sh
chat "" "AT&F1" OK "ATDT555-1212" CONNECT "\c"
stty evenp
chat ogin: pppuser ssword: "\q\U" % "exec pppd"
stty -evenp
```

▼ Création d'un programme de discussion exécutable

1. **Utilisez votre éditeur de texte pour créer un programme de discussion exécutable, comme dans l'exemple précédent.**

2. **Rendez le programme de discussion exécutable.**

   ```
   # chmod +x /etc/ppp/chatprogram
   ```

3. **Appelez le programme de discussion.**

   ```
   connect /etc/ppp/chatprogram
   ```

   Il n'est pas nécessaire que les programmes de discussion résident dans le système de fichiers `/etc/ppp`. Vous pouvez stocker les programmes de discussion dans n'importe quel emplacement.

Authentification des appelants sur une liaison

Cette section explique le fonctionnement des protocoles d'authentification PPP et décrit les bases de données qui leur sont associées.

Protocole d'authentification par mot de passe (PAP)

L'authentification PAP est similaire dans son fonctionnement au programme `login` d'UNIX, à ceci près que PAP n'accorde pas l'accès shell à l'utilisateur. PAP utilise les fichiers de configuration PPP et la base de données PAP sous forme de fichier `/etc/ppp/pap-secrets` pour configurer l'authentification. PAP utilise également `/etc/ppp/pap-secrets` pour définir les informations d'identification de sécurité PAP. Les informations d'identification se composent d'un nom de pair, “nom d'utilisateur” dans le jargon PAP, et d'un mot de passe. Les informations d'identification PAP contiennent également les informations associées à chaque appelant autorisé à se connecter à la machine locale. Les noms d'utilisateur et mots de passe PAP peuvent être identiques aux noms d'utilisateur et mots de passe UNIX de la base de données de mots de passe, ou bien différents.

Fichier `/etc/ppp/pap-secrets`

La base de données PAP est mise en œuvre dans le fichier `/etc/ppp/pap-secrets`. Pour que l'authentification réussisse, les informations d'identification PAP des machines situées des deux côtés de la liaison PPP doivent être correctement configurées dans les fichiers `/etc/ppp/pap-secrets`. L'appelant (l'authentifié) fournit les informations d'identification dans les colonnes `user` et `password` du fichier `/etc/ppp/pap-secrets` ou dans le fichier `+ua` obsolète. Le serveur (l'authentificateur) valide les informations d'identification par rapport aux informations contenues dans le fichier `/etc/ppp/pap-secrets`, par l'intermédiaire de la base de données UNIX `passwd` ou de l'utilitaire PAM.

Le fichier `/etc/ppp/pap-secrets` présente la syntaxe suivante.

```
myclient ISP-server mypassword *
```

Signification des paramètres :

`myclient`	Nom d'utilisateur PAP de l'appelant. Ce nom est souvent identique au nom d'utilisateur UNIX de l'appelant, en particulier si le serveur d'appel entrant utilise l'option `login` de PAP.
`ISP-server`	Nom de la machine distante, souvent un serveur d'appel entrant.
`mypassword`	Mot de passe PAP de l'appelant.
*	Adresse IP associée à l'appelant. L'astérisque (*) représente n'importe quelle adresse IP.

Création de mots de passe PAP

Les mots de passe PAP sont envoyés via la liaison *en clair*, c'est-à-dire dans un format ASCII lisible. Pour l'appelant (l'authentifié), le mot de passe PAP doit être stocké en clair dans l'un des emplacements suivants :

- dans `/etc/ppp/pap-secrets` ;
- dans un autre fichier externe ;
- dans un tube nommé par le biais de la fonction `pap-secrets @` ;
- en tant qu'option de `pppd`, sur la ligne de commande ou dans un fichier de configuration PPP ;
- par l'intermédiaire du fichier `+ua`.

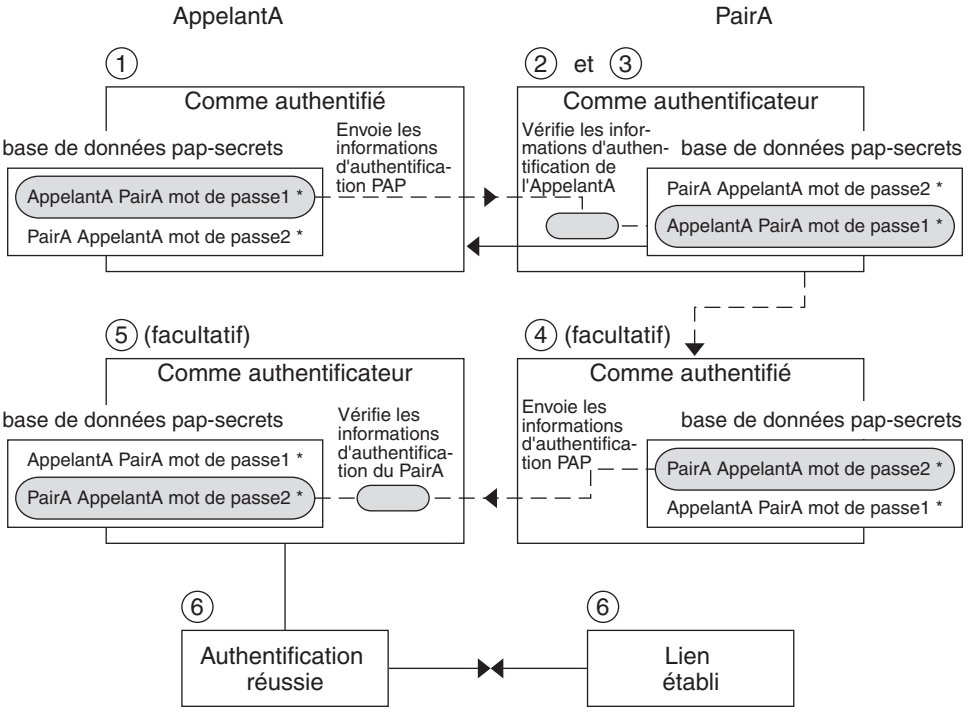
Sur le serveur (l'authentificateur), vous pouvez masquer le mot de passe PAP en effectuant l'une des opérations suivantes :

- Spécifiez `papcrypt` et utilisez des mots de passe hachés par `crypt`(3C) dans le fichier `pap-secrets`.
- Spécifiez l'option `login` sur `pppd` et omettez le mot de passe dans le fichier `pap-secrets` en plaçant des guillemets doubles ("") dans la colonne de mot de passe. Dans ce cas, l'authentification est effectuée par l'intermédiaire de la base de données passwd UNIX ou du mécanisme `pam`(3pam).

Description de l'authentification PAP

L'authentification PAP se déroule dans l'ordre indiqué ci-dessous.

FIGURE 22–1 Processus d'authentification PAP



1. L'appelant (l'authentifié) appelle le pair distant (authentificateur) et fournit ses nom d'utilisateur et mot de passe PAP dans le cadre de la négociation de liaison.
2. Le pair vérifie l'identité de l'appelant dans son fichier `/etc/ppp/pap-secrets`. S'il utilise l'option `login` de PAP, le pair vérifie le nom d'utilisateur et le mot de passe de l'appelant dans sa base de données de mots de passe.
3. Si l'authentification réussit, le pair continue la négociation de liaison avec l'appelant. Si l'authentification échoue, la liaison est interrompue.
4. (Facultatif) Si l'appelant authentifie les réponses de pairs distants, ceux-ci doivent lui envoyer leurs informations d'identification PAP. Ainsi, le pair distant devient l'authentifié et l'appelant l'authentificateur.
5. (Facultatif) L'appelant d'origine lit son fichier `/etc/ppp/pap-secrets` pour vérifier l'identité du pair distant.

Remarque – Si l'appelant d'origine ne nécessite pas les informations d'identification du pair distant, l'étape 1 et l'étape 4 se déroulent en parallèle.

Si le pair est authentifié, la négociation se poursuit. Dans le cas contraire, la liaison est interrompue.

6. La négociation entre l'appelant et le pair se poursuit jusqu'à ce que la liaison soit finalement établie.

Utilisation de l'option `login` avec `/etc/ppp/pap-secrets`

Vous pouvez ajouter l'option `login` pour authentifier les informations d'identification PAP dans les fichiers de configuration PPP. Lorsque vous spécifiez l'option `login` dans `/etc/ppp/options` par exemple, `pppd` vérifie que les informations d'identification PAP de l'appelant existent dans la base de données de mots de passe. L'exemple suivant représente le format d'un fichier `/etc/ppp/pap-secrets` avec l'option `login`.

```
joe    *  ""  *
sally  *  ""  *
sue    *  ""  *
```

Signification des paramètres :

Appelant	`joe`, `sally` et `sue` sont les noms des appelants autorisés.
Serveur	L'astérisque (*) indique que tous les noms de serveur sont valides. L'option `name` n'est pas obligatoire dans les fichiers de configuration PPP.
Mot de passe	Les guillemets doubles indiquent les mots de passe valides. Si un mot de passe figure dans cette colonne, le mot de passe du pair doit correspondre à la fois au mot de passe PAP et au mot de passe dans la base de données `passwd` UNIX.
Adresses IP	L'astérisque (*) indique que toutes les adresses IP sont valides.

Protocole CHAP (Challenge-Handshake Authentication Protocol)

L'authentification CHAP utilise la notion de *défi* et de *réponse*, ce qui signifie que le pair (l'authentificateur) défit l'appelant (l'authentifié) de prouver son identité. Le défi comprend un nombre aléatoire et un ID unique généré par l'authentificateur. L'appelant doit utiliser l'ID, le nombre aléatoire et ses informations d'identification de sécurité CHAP pour générer la réponse adéquate (protocole de transfert) à envoyer au pair.

Les informations d'identification de sécurité CHAP incluent un nom d'utilisateur CHAP et un “secret” CHAP. Le secret CHAP est une chaîne arbitraire, connue à la fois de l'appelant et du pair avant qu'ils ne négocient une liaison PPP. Vous pouvez configurer les informations d'identification de sécurité CHAP dans la base de données CHAP, `/etc/ppp/chap-secrets`.

Fichier `/etc/ppp/chap-secrets`

La base de données CHAP est mise en œuvre dans le fichier `/etc/ppp/chap-secrets`. Les machines de chaque côté de la liaison PPP doivent disposer de leurs informations d'identification CHAP mutuelles dans leurs fichiers `/etc/ppp/chap-secrets` pour que l'authentification réussisse.

Remarque – Contrairement à PAP, le secret partagé doit être en clair sur les deux pairs. Vous ne pouvez pas utiliser crypt, PAM ni l'option login PPP avec le protocole CHAP.

La syntaxe du fichier `/etc/ppp/chap-secrets` est la suivante.

```
myclient myserver secret5748 *
```

Signification des paramètres :

`myclient` Nom d'utilisateur CHAP de l'appelant. Ce nom peut être identique au nom d'utilisateur UNIX de l'appelant, ou bien différent.

`myserver` Nom de la machine distante, souvent un serveur d'appel entrant.

`secret5748` Secret CHAP de l'appelant.

Remarque – Contrairement aux mots de passe PAP, les secrets CHAP ne sont jamais envoyés via la liaison. Ils sont plutôt utilisés lorsque les machines locales calculent la réponse.

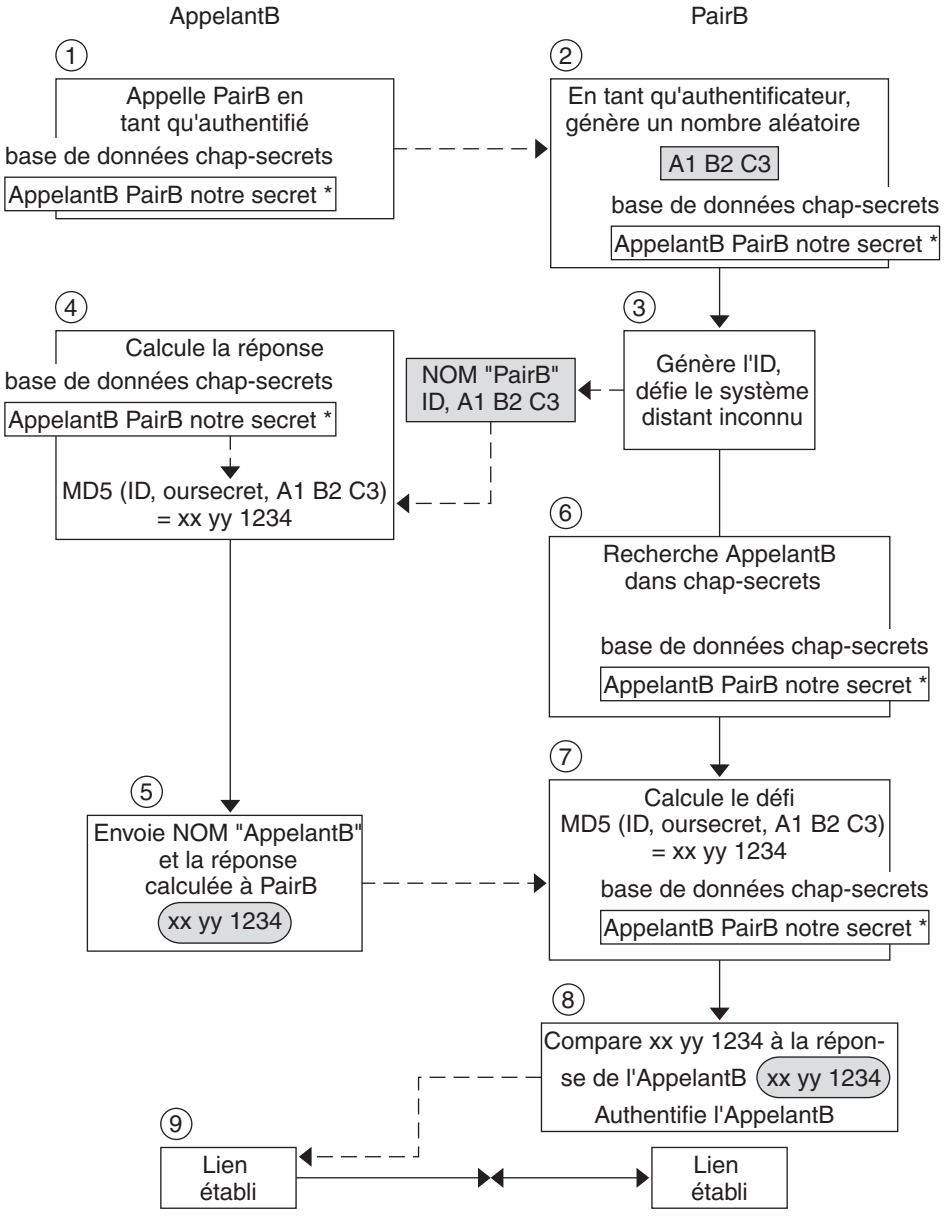
---

* Adresse IP associée à l'appelant. L'astérisque (*) représente n'importe quelle adresse IP.

Description de l'authentification CHAP

L'authentification CHAP se déroule dans l'ordre indiqué ci-dessous.

FIGURE 22–2 Ordre de l'authentification CHAP



1. Deux pairs sur le point d'initialiser la communication conviennent d'un secret à utiliser pour l'authentification lors de la négociation d'une liaison PPP.

2. Les administrateurs des deux machines ajoutent le secret, les noms d'utilisateur CHAP et d'autres informations d'identification CHAP dans la base de données `/etc/ppp/chap-secrets` de leur machine respective.
3. L'appelant (l'authentifié) appelle le pair distant (l'authentificateur).
4. L'authentificateur génère un numéro aléatoire et un ID, et envoie ces données à l'authentifié sous forme de défi.
5. L'authentifié recherche le nom et le secret du pair dans sa base de données `/etc/ppp/chap-secrets`.
6. L'authentifié calcule une réponse en appliquant l'algorithme de calcul MD5 au secret et au défi de numéro aléatoire du pair. Ensuite, l'authentifié envoie pour réponse les résultats à l'authentificateur.
7. L'authentificateur recherche le nom et le secret de l'authentifié dans sa base de données `/etc/ppp/chap-secrets`,
8. L'authentificateur calcule son propre chiffre en appliquant MD5 au numéro généré en tant que défi et secret pour l'authentifié dans la base de données `/etc/ppp/chap-secrets`.
9. L'authentificateur compare les résultats avec la réponse de l'appelant. Si les deux valeurs sont identiques, le pair a authentifié l'appelant et la négociation de liaison se poursuit. Dans le cas contraire, la liaison est interrompue.

Création d'un schéma d'adressage IP pour appelants

Envisagez de créer une ou plusieurs adresses IP pour tous les appels entrants au lieu d'affecter une adresse IP unique à chaque utilisateur distant. Les adresses IP dédiées sont particulièrement importantes si le nombre d'appelants dépasse le nombre de ports série et de modems sur le serveur d'appel entrant. Vous pouvez mettre en place des scénarios différents, en fonction des besoins de votre site. En outre, les scénarios ne s'excluent pas mutuellement.

Affectation des adresses IP dynamiques aux appelants

L'adressage dynamique implique l'affectation de l'adresse IP définie dans le fichier `/etc/ppp/options.` *ttyname*. L'adressage dynamique s'effectue sur chaque port série. À l'arrivée d'un appel sur une ligne série, l'appelant reçoit l'adresse IP dans le fichier `/etc/ppp/options.`*ttyname* de l'interface série de l'appel.

Par exemple, supposons qu'un serveur d'appel entrant dispose de quatre interfaces série fournissant un service d'accès commuté aux appels entrants :

- Pour le port série `term/a`, créez le fichier `/etc/ppp/options.term.a` avec l'entrée suivante :

  ```
  :10.1.1.1
  ```

- Pour le port série `term/b`, créez le fichier `/etc/ppp/options.term.b` avec l'entrée suivante :

  ```
  :10.1.1.2
  ```
- Pour le port série `term/c`, créez le fichier `/etc/ppp/options.term.c` avec l'entrée suivante :

  ```
  :10.1.1.3
  ```
- Pour le port série `term/d`, créez le fichier `/etc/ppp/options.term.d` avec l'entrée suivante :

  ```
  :10.1.1.4
  ```

Selon le schéma d'adressage précédent, un appel entrant sur l'interface série `/dev/term/c` reçoit l'adresse IP 10.1.1.3 pour la durée de l'appel. Une fois que le premier appelant raccroche, un appel ultérieur entrant par l'interface série `/dev/term/c` se voit également attribuer l'adresse IP 10.1.1.3.

Les avantages de l'adressage dynamique sont les suivants :

- Vous pouvez suivre l'utilisation du réseau PPP jusqu'au niveau du port série.
- Vous pouvez affecter un nombre minimal d'adresses IP à l'utilisation de PPP.
- Vous pouvez simplifier la gestion du filtrage IP.

Affectation des adresses IP statiques aux appelants

Si votre site met en œuvre l'authentification PPP, vous pouvez affecter des adresses IP *statiques* spécifiques à chaque appelant. Dans ce cas, chaque fois qu'une machine d'appel sortant appelle le serveur d'appel entrant, l'appelant reçoit la même adresse IP.

Vous mettez en œuvre les adresses statiques dans la base de données de secrets pap-secrets ou chap-secrets. Voici un exemple de fichier `/etc/ppp/pap-secrets` définissant des adresses IP statiques.

```
joe    myserver  joepasswd   10.10.111.240
sally  myserver  sallypasswd 10.10.111.241
sue    myserver  suepasswd   10.10.111.242
```

Appelant	`joe`, `sally` et `sue` sont les noms des appelants autorisés.
Serveur	`myserver` indique le nom du serveur.
Mot de passe	`joepasswd`, `sallypasswd` et `suepasswd` indiquent les mots de passe de chaque appelant.
Adresses IP	`10.10.111.240`, `10.10.111.241` et `10.10.111.242` sont les adresses IP affectées à chaque appelant.

Voici un exemple de fichier `/etc/ppp/chap-secrets` définissant des adresses IP statiques.

```
account1 myserver secret5748  10.10.111.244
account2 myserver secret91011 10.10.111.245
```

Appelant	`account1` et `account2` indiquent les noms des appelants.
Serveur	`myserver` indique le nom du serveur pour chaque appelant.
Mot de passe	`secret5748` et `secret91011` indiquent le secret CHAP de chaque appelant.
Adresses IP	`10.10.111.244` et `10.10.111.245` sont les adresses IP de chaque appelant.

Affectation d'adresses IP par numéro d'unité sppp

Si vous utilisez l'authentification PAP ou CHAP, vous pouvez affecter des adresses IP aux appelants par le numéro d'unité `sppp`. L'exemple suivant illustre ce type d'utilisation.

```
myclient ISP-server mypassword 10.10.111.240/28+
```

Le signe plus (+) indique que le numéro d'unité est ajouté à l'adresse IP. Prenez note des remarques suivantes :

- Les adresses comprises entre `10.10.111.240` et `10.10.111.255` sont affectées à des utilisateurs distants.
- `sppp0` obtient l'adresse IP `10.10.111.240`.
- `sppp1` obtient l'adresse IP `10.10.111.241` et ainsi de suite.

Création de tunnels PPPoE pour la prise en charge DSL

L'utilisation de PPPoE permet de fournir des services numériques haut débit PPP à plusieurs clients équipés d'un ou de plusieurs modems. Pour mettre en œuvre ces services, PPPoE crée un tunnel Ethernet par le biais de trois participants : l'entreprise, l'opérateur téléphonique et le fournisseur d'accès.

- Pour une présentation générale de PPPoE et une description de son fonctionnement, voir “Présentation PPPoE ” à la page 426.
- Pour une description des tâches de configuration des tunnels PPPoE, voir Chapitre 20, “Configuration d'un tunnel PPPoE (tâches)”.

Cette section contient des informations détaillées relatives aux commandes et fichiers PPPoE, qui sont résumées dans le tableau suivant.

TABLEAU 22–2 Commandes et fichiers de configuration PPPoE

Fichier ou commande	Description	Voir
`/etc/ppp/pppoe`	Fichier qui contient les caractéristiques appliquées par défaut à tous les tunnels configurés par PPPoE sur le système	"Fichier `/etc/ppp/pppoe`" à la page 547
`/etc/ppp/pppoe.`*device*	Fichier qui contient les caractéristiques d'une interface spécifique utilisée par PPPoE pour un tunnel	"Fichier `/etc/ppp/pppoe.` *device*" à la page 549
`/etc/ppp/pppoe.if`	Fichier qui indique l'interface Ethernet sur laquelle s'exécute le tunnel configuré par PPPoE	"Fichier `/etc/ppp/pppoe.if`" à la page 545
`/usr/sbin/sppptun`	Commande de configuration des interfaces Ethernet impliquées dans un tunnel PPPoE	"Commande `/usr/sbin/sppptun`" à la page 546
`/usr/lib/inet/pppoed`	Commande et options d'utilisation de PPPoE pour configurer un tunnel	"Démon `/usr/lib/inet/pppoed`" à la page 547

Fichiers de configuration d'interfaces PPPoE

Les interfaces utilisées à chaque extrémité du tunnel PPPoE doivent être configurées avant que le tunnel puisse prendre en charge les communications PPP. Utilisez les fichiers `/usr/sbin/sppptun` et `/etc/ppp/pppoe.if` à cette fin. Vous devez utiliser ces outils pour configurer les interfaces Ethernet sur tous les clients PPPoE Solaris et serveurs d'accès PPPoE.

Fichier `/etc/ppp/pppoe.if`

Le fichier `/etc/ppp/pppoe.if` répertorie les noms de toutes les interfaces Ethernet sur un hôte à utiliser pour les tunnels PPPoE. Ce fichier est traité lors de l'amorce du système, au moment du montage des interfaces répertoriées pour une utilisation dans des tunnels PPPoE.

Vous devez créer explicitement `/etc/ppp/pppoe.if`. Tapez le nom d'une interface à configurer pour PPPoE sur chaque ligne.

L'exemple ci-dessous illustre un fichier `/etc/ppp/pppoe.if` pour un serveur offrant trois interfaces pour des tunnels PPPoE.

```
# cat /etc/ppp/pppoe.if
hme1
hme2
hme3
```

Généralement, les clients PPPoE ont une seule interface répertoriée dans le fichier `/etc/ppp/pppoe.if` .

Commande /usr/sbin/sppptun

Vous pouvez utiliser la commande /usr/sbin/sppptun pour monter et démonter manuellement les interfaces Ethernet à utiliser pour les tunnels PPPoE. Par contraste, /etc/ppp/pppoe.if n'est lu qu'au démarrage du système. Ces interfaces doivent correspondre à celles qui sont répertoriées dans /etc/ppp/pppoe.if.

sppptun monte les interfaces Ethernet utilisées dans les tunnels PPPoE de manière similaire à la commande ifconfig. Contrairement à ifconfig, vous devez monter les interfaces deux fois pour prendre en charge PPPoE, car deux numéros de protocole Ethernet sont impliqués.

La syntaxe de base de sppptun est la suivante :

```
# /usr/sbin/sppptun plumb pppoed device-name
     device-name:pppoed
# /usr/sbin/sppptun plumb pppoe device-name
     device-name:pppoe
```

Dans cette syntaxe, *device-name* correspond au nom du périphérique à monter pour PPPoE.

La première fois que vous exécutez la commande sppptun, le protocole de découverte pppoed est monté sur l'interface. À la seconde exécution de sppptun, le protocole de session pppoe est monté. sppptun imprime le nom de l'interface qui vient d'être montée. Vous utilisez ce nom pour démonter l'interface, le cas échéant.

Pour plus d'informations, reportez-vous à la page de manuel sppptun(1M).

Exemples de commandes sppptun pour l'administration des interfaces

L'exemple suivant montre comment monter manuellement une interface pour PPPoE à l'aide de la commande /usr/sbin/sppptun.

```
# /usr/sbin/sppptun plumb pppoed hme0
hme0:pppoed
# /dev/sppptun plumb pppoe hme0
 hme0:pppoe
```

Cet exemple illustre comment répertorier les interfaces sur un serveur d'accès monté pour PPPoE.

```
# /usr/sbin/sppptun query
hme0:pppoe
hme0:pppoed
hme1:pppoe
hme1:pppoed
hme2:pppoe
hme2:pppoed
```

Cet exemple montre comment démonter une interface.

```
# sppptun unplumb hme0:pppoed
# sppptun unplumb hme0:pppoe
```

Fichiers et commandes du serveur d'accès PPPoE

Un prestataire de services qui offre des services ou une assistance DSL peut utiliser un serveur d'accès équipé de PPPoE. La relation entre le serveur et le client d'accès PPPoE est une relation client-serveur classique. Elle s'apparente à celle que la machine d'appel sortant et le serveur d'appel entrant entretiennent sur une liaison commutée. Un système PPPoE initialise la communication et un système PPPoE répond. Par contraste, le protocole PPP n'a aucune notion de la relation client-serveur. PPP place les deux systèmes sur un plan d'égalité.

Les commandes et fichiers qui permettent de configurer un serveur d'accès PPPoE sont les suivants :

- "Commande `/usr/sbin/sppptun`" à la page 546
- "Démon `/usr/lib/inet/pppoed`" à la page 547
- "Fichier `/etc/ppp/pppoe`" à la page 547
- "Fichier `/etc/ppp/pppoe.` *device*" à la page 549
- "Objet partagé `pppoe.so`" à la page 552

Démon `/usr/lib/inet/pppoed`

Le démon `pppoed` accepte des diffusions de services de clients PPPoE potentiels. En outre, `pppoed` négocie le côté serveur du tunnel PPPoE tunnel et exécute `pppd`, le démon PPP, sur ce tunnel.

Vous configurez les services `pppoed` dans les fichiers `/etc/ppp/pppoe` et `/etc/ppp/pppoe.`*device*. Si `/etc/ppp/pppoe` existe au démarrage du système, `pppoed` s'exécute automatiquement. Vous pouvez également exécuter explicitement le démon `pppoed` en tapant `/usr/lib/inet/pppoed` sur la ligne de commande.

Fichier `/etc/ppp/pppoe`

Le fichier `/etc/ppp/pppoe` décrit les services offerts par un serveur d'accès et les options définissant l'exécution de PPP sur le tunnel PPPoE. Vous pouvez définir des services pour chacune des interfaces ou de manière globale, c'est-à-dire pour toutes les interfaces du serveur d'accès. Le serveur d'accès envoie les informations dans le fichier `/etc/ppp/pppoe` en réponse à une diffusion d'un client potentiel PPPoE.

Ce qui suit est la syntaxe de base de `/etc/ppp/pppoe` :

global-options
service service-name
    service-specific-options
    device interface-name

Signification des paramètres :

global-options	Définit les options par défaut du fichier `/etc/ppp/pppoe`. Il s'agit d'options disponibles via `pppoed` ou `pppd`. Pour obtenir la liste complète de ces options, reportez-vous aux pages de manuel pppoed(1M) et pppd(1M). Par exemple, vous devez répertorier les interfaces Ethernet disponibles pour le tunnel PPPoE en tant qu'*options globales*. Si vous ne définissez pas de périphériques dans le fichier `/etc/ppp/pppoe`, les services ne sont proposés sur aucune interface. Pour définir `devices` en tant qu'option globale, utilisez le format suivant : *device interface <,interface>* *interface* spécifie l'interface où le service est à l'écoute des clients PPPoE potentiels. Si plusieurs interfaces sont associées au service, séparez leur nom par une virgule.
service service-name	Démarre la définition du service *service-name*. *service-name* est une chaîne qui peut être une expression appropriée aux services fournis.
service-specific-options	Répertorie les options PPP et PPPoE spécifiques à ce service.
`device` *interface-name*	Spécifie l'interface où le service énoncé précédemment est disponible.

Pour obtenir d'autres options de `/etc/ppp/pppoe`, reportez-vous aux pages de manuel pppoed(1M) et pppd(1M).

Un fichier `/etc/ppp/pppoe` standard ressemble à ceci.

EXEMPLE 22–2 Fichier `/etc/ppp/pppoe` de base

```
device hme1,hme2,hme3
service internet
   pppd "name internet-server"
service intranet
   pppd "192.168.1.1:"
service debug
   device hme1
   pppd "debug name internet-server"
```

Dans ce fichier, les valeurs suivantes s'appliquent.

`hme1,hme2,hme3`	Trois interfaces sur le serveur d'accès à utiliser pour les tunnels PPPoE.
`service internet`	Signale un service appelé `internet` aux clients potentiels. Le fournisseur qui propose le service

	détermine également comment `internet` est défini. Par exemple, un fournisseur peut interpréter `internet` au sens de services IP variés, ainsi qu'accès à Internet.
`pppd`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`. L'option "`name internet-server`" donne le nom `internet-server` à la machine locale, serveur d'accès.
`service intranet`	Signale un autre service appelé `internet` aux clients potentiels.
`pppd "192.168.1.1:"`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`. Lorsque l'appelant appelle `pppd`, 192.168.1.1 est défini comme l'adresse IP de la machine locale, serveur d'accès.
`service debug`	Signale un troisième service (débogage) sur les interfaces définies pour PPPoE.
`device hme1`	Restreint le débogage des tunnels PPPoE à `hme1`.
`pppd "debug name internet-server"`	Définit les options de ligne de commande utilisées lorsque l'appelant appelle `pppd`, dans ce cas, PPP déboguant la machine locale `internet-server` .

Fichier `/etc/ppp/pppoe.` *device*

Le fichier `/etc/ppp/pppoe.` *device* décrit les services qui sont offerts sur une interface d'un serveur d'accès aux PPPoE. `/etc/ppp/pppoe.` *device* comporte également des options qui définissent l'exécution de PPP sur le tunnel PPPoE. `/etc/ppp/pppoe.` *device* est un fichier facultatif, qui fonctionne exactement comme le fichier `/etc/ppp/pppoe` global. Cependant, lorsque `/etc/ppp/pppoe.`*device* est défini pour une interface, ses paramètres sont prioritaires pour cette interface par rapport aux paramètres globaux définis dans `/etc/ppp/pppoe`.

La syntaxe de base de `/etc/ppp/pppoe.`*device* est la suivante :

```
service service-name
        service-specific-options
service another-service-name
        service-specific-options
```

La seule différence avec la syntaxe de `/etc/ppp/pppoe` est l'impossibilité d'utiliser l'option `device` illustrée dans “Fichier `/etc/ppp/pppoe`” à la page 547.

Plug-in pppoe.so

pppoe.so est le fichier d'objet partagé PPPoE qui doit être appelé par les clients et serveurs d'accès PPPoE. Ce fichier limite MTU et MRU à 1492, filtre les paquets à partir du pilote et négocie le tunnel PPPoE, avec pppoed. Côté serveur d'accès, pppoe.so est automatiquement appelé par le démon pppd.

Configuration du serveur d'accès à l'aide des fichiers PPPoE et PPP

Cette section contient des exemples de tous les fichiers permettant de configurer un serveur d'accès. Le serveur d'accès est multiréseau. Le serveur est connecté à trois sous-réseaux : green, orange et purple. Par défaut, pppoed s'exécute en tant que root sur le serveur.

Les clients PPPoE peuvent accéder aux réseaux orange et purple par le biais des interfaces hme0 et hme1. Les clients se connectent au serveur à l'aide de la connexion UNIX standard. Le serveur authentifie les clients à l'aide de PAP.

Le réseau green n'est pas signalé aux clients. Le seul moyen pour les clients d'accéder au réseau green est de spécifier directement "green-net" et de fournir les informations d'identification CHAP. En outre, seuls les clients joe et mary sont autorisés à accéder au réseau green à l'aide d'adresses IP statiques.

EXEMPLE 22–3 Fichier /etc/ppp/pppoe pour un serveur d'accès

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
service purple-net
     device hme0,hme1
     pppd "require-pap login name purple-server purple-server:"
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

Cet exemple décrit les services disponibles à partir du serveur d'accès. La première section décrit les services du réseau orange.

```
service orange-net
     device hme0,hme1
     pppd "require-pap login name orange-server orange-server:"
```

Les clients accèdent au réseau orange via les interfaces hme0 et hme1. Les options données à la commande pppd force le serveur à demander aux clients potentiels leurs informations d'identification PAP. Les options pppd définissent également le nom du serveur sur orange-server, tel qu'il est utilisé dans le fichier pap-secrets.

La section des services du réseau `purple` est identique à celle du réseau `orange`, à l'exception des noms du réseau et du serveur.

La section suivante décrit les services du réseau `green` :

```
service green-net
     device hme1
     pppd "require-chap name green-server green-server:"
     nowildcard
```

Cette section restreint l'accès client à l'interface `hme1`. Les options données à la commande `pppd` forcent le serveur à demander aux clients potentiels leurs informations d'identification CHAP. Les options `pppd` définissent également le nom du serveur sur `green-server`, à utiliser dans le fichier `chap-secrets`. L'option `nowildcard` spécifie que l'existence du réseau green n'est pas signalée aux clients.

Pour le scénario décrit ci-dessus, vous pouvez configurer le fichier `/etc/ppp/options` suivant.

EXEMPLE 22–4 Fichier `/etc/ppp/options` pour un serveur d'accès

```
     auth
     proxyarp
     nodefaultroute
     name no-service    # don’t authenticate otherwise
```

L'option `name no-service` remplace le nom du serveur qui est normalement recherché au cours de l'authentification PAP ou CHAP. Le nom par défaut du serveur est celui trouvé par la commande `/usr/bin/hostname`. L'option `name` dans l'exemple précédent remplace le nom du serveur par `no-service`. Il est peu probable que le nom `no-service` soit trouvé dans un fichier `pap` ou `chap-secrets`. Cette action empêche un utilisateur aléatoire d'exécuter `pppd` et de remplacer les options `auth` et `name` définies dans le fichier `/etc/ppp/options`. `pppd` échoue, car aucun secret ne peut être trouvé pour le client avec le nom de serveur `no-service`.

Le scénario de serveur d'accès utilise le fichier `/etc/hosts` suivant.

EXEMPLE 22–5 Fichier `/etc/hosts` pour un serveur d'accès

```
     172.16.0.1    orange-server
     172.17.0.1    purple-server
     172.18.0.1    green-server
     172.18.0.2    joes-pc
     172.18.0.3    marys-pc
```

Voici le fichier `/etc/ppp/pap-secrets`, utilisé pour l'authentification PAP des clients qui tentent d'accéder aux réseaux `orange` et `purple`.

EXEMPLE 22–6 Fichier `/etc/ppp/pap-secrets` pour un serveur d'accès

```
* orange-server "" 172.16.0.2/16+
* purple-server "" 172.17.0.2/16+
```

Voici le fichier `/etc/ppp/chap-secrets`, utilisé pour l'authentification CHAP. Notez que seuls les clients `joe` et `mary` figurent dans la liste du fichier.

EXEMPLE 22–7 Fichier `/etc/ppp/chap-secrets` pour un serveur d'accès

```
 joe green-server "joe's secret" joes-pc
mary green-server "mary's secret" marys-pc
```

Commandes et fichiers du client PPPoE

Pour exécuter PPP sur un modem DSL, une machine doit devenir client PPPoE. Vous devez monter une interface pour exécuter PPPoE, puis détecter l'existence d'un serveur d'accès à l'aide de l'utilitaire `pppoec`. Le client peut alors créer le tunnel PPPoE via le modem DSL et exécuter PPP.

Le client PPPoE communique avec le serveur d'accès sur le modèle client-serveur classique. Le tunnel PPPoE n'est pas une liaison commutée, mais il est configuré et fonctionne de façon similaire.

Les commandes et fichiers qui configurent un client PPPoE sont les suivants :

- "Commande `/usr/sbin/sppptun`" à la page 546
- "Utilitaire `/usr/lib/inet/pppoec`" à la page 552
- "Objet partagé `pppoe.so`" à la page 552
- "Fichier `/etc/ppp/peers/` *peer-name*" à la page 523
- "Fichier de configuration `/etc/ppp/options`" à la page 518

Utilitaire `/usr/lib/inet/pppoec`

L'utilitaire `/usr/lib/inet/pppoec` est responsable de la négociation du côté client d'un tunnel PPPoE. `pppoec` est similaire à l'utilitaire `chat`. Vous n'appelez pas `pppoec` directement. Vous démarrez plutôt `/usr/lib/inet/pppoec` comme argument de l'option `connect` de la commande `pppd`.

Objet partagé `pppoe.so`

`pppoe.so` est l'objet partagé PPPoE que PPPoE doit charger pour fournir aux clients et serveurs d'accès la capacité PPPoE. L'objet partagé `pppoe.so` limite MTU et MRU à 1492, filtre les paquets en provenance du pilote et gère les messages PPPoE d'exécution.

Côté client, pppd charge pppoe.so lorsque l'utilisateur spécifie l'option plugin pppoe.so.

Fichier /etc/ppp/peers/ *peer-name* de définition d'un pair de serveur d'accès

Lorsque vous définissez un serveur d'accès pour qu'il soit découvert par pppoec, utilisez les options qui s'appliquent à la fois à pppoec et au démon pppd . Le fichier /etc/ppp/peers/*peer-name* du serveur d'accès requiert les paramètres suivants :

- sppptun : nom du périphérique série utilisé par le tunnel PPPoE.
- plugin pppoe.so : indique à pppd de charger l'objet partagé pppoe.so.
- connect "/usr/lib/inet/pppoec *device* " : démarre une connexion. connect appelle ensuite l'utilitaire pppoec sur *device*, l'interface montée pour PPPoE.

Les paramètres restants dans le fichier /etc/ppp/peers/ *peer-name* doivent s'appliquer à la liaison PPP sur le serveur. Utilisez les options que vous utiliseriez pour /etc/ppp/peers/ *peer-name* sur une machine d'appel sortant. Essayez de limiter le nombre d'options à celles dont vous avez vraiment besoin pour la liaison PPP.

L'exemple suivant est présenté dans la section "Définition d'un pair de serveur d'accès PPPoE" à la page 487.

EXEMPLE 22–8 Fichier /etc/ppp/peers/ *peer-name* de définition d'un serveur d'accès à distance

```
# cat /etc/ppp/peers/dslserve
sppptun
plugin pppoe.so
connect "/usr/lib/inet/pppoec hme0"
noccp
noauth
user Red
password redsecret
noipdefault
defaultroute
```

Ce fichier définit les paramètres à utiliser lors de la configuration d'un tunnel PPPoE et d'une liaison PPP pour accéder au serveur dslserve. Les options incluses sont les suivantes :

Option	Description
sppptun	Définit sppptun comme nom du périphérique série.
plugin pppoe.so	Demande à pppd de charger l'objet partagé pppoe.so.
connect "/usr/lib/inet/pppoec hme0"	Exécute pppoec et désigne hme0 en tant qu'interface pour le tunnel PPPoE et la liaison PPP.

Option	Description
`noccp`	Désactive la compression CCP sur la liaison. **Remarque –** De nombreux FAI utilisent uniquement les algorithmes de compression propriétaires. La désactivation de l'algorithme CCP mis à la disposition du public permet de réduire la durée de la négociation et d'éviter des problèmes d'interopérabilité peu fréquents.
`noauth`	Empêche `pppd` d'exiger les informations d'identification du serveur d'accès. La plupart des FAI ne fournissent pas d'informations d'identification aux clients.
`user Red`	Définit `Red` en tant que nom d'utilisateur du client, qui est requis pour l'authentification PAP par le serveur d'accès.
`password redsecret`	Définit `redsecret` comme le mot de passe à fournir au serveur d'accès pour l'authentification PAP.
`noipdefault`	Affecte 0.0.0.0 en tant qu'adresse IP initiale.
`defaultroute`	Indique à `pppd` d'installer une route IPv4 par défaut après la négociation IPCP. Vous devez inclure `defaultroute` dans le fichier `/etc/ppp/peers/`*peer-name* lorsque la liaison est la liaison du système à Internet, ce qui est le cas pour un client PPPoE.

◆ ◆ ◆ CHAPITRE 23

Migration de Solaris PPP asynchrone à Solaris PPP 4.0 (tâches)

Les versions antérieures du système d'exploitation Solaris incluaient une implémentation PPP différente, Solaris PPP asynchrone (`asppp`). Si vous souhaitez convertir des pairs qui exécutent `asppp` à la nouvelle implémentation PPP 4.0, vous devez exécuter un script de conversion. Ce chapitre aborde les points suivants de la conversion PPP :

Dans ce chapitre, un exemple de configuration `asppp` permet d'expliquer comment effectuer la conversion PPP. Vous trouverez une description des différences entre Solaris PPP 4.0 et `asppp` à la section "Quelle version de Solaris PPP utiliser" à la page 414.

Avant de convertir les fichiers `asppp`

Vous pouvez utiliser le script de conversion `/usr/sbin/asppp2pppd` pour convertir les fichiers qui composent une configuration `asppp` standard :

- `/etc/asppp.cf` : fichier de configuration PPP asynchrone
- `/etc/uucp/Systems` : fichier UUCP qui décrit les caractéristiques du pair distant
- `/etc/uucp/Devices` : fichier UUCP qui décrit le modem sur la machine locale
- `/etc/uucp/Dialers` fichier UUCP qui contient la séquence de connexion à utiliser par le modem décrit dans le fichier `/etc/uucp/Devices`

Pour plus d'informations sur `asppp`, reportez-vous au document *Solaris 8 System Administration collection, volume 3*, disponible sur le site Web `http://docs.sun.com`.

Exemple du fichier de configuration `/etc/asppp.cf`

La procédure illustrée à la section "Conversion de `asppp` à Solaris PPP 4.0" à la page 558 utilise le fichier `/etc/asppp.cf` suivant.

```
#
ifconfig ipdptp0 plumb mojave gobi up

path
 inactivity_timeout 120     # Approx. 2 minutes
    interface ipdptp0
    peer_system_name Pgobi    # The name we log in with (also in
                                  # /etc/uucp/Systems
```

Le fichier contient les paramètres suivants :

`ifconfig ipdptp0 plumb mojave gobi up`	Exécute la commande `ifconfig` pour configurer une liaison entre l'interface PPP `ipdptp0` sur la machine locale `mojave` et le pair distant `gobi`
`inactivity_timeout 120`	Met fin à la ligne après deux minutes d'inactivité
`interface ipdptp0`	Configure l'interface `ipdptp0` sur la machine d'appel sortant pour une liaison PPP asynchrone
`peer_system_name Pgobi`	Attribue le nom du pair distant, `Pgobi`

Exemple du fichier `/etc/uucp/Systems`

La procédure illustrée à la section “Conversion de asppp à Solaris PPP 4.0” à la page 558 utilise le fichier `/etc/uucp/Systems` suivant.

```
#ident  "@(#)Systems    1.5  92/07/14 SMI"  /* from SVR4 bnu:Systems 2.4 */
#

# .
# .
Pgobi Any ACU 38400 15551212 in:--in: mojave word: sand
```

Le fichier contient les paramètres suivants :

`Pgobi`	Utilise `Pgobi` comme nom d'hôte du pair distant
`Any ACU`	Indique au modem sur la machine d'appel sortant `mojave` d'établir une liaison avec un modem sur `Pgobi` à tout moment de la journée. ACU signifie "rechercher ACU dans le fichier `/etc/uucp/Devices`".
`38400`	Définit la vitesse maximale de la liaison sur 38400.
`15551212`	Indique le numéro de téléphone de `Pgobi`.

`in:–in: mojave word: sand`	Définit le script de connexion requis par `Pgobi` pour authentifier la machine d'appel sortant `mojave`.

Exemple de fichier `/etc/uucp/Devices`

La procédure illustrée à la section "Conversion de asppp à Solaris PPP 4.0" à la page 558 utilise le fichier `/etc/uucp/Devices` suivant.

```
#ident  "@(#)Devices  1.6  92/07/14 SMI"  /* from SVR4 bnu:Devices 2.7 */

.
.
#

TCP,et - - Any TCP -
.
.
#
ACU cua/b - Any hayes
# 0-7 are on a Magma 8 port card
Direct cua/0 - Any direct
Direct cua/1 - Any direct
Direct cua/2 - Any direct
Direct cua/3 - Any direct
Direct cua/4 - Any direct
Direct cua/5 - Any direct
Direct cua/6 - Any direct
Direct cua/7 - Any direct
# a is the console port (aka "tip" line)
Direct cua/a - Any direct
# b is the aux port on the motherboard
Direct cua/b - Any direct
# c and d are high speed sync/async ports
Direct cua/c - Any direct
Direct cua/d - Any direct
```

Le fichier prend en charge tous les modems Hayes connectés au port série `cua/b`.

Exemple de fichier `/etc/uucp/Dialers`

La procédure illustrée à la section "Conversion de asppp à Solaris PPP 4.0" à la page 558 utilise le fichier `/etc/uucp/Dialers` suivant.

```
#
#       <Much information about modems supported by Oracle Solaris UUCP>


penril    =W-P    "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
ventel    =&-%    "" \r\p\r\c $ k\c ONLINE!
```

```
vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE
develcon ""    "" \pr\ps\c est:\007 \E\D\e \n\007
micom    ""    "" \s\c NAME? \D\r\c GO
direct
#
#
#
#   Hayes Smartmodem -- modem should be set with the configuration
#   switches as follows:
#
#       S1 - UP        S2 - UP        S3 - DOWN    S4 - UP
#       S5 - UP        S6 - DOWN    S7 - ?        S8 - DOWN
#
hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT
```

<much more information about modems supported by Oraccle Solaris UUCP>

Ce fichier contient les scripts de discussion pour tous les types de modems, y compris les modems Hayes qui sont pris en charge dans le fichier `/etc/uucp/Dialers`.

Exécution du script de conversion `asppp2pppd` (tâches)

Le script `/usr/sbin/asppp2pppd` copie les informations PPP contenues dans les fichiers `/etc/asppp.cf` et UUCP PPP aux emplacements appropriés dans les fichiers Solaris PPP 4.0.

Tâches préliminaires

Avant de réaliser la tâche suivante, vous devez effectuer les opérations suivantes :

- Installation de Solaris sur la machine où résident également les fichiers de configuration `asppp` et UUCP
- Connexion en tant que superutilisateur sur la machine où résident les fichiers PPP, par exemple, `mojave`

▼ Conversion de `asppp` à Solaris PPP 4.0

1 Lancez le script de conversion.

```
# /usr/sbin/asppp2pppd
```

Le processus de conversion démarre et la sortie suivante s'affiche à l'écran.

```
This script provides only a suggested translation for your existing aspppd
configuration.  You will need to evaluate for yourself whether the translation
is appropriate for your operating environment.
Continue [Yn]?
```

2 Tapez "Y" pour continuer.

La sortie suivante s'affiche :

```
Chat cannot do echo checking; requests for this removed.
Adding 'noauth' to /etc/ppp/options

Preparing to write out translated configuration:
    1 chat file:
        1.  /etc/ppp/chat.Pgobi.hayes
    2 option files:
        2.  /etc/ppp/peers/Pgobi
        3.  /etc/ppp/options
    1 script file:
        4.  /etc/ppp/demand
```

Les nouveaux fichiers Solaris PPP 4.0 ont été générés.

▼ Affichage des résultats de la conversion

Vous pouvez afficher les fichiers Solaris PPP 4.0 créés par le script de conversion `/usr/sbin/asppp2pppd` à la fin du processus de conversion. Le script affiche la liste d'options suivante.

```
Enter option number:
        1 - view contents of file on standard output
        2 - view contents of file using /usr/bin/less
        3 - edit contents of file using /usr/bin/vi
        4 - delete/undelete file from list
        5 - rename file in list
        6 - show file list again
        7 - escape to shell (or "!")
        8 - abort without saving anything
        9 - save all files and exit (default)
Option:
```

1 Entrez 1 pour afficher le contenu des fichiers à l'écran.

Le script vous demande le numéro du fichier que vous souhaitez visualiser.

```
File number (1 .. 4):
```

Les numéros renvoient aux fichiers convertis qui sont répertoriés pendant le processus de conversion, comme indiqué à l'étape 2 précédente.

2 Entrez 1 pour visualiser le fichier de discussion /etc/ppp/chat.Pgobi.hayes.

```
File number (1 .. 4):  1
"" \d\dA\p\pTE1V1X1Q0S2=255S12=255\r\c
OK\r ATDT\T\r\c
CONNECT \c
in:--in: mojave
word: sand
```

Le script de discussion contient les informations de discussion du modem qui s'affichent sur la ligne hayes dans le fichier d'exemple /etc/uucp/Dialers. /etc/ppp/chat.Pgobi.hayes contient également la séquence de connexion pour Pgobi qui s'affiche dans le fichier d'exemple /etc/uucp/Systems. Le script de discussion se trouve à présent dans le fichier /etc/ppp/chat.Pgobi.hayes.

3 Entrez 2 pour visualiser le fichier de pairs /etc/ppp/peers/Pgobi.

```
File number (1 .. 4):  2
/dev/cua/b
38400
demand
idle 120
connect "/usr/bin/chat -f /etc/ppp/chat.Pgobi.hayes -T ’15551212’"
user NeverAuthenticate
mojave:gobi
```

Les informations sur le port série (/dev/cua/b) proviennent du fichier /etc/uucp/Devices. La vitesse de la liaison, le temps d'inactivité, les informations d'authentification et les noms des pairs proviennent du fichier /etc/asppp.cf. "demand" fait référence au script de demande, à appeler lorsque la machine d'appel sortant tente de se connecter au pair Pgobi.

4 Entrez 3 pour visualiser le fichier /etc/ppp/options créé pour la machine d'appel sortant mojave.

```
File number (1 .. 4):  3
#lock
noauth
```

Les informations dans /etc/ppp/options proviennent du fichier /etc/asppp.cf .

5 Entrez 4 pour visualiser le contenu du script demand.

```
File number (1 .. 4):  4
/usr/bin/pppd file /etc/ppp/peers/Pgobi
```

Ce script, lorsqu'il est appelé, exécute la commande pppd, qui lit ensuite le fichier /etc/ppp/peers/Pgobi pour initialiser la liaison entre mojave et Pgobi.

6 Entrez 9 pour enregistrer les fichiers créés. Quittez ensuite le script de conversion.

◆ ◆ ◆ CHAPITRE 24

UUCP (présentation)

Ce chapitre présente le programme UUCP (UNIX-to-UNIX Copy Program) et ses démons. Il aborde les sujets suivants :

UUCP permet aux ordinateurs de transférer des fichiers et d'échanger des messages électroniques entre eux. Le programme permet également aux ordinateurs d'être intégrés dans de grands réseaux tels que Usenet.

Le système d'exploitation Solaris fournit la version BNU (Basic Network Utilities) d'UUCP, également appelée HoneyDanBer UUCP. Le terme *UUCP* indique la plage complète de fichiers et d'utilitaires qui composent le système, dont le programme `uucp` n'est qu'une partie. Les utilitaires UUCP vont des utilitaires utilisés pour copier des fichiers entre ordinateurs (`uucp` et `uuto`) aux utilitaires utilisés pour la connexion à distance et l'exécution de commandes (`cu` et `uux a`).

Configurations matérielles UUCP

UUCP prend en charge les configurations matérielles suivantes :

Liens directs	Vous pouvez créer un lien direct vers un autre ordinateur en plaçant des câbles RS-232 entre les ports série des deux ordinateurs. Les liens directs sont utiles lorsque deux ordinateurs communiquent régulièrement et sont physiquement proches (dans un rayon de 15 mètres). Vous pouvez utiliser un modem courte distance pour augmenter quelque peu cette distance.
Lignes téléphoniques	En utilisant une unité d'appel automatique (ACU), telle qu'un modem haut débit, votre ordinateur peut communiquer avec d'autres ordinateurs via des lignes téléphoniques classiques. Le modem

compose le numéro de téléphone demandé par UUCP. L'ordinateur de destination doit disposer d'un modem capable de répondre aux appels entrants.

Réseau — UUCP peut également communiquer sur un réseau qui exécute le protocole TCP/IP ou une autre famille de protocole. Une fois que votre ordinateur a été défini en tant qu'hôte sur un réseau, il peut contacter n'importe quel hôte connecté au réseau.

Ce chapitre suppose que votre matériel UUCP a déjà été assemblé et configuré. Si vous devez configurer un modem, reportez-vous au *Guide d'administration système : administration de base* et aux manuels accompagnant le modem pour obtenir de l'aide.

Logiciel UUCP

Le logiciel UUCP est automatiquement inclus lorsque vous exécutez le programme d'installation Solaris et sélectionnez la distribution entière. Vous pouvez également ajouter le logiciel UUCP à l'aide de la commande `pkgadd`. Les programmes UUCP peuvent être divisés en trois catégories : démons, programmes d'administration et programmes utilisateur.

Démons UUCP

Le système UUCP possède quatre démons : `uucico`, `uuxqt`, `uusched` et `in.uucpd`. Ces démons gèrent les transferts de fichiers UUCP et l'exécution des commandes. Vous pouvez également les lancer manuellement à partir du shell, si nécessaire.

`uucico` — Permet de sélectionner le périphérique utilisé pour le lien, d'établir le lien vers l'ordinateur distant et d'exécuter la séquence de connexion et les vérifications d'autorisations requises. En outre, `uucico` transfère les fichiers de données, exécute les fichiers, résulte de journaux et notifie l'utilisateur par e-mail lorsque les transferts sont terminés. `uucico` agit comme shell de connexion pour les comptes de connexion UUCP. Lorsque le démon `uucico` local appelle une machine distante, il communique directement avec le démon `uucico` distant au cours de la session.

Une fois tous les fichiers créés, les programmes `uucp`, `uuto` et `uux` exécutent le démon `uucico` pour contacter l'ordinateur distant. Les commandes `uusched` et `Uutry` exécutent `uucico`. Pour plus d'informations, reportez-vous à la page de manuel `uucico(1M)`.

`uuxqt` — Permet d'exécuter des requêtes d'exécution distante. Ce démon effectue des recherches dans le répertoire spool pour exécuter des fichiers (toujours nommés `X.`*fichier*) envoyés à partir d'un ordinateur distant. Quand un fichier `X.`*fichier* est

trouvé, uuxqt l'ouvre pour obtenir la liste des fichiers de données nécessaires à l'exécution. uuxqt vérifie ensuite si les fichiers de données requis sont disponibles et accessibles. Si les fichiers sont disponibles, uuxqt vérifie le fichier Permissions afin de vérifier qu'il possède l'autorisation d'exécuter la commande demandée. Le démon uuxqt est exécuté par le script de shell uudemon.hour, qui est démarré par cron. Pour plus d'informations, reportez-vous à la page de manuel uuxqt(1M).

uusched — Permet de planifier les travaux en attente dans le répertoire spool. uusched est initialement exécuté au démarrage par le script de shell uudemon.hour, qui est démarré par cron. Pour plus d'informations, reportez-vous à la page de manuel uusched(1M). Avant de démarrer le démon uucico, uusched rend aléatoire l'ordre dans lequel les ordinateurs distants sont appelés.

in.uucpd — Permet de prendre en charge les connexions UUCP sur des réseaux. Le fichier inetd sur l'hôte distant appelle in.uucpd chaque fois qu'une connexion UUCP est établie. uucpd vous invite alors à saisir un nom de connexion. uucico sur l'hôte appelant doit répondre par un nom de connexion. in.uucpd vous invite ensuite à saisir un mot de passe, à moins qu'aucun mot de passe ne soit nécessaire. Pour plus d'informations, reportez-vous à la page de manuel in.uucpd(1M).

Programmes d'administration UUCP

D'autres programmes d'administration UUCP se trouvent sous /usr/lib/uucp. Les fichiers de base de données les plus basiques se trouvent dans /etc/uucp. La seule exception est uulog, qui se trouve sous /usr/bin. Le répertoire personnel de l'ID de connexion uucp est /usr/lib/uucp. Lorsque vous exécutez les programmes d'administration via su ou login, utilisez l'ID utilisateur uucp. L'ID utilisateur possède les programmes et fichiers de données de spool.

uulog — Affiche le contenu des fichiers journaux de l'ordinateur spécifié. Les fichiers journaux sont créés pour chaque ordinateur distant avec lequel votre machine communique. Les fichiers journaux enregistrent chaque utilisation de uucp, uuto et uux a. Pour plus d'informations, reportez-vous à la page de manuel uucp(1C).

uucleanup — Permet de nettoyer le répertoire spool. La commande uucleanup est généralement exécutée à partir du script de shell uudemon.cleanup, qui est démarré par cron . Pour plus d'informations, reportez-vous à la page de manuel uucleanup(1M).

Uutry — Permet de tester les capacités de traitement des appels et d'effectuer un débogage modéré. La commande Uutry appelle le démon uucico pour établir un lien de communication entre votre ordinateur et l'ordinateur distant spécifié. Pour plus d'informations, reportez-vous à la page de manuel Uutry(1M).

`uucheck` Permet de vérifier la présence des répertoires, programmes et fichiers d'aide UUCP. `uucheck` peut également vérifier certaines parties du fichier `/etc/uucp/Permissions` à la recherche d'erreurs de syntaxe évidentes. Pour plus d'informations, reportez-vous à la page de manuel `uucheck(1M)`.

Programmes utilisateur UUCP

Les programmes utilisateur UUCP se trouvent sous `/usr/bin`. Vous n'avez pas besoin d'autorisation spéciale pour utiliser ces programmes.

`cu` Permet de connecter votre ordinateur à un ordinateur distant afin que vous puissiez vous connecter aux deux machines en même temps. La commande `cu` vous permet de transférer des fichiers ou d'exécuter des commandes sur l'un ou l'autre des ordinateurs sans supprimer le lien initial. Pour plus d'informations, reportez-vous à la page de manuel `cu(1C)`.

`uucp` Permet de copier un fichier d'un ordinateur à un autre. La commande `uucp` crée des fichiers de travail et des fichiers de données, met le travail en attente de transfert et appelle le démon `uucico`, qui à son tour tente de contacter l'ordinateur distant. Pour plus d'informations, reportez-vous à la page de manuel `uucp(1C)`.

`uuto` Permet de copier les fichiers à partir de la machine locale sur le spool répertoire public `/var/spool/uucppublic/receive` sur l'ordinateur distant. Contrairement à la commande `uucp`, qui vous permet de copier un fichier sur n'importe quel répertoire accessible sur l'ordinateur distant, `uuto` place le fichier dans un répertoire spool approprié et indique à l'utilisateur distant de récupérer le fichier avec `uupick`. Pour plus d'informations, reportez-vous à la page de manuel `uuto(1C)`.

`uupick` Permet de récupérer les fichiers dans `/var/spool/uucppublic/receive` lorsque les fichiers sont transférés vers un ordinateur à l'aide de la commande `uuto`. Pour plus d'informations, reportez-vous à la page de manuel `uuto(1C)`.

`uux` Permet de créer le travail, les données et d'exécuter des fichiers nécessaires à l'exécution des commandes sur une machine distante. Pour plus d'informations, reportez-vous à la page de manuel `uux(1C)`.

`uustat` Permet d'afficher l'état des transferts demandés (`uucp`, `uuto` ou `uux a`). La commande `uustat` permet également de contrôler les transferts en attente. Pour plus d'informations, reportez-vous à la page de manuel `uustat(1C)`.

Fichiers de base de données UUCP

Une partie importante de la configuration UUCP est la configuration des fichiers qui composent la base de données UUCP. Ces fichiers se trouvent dans le répertoire `/etc/uucp`. Vous devez modifier ces fichiers pour configurer UUCP ou `asppp` sur votre machine. Les fichiers incluent les éléments suivants :

`Config` Contient une liste de paramètres variables. Vous pouvez définir manuellement ces paramètres pour configurer le réseau.

`Devconfig` Permet de configurer les communications réseau.

`Devices` Permet de configurer les communications réseau.

`Dialcodes` Contient les abréviations d'accès direct qui peuvent être utilisées dans le champ de numéro de téléphone des entrées du fichier `Systems`. Bien que ce ne soit pas obligatoire, le fichier `Dialcodes` peut être utilisé par `asppp`, ainsi que par UUCP.

`Dialers` Contient les chaînes de caractères qui sont requis pour négocier avec les modems pour établir des connexions à des ordinateurs distants. Le fichier `Dialers` est utilisé par `asppp`, ainsi que par UUCP.

`Grades` Définit les niveaux des travaux et les autorisations associées à chaque niveau, que les utilisateurs peuvent spécifier pour mettre des travaux en file d'attente sur un ordinateur distant.

`Limits` Permet de définir le nombre maximal de commandes `uucico`, `uuxqt` et `uusched` autorisées sur votre machine.

`Permissions` Permet de définir le niveau d'accès accordé à des hôtes distants qui tentent de transférer des fichiers ou d'exécuter des commandes sur votre ordinateur.

`Poll` Permet de définir les ordinateurs devant être interrogés par votre système et le moment où ils sont interrogés.

`Sysfiles` Permet d'affecter des fichiers multiples ou différents qui doivent être utilisés par `uucico` et `cu` en tant que fichiers `Systems`, `Devices` et `Dialers`.

`Sysname` Permet de définir un nom UUCP unique pour une machine, en plus de son nom d'hôte TCP/IP.

`Systems` Contient des informations requises par le démon `uucico`, `cu` et `asppp` pour établir un lien vers un ordinateur distant. Les éléments suivants sont inclus :

- Nom de l'hôte distant
- Nom du périphérique de connexion associé à l'hôte distant
- Heure à laquelle l'hôte peut être contacté
- Numéro de téléphone
- ID de connexion

- Password (Mot de passe)

Plusieurs autres fichiers peuvent être considérés comme faisant partie de la base de données de prise en charge mais ne sont pas directement impliqués dans l'établissement d'un lien et le transfert des fichiers.

Configuration des fichiers de base de données UUCP

La base de données UUCP est constituée des fichiers présentées à la section "Fichiers de base de données UUCP" à la page 565. Toutefois, la configuration UUCP de base implique uniquement les fichiers critiques suivants :

- `/etc/uucp/Systems`
- `/etc/uucp/Devices`
- `/etc/uucp/Dialers`

La commande `asppp` utilisant certaines des bases de données UUCP, vous devez comprendre un minimum les fichiers de bases de données importants si vous envisagez de configurer `asppp`. Une fois ces bases de données configurées, l'administration UUCP est relativement simple. En règle générale, vous modifiez d'abord le fichier `Systems`, puis le fichier `Devices`. En général, vous pouvez utiliser le fichier `/etc/uucp/Dialers` par défaut, sauf si vous envisagez d'ajouter des dialers qui ne se trouvent pas dans le fichier par défaut. En outre, vous pouvez également souhaiter utiliser les fichiers suivants pour la configuration UUCP et `asppp` de base :

- `/etc/uucp/Sysfiles`
- `/etc/uucp/Dialcodes`
- `/etc/uucp/Sysname`

Étant donné que ces fichiers travaillent en étroite collaboration, vous devez comprendre l'ensemble de leur contenu avant d'apporter des modifications. Une modification apportée à une entrée dans un des fichiers peut nécessiter d'appliquer une modification à une entrée associée dans un autre fichier. Les autres fichiers répertoriés à la section "Fichiers de base de données UUCP" à la page 565 ne sont pas aussi dépendants les uns des autres.

Remarque – `asppp` utilise uniquement les fichiers décrits dans cette section. `asppp` n'utilise pas les autres fichiers de base de données UUCP.

◆ ◆ ◆ CHAPITRE 25

Administration du protocole UUCP (tâches)

Ce chapitre explique comment démarrer les opérations UUCP après avoir modifié le fichier de base de données qui est pertinent pour vos machines. Le chapitre contient des procédures et des informations sur le dépannage de la configuration et de la maintenance du protocole UUCP sur les machines qui exécutent le système d'exploitation Solaris, telles que les opérations suivantes :

Administration du protocole UUCP (liste des tâches)

Le tableau ci-dessous fournit des liens vers les procédures qui sont traitées dans ce chapitre, ainsi qu'une brève description de chaque procédure.

TABLEAU 25–1 Liste des tâches pour l'administration du protocole UUCP

Tâche	Description	Voir
Autorisation des machines distantes à accéder à votre système	Modifiez le fichier `/etc/passwd` pour ajouter des entrées afin d'identifier les machines qui sont autorisées à accéder à votre système.	"Ajout de connexions UUCP" à la page 568
Démarrage d'UUCP	Utilisez les scripts shell fournis pour démarrer UUCP.	"Démarrage d'UUCP" à la page 569
Activation d'UUCP pour travailler avec TCP/IP	Modifiez les fichiers `/etc/inetd.conf` et `/etc/uucp/Systems` pour activer UUCP pour TCP/IP.	"Activation du protocole UUCP pour TCP/IP" à la page 571
Dépannage de problèmes UUCP communs	Utilisez les étapes de diagnostic pour rechercher les modems ou ACU défectueux.	"Recherche de modems ou d'ACU défectueux" à la page 574

TABLEAU 25–1 Liste des tâches pour l'administration du protocole UUCP *(Suite)*

Tâche	Description	Voir
	Utilisez les étapes de diagnostic pour déboguer les transmissions.	"Débogage des transmissions" à la page 574

Ajout de connexion UUCP

Pour le traitement correct des requêtes UUCP (`uucico`) entrantes provenant des machines distantes, chaque machine doit avoir une connexion sur votre système.

▼ Ajout de connexions UUCP

Pour permettre à une machine distante d'accéder à votre système, vous devez ajouter une entrée au fichier `/etc/passwd` comme suit :

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez le fichier `/etc/passwd` et ajoutez l'entrée afin d'identifier la machine qui est autorisée à accéder à votre système.**

Ci-dessous, une entrée type que vous pourriez placer dans le fichier `/etc/passwd` pour une machine distante autorisée à accéder à votre système avec une connexion UUCP :

```
Ugobi:*:5:5:gobi:/var/spool/uucppublic:/usr/lib/uucp/uucico
```

Par convention, le nom de connexion d'une machine distante est le nom de machine précédé par la lettre majuscule `U`. Notez que le nom ne doit pas dépasser huit caractères. Sinon, vous devrez peut-être le tronquer ou l'abréger.

L'entrée précédente montre qu'une demande de connexion par `Ugobi` est résolue par `/usr/lib/uucp/uucico`. Le répertoire personnel est `/var/spool/uucppublic`. Le mot de passe est obtenu à partir du fichier `/etc/shadow`. Vous devez accorder du mot de passe et du nom de connexion avec l'administrateur UUCP de la machine distante. L'administrateur distant doit ensuite ajouter une entrée appropriée, avec le nom de connexion et le mot de passe non chiffré, dans le fichier `Systems` de la machine distante.

3 **Accordez du nom de votre machine avec les administrateurs UUCP sur d'autres systèmes.**

De la même façon, vous devez accorder les nom et mot de passe de votre machine avec les administrateurs UUCP de toutes les machines auxquelles vous souhaitez accéder via UUCP.

Démarrage du protocole UUCP

UUCP inclut quatre scripts shell qui interrogent les machines distantes, replanifient les transmissions et nettoient les anciens fichiers journaux et les transmissions ayant échoué. Les scripts se présentent comme suit :

- `uudemon.poll`
- `uudemon.hour`
- `uudemon.admin`
- `uudemon.cleanup`

Ces scripts shell doivent être exécutés régulièrement de manière à ce que le protocole UUCP s'exécute sans problème. Le fichier `crontab` permettant d'exécuter les scripts est automatiquement créé dans `/usr/lib/uucp/uudemon.crontab` dans le cadre du processus d'installation de Solaris, si vous sélectionnez l'installation complète. Sinon, le fichier est créé lorsque vous installez le package UUCP.

Vous pouvez également exécuter les scripts shell UUCP de manière manuelle. Vous pouvez personnaliser le fichier `uudemon.crontab` prototype ci-après pour une machine donnée :

```
#
#ident  "@(#)uudemon.crontab    1.5     97/12/09 SMI"
#
# This crontab is provided as a sample. For systems
# running UUCP edit the time schedule to suit, uncomment
# the following lines, and use crontab(1) to activate the
# new schedule.
#
#48 8,12,16 * * * /usr/lib/uucp/uudemon.admin
#20 3 * * * /usr/lib/uucp/uudemon.cleanup
#0 * * * * /usr/lib/uucp/uudemon.poll
#11,41 * * * * /usr/lib/uucp/uudemon.hour
```

Remarque – Par défaut, les opérations UUCP sont désactivées. Pour activer UUCP, modifiez le calendrier et supprimez le commentaire des lignes appropriées dans le fichier `uudemon.crontab` .

▼ Démarrage d'UUCP

Pour activer le fichier `uudemon.crontab`, effectuez les opérations suivantes :

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Modifiez le fichier `/usr/lib/uucp/uudemon.crontab` et modifiez les entrées selon les besoins.**

3 **Activez le fichier `uudemon.crontab` en exécutant la commande suivante :**

```
crontab < /usr/lib/uucp/uudemon.crontab
```

Script shell `uudemon.sondage`

Le script shell `uudemon.poll` par défaut lit le fichier `/etc/uucp/Poll` une fois par heure. S'il est prévu que des machines dans le fichier `Poll` soient interrogées, un fichier de travail (`C.` *sysnxxxx*) est placé dans le répertoire `/var/spool/uucp/`*nodename*. *nodename* représente le nom de nœud UUCP de la machine.

Le script shell est planifié pour s'exécuter une fois par heure, avant `uudemon.hour`, de sorte que les fichiers de travail sont en place lorsque `uudemon.hour` est appelé.

Script shell `uudemon.hour`

Le script shell `uudemon.hour` par défaut effectue les actions suivantes :

- Appelle le programme `uusched` afin de rechercher les répertoires de spool pour les fichiers de travail (`C.`) qui n'ont pas été traités. Le script programme ensuite le transfert de ces fichiers vers une machine distante.
- Appelle le démon `uuxqt` afin de rechercher les répertoires de spool pour exécuter des fichiers (`X.`) qui ont été transférés à votre ordinateur et n'ont pas été traités à ce moment-là.

Par défaut, `uudemon.hour` s'exécute deux fois par heure. Il se peut que vous souhaitiez que `uudemon.hour` soit exécuté plus souvent si vous prévoyez un très fort taux d'échec des appels à des machines distantes.

Script shell `uudemon.admin`

Le script shell `uudemon.admin` par défaut effectue les opérations suivantes :

- Exécute la commande `uustat` avec les options `p` et `q`. L'option `q` donne des informations sur l'état des fichiers de travail (`C.`), des fichiers de données (`D.`) et exécute les fichiers (`X.`) qui sont mis en file d'attente. L'option `p` imprime les informations sur les traitements réseau qui sont répertoriés dans les fichiers de verrouillage (`/var/spool/locks`).
- Envoie les informations d'état obtenues à la connexion en tant qu'administrateur `uucp` en utilisant la commande `mail`.

`uudemon.cleanup`, script shell

Le script shell `uudemon.cleanup` par défaut effectue les actions suivantes :

- Collecte les fichiers journaux de machines individuelles dans le répertoire `/var/uucp/.Log`, fusionne ces fichiers et les place dans le répertoire `/var/uucp/.Old` avec les autres informations sur des journaux antérieurs.
- Supprime les fichiers de travail (`C.`) vieux de sept jours ou plus, les fichiers de données (`D.`) vieux de sept jours ou plus et les fichiers d'exécution (`X.`) vieux de deux jours ou plus des fichiers spool.
- Renvoie à l'expéditeur le courrier qui ne peut pas être distribué.
- Envoie par courrier un récapitulatif des informations d'état qui ont été rassemblées au cours de la journée à la connexion en tant qu'administrateur UUCP (`uucp`).

Exécution du protocole UUCP sur TCP/IP

Pour exécuter UUCP sur un réseau TCP/IP, vous devez effectuer quelques modifications, comme décrit dans cette section.

▼ Activation du protocole UUCP pour TCP/IP

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Modifiez le fichier `/etc/uucp/Systems` pour vous assurer que les entrées présentent les champs suivants :**

System-Name Time TCP Port networkname Standard-Login-Chat

Une entrée standard ressemble à ceci :

```
rochester Any TCP - ur-seneca login: Umachine password: xxx
```

Notez que le champ *networkname* vous permet de spécifier explicitement le nom d'hôte TCP/IP. Cette capacité est importante pour certains sites. Dans l'exemple précédent, le site a le nom de nœud UUCP `rochester`, qui est différent de son nom d'hôte TCP/IP `ur-seneca`. En outre, une toute autre machine pourrait facilement exécuter UUCP et avoir le nom d'hôte TCP/IP de `rochester`.

Le champ Port du fichier `Systems` doit comporter l'entrée `-`. Cette syntaxe revient à répertorier l'entrée comme `uucp`. Dans la plupart des cas, le champ *networkname* contient la même valeur que le nom de système et le champ Port est `-`, qui dit d'utiliser le port uucp standard à partir de la

base de données `services`. Le démon `in.uucpd` s'attend à ce que la machine distante envoie son ID de connexion et mot de passe pour authentification et `in.uucpd` vous invite à les renseigner, de la même façon que `getty` et `login`.

3 **Modifiez le fichier `/etc/inet/services` pour configurer un port pour UUCP :**

```
uucp    540/tcp    uucpd        # uucp daemon
```

Vous ne devriez pas avoir à modifier l'entrée. Cependant, si votre machine exécute NIS ou NIS+ en tant que service de noms, vous devez changer l'entrée `/etc/nsswitch.conf` pour `/etc/services` afin de vérifier d'abord `files`, puis `nis` ou `nisplus`.

4 **Vérifiez qu'UUCP est activé.**

```
# svcs network/uucp
```

Le service UUCP est géré par l'utilitaire de gestion des services (Service Management Facility). Pour lancer une interrogation sur l'état de ce service, vous pouvez utiliser la commande `svcs`. Pour une présentation de l'utilitaire SMF (Service Management Facility), reportez-vous au Chapitre 18, “Gestion des services (présentation) ” du *Guide d'administration système : administration de base*.

5 **(Facultatif) Si nécessaire, activez UUCP en tapant la commande suivante :**

```
# inetadm -e network/uucp
```

Sécurité et maintenance du protocole UUCP

Une fois que vous avez configuré UUCP, sa maintenance est relativement simple. Cette section explique les tâches UUCP continues liées à la sécurité, à la maintenance et au dépannage.

Configuration de la sécurité du protocole UUCP

Le fichier `/etc/uucp/Permissions` par défaut offre une sécurité maximale pour vos liens UUCP. Le fichier `Permissions` par défaut ne contient aucune entrée.

Pour chaque machine distante, vous pouvez définir d'autres paramètres pour définir ce qui suit :

- Les moyens par lesquels la machine distante peut recevoir les fichiers à partir de votre machine
- Les répertoires pour lesquels la machine distante dispose d'une autorisation d'accès en lecture et en écriture
- Les commandes que l'ordinateur distant peut utiliser pour une exécution à distance

Ci-dessous, une entrée du fichier `Permissions` standard :

```
MACHINE=datsun LOGNAME=Udatsun VALIDATE=datsun
COMMANDS=rmail REQUEST=yes SENDFILES=yes
```

Cette entrée permet aux fichiers d'être envoyés vers et reçus de répertoires UUCP “normaux”, et non à partir de n'importe où dans le système. L'entrée permet également la validation du nom d'utilisateur UUCP au moment de la connexion.

Maintenance régulière du protocole UUCP

UUCP requiert peu de maintenance. Toutefois, vous devez vous assurer que le fichier `crontab` est en place, comme décrit dans la section “Démarrage d'UUCP” à la page 569. Votre devez surveiller l'augmentation de la taille des fichiers de courrier et du répertoire public.

E-mail pour UUCP

Tous les messages électroniques générés par les programmes et les scripts UUCP sont envoyés à l'ID utilisateur `uucp`. Si vous ne vous connectez pas fréquemment sous l'identité de cet utilisateur, vous n'aurez peut-être pas conscience du fait que le courrier s'accumule et consomme l'espace disque. Pour résoudre ce problème, créez un alias dans `/etc/mail/aliases` et redirigez ce courrier vers l'utilisateur `root` ou vers vous-même et les autres personnes chargées de la maintenance d'UUCP. N'oubliez pas d'exécuter la commande `newaliases` après avoir modifié le fichier `aliases`.

Répertoire public UUCP

Le répertoire `/var/spool/uucppublic` est l'emplacement unique sur chaque système, dans lequel le protocole UUCP est habilité par défaut à copier des fichiers. Chaque utilisateur a l'autorisation de modifier `/var/spool/uucppublic`, ainsi que de lire et d'écrire des fichiers du répertoire. Toutefois, le sticky bit du répertoire étant défini, le mode de ce répertoire est 01777. Par conséquent, les utilisateurs ne peuvent pas supprimer les fichiers qui ont été copiés sur celui-ci et qui appartiennent à `uucp`. Vous seul, en tant qu'administrateur UUCP connecté comme utilisateur `root` ou `uucp`, pouvez supprimer des fichiers de ce répertoire. Afin d'éviter l'accumulation incontrôlée des fichiers dans ce répertoire, vous devez vous assurer que vous en supprimez régulièrement.

Si cette maintenance n'arrange pas les utilisateurs, encouragez-les à utiliser les commandes `uuto` et `uupick` au lieu de supprimer le sticky bit, qui est défini pour des raisons de sécurité. Reportez-vous à la page de manuel `uuto(1C)` pour obtenir plus d'instructions sur l'utilisation des commandes `uuto` et `uupick`. Vous pouvez également restreindre le mode du répertoire sur un seul groupe de personnes. Si vous ne souhaitez pas prendre le risque que quelqu'un sature votre disque, vous pouvez même refuser l'accès UUCP à ce disque.

Dépannage du protocole UUCP

Ces procédures décrivent la résolution des problèmes d'UUCP courants.

▼ Recherche de modems ou d'ACU défectueux

Vous pouvez vérifier si les modems ou d'autres ACU montrent des comportements anormaux.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Obtenez le compte et les motifs des échecs de contact en exécutant la commande suivante :**

```
# uustat -q
```

3 **Appelez via une ligne particulière et imprimez les informations relatives à la tentative de débogage.**

La ligne doit être définie comme `direct` dans le fichier `/etc/uucp/Devices`. Vous devez ajouter un numéro de téléphone à la fin de la ligne de commande si la ligne est connectée à un composeur automatique, ou le périphérique doit être configuré comme `direct`. Type :

```
# cu -d -lline
```

line est `/dev/cua/un`.

▼ Débogage des transmissions

Si vous ne pouvez pas contacter une machine en particulier, vous pouvez vérifier les communications vers cette machine avec les commandes `Uutry` et `uucp`.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Essayez d'établir le contact :**

```
# /usr/lib/uucp/Uutry -r machine
```

Remplacez *machine* par le nom d'hôte de la machine que vous n'êtes pas en mesure de contacter. Cette commande effectue les opérations suivantes :

- Démarre le démon de transfert (`uucico`) au moment du débogage. Vous pouvez obtenir des informations de débogage si vous êtes utilisateur `root`.
- Dirige les résultats du débogage vers `/tmp/` *machine*.
- Imprime les résultats du débogage vers votre terminal en émettant la commande suivante :

  ```
  # tail -f
  ```

  Appuyez sur Ctrl-C pour arrêter l'émission des résultats. Vous pouvez copier les résultats de `/tmp/` *machine* si vous souhaitez les enregistrer.

3 Si `Uutry` n'isole pas le problème, essayez de mettre en file d'attente une tâche :

```
# uucp -r file machine\!/dir/file
```

fichier Utilisez le nom du fichier que vous souhaitez transférer.

machine Utilisez le nom de la machine vers laquelle vous voulez effectuer la copie.

/dir/file Spécifiez l'emplacement du fichier pour l'autre machine.

4 Exécutez la commande suivante :

```
# Uutry
```

Si vous ne parvenez toujours pas à résoudre le problème, il vous faudra peut-être appeler votre représentant du support technique local. Enregistrez les résultats du débogage, qui peuvent vous aider à diagnostiquer le problème.

Remarque – Vous pouvez également augmenter ou réduire le niveau de débogage qui est fourni par `Uutry` via l'option `-x` *n*. *n* indique le niveau de débogage. Le niveau de débogage par défaut pour `Uutry` est 5.

Le niveau de débogage 3 fournit des informations de base sur la manière et le moment où la connexion est établie, mais peu d'informations relatives à la transmission. Le niveau de débogage 9, cependant, fournit des informations exhaustives sur le processus de transmission. N'oubliez pas que le débogage se produit aux deux extrémités de la transmission. Si vous avez l'intention d'utiliser un niveau supérieur à 5 sur un texte relativement grand, contactez l'administrateur de l'autre site et déterminez à quel moment modifier le niveau.

Vérification du fichier UUCP `/etc/uucp/Systems`

Vérifiez que vous disposez d'informations à jour dans votre fichier `Systems` si vous rencontrez des problèmes lorsque vous contactez une machine particulière. Certaines informations susceptibles d'être obsolètes pour une machine sont les suivantes :

- Numéro de téléphone
- ID de connexion
- Mot de passe

Vérification des messages d'erreur UUCP

UUCP a deux types de messages d'erreur : `ASSERT` et `STATUS`.

- Lorsqu'un processus est abandonné, les messages d'erreur `ASSERT` sont enregistrés dans `/var/uucp/.Admin/errors`. Ces messages incluent le nom de fichier, `sccsid`, le numéro de ligne et le texte. Ces messages sont généralement le résultat de problèmes au niveau du système.
- Les messages d'erreur `STATUS` sont stockés dans le répertoire `/var/uucp/.Status`. Le répertoire contient un fichier distinct pour chaque machine distante avec laquelle votre ordinateur tente de communiquer. Ces fichiers contiennent des informations d'état à propos de tentatives de communication et indiquant si la communication a été effectuée avec succès.

Vérification des informations de base

Plusieurs commandes sont disponibles pour la vérification des informations réseau de base :

- Utilisez la commande `uuname` pour répertorier les machines que votre machine peut contacter.
- Utilisez la commande `uulog` pour afficher le contenu des répertoires des journaux d'hôtes particuliers.
- Utilisez la commande `uucheck -v` pour vérifier la présence des fichiers et répertoires qui sont nécessaires pour `uucp`. Cette commande vérifie également le fichier `Permissions` et affiche des informations sur les autorisations que vous avez configurés.

◆ ◆ ◆ CHAPITRE 26

UUCP (référence)

Ce chapitre fournit des informations de référence pour l'utilisation d'UUCP. Il aborde les sujets suivants :

Fichier `/etc/uucp/Systems` UUCP

Le fichier `/etc/uucp/Systems` contient les informations requises par le démon `uucico` pour établir un lien de communication vers un ordinateur distant. Le fichier `/etc/uucp/Systems` est le premier fichier que vous devez modifier pour configurer UUCP.

Chaque entrée du fichier `Systems` représente un ordinateur distant avec lequel votre hôte communique. Un hôte particulier peut avoir plusieurs entrées. Les entrées supplémentaires représentent d'autres chemins de communication qui sont testés dans un ordre séquentiel. En outre, par défaut, UUCP empêche tout ordinateur qui n'apparaît pas dans le fichier `/etc/uucp/Systems` de se connecter à votre hôte.

À l'aide du fichier `Sysfiles`, vous pouvez définir plusieurs fichiers à utiliser comme fichiers `Systems`. Reportez-vous à la section "Fichier `/etc/uucp/Sysfiles` UUCP" à la page 597 pour obtenir une description des fichiers `Sysfiles`.

La syntaxe suivante s'applique à une entrée dans le fichier Systems :

```
System-Name    Time    Type    Speed    Phone    Chat Script
```

Consultez l'exemple suivant d'entrée du fichier Systems.

EXEMPLE 26–1 Entrées du fichier /etc/uucp/Systems

```
Arabian     Any  ACUEC 38400 111222  ogin: Puucp ssword:beledi
```

Arabian	Entrée pour le champ System-Name (Nom du système). Pour plus d'informations, reportez-vous à la section "Champ System-Name du fichier /etc/uucp/Systems" à la page 578.
Any	Entrée pour le champ Time (Date et heure). Pour plus d'informations, reportez-vous à la section "Champ Time du fichier /etc/uucp/Systems" à la page 579.
ACUEC	Entrée pour le champ Type. Pour plus d'informations, reportez-vous à la section "Champ Type du fichier /etc/uucp/Systems" à la page 580.
38400	Entrée pour le champ Speed (Vitesse). Pour plus d'informations, reportez-vous à la section "Champ Speed du fichier /etc/uucp/Systems" à la page 580.
111222	Entrée pour le champ Phone (Téléphone). Pour plus d'informations, reportez-vous à la section "Champ Phone du fichier /etc/uucp/Systems" à la page 581.
ogin: Puucp ssword:beledi	Entrée pour le champ Chat Script (script de discussion). Pour plus d'informations, reportez-vous à la section "Champ Chat-Script du fichier /etc/uucp/Systems" à la page 581.

Champ System-Name du fichier /etc/uucp/Systems

Ce champ contient le nom du nœud de l'ordinateur distant. Sur les réseaux TCP/IP, ce nom peut être le nom d'hôte de l'ordinateur ou un nom spécialement créé pour les communications UUCP via le fichier /etc/uucp/Sysname. Reportez-vous à la section "Fichier /etc/uucp/Systems UUCP" à la page 577. Dans l'Exemple 26–1, le champ System-Name contient une entrée pour l'hôte distant Arabian.

Champ Time du fichier /etc/uucp/Systems

Ce champ permet de spécifier le jour de la semaine et l'heure auxquels l'ordinateur distant peut être appelé. Le format du champ Time est le suivant :

```
daytime[;retry]
```

Portion *day* du champ Time

La portion *day* peut être une liste contenant certaines des entrées suivantes.

`Su Mo Tu We Th Fr Sa`	Pour des jours distincts.
`Wk`	Pour n'importe quel jour de la semaine.
`Any`	Pour n'importe quel jour.
`Never`	Votre hôte n'appelle jamais l'ordinateur distant. L'appel doit être initié par l'ordinateur distant. Votre hôte fonctionne ensuite en *mode passif*.

Portion *time* du champ Time

L'Exemple 26–1 présente la valeur `Any` dans le champ Time, ce qui indique que l'hôte `Arabian` peut être appelé à tout moment.

La portion *time* doit être une plage d'heures spécifiées au format 24 heures, par exemple `0800-1230` pour la période allant de 8h30 à 00h30. Si aucune portion *time* n'est spécifiée, on part du principe que les appels peuvent être effectués à tout moment de la journée.

Une plage d'heures qui s'étend sur 0000 est autorisée. Par exemple, `0800-0600` signifie que, mis à part la période entre 6h et 9h du matin, toutes les heures sont autorisés.

Portion *retry* du champ Time

Le sous-champ *retry* vous permet de spécifier la durée minimale (en minutes) avant une nouvelle tentative, après l'échec de la précédente. L'attente par défaut est de 60 minutes. Le séparateur de sous-champ est un point-virgule (;). Par exemple, `Any;9` est interprété suit : possibilité d'appeler l'ordinateur à tout moment, mais attente d'au moins 9 minutes avant la tentative suivante en cas de défaillance.

Si vous ne spécifiez pas d'entrée *retry*, un algorithme back-off exponentiel est utilisé. Cela signifie que UUCP démarre après un temps d'attente par défaut qui augmente à mesure que le nombre d'échecs augmente. Par exemple, supposons que le délai initial entre les nouvelles tentatives est de 5 minutes. Si aucune réponse ne se produit, la tentative suivante a lieu 10 minutes plus tard. La tentative suivante aura ensuite lieu 20 minutes plus tard, et ainsi de

suite jusqu'à ce que le délai maximal (23 heures) soit atteint. Si *retry* est spécifié, la valeur indiquée spécifie toujours la durée avant le prochain essai. Sinon, l'algorithme back-off est utilisé.

Champ Type du fichier /etc/uucp/Systems

Ce champ contient le type de périphérique qui doit être utilisé pour établir le lien de communication avec l'ordinateur distant. Le mot-clé utilisé dans ce champ est mis en correspondance avec le premier champ des entrées du fichier Devices.

EXEMPLE 26–2 Mot-clé associé au champ Type

```
Arabian    Any    ACUEC, g    38400    1112222    ogin: Puucp ssword:beledi
```

Vous pouvez définir le protocole utilisé pour établir le contact avec le système en ajoutant le protocole au champ Type. L'exemple précédent montre comment attacher le protocole g pour le type de périphérique ACUEC. Pour plus d'informations sur les protocoles, reportez-vous à la section “Définitions de protocole dans le fichier /etc/uucp/Devices ” à la page 590.

Champ Speed du fichier /etc/uucp/Systems

Ce champ, également appelé champ Class (Classe), spécifie la vitesse de transfert du périphérique utilisé pour établir le lien de communication. Le champ Speed UUCP peut contenir une lettre et une vitesse, C1200 ou D1200 par exemple, pour faire la différence entre les classes de dialers. Reportez-vous à la section “Champ Class du fichier /etc/uucp/Devices” à la page 587.

Certains périphériques peuvent être utilisés à n'importe quelle vitesse, de sorte que le mot-clé Any peut être utilisé. Ce champ doit correspondre au champ Class de l'entrée du fichier Devices associée.

EXEMPLE 26–3 Entrée dans le champ Speed

```
eagle    Any    ACU, g    D1200    NY3251    ogin: nuucp ssword:Oakgrass
```

Si ce champ ne requiert aucune information, utilisez un trait d'union (-) en tant que paramètre de substitution pour le champ.

Champ Phone du fichier /etc/uucp/Systems

Ce champ vous permet de spécifier le numéro de téléphone, connu comme un *jeton*, de l'ordinateur distant pour les dialers automatiques, également connus comme *sélecteurs de port*. Le numéro de téléphone est constitué d'une abréviation alphabétique facultative et d'une partie numérique. Si une abréviation est utilisé, elle doit être répertoriée dans le fichier `Dialcodes`.

EXEMPLE 26–4 Entrée du champ Phone

```
nubian     Any     ACU       2400    NY555-1212     ogin: Puucp ssword:Passuan
eagle      Any     ACU, g    D1200   NY=3251        ogin: nuucp ssword:Oakgrass
```

Dans le champ `Phone`, un signe égale (=) indique à l'`ACU` d'attendre une seconde tonalité d'invitation à numéroter avant de composer les numéros suivants. Un tiret (-) dans la chaîne indique à l'`ACU` d'effectuer une pause de quatre secondes avant de composer le prochain numéro.

Si votre ordinateur est connecté à un sélecteur de port, vous pouvez accéder à d'autres ordinateurs connectés à ce sélecteur. Les entrées du fichier `Systems` pour ces machines distantes ne doivent pas posséder de numéro de téléphone dans le champ `Phone`. Au lieu de cela, ce champ doit contenir le jeton à transmettre au commutateur. De cette façon, le sélecteur de port connaît l'ordinateur distant avec lequel votre hôte souhaite communiquer, généralement simplement le nom du système. L'entrée du fichier `Devices` associé doit avoir un `\D` à la fin de l'entrée afin de s'assurer que ce champ n'est pas traduit à l'aide du fichier `Dialcodes`.

Champ Chat-Script du fichier /etc/uucp/Systems

Ce champ, également connu comme champ Login (Connexion), contient une chaîne de caractères appelée *script de connexion*. Le script de discussion contient les caractères que les ordinateurs locaux et distants doivent se transmettre lors de leur première conversation. Les scripts de discussion ont le format suivant :

expect send [expect send] ....

expect représente la chaîne que l'hôte local s'attend à recevoir de l'hôte distant pour lancer la conversation. *send* est la chaîne que l'hôte local envoie une fois que l'hôte local a reçu la chaîne *expect* de l'hôte distant. Un script de discussion peut avoir plus d'une séquence Send-Expect.

Un script de discussion de base peut contenir les éléments suivants :

- Invite de connexion que l'hôte local s'attend à recevoir de l'ordinateur distant
- Nom de connexion que l'hôte local envoie à l'ordinateur distant afin d'établir la connexion
- Invite de mot de passe que l'hôte local s'attend à recevoir de l'ordinateur distant

- Mot de passe que l'hôte local envoie à l'ordinateur distant

Le champ *expect* peut être composé de sous-champs de la forme suivante :

expect[-send-expect]...

L'option *-send* est envoyée si la valeur *expect* précédente n'est pas lue correctement. L'option *-expect* qui suit *-send* est la chaîne attendue suivante.

Par exemple, avec les chaînes `login--login`, l'UUCP sur l'hôte local attend `login`. Si l'UUCP reçoit `login` à partir de l'ordinateur distant, l'UUCP passe au champ suivant. Si l'UUCP ne reçoit pas `login`, l'UUCP envoie un retour chariot, puis recherche de nouveau `login`. Si l'ordinateur local n'attend pas initialement de caractères, utilisez les caractères "", pour la chaîne NULL, dans le champ *expect*. Tous les champs *send* sont envoyés avec un retour chariot à la fin, sauf si la chaîne *send* se termine par un `\c`.

Ce qui suit est un exemple d'entrée du fichier `Systems` qui utilise une chaîne *expect-send* :

```
sonora Any ACUEC 9600 2223333 "" \r \r ogin:-BREAK-ogin: Puucpx ssword:xyzzy
```

Cet exemple indique à l'UUCP sur l'hôte local d'envoyer deux retours chariot et d'attendre `ogin:` (pour `Login:`). Si `ogin:` n'est pas reçu, envoyez un `BREAK`. Lorsque vous recevez `ogin:`, envoyez le nom de connexion `Puucpx`. Lorsque vous recevez `ssword:` (pour `Password:`), envoyez le mot de passe `xyzzy`.

Le tableau suivant répertorie des caractères d'échappement utiles.

TABLEAU 26–1 Caractères d'échappement utilisés dans le champ Chat-Script du fichier `Systems`

Caractère d'échappement	Signification
`\b`	Envoie ou attend un caractère de retour arrière.
`\c`	Placé à la fin d'une chaîne, supprime le retour chariot normalement envoyé. Sinon il est ignoré.
`\d`	Attend 1 à 3 secondes avant d'envoyer d'autres caractères.
`\E`	Démarre la vérification d'écho. À partir de ce point, chaque fois qu'un caractère est transmis, l'UUCP attend que le caractère soit reçu avant de poursuivre ses vérifications.
`\e`	Renvoie des marques en écho.
`\H`	Ignore une déconnexion. Utilisez cette option pour les modems de rappel automatique.
`\K`	Envoie un caractère BREAK.
`\M`	Active un indicateur `CLOCAL`.

TABLEAU 26–1 Caractères d'échappement utilisés dans le champ Chat-Script du fichier Systems *(Suite)*

Caractère d'échappement	Signification
\m	Désactive l'indicateur CLOCAL.
\n	Envoie ou attend un caractère de nouvelle ligne.
\N	Envoie un caractère NUL (ASCII NUL).
\p	Effectue une pause pendant environ 1/4 à 1/2 seconde.
\r	Envoie ou attend un retour chariot.
\s	Envoie ou attend un caractère d'espace.
\t	Envoie ou attend un caractère de tabulation.
EOT	Envoie un EOT, suivi d'une nouvelle ligne, deux fois.
BREAK	Envoie un caractère BREAK.
ddd	Envoie ou attend le caractère représenté par les nombres octaux (*ddd*).

Activation du rappel automatique par l'intermédiaire du script de discussion

Certaines sociétés configurent des serveurs d'appels entrants afin de gérer les appels à partir des ordinateurs distants. Par exemple, votre société peut avoir un serveur d'appels entrants avec un modem de rappel automatique que les employés peuvent appeler à partir de leurs ordinateurs personnels. Une fois que le serveur d'appels entrants a identifié l'ordinateur distant, le serveur d'appels entrants déconnecte le lien vers l'ordinateur distant, puis le rappelle. Le lien de communication est alors rétabli.

Vous pouvez faciliter le rappel automatique en utilisant l'option \H dans le script de discussion du fichier Systems à l'endroit où le rappel automatique doit se produire. Incluez l'option \H dans une chaîne Expect à l'endroit où le serveur d'appels entrants devrait raccrocher.

Par exemple, supposons que le script de discussion qui appelle un serveur d'appels entrants contienne la chaîne suivante :

```
INITIATED\Hogin:
```

La fonction de numérotation UUCP sur l'ordinateur local s'attend à recevoir les caractères, INITIATED, depuis le serveur d'appels entrants. Une fois les caractères INITIATED mis en correspondance, l'utilitaire de numérotation vide tous les caractères suivants que l'utilitaire de numérotation reçoit jusqu'à ce que le serveur d'appels entrants raccroche. L'utilitaire de numérotation local attend jusqu'à ce qu'il reçoive la partie suivante de la chaîne attendue, les caractères ogin:, à partir du serveur d'appels entrants. Une fois ogin: reçu, l'utilitaire de numérotation continue alors à exécuter le script de discussion.

Une chaîne de caractères n'a pas besoin de directement précéder ou suivre l'option \H, comme illustré dans l'exemple précédent.

Contrôle de flux matériel dans le fichier /etc/uucp/Systems

Vous pouvez également utiliser la chaîne de pseudo-envoi STTY=*valeur* pour définir les caractéristiques du modem. Par exemple, STTY=crtscts permet de contrôler le flux matériel. STTY accepte tous les modes stty. Pour plus de détails, reportez-vous aux pages de manuel stty(1) et termio(7I).

L'exemple suivant active le contrôle de flux matériel dans une entrée du fichier Systems :

```
unix Any ACU 2400 12015551212 "" \r ogin: Puucp ssword:Passuan "" \ STTY=crtscts
```

Cette chaîne de pseudo-envoi peut également être utilisée dans les entrées du fichier Dialers.

Définition de la parité dans le fichier /etc/uucp/Systems

Dans certains cas, il est nécessaire de réinitialiser la parité car le système que vous appelez vérifie la parité des ports et ignore la ligne si elle est fausse. La paire expect-send, "" P_ZERO, définit le bit de gauche (bit de parité) sur 0. Consultez la paire expect-send dans l'exemple suivant :

```
unix Any ACU 2400 12015551212 "" P_ZERO "" \r ogin: Puucp ssword:Passuan
```

Les éléments suivants sont des paires de parité qui peuvent suivre la paire expect-send, "" P_ZERO :

"" P_EVEN	Définit la parité sur pair, qui est la valeur par défaut
"" P_ODD	Définit la parité sur impair
"" P_ONE	Définit le bit de parité sur 1

Ces paires de parité peuvent être insérées n'importe où dans le script de discussion. Les paires de parité s'appliquent à toutes les informations du script de discussion qui suivent "" P_ZERO, la paire expect-send. Une paire de parité peut également être utilisée dans le fichier Dialers. L'exemple suivant inclut les données de la paire de parité, "" P_ONE :

```
unix Any ACU 2400 12015551212 "" P_ZERO "" P_ONE "" \r ogin: Puucp ssword:Passuan
```

Fichier /etc/uucp/Devices UUCP

Le fichier /etc/uucp/Devices contient des informations relatives à tous les périphériques pouvant être utilisés pour établir un lien vers un ordinateur distant. Ces périphériques incluent les ACU (dont les modems haut-débit), les liens directs et les connexions réseau.

Une entrée du fichier /etc/uucp/Devices respecte la syntaxe suivante :

```
Type   Line   Line2   Class   Dialer-Token-Pairs
```

L'entrée ci-dessous est une entrée du fichier Devices pour un modem U.S. Robotics V.32bis connecté au port A et en cours d'exécution à 38 400 bit/s.

```
ACUEC   cua/a   -   38400   usrv32bis-ec
```

ACUEC	Entrée du champ Type. Pour plus d'informations, reportez-vous à la section “Champ Type du fichier /etc/uucp/Devices” à la page 585.
cua/a	Entrée du champ Line (Ligne). Pour plus d'informations, reportez-vous à la section “Champ Line du fichier /etc/uucp/Devices” à la page 587.
-	Entrée du champ Line2 (Ligne 2). Pour plus d'informations, reportez-vous à la section “Champ Line 2 dans le fichier /etc/uucp/Devices” à la page 587.
38400	Entrée du champ Class. Pour plus d'informations, reportez-vous à la section “Champ Class du fichier /etc/uucp/Devices” à la page 587.
usrv32bis-ec	Entrée du champ Dialer-Token-Pair (Paire jeton-dialer). Pour plus d'informations, reportez-vous à la section “Champ Dialer-Token-Pairs du fichier /etc/uucp/Devices” à la page 588.

Chaque champ est décrit dans la section suivante.

Champ Type du fichier /etc/uucp/Devices

Ce champ décrit le type de lien que le périphérique établit. Le champ Type UUCP peut contenir l'un des mots-clés décrits dans les sections suivantes.

Mot-clé Direct

Le mot-clé Direct apparaît principalement dans les entrées pour les connexions cu . Il indique que le lien est un lien direct vers un autre ordinateur ou un sélecteur de port. Créez une entrée distincte pour chaque ligne à laquelle vous voulez faire référence à l'aide de l'option -l de cu.

Mot-clé ACU

Le mot-clé ACU indique que le lien vers un ordinateur distant (via cu, UUCP, asppp, ou Solaris PPP 4.0) est effectué par le biais d'un modem. Ce modem peut être connecté directement à votre ordinateur ou indirectement via un sélecteur de port.

Sélecteur de port

Le sélecteur de port est une variable qui est remplacé dans le champ Type par le nom d'un sélecteur de port. Les sélecteurs de port sont des périphériques connectés à un réseau qui invitent à fournir le nom d'un modem appelant, puis y fournissent l'accès. Le fichier /etc/uucp/Dialers contient les scripts appelant uniquement pour les sélecteurs de port micom et develcon. Vous pouvez ajouter vos propres entrées de sélecteur de port au fichier Dialers. Pour plus d'informations, reportez-vous à la section "Fichier /etc/uucp/Dialers UUCP" à la page 591.

Variable System-Name

Cette variable est remplacée par le nom d'un ordinateur dans le champ Type, ce qui indique que le lien est un lien direct vers cet ordinateur. Ce schéma est utilisé pour associer la ligne dans cette entrée du fichier Devices avec une entrée du fichier /etc/uucp/Systems pour l'ordinateur *nom du système* .

Champs Type des fichiers Devices et Systems

L'Exemple 26–5 présente une comparaison des champs du fichier /etc/uucp/Devices et du fichier /etc/uucp/Systems. Le mot-clé utilisé dans le champ Type du fichier Devices est comparé au troisième champ des entrées du fichier Systems. Dans le fichier Devices, le champ Type dispose d'une entrée ACUEC, qui indique une unité d'appel automatique, dans cet exemple un modem V. 32bis. Cette valeur est mise en correspondance avec le champ Type du fichier Systems, qui contient également l'entrée ACUEC. Pour plus d'informations, reportez-vous à la section "Fichier /etc/uucp/Systems UUCP" à la page 577.

EXEMPLE 26–5 Comparaison des champs Type dans les fichiers Devices et Systems

Vous trouverez ci-dessous un exemple d'entrée dans le fichier Devices.

```
ACUEC cua/a - 38400 usrv32bis-ec
```

Vous trouverez ci-dessous un exemple d'entrée dans le fichier Systems.

```
Arabian Any ACUEC 38400 111222 ogin: Puucp ssword:beledi
```

Champ Line du fichier /etc/uucp/Devices

Ce champ contient le nom du périphérique de la ligne (ou port) associée à l'entrée du fichier `Devices`. Si le modem associé à une entrée spécifique était connecté à un périphérique `/dev/cua/a` (port série A), le nom saisi dans ce champ serait `cua/a`. Un indicateur de contrôle de modem facultatif, `M`, peut être utilisé dans le champ Line pour indiquer que le périphérique doit être ouvert sans attendre de porteuse. Par exemple :

```
cua/a,M
```

Champ Line 2 dans le fichier /etc/uucp/Devices

Ce champ est un paramètre substituable. Utilisez toujours un trait d'union (-) ici. Les dialers de type 801, qui ne sont pas pris en charge dans le système d'exploitation Solaris, utilisent le champ Line2. Les autres dialers n'utilisent normalement pas cette configuration, mais nécessitent tout de même un trait d'union dans ce champ.

Champ Class du fichier /etc/uucp/Devices

Le champ Class contient la vitesse du périphérique, si le mot-clé `ACU` ou `Direct` est utilisé dans le champ Type. Cependant, le champ Class peut contenir une lettre et une vitesse, `C1200` ou `D1200` par exemple, pour faire la différence entre les classes de dialers (Centrex ou Dimension PBX par exemple).

Cette distinction est nécessaire car de nombreux bureaux de grande taille possèdent plusieurs types de réseaux téléphoniques. Un réseau peut être dédié aux communications internes d'un bureau uniquement, tandis qu'un autre réseau gère les communications externes. Dans une telle situation, vous devez distinguer la ou des lignes utilisée(s) pour les communications internes et pour les communications externes.

Le mot-clé utilisé dans le champ Class du fichier `Devices` est mis en correspondance avec le champ Speed du fichier `Systems`.

EXEMPLE 26–6 Champ Class du fichier `Devices`

```
ACU   cua/a   -   D2400  hayes
```

Certains périphériques peuvent être utilisés à n'importe quelle vitesse, de sorte que le mot-clé `Any` peut être utilisé dans le champ Class. Si l'option `Any` est utilisée, la ligne correspond à n'importe quelle vitesse demandée dans le champ Speed du fichier `Systems`. Si ce champ porte la valeur `Any` et le champ Speed du fichier `Systems` également, la vitesse par défaut est de 2 400 bit/s.

Champ Dialer-Token-Pairs du fichier /etc/uucp/Devices

Le champ Dialer-Token-Pairs (DTP) contient le nom d'un dialer et le jeton permettant de passer. Le champ DTP présente la syntaxe suivante :

dialer token [dialer token]

La partie *dialer* peut être le nom d'un modem, d'un port moniteur ou le mot-clé `Direct` ou `Uudirect` pour un périphérique avec lien direct. Il n'existe aucune limite au nombre de paires dialer-jeton. Si la partie *dialer* n'est pas présente, elle est tirée d'une entrée associée dans le fichier `Systems`. La partie *token* peut être fournie immédiatement après la partie dialer.

La dernière paire dialer-jeton peut ne pas être présente, selon le dialer associé. Dans la plupart des cas, la dernière paire comporte uniquement une partie *dialer*. La partie *token* est récupérée à partir du champ Phone de l'entrée du fichier `Systems` associé.

Une entrée valide dans la partie *dialer* partie peut être définie dans le fichier `Dialers` ou peut être l'un de plusieurs types de dialers. Ces types de dialers spéciaux sont compilés dans le logiciel et sont donc disponibles sans qu'aucune entrée ne soit présente dans le fichier `Dialers`. La liste ci-dessous présente les types de dialers spéciaux.

`TCP`	Réseau TCP/IP
`TLI`	Réseau Transport Level Interface (sans STREAMS)
`TLIS`	Réseau Transport Level Interface (avec STREAMS)

Pour plus d'informations, reportez-vous à la section "Définitions de protocole dans le fichier /etc/uucp/Devices " à la page 590.

Structure du champ Dialer-Token-Pairs dans le fichier /etc/uucp/Devices

Le champ DTP peut être structuré de quatre manières différentes, selon le périphérique associé à l'entrée.

Voici la première manière de structurer le champ DTP :

Modem connecté directement : si un modem est connecté directement à un port de votre ordinateur, le champ DTP de l'entrée du fichier `Devices` associé ne dispose que d'une seule paire. Cette paire porte normalement le nom du modem. Ce nom permet de mettre en correspondance l'entrée du fichier `Devices` avec une entrée du fichier `Dialers`. Par conséquent, le champ Dialer doit correspondre au premier champ d'une entrée du fichier `Dialers`.

EXEMPLE 26–7 Champ Dialers pour un modem connecté directement

```
Dialers   hayes =,-,  ""          \\dA\pTE1V1X1Q0S2=255S12=255\r\c
                                  \EATDT\T\r\c CONNECT
```

Notez que seule la partie dialer (`hayes`) est présente dans le champ DTP de l'entrée du fichier `Devices`. Cela signifie que le *jeton* à transmettre au dialer (dans cet exemple, le numéro de téléphone) est tiré du champ Phone d'une entrée du fichier `Systems`. (`\T` est implicite, comme décrit dans l'Exemple 26–9.)

Voici la seconde et la troisième manières de structurer le champ DTP :

- **Lien direct** : pour créer un lien direct vers un ordinateur particulier, le champ DTP de l'entrée associée doit contenir le mot-clé `Direct`. Cette condition s'applique aux deux types d'entrées de lien direct, `direct` et *System-Name*. Reportez-vous à la section "Champ Type du fichier /etc/uucp/Devices" à la page 585.
- **Ordinateurs sur le même sélecteur de port** : si un ordinateur avec lequel vous avez l'intention de communiquer se trouve sur le même commutateur de sélecteur de port que votre ordinateur, vous devez d'abord accéder au commutateur. Le commutateur établit ensuite la connexion à l'autre ordinateur. Ce type d'entrée n'a qu'une seule paire. La partie *dialer* permet de faire correspondre une entrée du fichier `Dialers`.

EXEMPLE 26–8 Champ Dialers UUCP pour les ordinateurs sur le même sélecteur de port

```
Dialers    develcon ,""   ""            \pr\ps\c est:\007 \E\D\e \007
```

Comme indiqué, la partie *jeton* n'est pas renseignée. Cette désignation indique que le jeton est tiré du fichier `Systems`. L'entrée du fichier `Systems` pour cet ordinateur contient le jeton dans le champ Phone, qui est normalement réservé au numéro de téléphone de l'ordinateur. Pour plus d'informations, reportez-vous à la section "Fichier /etc/uucp/Systems UUCP" à la page 577. Ce type de DTP contient un caractère d'échappement (`\D`), ce qui permet de s'assurer que le contenu du champ Phone n'est pas interprété comme une entrée valide dans le fichier `Dialcodes`.

Voici la quatrième manière de structurer le champ DTP :

Modems connectés au sélecteur de port : si un modem haut-débit est connecté à un port d'un sélecteur, votre ordinateur doit d'abord accéder au commutateur du sélecteur de port. Le commutateur établit la connexion au modem. Ce type d'entrée nécessite deux paires dialer-jeton. La partie *dialer* de chaque paire (cinquième et septième champs de l'entrée) permet de mettre en correspondance les entrées dans le fichier `Dialers`, comme suit.

EXEMPLE 26–9 Champ Dialers UUCP pour les modems connectés au sélecteur de port

```
develcon ""     ""    \pr\ps\c  est:\007    \E\D\e      \007
ventel   =&-%   t""   \r\p\r\c  $           <K\T%\r>\c  ONLINE!
```

Dans la première paire, develcon est le dialer et vent le jeton transmis au commutateur Develcon afin de lui indiquer quel périphérique, tel qu'un modem Ventel, connecter à votre ordinateur. Ce jeton est unique pour chaque sélecteur de port, chaque commutateur pouvant être défini différemment. Une fois le modem Ventel connecté, la seconde paire est accessible. Ventel est le dialer et le jeton est extrait du fichier Systems.

Deux caractères d'échappement peuvent s'afficher dans un champ DTP :

- \T : indique que le champ Phone (*jeton*) doit être traduit en utilisant le fichier /etc/uucp/Dialcodes. Ce caractère d'échappement est normalement placé dans le fichier /etc/uucp/Dialers fichier pour chaque script appelant associé à un modem (Hayes et U.S. Robotics par exemple). Par conséquent, aucune traduction n'a lieu avant l'accès au script appelant.
- \D : indique que le champ Phone (*jeton*) ne doit pas être traduit à l'aide du fichier /etc/uucp/Dialcodes . Si aucun caractère d'échappement n'est spécifié à la fin d'une entrée Devices, l'option \D est appliquée (par défaut). Une option \D est également utilisée dans le fichier /etc/uucp/Dialers avec les entrées associées aux commutateurs réseau develcon et micom.

Définitions de protocole dans le fichier /etc/uucp/Devices

Vous pouvez définir le protocole à utiliser avec chaque périphérique dans le fichier /etc/uucp/Devices. Cette spécification est généralement inutile car vous pouvez utiliser la valeur par défaut ou définir le protocole à l'aide du système spécifique que vous appelez. Pour plus d'informations, reportez-vous à la section "Fichier /etc/uucp/Systems UUCP" à la page 577. Si vous spécifiez un protocole, utilisez la forme suivante :

Type,*Protocol [parameters]*

Par exemple, vous pouvez utiliser l'option TCP,te pour spécifier le protocole TCP/IP.

Le tableau suivant montre les protocoles disponibles pour le fichier Devices.

TABLEAU 26–2 Protocoles utilisés dans le fichier /etc/uucp/Devices

Protocole	Description
t	Ce protocole est couramment utilisé pour les transmissions des données sur TCP/IP et autres connexions fiables. t suppose des transmissions sans erreur.
g	Ce protocole est le protocole UUCP natif. g est lent, fiable et adapté pour la transmission sur des lignes téléphoniques perturbées.

TABLEAU 26–2 Protocoles utilisés dans le fichier /etc/uucp/Devices *(Suite)*

Protocole	Description
e	Ce protocole suppose la transmission sur des canaux exempts d'erreur orientés message (par opposition aux canaux orientés flux d'octets), tels que TCP/IP.
f	Ce protocole est utilisé pour la transmission sur des connexions X.25. La valeur f s'appuie sur le contrôle du flux de données et est destinée à fonctionner sur des liens qui peuvent (presque) être garantis comme étant exempts d'erreurs, plus particulièrement les liens X.25/PAD. Une somme de contrôle est appliquée sur un fichier dans son intégralité uniquement. Si un transport échoue, le récepteur peut requérir la ou les retransmission(s).

Voici un exemple qui montre une désignation de protocole pour une entrée de périphérique :

```
TCP,te - - Any TCP -
```

Cet exemple indique que, pour le TCP du périphérique, vous devez essayer d'utiliser le protocole t. Si l'autre extrémité de la transmission refuse, utilisez le protocole e.

Ni e ni t ne sont adaptés pour être utilisés avec des modems. Même si le modem garantit une transmission exempte d'erreur, les données peuvent toujours être perdues entre le modem et l'UC.

Fichier /etc/uucp/Dialers UUCP

Le fichier /etc/uucp/Dialers contient des instructions de numérotation pour les modems les plus courants. Il est probable que vous n'ayez pas besoin de modifier ou d'ajouter d'entrées à ce fichier, sauf si vous prévoyez d'utiliser un modem non standard ou si vous envisagez de personnaliser votre environnement UUCP. Néanmoins, vous devez connaître le contenu de ce fichier et comment il se rapporte aux fichiers Systems et Devices.

Le texte rapporte la conversation initiale qui doit se produire sur une ligne avant la ligne qu'elle ne soit mise à disposition pour le transfert de données. Cette conversation, connue comme un script de discussion, est généralement une séquence de chaînes ASCII expect-send. Un script de discussion est souvent utilisé pour composer un numéro de téléphone.

Comme indiqué dans les exemples de la section “Fichier /etc/uucp/Devices UUCP” à la page 585, le cinquième champ d'une entrée du fichier Devices est un index renvoyant au fichier Dialers ou un type de dialer spécial, tel que TCP, TLI ou TLIS. Le démon uucico tente de faire correspondre le cinquième champ du fichier Devices avec le premier champ de chaque entrée du fichier Dialers. En outre, tous les champs impairs du fichier Devices, à partir de la septième position, sont utilisés comme un index vers le fichier Dialers. Si la correspondance est établie, l'entrée du fichier Dialers est interprétée afin d'effectuer la conversation avec le dialer.

Les entrées du fichier Dialers suivent la syntaxe suivante :

```
dialer   substitutions   expect-send
```

L'exemple suivant montre l'entrée d'un modem U.S. Robotics V.32bis.

EXEMPLE 26–10 Entrée du fichier /etc/uucp/fichier Dialers

```
usrv32bis-e    =,-,  ""    dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
                           \EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
```

usrv32bis-e
: Entrée du champ Dialer. Le champ Dialer correspond au cinquième champ et aux champs impairs supplémentaires du fichier Devices.

=,-, ""
: Entrée du champ Substitutions. Le champ Substitutions est une chaîne de translation. Le premier caractère de chaque paire est mappé avec le second caractère de la paire. Ce mappage est généralement utilisé pour traduire = et - au format requis par le dialer pour "attendre la tonalité" et "effectuer une pause".

dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r
: Entrée dans le champ Expect-Send. Les champs Expect-Send sont des chaînes de caractères.

\EATDT\T\r\c CONNECT\s14400/ARQ STTY=crtscts
: Plus de détails du champ Expect-Send.

L'exemple ci-dessous présente des échantillons d'entrées du fichier Dialers, comme distribuées lorsque vous installez UUCP dans le cadre du programme d'installation Solaris.

EXEMPLE 26–11 Extraits du fichier /etc/uucp/Dialers

```
penril    =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK

ventel    =&-%    "" \r\p\r\c $ <K\T%%\r>\c ONLINE!

vadic    =K-K    "" \005\p *-\005\p-*\005\p-* D\p BER? \E\T\e \r\c LINE

develcon    ""    "" \pr\ps\c est:\007

\E\D\e \n\007 micom    ""    "" \s\c NAME? \D\r\c GO

hayes    =,-,    "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r \EATDT\T\r\c CONNECT

#   Telebit TrailBlazer
tb1200    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=2\r\c OK\r
\EATDT\T\r\c CONNECT\s1200
tb2400    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=3\r\c OK\r
\EATDT\T\r\c CONNECT\s2400
tbfast    =W-,    "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=255\r\c OK\r
\EATDT\T\r\c CONNECT\sFAST

# USrobotics, Codes, and DSI modems

dsi-ec  =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
```

EXEMPLE 26–11 Extraits du fichier /etc/uucp/Dialers *(Suite)*

```
CONNECT\sEC STTY=crtscts,crtsxoff

dsi-nec =,-,    "" \dA\pTE1V1X5Q0S2=255S12=255*E0*F3*M1*S1\r\c OK\r \EATDT\T\r\c CONNECT
STTY=crtscts,crtsxoff

usrv32bis-ec =,-,  "" \dA\pT&FE1V1X1Q0S2=255S12=255&A1&H1&M5&B2&W\r\c OK\r \EATDT\T\r\c
CONNECT\s14400/ARQ STTY=crtscts,crtsxoff

usrv32-nec =,-, "" \dA\pT&FE1V1X1Q0S2=255S12=255&A0&H1&M0&B0&W\r\c OK\r \EATDT\T\r\c
CONNECT STTY=crtscts,crtsxoff

codex-fast =,-, "" \dA\pT&C1&D2*MF0*AA1&R1&S1*DE15*FL3S2=255S7=40S10=40*TT5&W\r\c OK\r
\EATDT\T\r\c CONNECT\s38400 STTY=crtscts,crtsxoff

tb9600-ec =W-,  "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6\r\c OK\r
\EATDT\T\r\cCONNECT\s9600 STTY=crtscts,crtsxoff

tb9600-nec =W-, "" \dA\pA\pA\pTE1V1X1Q0S2=255S12=255S50=6S180=0\r\c OK\r \EATDT\T\r\c
CONNECT\s9600 STTY=crtscts,crtsxoff
```

Le tableau suivant répertorie les caractères d'échappement couramment utilisés dans les chaînes send du fichier `Dialers`.

TABLEAU 26–3 Caractères backslash pour le fichier /etc/uucp/Dialers

Caractère	Description
\b	Envoie ou attend un caractère de retour arrière.
\c	Aucune nouvelle ligne ni aucun retour chariot.
\d	Applique un délai d'environ 2 secondes.
\D	Numéro de téléphone ou jeton sans translation dans le fichier `Dialcodes`.
\e	Désactive la vérification d'écho.
\E	Active la vérification d'écho pour les périphériques lents.
\K	Insère un caractère de saut.
\n	Envoie une nouvelle ligne.
\nnn	Envoie un nombre octal. Des caractères d'échappement supplémentaires pouvant être utilisés sont répertoriés à la section "Fichier /etc/uucp/Systems UUCP" à la page 577.
\n	Envoie ou attend un caractère NUL (ASCII NUL).
\p	S'interrompt pendant environ 12 à 14 secondes.
\r	Applique un renvoi.

TABLEAU 26–3 Caractères backslash pour le fichier /etc/uucp/Dialers *(Suite)*

Caractère	Description
\s	Envoie ou attend un caractère d'espace.
\T	Numéro de téléphone ou jeton avec translation dans le fichier Dialcodes.

Voici une entrée penril dans le fichier Dialers :

```
penril =W-P "" \d > Q\c : \d- > s\p9\c )-W\p\r\ds\p9\c-) y\c : \E\TP > 9\c OK
```

Tout d'abord, le mécanisme de substitution pour l'argument de numéro de téléphone est établi afin que tout signe = soit remplacé par un W (attendre la tonalité) et tout signe - par un P (pause).

La procédure d'établissement de connexion donnée par le reste de la ligne fonctionne comme indiqué :

- "" : n'attend rien, ce qui signifie passer à l'étape suivante.
- \d : applique un délai d'attente de 2 secondes, puis envoie un retour chariot.
- > : attend un signe >.
- Q\c : envoie un caractère Q sans retour chariot.
- : : attend un signe :.
- \d- : applique un délai de 2 secondes, envoie un signe - et un retour chariot.
- > : attend un signe >.
- s\p9\c : envoie un signe s, effectue une pause, envoie un caractère 9 sans retour chariot.
-)-W\p\r\ds\p9\c-) : attend un signe) . Si) n'est pas reçu, traite la chaîne entre caractères - comme suit. Envoie un caractère W, effectue une pause, envoie un retour chariot, applique des délais, envoie un caractère s, effectue une pause, envoie un caractère 9 sans retour chariot, puis attend le caractère).
- y\c : envoie un caractère y sans retour chariot.
- : : attend un caractère :.
- \E\TP : \E permet la vérification d'écho. À partir de ce point, chaque fois qu'un caractère est transmis, l'UUCP attend que le caractère soit reçu avant de poursuivre. Ensuite, UUCP envoie le numéro de téléphone. Le caractère \T indique de prendre le numéro de téléphone transmis sous la forme d'un argument. Le caractère \T applique la translation du fichier Dialcodes et la translation de la fonction du modem spécifiée par le champ 2 de cette entrée. Le caractère \T envoie alors un caractère P et un retour chariot.
- > : attend un signe >.
- 9\c : envoie un caractère 9 sans nouvelle ligne.
- OK : attend la chaîne OK.

Activation du contrôle de flux matériel dans le fichier /etc/uucp/Dialers

Vous pouvez également utiliser la chaîne de pseudo-envoi STTY=*valeur* pour définir les caractéristiques du modem. Par exemple, STTY=crtscts active le contrôle de flux matériel sortant. STTY=crtsxoff active le contrôle de flux matériel entrant. STTY=crtscts,crtsxoff active le contrôle de flux matériel à la fois entrant et sortant.

STTY accepte tous les modes stty. Reportez-vous aux pages de manuel stty(1) et termio(7I).

L'exemple suivant activerait le contrôle de flux matériel dans une entrée du fichier Dialers :

```
dsi =,–, "" \dA\pTE1V1X5Q0S2=255S12=255*E1*F3*M1*S1\r\c OK\r \EATDT\T\r\c
CONNECT\sEC STTY=crtscts
```

Cette chaîne de pseudo-envoi peut également être utilisée dans les entrées du fichier Systems.

Définition de la parité dans le fichier /etc/uucp/Dialers

Dans certaines situations, vous devez réinitialiser la parité car le système que vous appelez vérifie la parité des ports et supprime la ligne si elle est incorrecte. La paire Expect-Send P_ZERO définit la parité à zéro :

```
foo =,-, "" P_ZERO "" \dA\pTE1V1X1Q0S2=255S12=255\r\c OK\r\EATDT\T\r\c CONNECT
```

Vous trouverez ci-dessous les paires de parité pouvant suivre la paire Expect-Send :

"" P_EVEN Définit la parité sur pair, qui est la valeur par défaut

"" P_ODD Définit la parité sur impair

"" P_ONE Définit la parité sur un

Cette chaîne de pseudo-envoi peut également être utilisée dans les entrées du fichier Systems.

Autres fichiers de configuration UUCP de base

Vous pouvez utiliser les fichiers de cette section en plus des fichiers Systems, Devices et Dialers lorsque vous effectuez la configuration de base d'UUCP.

Fichier /etc/uucp/Dialcodes UUCP

Le fichier /etc/uucp/Dialcodes permet de définir les abréviations d'accès direct pouvant être utilisées dans le champ Phone du fichier /etc/uucp/Systems. Vous pouvez utiliser le fichier Dialcodes pour fournir des informations supplémentaires sur un numéro de téléphone de base utilisé par plusieurs systèmes sur le même site.

Chaque entrée applique la syntaxe suivante :

```
Abbreviation   Dial-Sequence
```

Abbreviation — Ce champ fournit l'abréviation utilisée dans le champ Phone du fichier Systems.

Dial-Sequence — Ce champ indique la séquence de numérotation transmise au dialer lors de l'accès à cette entrée particulière du fichier Systems.

Comparez les champs dans les deux fichiers. Les champs suivants sont ceux du fichier Dialcodes.

```
Abbreviation   Dial-Sequence
```

Les champs suivants sont ceux du fichier Systems.

```
System-Name   Time   Type   Speed   Phone   Chat Script
```

Le tableau ci-après contient un exemple de contenu pour les champs d'un Dialcodes.

TABLEAU 26–4 Entrées dans le fichier Dialcodes

Abréviation	Séquence de numérotation
NY	1=212
jt	9+847

Dans la première ligne, NY est l'abréviation qui s'affichera dans le champ Phone du fichier Systems. Le fichier System peut par exemple contenir l'entrée suivante :

```
NY5551212
```

Lorsque le démon uucico lit NY dans le fichier Systems, uucico recherche NY dans le fichier Dialcodes et obtient la séquence de numérotation 1=212 . 1=212 est la séquence de numérotation requise pour tout appel téléphonique à New York. Cette séquence inclut le nombre 1, un signe égale (=) qui indique d'effectuer une pause et d'attendre une tonalité secondaire, et l'indicatif de zone 212. uucico envoie ces informations au dialer, puis revient au fichier Systems pour le reste du numéro de téléphone, 5551212.

L'entrée `jt 9=847-` fonctionnerait avec un champ Phone tel que `jt7867` dans le fichier `Systems`. Quand `uucico` lit l'entrée qui contient `jt7867` dans le fichier `Systems`, `uucico` envoie la séquence `9=847-7867` au dialer, si le jeton dans la paire dialer-jeton est `\T`.

Fichier `/etc/uucp/Sysfiles` UUCP

Le fichier `/etc/uucp/Sysfiles` vous permet d'assigner des fichiers différents à utiliser aux commandes `uucp` et `cu` comme fichiers `Systems`, `Devices` et `Dialers`. Pour plus d'informations sur la commande `cu`, reportez-vous à la page de manuel cu(1C) Vous pouvez utiliser le fichier `Sysfiles` pour l'un des éléments suivants :

- Fichiers `Systems` différents de façon à ce que les requêtes de services de connexion puissent être effectuées à d'autres adresses que les services `uucp`.
- Fichiers `Dialers` différents de façon à ce que vous puissiez affecter différents protocoles d'établissement de connexion aux commandes `cu` et `uucp`.
- Fichiers `Systems`, `Dialers` et `Devices` multiples. Le fichier `Systems` en particulier peut devenir important, de sorte qu'il s'avère plus pratique de le diviser en plusieurs fichiers de plus petite taille.

La syntaxe du fichier `Sysfiles` est la suivante :

```
service=w systems=x:x dialers=y:y devices=z:z
```

w Représente `uucico`, `cu` ou les deux commandes séparées par deux-points

x Représente un ou plusieurs fichiers à utiliser comme fichier `Systems`, les noms de fichiers étant séparés par une virgule et lus dans l'ordre dans lequel ils se présentent

y Représente un ou plusieurs fichiers à utiliser comme fichier `Dialers`

z Représente un ou plusieurs fichiers à utiliser comme fichier `Devices`

On suppose que le nom de chaque fichier est relatif au répertoire `/etc/uucp`, sauf si un chemin d'accès complet est fourni.

L'exemple suivant, `/etc/uucp/Sysfiles`, définit un fichier `Systems` local (`Local_Systems`) en plus du fichier `/etc/uucp/Systems` standard :

```
service=uucico:cu systems=Systems :Local_Systems
```

Lorsque cette entrée se trouve dans le fichier `/etc/uucp/Sysfiles`, les commandes `uucico` et `cu` vérifient d'abord dans le fichier `/etc/uucp/Systems` standard. Si le système appelé ne possède pas d'entrée dans ce fichier ou si les entrées dans le fichier échouent, les deux commandes vérifient le fichier `/etc/uucp/Local_Systems`.

Comme indiqué dans l'entrée précédente, les commandes `cu` et `uucico` partagent les fichiers `Dialers` et `Devices`.

Lorsque plusieurs fichiers Systems sont définis pour les services uucico et cu, votre ordinateur enregistre deux listes différentes pour Systems. Vous pouvez imprimer la liste uucico en utilisant la commande uuname ou la liste cu en utilisant la commande uuname -C. Voici un autre exemple de fichier, qui indique que d'autres fichiers sont consultés en premier, puis les fichiers par défaut sont consultés si nécessaire :

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
devices=Devices.cico:Devices
  service=cu systems=Systems.cu:Systems \
dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

Fichier /etc/uucp/Sysname UUCP

Chaque ordinateur qui utilise UUCP doit avoir un nom d'identifiant, souvent appelé *nom de nœud*. Le nom du nœud apparaît dans le fichier /etc/uucp/Systems de l'ordinateur distant, de même que le script de discussion et d'autres informations d'identification. Normalement, UUCP utilise le même nom de nœud que celui renvoyé par la commande uname -n, également utilisé par le protocole TCP/IP.

Vous pouvez spécifier un nom de nœud UUCP indépendant du nom d'hôte TCP/IP en créant le fichier /etc/uucp/Sysname. Le fichier possède une entrée d'une ligne qui contient le nom du nœud UUCP pour votre système.

Fichier /etc/uucp/Permissions UUCP

Le fichier /etc/uucp/Permissions spécifie les autorisations des ordinateurs distants en matière de connexion, d'accès aux fichiers et d'exécution des commandes. Certaines options restreignent la capacité de l'ordinateur distant à envoyer des requêtes aux fichiers et sa capacité à recevoir les fichiers mis en file d'attente par l'ordinateur local. Une autre option disponible permet de spécifier les commandes qu'un ordinateur distant peut exécuter sur l'ordinateur local.

Structuration des entrées UUCP

Chaque entrée est une ligne logique, avec des lignes physiques terminées par un backslash (\) pour indiquer qu'elles continuent. Les entrées sont composés d'options délimitées par une espace. Chaque option est une paire nom-valeur dans le format suivant :

name=value

values peut consister en des listes séparés par deux points. Aucune espace n'est autorisée au sein d'une affectation d'option.

Les lignes de commentaires commencent par le signe dièse (#) et occupent l'intégralité de la ligne jusqu'à un caractère de nouvelle ligne. Les lignes vides sont ignorées, même au sein d'entrées à plusieurs lignes.

Les types d'entrées du fichier `Permissions` sont les suivants :

- `LOGNAME` : spécifie les autorisations qui entrent en vigueur lorsqu'un ordinateur distant se connecte à (appelle) votre ordinateur.

  Remarque – Lorsqu'un ordinateur distant vous appelle, son identité est douteuse sauf si l'ordinateur distant possède un identifiant de connexion unique et un mot de passe vérifiable.

- `MACHINE` : spécifie les autorisations qui entrent en vigueur lorsque votre ordinateur se connecte à (appelle) un ordinateur distant.

Les entrées `LOGNAME` contiennent une option `LOGNAME`. Les entrées `MACHINE` contiennent une option `MACHINE`. Une entrée peut contenir les deux options.

Éléments à prendre en compte relatifs au protocole UUCP

Lors de l'utilisation du fichier `Permissions` pour limiter les autorisations accordées à des ordinateurs distants, vous devez prendre en compte les éléments suivants :

- Tous les ID de connexion utilisés par les ordinateurs distants pour se connecter pour les communications UUCP doivent apparaître dans une seule et unique entrée `LOGNAME`.
- Tous les sites appelés avec un nom qui ne figure pas dans une entrée `MACHINE` comportent les autorisations ou restrictions par défaut suivantes :
  - Les requêtes d'envoi et de réception locales sont exécutées.
  - L'ordinateur distant peut envoyer des fichiers au répertoire `/var/spool/uucppublic` de votre ordinateur.
  - Les commandes qui sont envoyées par l'ordinateur distant pour être exécutées sur votre ordinateur doit être l'une des commandes par défaut, généralement `rmail`.

Option REQUEST UUCP

Lorsqu'un ordinateur distant appelle votre ordinateur et effectue une requête de réception de fichier, cette requête peut être autorisée ou refusée. L'option REQUEST indique si l'ordinateur distant peut envoyer une requête afin de configurer les transferts de fichiers à partir de votre ordinateur. La chaîne REQUEST=yes indique que l'ordinateur distant peut demander à transférer des fichiers à partir de votre ordinateur. La chaîne REQUEST=no indique que l'ordinateur distant ne peut pas demander à recevoir de fichiers depuis votre ordinateur. REQUEST=no, la valeur par défaut, est utilisée si l'option REQUEST n'est pas spécifiée. L'option REQUEST peut apparaître dans une entrée LOGNAME, de sorte que l'ordinateur distant vous appelle, ou dans l'entrée MACHINE, de sorte que vous pouvez appeler l'ordinateur distant.

Option SENDFILES UUCP

Lorsqu'un ordinateur distant appelle votre ordinateur et termine son travail, l'ordinateur distant peut tenter de récupérer le travail que votre ordinateur a mis en file d'attente. L'option SENDFILES indique si votre ordinateur peut envoyer le travail mis en file d'attente pour l'ordinateur distant.

La chaîne SENDFILES=yes indique que l'ordinateur peut envoyer le travail en attente pour l'ordinateur distant si la connexion est établie à l'un des noms figurant dans l'option LOGNAME. Cette chaîne est *obligatoire* si vous avez saisi Never dans le champ Time du fichier /etc/uucp/Systems. Cette désignation configure votre machine locale en mode passif, mais ne l'autorise pas à lancer un appel vers cet ordinateur distant. Pour plus d'informations, reportez-vous à la section “Fichier /etc/uucp/Systems UUCP” à la page 577.

La chaîne SENDFILES=call indique que les fichiers en attente sur votre ordinateur sont envoyés uniquement lorsque votre ordinateur appelle l'ordinateur distant. La valeur call est la valeur par défaut pour l'option SENDFILES. Cette option est significative uniquement dans les entrées LOGNAME, car les entrées MACHINE s'appliquent lorsque des appels sont envoyés vers des ordinateurs distants. Si l'option est utilisée avec une entrée MACHINE, elle est ignorée.

Option MYNAME UUCP

Cette option vous permet de définir un nom de nœud UUCP unique pour votre ordinateur en plus de son nom d'hôte TCP/IP, tel que renvoyé par la commande hostname. Par exemple, si vous avez involontairement donné à votre hôte le même nom que celui d'un autre système, vous pouvez définir l'option MYNAME du fichier Permissions. Supposons que vous souhaitiez que votre société soit connue sous le nom widget. Si tous les modems sont connectés à une machine avec le nom d'hôte gadget , vous pouvez avoir une entrée dans le fichier Permissions de gadgettelle que la suivante :

```
service=uucico systems=Systems.cico:Systems
  dialers=Dialers.cico:Dialers \
  devices=Devices.cico:Devices
service=cu systems=Systems.cu:Systems \
  dialers=Dialers.cu:Dialers \
  devices=Devices.cu:Devices
```

À présent, le système `world` peut se connecter à l'ordinateur `gadget` de la même manière que si il se connectait à `widget`. Afin que la machine `world` vous connaisse également par l'alias `widget` lorsque vous appelez, vous pouvez avoir une entrée similaire à la suivante :

```
MACHINE=world MYNAME=widget
```

Vous pouvez également utiliser l'option `MYNAME` à des fins de test, étant donné que cette option permet à votre ordinateur de s'appeler lui-même. Toutefois, étant donné que cette option pourrait être utilisée pour masquer l'identité réelle d'un ordinateur, vous devez utiliser l'option `VALIDATE`, tel que décrit à la section “Option `VALIDATE` UUCP” à la page 604.

Options `READ` et `WRITE` UUCP

Ces options spécifient les différentes parties du système de fichiers que la commande `uucico` peut lire ou sur lesquelles elle peut écrire. Vous pouvez désigner les options `READ` et `WRITE` avec une entrée `MACHINE` ou `LOGNAME`.

La valeur par défaut des options `READ` et `WRITE` est le répertoire `uucppublic`, comme indiqué dans les chaînes suivantes :

```
READ=/var/spool/uucppublic WRITE=/var/spool/uucppublic
```

Les chaînes `READ=/` et `WRITE=/` indiquent l'autorisation d'accéder à tous les fichiers accessibles par un utilisateur local disposant d'autorisations Other.

La valeur de ces entrées est une liste séparée par deux-points de noms de chemin. L'option `READ` permet de demander des fichiers et l'option `WRITE` de déposer des fichiers. L'une des valeurs doit être le préfixe du nom du chemin d'accès complet d'un fichier entrant ou sortant. Pour accorder l'autorisation de déposer des fichiers dans `/usr/news`, ainsi que dans le répertoire public, utilisez les valeurs suivantes avec l'option `WRITE` :

```
WRITE=/var/spool/uucppublic:/usr/news
```

Si les options `READ` et `WRITE` sont utilisées, tous les noms de chemin doivent être spécifiés car ils ne sont pas ajoutés à la liste par défaut. Par exemple, si le nom de chemin `/usr/news` était le seul chemin spécifié dans une option `WRITE`, l'autorisation de déposer des fichiers dans le répertoire public serait refusée.

Soyez prudent lorsque vous définissez les répertoires accessibles en lecture et en écriture aux systèmes distants. Par exemple, le répertoire /etc contient de nombreux fichiers système critiques. Les utilisateurs distants ne doivent pas être autorisés à déposer des fichiers dans ce répertoire.

Options NOREAD et NOWRITE UUCP

Les options NOREAD et NOWRITE permettent de spécifier des exceptions aux options READ et WRITE ou aux valeurs par défaut. L'entrée suivante autorise la lecture de n'importe quel fichier, à l'exception des fichiers présents dans le répertoire /etc (et ses sous-répertoires). N'oubliez pas que ces options sont des préfixes.

```
READ=/ NOREAD=/etc WRITE=/var/spool/uucppublic
```

Cette entrée autorise uniquement à écrire dans le répertoire /var/spool/uucppublic par défaut. L'option NOWRITE fonctionne de la même manière que l'option NOREAD. Vous pouvez utiliser les options NOREAD et NOWRITE dans les entrées LOGNAME et MACHINE.

Option CALLBACK UUCP

Vous pouvez utiliser l'option CALLBACK des entrées LOGNAME pour indiquer qu'aucune transaction ne se produit jusqu'à ce que le système appelant soit rappelé. Les raisons de configurer l'option CALLBACK sont les suivantes :

- Sécurité : si vous rappelez un ordinateur, vous pouvez être sûr qu'il s'agit du bon ordinateur.
- Comptabilité : si vous effectuez de longues transmissions de données, vous pouvez choisir l'ordinateur facturé pour l'appel le plus long.

La chaîne CALLBACK=yes indique que votre ordinateur doit rappeler l'ordinateur distant avant que le transfert de fichiers ne se produise.

La valeur par défaut pour l'option CALLBACK est CALLBACK=no. Si vous définissez l'option CALLBACK sur yes, les autorisations qui ont une incidence sur le reste de la conversation doivent être spécifiées dans l'entrée MACHINE correspondant à l'appelant. N'indiquez pas ces autorisations dans l'entrée LOGNAME ou dans l'entrée LOGNAME que l'ordinateur distant peut avoir défini pour votre hôte.

Remarque – Si l'option CALLBACK est définie mutuellement pour deux sites, aucune conversation n'est jamais démarrée.

Option COMMANDS UUCP

Attention – L'option COMMANDS peut compromettre la sécurité de votre système. Utilisez-la avec une extrême précaution.

Vous pouvez utiliser l'option COMMANDS des entrées MACHINE pour spécifier les commandes qu'un ordinateur distant peut exécuter sur votre ordinateur. Le programme uux génère des requêtes d'exécution à distance et établit des files d'attente des requêtes à transférer vers l'ordinateur distant. Les commandes et fichiers sont envoyés à l'ordinateur cible pour une exécution à distance, ce qui est une exception à la règle selon laquelle les entrées MACHINE s'appliquent uniquement lorsque votre système appelle.

Notez que l'option COMMANDS n'est pas utilisée dans une entrée LOGNAME. L'option COMMANDS dans les entrées MACHINE définit les autorisations des commandes, que vous appeliez le système distant ou vice-versa.

La chaîne COMMANDS=rmail spécifie les commandes par défaut qu'un ordinateur distant peut exécuter sur votre ordinateur. Si une chaîne de commande est utilisée dans une entrée MACHINE, les commandes par défaut sont remplacées. Par exemple, l'entrée suivante remplace l'option COMMAND par défaut, de sorte que les ordinateurs nommés owl, raven, hawk et dove peuvent désormais exécuter les commandes rmail, rnews et lp sur votre ordinateur.

```
MACHINE=owl:raven:hawk:dove COMMANDS=rmail:rnews:lp
```

En plus des noms, tels que ceux de l'exemple précédent, vous pouvez spécifier des noms du chemin d'accès complet des commandes. Par exemple, l'entrée suivante indique que la commande rmail utilise le chemin de recherche par défaut.

```
COMMANDS=rmail:/usr/local/rnews:/usr/local/lp
```

Le chemin de recherche par défaut pour UUCP est /bin et /usr/bin. Lorsque l'ordinateur distant spécifie rnews ou /usr/local/rnews pour la commande à exécuter, la commande /usr/local/rnews est exécutée indépendamment de ce chemin d'accès par défaut. De même, /usr/local/lp est la commande lp qui est exécutée.

L'inclusion de la valeur ALL dans la liste signifie que toute commande émise par les ordinateurs distants spécifiés dans l'entrée est exécutée. Si vous utilisez cette valeur, vous donnez aux ordinateurs distants un accès complet à votre ordinateur.

Attention – Cette valeur autorise davantage d'accès que celui qu'ont les utilisateurs standard. N'utilisez cette valeur que lorsque les deux ordinateurs se trouvent sur le même site, sont étroitement liés et que les utilisateurs sont de confiance.

Voici la chaîne avec la valeur ALL ajoutée :

```
COMMANDS=/usr/local/rnews:ALL:/usr/local/lp
```

Cette chaîne illustre deux points :

- La valeur ALL peut figurer n'importe où dans la chaîne.
- Les noms de chemin d'accès spécifiés pour rnews et lp sont utilisés (au lieu du nom par défaut) si la commande demandée ne contient pas les noms de chemin d'accès complets pour rnews ou lp.

Utilisez l'option VALIDATE chaque fois que vous indiquez des commandes potentiellement dangereuses, telles que cat et uucp avec l'option COMMANDS. Toute commande qui lit ou écrit des fichiers présente un danger potentiel pour la sécurité locale lorsque la commande est exécutée par le démon d'exécution à distance UUCP (uuxqt).

Option VALIDATE UUCP

Utilisez l'option VALIDATE avec l'option COMMANDS chaque fois que vous spécifiez des commandes présentant un danger potentiel pour la sécurité de votre ordinateur. L'option VALIDATE est simplement un niveau de sécurité supplémentaire ajouté à l'option COMMANDS, bien qu'elle représente un moyen plus sécurisé d'ouvrir l'accès aux commandes que l'option ALL.

L'option VALIDATE fournit un certain degré de vérification de l'identité de l'appelant en effectuant un contrôle croisé du nom d'hôte d'un ordinateur appelant par rapport au nom de connexion qu'il utilise. La chaîne suivante garantit que si un ordinateur autre que widget ou gadget tente de se connecter en tant que Uwidget, la connexion sera refusée.

```
LOGNAME=Uwidget VALIDATE=widget:gadget
```

L'option VALIDATE requiert que les ordinateurs disposant de privilèges aient un identifiant de connexion unique et un mot de passe pour les transactions UUCP. L'un des aspects importants de cette validation est que l'identifiant de connexion et le mot de passe associés à cette entrée soient protégés. Si un intrus obtient ces informations, cette option VALIDATE particulière ne peut plus être considérée comme sécurisée.

Réfléchissez bien aux ordinateurs distants auxquels vous accordez des identifiants et des mots de passe disposant de privilèges pour les transactions UUCP. L'attribution d'un identifiant de connexion et d'un mot de passe spéciaux à un ordinateur distant avec la possibilité d'accéder aux fichiers et d'exécuter des commandes à distance revient à donner à une personne sur cet ordinateur un identifiant de connexion et un mot de passe normaux sur votre ordinateur. Par conséquent, si vous ne pouvez pas faire confiance à quelqu'un sur l'ordinateur distant, vous ne devez pas fournir d'identifiant de connexion disposant de privilèges et de mot de passe à cet ordinateur.

L'entrée LOGNAME suivante spécifie que si l'un des ordinateurs distants qui prétend être eagle, owl ou hawk se connecte sur votre ordinateur, il doit avoir utilisé l'identifiant de connexion uucpfriend :

```
LOGNAME=uucpfriend VALIDATE=eagle:owl:hawk
```

Si un intrus obtient l'identifiant et le mot de passe uucpfriend, l'usurpation d'identité est facile.

Quel est le rapport de cette entrée avec l'option COMMANDS, qui apparaît uniquement dans les entrées MACHINE ? Cette entrée lie l'entrée MACHINE (et l'option COMMANDS) à une entrée LOGNAME associée à un identifiant de connexion disposant de privilèges. Ce lien est nécessaire car le démon d'exécution n'est pas exécuté pendant que l'ordinateur distant est connecté. En fait, le lien est un processus asynchrone qui ne sait pas quel ordinateur a envoyé la requête d'exécution. Par conséquent, la vraie question est celle-ci : comment votre ordinateur connaît-il la provenance des fichiers d'exécution ?

Chaque ordinateur distant dispose de son propre répertoire spool sur votre machine locale. Ces répertoires spool disposent d'une autorisation d'écriture qui est uniquement accordée aux programmes UUCP. Les fichiers d'exécution issus de l'ordinateur distant sont placés dans son répertoire spool après avoir été transférés sur votre ordinateur. Lorsque le démon uuxqt s'exécute, il peut utiliser le nom du répertoire spool pour rechercher l'entrée MACHINE dans le Permissions et obtenir la liste COMMANDS. Ou, si le nom de l'ordinateur n'apparaît pas dans le fichier Permissions, la liste par défaut est utilisée.

Cet exemple montre la relation entre les entrées MACHINE et LOGNAME :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
COMMANDS=rmail:/usr/local/rnews \
READ=/ WRITE=/
LOGNAME=uucpz VALIDATE=eagle:owl:hawk \
REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

La valeur dans l'option COMMANDS signifie que les utilisateurs distants peuvent exécuter les commandes rmail et /usr/local/rnews .

Dans la première entrée, vous devez supposer que lorsque vous souhaitez appeler l'un des ordinateurs répertoriés, vous êtes appelez en fait eagle, owl ou hawk. Par conséquent, tous les fichiers placés dans l'un des répertoires spool eagle, owl ou hawk l'est par l'un de ces ordinateurs. Si un ordinateur distant se connecte et dit qu'il s'agit de l'un de ces trois ordinateurs, ses fichiers d'exécution sont également placés dans le répertoire spool disposant de privilèges. Par conséquent, vous devez confirmer que l'ordinateur possède l'identifiant de connexion disposant de privilège uucpz.

Entrée MACHINE UUCP pour l'option OTHER

Vous pouvez spécifier différentes valeurs d'option pour les ordinateurs distants qui ne sont pas mentionnés dans des entrées MACHINE spécifiques. Cela peut s'avérer nécessaire lorsque de nombreux ordinateurs appellent votre hôte et que l'ensemble de commandes change de temps en temps. Le nom OTHER pour le nom de l'ordinateur est utilisée pour cette entrée comme indiqué dans cet exemple :

```
MACHINE=OTHER \
COMMANDS=rmail:rnews:/usr/local/Photo:/usr/local/xp
```

Toutes les autres options disponibles pour l'entrée MACHINE peuvent également être définies pour les ordinateurs qui ne sont pas mentionnées dans d'autres entrées MACHINE.

Combinaison des entrées MACHINE et LOGNAME pour UUCP

Vous pouvez combiner les entrées MACHINE et LOGNAME en une seule entrée lorsque les options communes sont identiques. Par exemple, les deux ensembles d'entrées qui suivent partagent les mêmes options REQUEST, READ et WRITE :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
READ=/ WRITE=/
```

et

```
LOGNAME=uupz REQUEST=yes SENDFILES=yes \
READ=/ WRITE=/
```

Vous pouvez fusionner ces entrées, comme indiqué ci-dessous :

```
MACHINE=eagle:owl:hawk REQUEST=yes \
logname=uucpz SENDFILES-yes \
READ=/ WRITE=/
```

La combinaison des entrées MACHINE et LOGNAME facilite la gestion et améliore l'efficacité du fichier Permissions.

Transfert UUCP

Lors de l'envoi de fichiers via plusieurs ordinateurs, les ordinateurs intermédiaires doivent posséder la commande uucp parmi leurs options COMMANDS. Si vous saisissez la commande suivante, l'opération de transfert ne fonctionnera que si l'ordinateur willow autorise l'ordinateur oak à exécuter le programme uucp.

```
% uucp sample.txt oak\!willow\!pine\!/usr/spool/uucppublic
```

L'ordinateur oak doit également autoriser votre ordinateur à exécuter le programme uucp. L'ordinateur pine, en tant que dernier ordinateur désigné, n'a pas à autoriser la commande uucp car l'ordinateur n'effectue aucune opération de transfert. Les ordinateurs ne sont généralement pas configurés de cette manière.

Fichier /etc/uucp/Poll UUCP

Le fichier /etc/uucp/sondage contient des informations pour l'interrogation des ordinateurs distants. Chaque entrée du fichier Poll contient le nom d'un ordinateur distant à appeler, suivi d'un caractère de tabulation ou une espace, puis des heures auxquelles l'ordinateur doit être appelé. Le format des entrées dans le fichier Poll est le suivant :

sys-name hour ...

Par exemple, l'entrée **eagle 0 4 8 12 16 20** définit l'interrogation de l'ordinateur eagle toutes les quatre heures.

Le script uudemon.poll traite le fichier Poll mais n'effectue pas vraiment le sondage. Le script configure simplement un fichier de travail d'interrogation (toujours nommé C.*file*) dans le répertoire spool. Le script uudemon.poll lance l'ordonnanceur, et celui-ci examine tous les fichiers de travail du répertoire spool.

Fichier /etc/uucp/Config UUCP

Le fichier /etc/uucp/Config permet de remplacer certains paramètres manuellement. Chaque entrée du fichier Config adopte le format suivant :

paramètre=valeur

Reportez-vous au fichier Config fourni avec votre système pour une liste complète des noms de paramètres configurables.

L'entrée Config suivante définit l'ordre du protocole par défaut sur Gge et modifie la valeur par défaut du protocole G à 7 fenêtres et paquets de 512 octets.

```
Protocol=G(7,512)ge
```

Fichier /etc/uucp/Grades UUCP

Le fichier /etc/uucp/Grades contient les définitions des niveaux de travail pouvant être utilisés pour mettre des travaux en attente sur un ordinateur distant. Ce fichier contient également les autorisations correspondant à chaque niveau de travail. Chaque entrée de ce fichier représente une définition d'un niveau de travail défini par l'administrateur qui permet aux utilisateurs de mettre des travaux en attente.

Chaque entrée du fichier Grades adopte le format suivant :

User-job-grade System-job-grade Job-size Permit-type ID-list

Chaque entrée contient des champs séparés par une espace. Le dernier champ de l'entrée est composé de sous-champs également séparés par des espaces. Si une entrée occupe plus d'une ligne physique, vous pouvez utiliser un backslash pour continuer l'entrée sur la ligne suivante. Les lignes de commentaires commencent par le signe dièse (#) et occupent l'intégralité de la ligne. Les lignes vides sont toujours ignorées.

Champ User-job-grade UUCP

Ce champ contient un nom de niveau de travail utilisateur défini par l'administrateur, d'un maximum de 64 caractères.

Champ System-job-grade UUCP

Ce champ contient un niveau de travail d'un caractère auquel la valeur *User-job-grade* est mappée. La liste des caractères valides est A à Z, a à z, A ayant la priorité la plus élevée et z la plus basse.

Relations entre les niveaux de travail utilisateur et système

Le niveau de travail utilisateur peut être lié à plusieurs niveaux de travail système. Notez que les occurrences d'un niveau de travail utilisateur sont recherchée de manière séquentielle dans le fichier Grades. Par conséquent, les occurrences multiples d'un niveau de travail système doivent être répertoriées conformément aux restrictions en termes de taille maximale d'un travail.

Bien qu'aucun nombre maximal n'existe pour les niveaux de travail utilisateur, le nombre maximal de niveaux de travail système autorisé est de 52. La raison en est que plusieurs *User-job-grade* peuvent être mappés à un *System-job-grade*, mais chaque *User-job-grade* doit figurer sur une ligne distincte dans le fichier. Voici un exemple concret :

```
mail N Any User Any netnews N Any User Any
```

Si cette configuration se trouve dans un fichier Grades, ces deux champs *User-job-grade* partagent le même niveau *System-job-grade* . Les autorisations pour un *travail-grade* étant associées à un *User-job-grade* et non un *System-job-grade*, deux *User-job-grade* peuvent partager le même *System-job-grade* et avoir deux ensembles d'autorisations différents.

Niveau par défaut

Vous pouvez définir la liaison d'une valeur *User-job-grade* par défaut avec un niveau de travail système. Vous devez utiliser le mot-clé par défaut en tant que niveau de travail utilisateur dans le champ *User-job-grade* du fichier Grades et le niveau de travail système auquel il est lié. Les champs Restrictions et ID devraient être définis sur Any de sorte que tous les utilisateurs et les travaux de toutes tailles puissent être mis en attente à ce niveau. Voici un exemple concret :

```
default a Any User Any
```

Si vous ne définissez pas de niveau de travail utilisateur par défaut, le niveau par défaut intégré, Z, est utilisé. La valeur par défaut du champ Restriction étant Any, les occurrences multiples du niveau par défaut ne sont pas vérifiées.

Champ Job-size UUCP

Ce champ indique la taille maximale d'un travail pouvant être intégré à la file d'attente. La valeur *Job-size* est mesurée en octets et peut être une liste des options décrites dans la liste suivante.

nnnn	Nombre entier qui spécifie la taille maximale d'un travail pour ce niveau de travail
n K	Nombre décimal qui représente le nombre de kilo-octets (K est l'abréviation de kilo-octets)
n M	Nombre décimal qui représente le nombre de méga-octets (M est l'abréviation de méga-octets)
Any	Mot-clé qui indique qu'aucune la taille maximale de travail ne s'applique

Voici quelques exemples :

- 5000 représente 5 000 octets
- 10K représente 10 Ko
- 2M représente 2 Mo

Champ Permit-type UUCP

Ce champ contient un mot-clé qui indique la manière d'interpréter la liste d'identifiants. Le tableau suivant répertorie les mots-clés et leur signification.

TABLEAU 26–5 Champ Permit-type

Mot-clé	Contenu de la liste d'identifiants
`User`	Identifiants de connexion des utilisateurs autorisés à utiliser ce niveau de travail
`Non-user`	Identifiants de connexion des utilisateurs qui ne sont pas autorisés à utiliser ce niveau de travail
`Group`	Noms des groupes dont les membres sont autorisés à utiliser ce groupe
`Non-group`	Noms des groupes dont les membres ne sont pas autorisés à utiliser ce niveau de travail

Champ ID-list UUCP

Ce champ contient une liste des identifiants de connexion ou noms de groupes autorisés ou non à mettre des travaux en attente pour ce niveau de travail. Les noms de la liste sont séparés par une espace et elle se termine par un caractère de saut de ligne. Le mot-clé `Any` est utilisé pour indiquer que tout le monde est autorisé à mettre des travaux en attente pour ce niveau de travail.

Autres fichiers de configuration UUCP

Cette section décrit trois fichiers plus rarement modifiés qui ont un impact sur l'utilisation des équipements UUCP.

Fichier `/etc/uucp/Devconfig` UUCP

Le fichier `/etc/uucp/Devconfig` permet de configurer les périphériques par service, tel que `uucp` ou `cu`. Les entrées `Devconfig` définissent les modules STREAMS utilisés pour un périphérique donné. Ces entrées ont le format suivant :

`service=`*x* `device=`*y* `push=`*z*[:*z*...]

x peut adopter la valeur `cu`, `uucico` ou les deux services séparés par deux-points. *y* est le nom d'un réseau et doit correspondre à une entrée dans le fichier `Devices`. *z* est remplacé par les noms des modules STREAMS dans l'ordre dans lequel ils doivent être insérés dans le flux de données. Différents modules et périphériques peuvent être définis pour les services `cu` et `uucp`.

Les entrées suivantes s'appliquent à un réseau STARLAN et seraient plus couramment utilisées dans le fichier :

```
service=cu       device=STARLAN     push=ntty:tirdwr
service=uucico   device=STARLAN     push=ntty:tirdwr
```

Cet exemple insère d'abord `ntty`, puis `tirdwr`.

Fichier `/etc/uucp/Limits` UUCP

Le fichier `/etc/uucp/Limits` contrôle le nombre maximal de commandes `uucico`, `uuxqt` et `uusched` exécutées simultanément sur le réseau `uucp`. Dans la plupart des cas, les valeurs par défaut sont acceptables et aucune modification n'est nécessaire. Si vous souhaitez toute de même les modifier, utilisez un éditeur de texte.

Le format du fichier `Limits` est le suivant :

`service=` *x* `max=` *y*:

x peut être `uucico`, `uuxqt` ou `uusched`, et *y* est la limite autorisée pour ce service. Les champs peuvent se trouver dans n'importe quel ordre et en minuscules.

Les entrées suivantes doivent généralement être utilisées dans le fichier `Limits` :

```
service=uucico max=5
service=uuxqt max=5
service=uusched max=2
```

L'exemple permet l'exécution simultanée de cinq commandes `uucico`, cinq commandes `uuxqt` et deux commandes `uusched` sur votre ordinateur.

Fichier `remote.unknown` UUCP

L'autre fichier qui a une incidence sur l'utilisation des fonctions de communication est le fichier `remote.unknown`. Ce fichier est un programme binaire qui s'exécute lorsqu'aucun ordinateur n'est trouvé lorsque l'un des fichiers `Systems` lance une conversation. Ce programme enregistre la tentative de conversation et abandonne la connexion.

Attention – Si vous changez les autorisations du fichier `remote.unkown` de sorte qu'il ne puisse pas s'exécuter, votre système accepte les connexions à partir de n'importe quel système.

Ce programme s'exécute lorsqu'un ordinateur qui ne se trouve pas dans l'un des fichiers `Systems` démarre une conversation. Le programme enregistre la tentative de conversation, mais ne parvient pas à établir une connexion. Si vous modifiez les autorisations de ce fichier de sorte qu'il ne puisse pas s'exécuter (`chmod 000 remote.unknown`), votre système accepte toutes les requêtes de conversation. Cette modification n'est pas sans impact. Vous devez avoir de bonnes raisons pour procéder à cette modification.

Fichiers d'administration UUCP

Les fichiers d'administration UUCP sont décrits ci-après. Ces fichiers sont créés dans les répertoires spool pour verrouiller les périphériques, maintenir les données temporaires ou conserver les informations relatives aux transferts ou exécutions à distance.

- *Fichier de données temporaire* (`TM`) : ces fichiers de données sont créés par les processus UUCP sous le répertoire spool `/var/spool/uucp/`*x* lorsqu'un fichier est reçu depuis un autre ordinateur. Le répertoire *x* porte le même nom que l'ordinateur distant qui envoie le fichier. Les noms des fichiers de données temporaires ont le format suivant :

  `TM.` *pid.ddd*

  pid est un ID de processus et *ddd* est un nombre séquentiel à trois chiffres qui commence à 0.

  Lorsque le fichier entier est reçu, le fichier `TM`*pid.ddd* est déplacé vers le nom du chemin d'accès spécifié dans le fichier `C.`*sysnxxxx* (présenté par la suite) qui a lancé la transmission. Si la transformation se termine de manière anormale, le fichier `TM.`*pid.ddd* peut rester dans le répertoire *x*. Ces fichiers sont normalement automatiquement supprimés par la commande `uucleanup`.
- *Fichier de verrouillage* (`LCK`) : les fichiers de verrouillage sont créés dans le répertoire `/var/spool/locks` pour chaque périphérique en cours d'utilisation. Les fichiers de verrouillage empêchent les conversations dupliquées et les tentatives multiples d'utilisation du même périphérique appelant. Le tableau suivant présente les différents types de fichiers de verrouillage UUCP.

TABLEAU 26–6 Fichiers de verrouillage UUCP

Nom de fichier	Description
`LCK.` *sys*	*sys* représente le nom de l'ordinateur qui utilise le fichier
`LCK.` *dev*	*dev* représente le nom d'un périphérique qui utilise le fichier
`LCK.`*LOG*	*LOG* représente un fichier journal UUCP verrouillé

Ces fichiers peuvent rester dans le répertoire spool si le lien de communication est inopinément coupé, comme par exemple lorsque votre ordinateur tombe en panne. Le fichier de verrouillage est ignoré (supprimé) une fois que le processus parent n'est plus actif. Le fichier de verrouillage contient l'ID de processus du processus qui a créé le verrou.

- *Fichier de travail* (`C.`) : les fichiers de travail sont créés dans un répertoire spool lorsqu'un travail (transfert de fichiers ou exécution de commandes à distance par exemple) a été mis en attente pour un ordinateur distant. Les noms des fichiers de travail ont le format suivant :

  `C.` *sysnxxxx*

sys est le nom de l'ordinateur distant, *n* est le caractère ASCII qui représente le niveau (priorité) du travail et *xxxx* est le numéro séquentiel à quatre chiffres du travail affecté par UUCP. Les fichiers de travail contiennent les informations suivantes :

- Nom du chemin d'accès complet du fichier à envoyer ou à requérir.
- Nom du chemin d'accès complet de la destination, utilisateur ou nom de fichier.
- Nom de connexion de l'utilisateur.
- Liste d'options.
- Nom des fichiers de données associés dans le répertoire spool. Si l'option `uucp -C` ou `uuto -p` a été spécifiée, un faux nom (`D.0`) est utilisé.
- Bits de mode du fichier source.
- Nom de connexion de l'utilisateur distant à notifier de l'achèvement du transfert.

- *Fichier de données*(`D.`) : les fichiers de données sont créés lorsque vous indiquez sur la ligne de commande de copier le fichier source dans le répertoire spool. Les noms des fichiers de données ont le format suivant :

  `D.` *systmxxxxyyy* – *systm* représente les cinq premiers caractères du nom de l'ordinateur distant. *xxxx* est le numéro séquentiel à quatre chiffres du travail affecté par `uucp`. Ce numéro peut être suivi d'un autre nombre. *yyy* est utilisé lorsque plusieurs fichiers `D.` sont créés pour un fichier de travail (`C.`).

- `X.` *(execute file)* : les fichiers d'exécution sont créés dans le répertoire spool avant l'exécution de commandes à distance. Les noms des fichiers d'exécution ont le format suivant :

  `X.` *sysnxxxx*

  sys est le nom de l'ordinateur distant. *n* est le caractère qui représente le niveau (priorité) du travail. *xxxx* est un numéro de séquence à quatre chiffres assigné par UUCP. Les fichiers d'exécution contiennent les informations suivantes :

  - Identifiant de connexion et nom de l'ordinateur du demandeur
  - Noms des fichiers requis pour l'exécution
  - Entrée à utiliser comme entrée standard pour la chaîne de commande
  - Nom de l'ordinateur et du fichier qui recevront une sortie standard après exécution de la commande
  - Chaîne de commande
  - Lignes d'option pour les requêtes d'état de retour

Messages d'erreur UUCP

Cette section répertorie les messages d'erreur associés avec UUCP.

Messages d'erreur UUCP ASSERT

Le tableau suivant répertorie les messages d'erreur ASSERT.

TABLEAU 26–7 Messages d'erreur ASSERT

Message d'erreur	Description ou action
`CAN'T OPEN`	Une commande `open()` ou `fopen()` a échoué.
`CAN'T WRITE`	Une commande `write()`, `fwrite()`, `fprint()` ou une autre commande similaire a échoué.
`CAN'T READ`	Une commande `read()`, `fgets()` ou une autre commande similaire a échoué.
`CAN'T CREATE`	Un appel `creat()` a échoué.
`CAN'T ALLOCATE`	Une allocation dynamique a échoué.
`CAN'T LOCK`	Une tentative de création d'un fichier `LCK` (fichier de verrouillage) a échoué. Dans certains cas, cette erreur est fatale.
`CAN'T STAT`	Un appel `stat()` a échoué.
`CAN'T CHMOD`	Un appel `chmod()` a échoué.
`CAN'T LINK`	Un appel `link()` a échoué.
`CAN'T CHDIR`	Un appel `chdir()` a échoué.
`CAN'T UNLINK`	Un appel `unlink()` a échoué.
`WRONG ROLE`	Il s'agit d'un problème de logique interne.
`CAN'T MOVE TO CORRUPTDIR`	Une tentative de déplacer des fichiers `C.` ou `X.` corrompus vers le répertoire `/var/spool/uucp/.Corrupt` a échoué. Le répertoire est probablement manquant ou le mode ou le propriétaire est incorrect.
`CAN'T CLOSE`	Un appel `close()` ou `fclose()` a échoué.
`FILE EXISTS`	La création d'un fichier `C.` ou `D.` a été tentée, mais le fichier existe déjà. Cette erreur se produit lorsqu'un problème survient avec la séquence d'accès aux fichiers, ce qui indique généralement une erreur du logiciel.
`NO uucp SERVICE NUMBER`	Un appel TCP/IP est tenté, mais aucune entrée ne se trouve dans le fichier `/etc/services` pour UUCP.
`BAD UID`	L'ID de l'utilisateur ne figure pas dans la base de données de mots de passe. Vérifiez la configuration du service de noms.
`BAD LOGIN_UID`	Identique à la description précédente.

TABLEAU 26–7 Messages d'erreur ASSERT *(Suite)*

Message d'erreur	Description ou action
BAD LINE	Une ligne incorrecte se trouve dans le fichier `Devices`. Pas assez d'arguments sur une ou plusieurs lignes.
SYSLST OVERFLOW	Une table interne dans le fichier `gename.c` est saturée. Un travail unique a tenté de communiquer avec plus de 30 systèmes.
TOO MANY SAVED C FILES	Identique à la description précédente.
RETURN FROM `fixline ioctl`	Une commande `ioctl(2)`, qui ne devrait jamais échouer, a échoué. Un problème s'est produit au niveau du pilote système.
BAD SPEED	Une vitesse de ligne erronée s'affiche dans le fichier `Devices` ou `Systems` (champ Class ou Speed).
BAD OPTION	Une ligne ou une option incorrecte se trouve dans le fichier `Permissions`. Cette erreur doit être corrigée immédiatement.
PKCGET READ	L'ordinateur distant est probablement bloqué. Aucune action n'est nécessaire.
PKXSTART	L'ordinateur distant a été interrompu de manière irrécupérable. Généralement, cette erreur peut être ignorée.
TOO MANY LOCKS	Un problème interne s'est produit. Contactez votre fournisseur système.
XMV ERROR	Un problème avec un fichier ou un répertoire s'est produit. Le répertoire spool est la cause probable, puisque les modes des destinations sont censés être vérifiés avant que ce processus ne soit lancé.
CAN'T FORK	Une tentative de création de commandes `fork` et `exec` a échoué. Le travail en cours ne sera pas perdu, mais retenté ultérieurement (`uuxqt`). Aucune action n'est nécessaire.

Messages d'erreur UUCP STATUS

Le tableau suivant répertorie les principaux messages d'erreur STATUS.

TABLEAU 26–8 Messages UUCP STATUS

Message d'erreur	Description/Action
OK	Le statut est acceptable.
NO DEVICES AVAILABLE	Aucun périphérique n'est actuellement disponible pour l'appel. Vérifiez si un périphérique se trouve dans le fichier `Devices` pour le système spécifique. Recherchez le périphérique à utiliser pour appeler le système dans le fichier `Systems`.
WRONG TIME TO CALL	Un appel a été passé sur le système à un moment autre que celui spécifié dans le fichier `Systems`.
TALKING	Explicite.

TABLEAU 26–8 Messages UUCP STATUS *(Suite)*

Message d'erreur	Description/Action
`LOGIN FAILED`	La connexion à un ordinateur spécifique a échoué. La cause peut être un identifiant de connexion ou mot de passe incorrect, un mauvais numéro, un ordinateur lent ou une erreur d'exécution du script DTP.
`CONVERSATION FAILED`	La conversation a échoué après un démarrage réussi. Cette erreur signifie généralement qu'un côté s'est arrêté, le programme a été interrompu ou la ligne (le lien) a été supprimée.
`DIAL FAILED`	L'ordinateur distant n'a jamais répondu. La cause peut être un dialer incorrect ou un numéro de téléphone erroné.
`BAD LOGIN/MACHINE COMBINATION`	L'ordinateur a été appelé avec un identifiant de connexion/nom d'ordinateur qui ne respecte pas le fichier `Permissions`. Cette erreur peut être une tentative d'usurpation d'identité.
`DEVICE LOCKED`	Le périphérique appelant à utiliser est actuellement verrouillé et en cours d'utilisation par un autre processus.
`ASSERT ERROR`	Une erreur `ASSERT` s'est produite. Vérifiez le fichier `/var/uucp/.Admin/errors` afin de connaître le message d'erreur et reportez-vous à la section "Messages d'erreur UUCP ASSERT" à la page 614.
`SYSTEM NOT IN Systems FILE`	Le système n'apparaît pas dans le fichier `Systems`.
`CAN'T ACCESS DEVICE`	Le périphérique ayant fait l'objet d'une tentative n'existe pas ou les modes sont incorrects. Vérifiez les entrées correspondantes dans les fichiers `Systems` et `Devices`.
`DEVICE FAILED`	Le périphérique n'a pas pu être ouvert.
`WRONG MACHINE NAME`	L'ordinateur appelé porte un autre nom que celui attendu.
`CALLBACK REQUIRED`	L'ordinateur appelé nécessite d'appeler votre ordinateur.
`REMOTE HAS A LCK FILE FOR ME`	L'ordinateur distant possède un fichier `LCK` pour votre ordinateur. L'ordinateur distant pourrait être en train d'essayer d'appeler votre ordinateur. Si l'ordinateur distant dispose d'une version plus ancienne d'UUCP, le processus qui s'adressait à votre ordinateur peut avoir échoué, en laissant le fichier `LCK`. Si l'ordinateur distant dispose de la nouvelle version d'UUCP et ne communique pas avec votre ordinateur, le processus possédant un fichier `LCK` est bloqué.
`REMOTE DOES NOT KNOW ME`	L'ordinateur distant n'a pas le nom de nœud de votre ordinateur dans son fichier `Systems`.
`REMOTE REJECT AFTER LOGIN`	L'identifiant de connexion utilisé par votre ordinateur pour la connexion ne correspond pas à ce que l'ordinateur distant attendait.
`REMOTE REJECT, UNKNOWN MESSAGE`	L'ordinateur distant a rejeté la communication avec votre ordinateur pour une raison inconnue. L'ordinateur distant n'exécute peut-être pas une version standard d'UUCP.
`STARTUP FAILED`	La connexion a réussi, mais la procédure d'établissement de connexion initiale a échoué.
`CALLER SCRIPT FAILED`	Cette erreur est généralement identique à l'erreur `DIAL FAILED`. Toutefois, si cette erreur se produit souvent, considérez le script appelant dans le fichier `Dialers`. Utilisez `Uutry` pour procéder à la vérification.

Messages d'erreur numériques UUCP

Le tableau ci-dessous répertorie les numéros de code de sortie que les messages de statut d'erreur produites par le fichier `/usr/include/sysexits.h`. Ils ne sont pas tous actuellement utilisés par `uucp` .

TABLEAU 26–9 Messages d'erreur UUCP par numéro

Numéro de message	Description	Signification
`64`	Valeur de base pour les messages d'erreur	Les messages d'erreur commencent par cette valeur.
`64`	Erreur d'utilisation de la ligne de commande	La commande a été utilisée de façon incorrecte, par exemple, avec un nombre d'arguments incorrect, un mauvais indicateur ou une syntaxe erronée.
`65`	Erreur de formatage des données	Les données d'entrée étaient incorrectes d'une manière ou d'une autre. Ce format de données doit uniquement être utilisé pour les données d'utilisateur et non pas les fichiers système.
`66`	Impossible d'ouvrir l'entrée	Un fichier d'entrée, et non un fichier système, n'existe pas ou n'a pas pu être lu. Ce problème peut également inclure des erreurs telles que "Aucun message" pour un logiciel de messagerie.
`67`	Adresse inconnue	L'utilisateur qui a été spécifié n'existe pas. Cette erreur peut s'appliquer aux adresses électroniques ou aux connexions distantes.
`68`	Nom d'hôte inconnu	L'hôte n'existe pas. Cette erreur s'applique aux adresses électroniques ou aux requêtes réseau.
`69`	Service non disponible	Un service n'est pas disponible. Cette erreur peut se produire si un programme d'assistance ou un fichier n'existe pas. Ce message peut également simplement indiquer que quelque chose ne fonctionne pas et que la cause n'est actuellement pas identifiable.
`70`	Erreur logicielle interne	Une erreur logicielle interne a été détectée. Cette erreur doit être limitée aux erreurs qui ne sont pas relatives au système d'exploitation, dans la mesure du possible.
`71`	Erreur système	Une erreur du système d'exploitation a été détectée. Ce message d'erreur est destiné à être utilisé lorsque des erreurs telles que les suivantes se produisent : "impossible d'effectuer un clonage", "impossible de créer des tubes". Par exemple, cette erreur inclut un retour `getuid` d'un utilisateur qui n'existe pas dans le fichier `passwd`.
`72`	Fichier critique du système d'exploitation manquant	Un système de fichiers tel que `/etc/passwd` ou `/var/admin/utmpx` n'existe pas, ne peut pas être ouvert ou possède une erreur, telle qu'une erreur de syntaxe.
`73`	Impossible de créer le fichier de sortie	Un fichier de sortie spécifié par l'utilisateur ne peut pas être créé.
`74`	Erreur d'entrée/sortie	Une erreur s'est produite lors de l'E/S sur certains fichiers.

TABLEAU 26–9 Messages d'erreur UUCP par numéro *(Suite)*

Numéro de message	Description	Signification
75	Panne temporaire. L'utilisateur est invité à procéder à une nouvelle tentative	Panne temporaire qui n'est pas vraiment une erreur. Dans la commande `sendmail`, cela signifie qu'un logiciel de messagerie, par exemple, n'a pas pu établir de connexion et que la requête doit être réessayée ultérieurement.
76	Erreur distance dans le protocole	Le système distant a renvoyé un élément "impossible" au cours d'un protocole d'échange.
77	Autorisation refusée	Vous ne disposez pas des autorisations suffisantes pour exécuter cette opération. Ce message n'est pas conçu pour les problèmes de système de fichiers, qui doivent utiliser `NOINPUT` ou `CANTCREAT`, mais plutôt pour les autorisations de niveau plus élevé. Par exemple, `kre` utilise ce message pour limiter les élèves pouvant leur envoyer des e-mail.
78	Erreur de configuration	Le système a détecté une erreur dans la configuration.
79	Entrée non trouvée	Entrée non trouvée.
79	Valeur maximale répertoriée	Valeur la plus élevée pour les messages d'erreur.

PARTIE VI

Utilisation de systèmes distants

Cette section fournit des instructions relatives à l'administration d'un serveur FTP et à l'accès aux systèmes distants dans l'environnement Solaris.

◆ ◆ ◆ CHAPITRE 27

Utilisation de systèmes distants (présentation)

Cette section contient des informations sur l'utilisation des fichiers distants.

Qu'est-ce que le serveur FTP ?

Le serveur FTP est basé sur wu-ftpd. Initialement développé par la Washington University de Saint Louis, wu-ftpd est largement utilisé pour la distribution de masse de données par l'intermédiaire d'Internet et est la norme préférée pour les grands sites FTP. Pour plus d'informations sur le contrat de licence, reportez-vous à la documentation qui est intégrée à `/var/smap/pkg/SUNWftpu/install/copyright`.

Qu'est-ce qu'un système distant ?

Pour l'objectif de ce chapitre, un *système distant* est un poste de travail ou un serveur qui est connecté au système local avec n'importe quel type de réseau physique et configuré pour la communication TCP/IP.

Sur les systèmes exécutant une version de Solaris, la configuration TCP/IP est établie automatiquement lors du démarrage. Pour plus d'informations, reportez-vous à la section *Guide d'administration système : services IP*.

Modifications récentes apportées au service FTP

Les versions précédentes incluent plusieurs modifications au service FTP. Les modifications comprennent des améliorations apportées au serveur FTP et les changements apportés aux commandes `ftpcount`, `ftpwho` et `ftp`.

Les modifications apportées au serveur FTP améliorent l'évolutivité et la consignation des transferts. Ces options sont couvertes à la section "Une aide à la configuration des sites occupés" à la page 652 et à la page de manuel `ftpaccess(4)` En particulier :

- La fonction `sendfile()` est utilisée pour les téléchargements binaires
- De nouvelles fonctionnalités sont prises en charge dans le fichier `ftpaccess`
  - `flush-wait` contrôle le comportement en fin de téléchargement ou d'énumération des répertoires
  - `ipcos` définit la classe IP de service pour la connexion des données ou le contrôle
  - `passive ports` peut être configuré afin que le noyau sélectionne le port TCP d'écoute
  - `quota-info` permet d'extraire des informations sur les quotas
  - `recvbuf` définit la taille du tampon de réception (chargement) utilisée pour les transferts binaires
  - `rhostlookup` active ou désactive la recherche du nom de l'hôte distant
  - `sendbuf` définit la taille du tampon d'envoi (téléchargement) utilisée pour les transferts binaires
  - `xferlog` personnalise le format de l'entrée du journal de transfert
- Grâce à l'option `-4`, le serveur FTP ne recherche que les connexions sur un socket IPv4 lors de l'exécution en mode autonome

De plus, les commandes `ftpcount` et `ftpwho` prennent maintenant en charge l'option `-v`, qui affiche les comptes utilisateur et des informations sur le processus pour les classes du serveur FTP définies dans les fichiers `ftpaccess` de l'hôte virtuel. Pour plus d'informations, reportez-vous aux pages de manuel `ftpcount(1)` et `ftpwho(1)`.

Le client et le serveur FTP prennent désormais en charge le protocole Kerberos. Pour plus d'informations, reportez-vous à la page de manuel `ftp(4)` et à la section "Kerberos User Commands" du *System Administration Guide: Security Services*.

La commande `ftp` a été modifiée. Par défaut, un client FTP Solaris connecté à un serveur FTP Solaris établit une liste des répertoires ainsi que des fichiers standard lorsque la commande `ls` est émise pour le client. Si le serveur FTP n'est pas exécuté dans le système d'exploitation Solaris, les répertoires risquent de ne pas être énumérés. Pour utiliser le comportement par défaut de Solaris lors de la connexion à des serveurs FTP autres que Solaris, le fichier `/etc/default/ftp` peut être modifié sur chaque client Solaris. Pour appliquer cette modification aux utilisateurs de façon individuelle, la variable d'environnement `FTP_LS_SENDS_NLST` peut être définie sur `yes`. Pour plus d'informations, reportez-vous à la page de manuel `ftp(4)`.

Le démon `ftpd` est géré par l'utilitaire de gestion des services. Les actions administratives sur ce service, telles que l'activation, la désactivation ou le redémarrage, peuvent être effectuées à l'aide de la commande `svcadm`. Servez-vous de la commande `svcs` pour connaître l'état du service de tous les démons. Pour une présentation de l'utilitaire SMF (Service Management Facility), reportez-vous au Chapitre 18, "Gestion des services (présentation) " du *Guide d'administration système : administration de base*.

◆ ◆ ◆ CHAPITRE 28

Administration du serveur FTP (tâches)

Ce chapitre inclut les tâches qui sont décrites dans le tableau ci-dessous pour configurer et administrer un serveur FTP.

Administration du serveur FTP (liste des tâches)

TABLEAU 28–1 Liste des tâches : Administration du serveur FTP

Tâche	Description	Voir
Configuration de l'accès au serveur FTP	Utilisez les fichiers `ftpaccess`, `ftpusers` et `ftphosts` dans le répertoire `/etc/ftpd` pour établir ou restreindre l'accès au serveur FTP.	“Définition de limites de connexions d'utilisateurs” à la page 628 “Contrôle du nombre de tentatives de connexion non valides” à la page 629 “Interdiction de l'accès au serveur FTP à certains utilisateurs” à la page 630 “Restriction de l'accès au serveur FTP par défaut” à la page 631 “Définitions des classes de serveur FTP” à la page 627

TABLEAU 28–1 Liste des tâches : Administration du serveur FTP *(Suite)*

Tâche	Description	Voir
Configuration des connexions au serveur FTP	Établissez des comptes de connexion pour des utilisateurs réels, invités et anonymes.	"Configuration d'utilisateurs FTP réels" à la page 633 "Configuration des utilisateurs FTP invités" à la page 634 "Configuration des utilisateurs FTP anonymes" à la page 635 "Création du fichier `/etc/shells`" à la page 635
Personnalisation des fichiers de message	Modifiez le fichier `/etc/ftpd/ftpaccess` pour configurer le serveur FTP de sorte qu'il renvoie les messages au client FTP lié aux événements en question.	"Personnalisation des fichiers de message" à la page 637 "Création de messages à envoyer aux utilisateurs" à la page 637 "Configuration de l'option README" à la page 638
Configuration de l'accès à des fichiers du serveur FTP	Utilisez le fichier `/etc/ftpd/ftpaccess` pour indiquer les classes d'utilisateurs qui sont autorisées à exécuter certaines commandes ou à télécharger et charger des fichiers sur le serveur FTP.	"Configuration de la découverte DA pour les réseaux commutés" à la page 248 "Contrôle des chargements et téléchargements sur le serveur FTP" à la page 641
Activation de l'hébergement virtuel limité ou complet	Utilisez le fichier `/etc/ftpd/ftpaccess` pour configurer le serveur FTP de sorte qu'il prenne en charge plusieurs domaines sur la même machine.	"Activation de l'hébergement virtuel limité" à la page 644 "Activation de l'hébergement virtuel complet" à la page 646
Démarrage du serveur FTP	Modifiez les propriétés du service pour démarrer le serveur FTP en mode `nowait`, autonome ou premier plan.	"Démarrage d'un serveur FTP à l'aide de SMF" à la page 648 "Démarrage d'un serveur FTP autonome en arrière-plan" à la page 649 "Démarrage d'un serveur FTP autonome au premier plan" à la page 649
Arrêt du serveur FTP	Utilisez le fichier `/etc/ftpd/ftpaccess` et exécutez la commande `ftpshut` pour arrêter le serveur FTP.	"Arrêt du serveur FTP" à la page 650
Résolution des problèmes courants du serveur FTP	Vérifiez `syslogd` et utilisez `greeting text` et `log commands` pour déboguer les problèmes sur le serveur FTP.	"Vérification de `syslogd` pour les messages du serveur FTP" à la page 651 "Utilisation de `greeting text` pour vérifier `ftpaccess`" à la page 651 "Vérification des commandes exécutées par les utilisateurs FTP" à la page 652

Contrôle de l'accès au serveur FTP

Vous pouvez utiliser les fichiers de configuration suivants dans le répertoire `/etc/ftpd` pour contrôler l'accès au serveur FTP.

- `ftpusers` est utilisé pour afficher une liste des utilisateurs qui se voient refuser l'accès au serveur FTP.
- `ftphosts` est utilisé pour autoriser ou refuser la connexion de différents hôtes à divers comptes sur le serveur FTP.
- `ftpaccess` est le fichier de configuration FTP principal. Le serveur FTP lit uniquement le fichier `/etc/ftpd/ftpaccess` s'il est appelé avec l'option `-a`. Lorsque le fichier `ftpaccess` est utilisé, tous les utilisateurs doivent être membres d'une classe pour être autorisé à accéder au serveur FTP. Vous pouvez spécifier de nombreuses directives `ftpaccess` qui s'appliquent uniquement à une classe particulière.

  Pour plus d'informations, reportez-vous aux pages de manuel `ftpusers(4)`, `ftphosts(4)` et `ftpaccess(4)`.

Remarque – Dans tous les fichiers de configuration du serveur FTP, les lignes commençant par le signe # sont considérées comme des commentaires.

▼ Définitions des classes de serveur FTP

Pour se connecter au serveur FTP, les utilisateurs doivent être membres d'une classe lorsque le fichier `ftpaccess` est utilisé. Pour ajouter la directive `class` au fichier `ftpaccess`, vous spécifiez le nom de *class* et la *typelist* d'utilisateurs qui sont autorisés à y accéder à partir d'un hôte particulier.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez des entrées pour les utilisateurs anonymes (anonymous), invités (guest) et réels (real) dans le fichier `ftpaccess`.

`class` *class typelist addrglob*`[`*addrglob...*`]`

`class` Mot-clé utilisé pour définir les utilisateurs FTP.

class Nom qui est défini par le mot-clé `class`. Chaque connexion est comparée à une liste de classes définies. L'utilisateur connecté est considéré comme un membre de la première classe qui correspond.

typelist Une liste de mots-clés séparés par des virgules qui correspondent aux trois types d'utilisateurs : `anonymous`, `guest` et `real`.

addrglob Nom de domaine ou adresse numérique glob. *addrglob* peut également être le nom d'un fichier, commençant par une barre oblique (‘/‘), qui contient d'autres globs d'adresse : `address:netmask` ou `address/cidr`.

Voici quelques exemples d'adresses glob :

- Adresse numérique IPv4 : **`10.1.2.3`**
- Nom de domaine glob **`*.provider.com`**
- Adresse numérique IPv4 glob **`10.1.2.*`**
- Adresse numérique IPv4 : masque de réseau **`10.1.2.0:255.255.255.0`**
- Adresse numérique IPv4/CIDR **`10.1.2.0/24`**
- Adresse numérique IPv6 : **`2000::56:789:21ff:fe8f:ba98`**
- Adresse numérique IPv6/CIDR : **`2000::56:789:21ff:fe8f:ba98/120`**

Exemple 28–1 Définition des classes du serveur FTP

```
class  local  real,guest,anonymous *.provider.com
class  remote real,guest,anonymous *
```

L'exemple précédent définit la classe `local` en tant qu'utilisateur de type `real`, `guest` ou `anonymous` qui se connecte à partir de `*.provider.com`. La dernière ligne définit `remote` en tant qu'utilisateur qui se connecte à partir de n'importe où excepté `*.provider.com`.

▼ Définition de limites de connexions d'utilisateurs

Vous pouvez limiter le nombre de connexions simultanées par les utilisateurs d'une classe donnée à l'aide de directives qui sont définies dans le fichier `ftpaccess`. Chaque limite de connexion contient le nom d'une classe, une liste des jours de la semaine de type UUCP et un fichier du message à afficher si la limite est dépassée.

Pour définir les limites de connexions d'utilisateurs, suivez les étapes de la procédure suivante.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section “Configuring RBAC (Task Map)” du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess` :

`limit` *class n times* [*message-file*]

`limit` Mot-clé qui est utilisé pour limiter les connexions simultanées par le nombre indiqué d'utilisateurs d'une classe définie sur des périodes de temps données.

class	Nom qui est défini par le mot-clé `class`. Chaque connexion est comparée à une liste de classes définies. L'utilisateur connecté est considéré comme un membre de la première classe qui correspond.
n	Nombre d'utilisateurs.
times	Jour de la semaine et heure de la journée auxquels la classe peut se connecter. Utilisez `Any` pour n'importe quel jour.
message-file	Fichier de message qui s'affiche si un utilisateur se voit refuser l'accès.

Exemple 28–2 Définition des limites de connexions d'utilisateurs

```
limit   anon     50  Wk0800-1800        /etc/ftpd/ftpmsg.deny
limit   anon    100  Any                 /etc/ftpd/ftpmsg.deny
limit   guest   100  Any                 /etc/ftpd/ftpmsg.deny
```

La première ligne de l'exemple ci-dessus présente une limite de 50 connexions simultanées autorisées pour les utilisateurs de la classe `anon` pendant les heures de travail hebdomadaires. La deuxième ligne limite les utilisateurs `anon` à 100 connexions simultanées en dehors des heures de travail. La dernière ligne montre une limite de 100 connexions `guest` qui sont autorisées à tout moment. Pour obtenir des informations sur la spécification des paramètres de jour et d'heure, reportez-vous à la page de manuel `ftpaccess(4)`.

L'exemple indique en détails que le contenu du fichier `/etc/ftpd/ftpmsg.deny` est renvoyé lorsqu'une limite de connexion spécifiée est atteinte, en supposant que `ftpmsg.deny` existe. Pour plus d'informations sur l'utilisation de la commande `/usr/sbin/ftpcount` pour afficher le nombre et la limite de connexions pour chaque classe d'utilisateurs connectés à un moment donné, reportez-vous à la page de manuel `ftpcount(1)`.

Les utilisateurs sont autorisés à se connecter au serveur FTP sauf si une limite spécifiée est atteinte. Les utilisateurs anonymes sont connectés en tant qu'utilisateur `ftp`. Les utilisateurs réels se connectent sous leur propre identité et les invités se connectent en tant qu'utilisateurs réels avec un environnement `chroot` pour limiter les privilèges d'accès.

Pour plus d'informations sur l'utilisation de la commande `/usr/sbin/ftpwho` pour vérifier les identités des utilisateurs connectés au serveur FTP, reportez-vous à la page de manuel `ftpwho(1)`.

▼ Contrôle du nombre de tentatives de connexion non valides

Si une connexion au serveur FTP échoue en raison d'un problème tel qu'une faute d'orthographe dans les informations requises, la connexion est généralement répétée. Un nombre spécifique de tentatives de connexion consécutives sont accordées à l'utilisateur avant

qu'un message soit consigné dans le fichier `syslog`. À ce stade, l'utilisateur est déconnecté. Vous pouvez définir une limite d'échecs pour le nombre de tentatives de connexion en suivant les étapes de la procédure suivante.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez les entrées suivantes au fichier `ftpaccess`.**

```
loginfails n
```

loginfails — Mot-clé qui permet d'affecter le nombre d'échecs de connexion autorisés avant que la connexion FTP soit interrompue.

n — Nombre de fois qu'une connexion peut échouer.

Exemple 28–3 Contrôle du nombre de tentatives de connexion non valides

```
loginfails 10
```

L'exemple ci-dessus indique que l'utilisateur est déconnecté du serveur FTP après 10 tentatives de connexion ayant abouti à un échec.

▼ Interdiction de l'accès au serveur FTP à certains utilisateurs

Le fichier `/etc/ftpd/ftpusers` répertorie les noms des utilisateurs qui ne sont pas autorisés à se connecter au serveur FTP. Lorsqu'une connexion est effectuée, le serveur FTP vérifie le fichier `/etc/ftpd/ftpusers` afin de déterminer si l'accès doit être refusé à l'utilisateur. Si le nom de l'utilisateur n'est pas trouvé dans ce fichier, le serveur recherche ensuite dans le fichier `/etc/ftpusers`.

Si le nom de l'utilisateur est trouvé dans `/etc/ftpusers`, un message `syslogd` est écrit et contient une déclaration indiquant que la correspondance a été trouvée dans un fichier désapprouvé. Le message recommande également l'utilisation de `/etc/ftpd/ftpusers` au lieu de `/etc/ftpusers`.

Remarque – La prise en charge du fichier `/etc/ftpusers` a été désapprouvée dans cette version. Si le fichier `/etc/ftpusers` existe lorsque le serveur FTP est installé, le fichier est déplacé vers `/etc/ftpd/ftpusers`.

Pour plus d'informations, reportez-vous aux pages de manuel `syslogd(1M)`, `in.ftpd(1M)` et `ftpusers(4)`.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez des entrées au fichier `/etc/ftpd/ftpusers` pour les utilisateurs qui ne sont pas autorisés à se connecter au serveur FTP.**

Exemple 28–4 Désactivation de l'accès au serveur FTP

```
root
daemon
bin
sys
adm
lp
uccp
nuucp
listen
nobody
noaccess
nobody4
```

L'exemple précédent répertorie les entrées standard dans le fichier `ftpusers`. Les noms d'utilisateur correspondent aux entrées de `/etc/passwd`. La liste inclut généralement l'utilisateur `root` et d'autres identités d'administration et d'applications du système.

L'entrée racine est incluse dans le fichier `ftpusers` comme mesure de sécurité. La stratégie de sécurité par défaut est d'interdire les connexions à distance pour `root`. La stratégie est également suivie pour la valeur par défaut qui est définie comme l'entrée CONSOLE dans `/etc/default/loginfile`. Reportez-vous à la page de manuel `login(1)`.

▼ Restriction de l'accès au serveur FTP par défaut

Outre les commandes mentionnées précédemment, vous pouvez ajouter des déclarations explicites dans le fichier `ftpaccess` pour restreindre l'accès au serveur FTP.

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess`.

a. Par défaut, tous les utilisateurs sont autorisés à accéder au serveur FTP (non virtuel) par défaut. Pour refuser l'accès à des utilisateurs spécifiques (autres que `anonymous`), ajoutez l'entrée suivante :

```
defaultserver deny username [username...]
```

`defaultserver`	Mot-clé qui est utilisé pour identifier le serveur non virtuel auquel l'accès peut être refusé ou autorisé.
username	Nom de connexion d'un utilisateur avec un accès restreint au `defaultserver`.

b. Afin d'autoriser l'accès aux utilisateurs qui ne sont pas répertoriés sur la ligne `deny`, ajoutez la ligne suivante :

```
defaultserver allow username [username...]
```

c. Pour empêcher l'accès aux utilisateurs anonymes, ajoutez l'entrée :

```
defaultserver private
```

Exemple 28–5 Restriction de l'accès au serveur FTP par défaut

```
defaultserver deny *
defaultserver allow username
```

L'exemple précédent indique que le serveur FTP refuse l'accès à tous les utilisateurs à l'exception des utilisateurs anon et des utilisateurs qui sont répertoriés sur la ligne `allow`.

Vous pouvez également utiliser le fichier `ftphosts` pour refuser l'accès à des comptes de connexion donnés de divers hôtes. Pour plus d'informations, reportez-vous à la page de manuel `ftphosts(4)`.

Configuration des connexions au serveur FTP

Pour accéder à un serveur FTP, vous devez d'abord vous connecter. Le serveur FTP prend en charge trois types de comptes de connexion pour les utilisateurs *real*, *guest* et *anonymous*.

- Les utilisateurs *real* ont des comptes qui leur permettent d'établir des sessions de terminal sur des systèmes qui exécutent le serveur FTP. Soumise aux autorisations d'accès aux répertoires et aux fichiers, l'ensemble de la structure du disque est visible aux utilisateurs réels.
- Les utilisateurs *Guest* ont également besoin de comptes pour se connecter au serveur FTP. Chaque compte invité est configuré avec un nom d'utilisateur et un mot de passe. Les shells de connexion en exécution ne sont pas affectés aux invités pour empêcher les utilisateurs

d'établir des sessions de terminal. Au moment de la connexion, le serveur FTP effectue une opération `chroot(2)` pour restreindre la vue d'un invité sur la structure du disque du serveur.

Remarque – Les shells de connexion pour les utilisateurs réels et invités doivent être répertoriés dans le fichier `/etc/shells` pour autoriser l'accès au serveur FTP.

- Les utilisateurs *anonymous* se connectent au serveur FTP avec `ftp` ou `anonymous` comme nom d'utilisateur. Par convention, les utilisateurs anonymes fournissent une adresse e-mail lorsqu'ils sont invités à saisir un mot de passe.

  Au moment de la connexion, le serveur FTP effectue une opération `chroot(2)` pour restreindre la vue d'un utilisateur anonyme sur la structure du disque du serveur. Une seule zone de fichiers est partagée par tous les utilisateurs anonymes, à la différence des zones distinctes qui peuvent être créées pour chaque utilisateur invité.

  Les utilisateurs réels et invités se connectent en utilisant des comptes individuels et de mots de passe connus que d'une seule personne. Les utilisateurs anonymes se connectent à un compte connu qui est potentiellement disponible à toute personne. La plupart des distributions de fichiers à grande échelle sont créées en utilisant le compte anonyme.

▼ Configuration d'utilisateurs FTP réels

Pour autoriser l'accès pour les utilisateurs réels au serveur FTP, suivez les instructions ci-dessous :

1. **Vérifiez que l'utilisateur dispose d'un compte qui est configuré avec un nom d'utilisateur et un mot de passe pouvant être utilisés pour l'établissement d'une session de terminal.**

   Pour plus d'informations, reportez-vous au Chapitre 4, “Gestion des comptes utilisateur et des groupes (présentation) ” du *Guide d'administration système : administration de base*.

2. **Confirmez que l'utilisateur réel est membre d'une classe dans le fichier `ftpaccess`.**

   Pour plus d'informations sur les classes d'utilisateur qui sont définies dans le fichier `ftpaccess`, reportez-vous à la section “Définitions des classes de serveur FTP” à la page 627.

3. **Vérifiez que le shell de connexion de l'utilisateur est répertorié dans le fichier `/etc/shells`.**

Configuration des utilisateurs FTP invités

Le script `ftpconfig` est utilisé pour copier tous les fichiers système nécessaires dans le répertoire personnel. Lorsque l'utilisateur invité et son répertoire personnel existent déjà, le script `ftpconfig` met à jour la zone avec les fichiers système courants.

Pour plus d'informations, reportez-vous à la page de manuel `ftpconfig(1M)`

Remarque – À l'inverse du nom d'utilisateur (`anonymous` ou `ftp`) qui est défini pour les utilisateurs anonymes, les noms d'utilisateur pour les invités FTP ne sont pas fixes. N'importe quel nom qui fonctionne comme un nom d'utilisateur réel peut être sélectionné.

Pour autoriser l'accès par un utilisateur invité au serveur FTP, procédez de la façon suivante :

1 **Utilisez le script `useradd` pour créer un compte d'utilisateur invité avec un shell de connexion de `/bin/true` et un répertoire personnel de** */root-dir/./home-dir***.**

Pour plus d'informations, reportez-vous à la page de manuel `useradd(1M)` et au Chapitre 4, “Gestion des comptes utilisateur et des groupes (présentation) ” du *Guide d'administration système : administration de base*.

Remarque – Dans cette procédure, **`/home/guests/./guest1`** est utilisé comme nom de répertoire personnel pour un utilisateur appelé `guest1`.

```
# /usr/sbin/useradd -m -c "Guest FTP" -d \
  /home/guests/./guest1 -s /bin/true guest1
```

2 **Attribuez un mot de passe au compte invité.**

3 **Ajoutez une entrée `guestuser` au fichier `ftpaccess`.**

```
guestuser guest1
```

Remarque – Vous pouvez également utiliser la fonction `guestgroup` dans le fichier `ftpaccess` pour spécifier les utilisateurs invités. La fonction `guest-root` dans `ftpaccess` élimine le besoin de `/./` dans le chemin d'accès au répertoire personnel de l'utilisateur invité.

---

4 **Confirmez que l'utilisateur invité est membre d'une `class` dans le fichier `ftpaccess`. Pour plus d'informations, reportez-vous à la section “Définitions des classes de serveur FTP” à la page 627.**

5 **Utilisez le script `ftpconfig` pour créer les fichiers requis dans la zone `chroot`.**

```
/usr/sbin/ftpconfig -d /home/guests
```

6 **Confirmez que `/bin/true` est répertorié dans le fichier `/etc/shells`. Reportez-vous à la section "Création du fichier `/etc/shells`" à la page 635.**

Exemple 28–6 Configuration d'un serveur FTP invité

Dans cet exemple, la zone FTP est configurée dans le répertoire `/home/guests`.

```
# /usr/sbin/ftpconfig -d /home/guests
Updating directory /home/guests
```

▼ Configuration des utilisateurs FTP anonymes

Le script `ftpconfig` crée le compte utilisateur `anonymous` et renseigne le répertoire personnel avec les fichiers requis.

Pour plus d'informations, reportez-vous à la page de manuel `ftpconfig(1M)`.

Pour autoriser l'accès par un utilisateur anonyme au serveur FTP, suivez les instructions ci-dessous :

1 **Utilisez le script `ftpconfig` pour créer le compte d'utilisateur anonyme.**

`/usr/sbin/ftpconfig` *anonymous-ftp-directory*

2 **Confirmez que l'utilisateur anonyme est affecté à une `class` dans le fichier `ftpaccess`.**

Pour plus d'informations, reportez-vous à la section "Définitions des classes de serveur FTP" à la page 627.

Exemple 28–7 Configuration des utilisateurs FTP anonymes

Dans cet exemple, la zone FTP est configurée dans le répertoire `/home/ftp`.

```
# /usr/sbin/ftpconfig /home/ftp
Creating user ftp
Updating directory /home/ftp
```

▼ Création du fichier `/etc/shells`

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Créez le fichier `/etc/shells`.**

3. **Modifiez `/etc/shells`. Ajoutez le chemin d'accès complet à chaque shell sur une seule ligne.**

Exemple 28–8 Création du fichier /etc/shells

À continuation, un exemple d'un fichier `/etc/shells` avec `/bin/true` répertorié pour les utilisateurs FTP invités :

```
/sbin/sh
/bin/csh
/bin/jsh
/bin/ksh
/bin/remsh
/bin/rksh
/bin/rsh
/bin/sh
/usr/bin/csh
/usr/bin/ksh
/usr/bin/bash
/usr/bin/tcsh
/usr/bin/zsh
/bin/true
```

Personnalisation des fichiers de message

Vous pouvez configurer le serveur FTP pour renvoyer des messages qui sont liés à des événements spécifiques au client FTP. Un message d'accueil peut être défini de façon à s'afficher lorsqu'un utilisateur se connecte au serveur FTP. Un autre message pourrait s'afficher lorsque l'utilisateur procède à un changement de répertoire.

En plus du texte brut, les fichiers de message peuvent contenir un ou plusieurs *magic cookies*. Un cookie magique est composé d'un `%` (signe de pourcentage), suivi d'un caractère unique. Lorsque vous incorporez un cookie dans le texte d'un message, les informations associées à ce cookie s'affiche à l'écran au moment où le fichier de message est appelé.

Par exemple, le texte du message peut contenir le cookie `%L` :

```
Welcome to %L!
```

Lorsque le message est affiché, le cookie magique `%L` est remplacé par le nom du serveur tel qu'il est défini par l'instruction `hostname` dans le fichier `ftpaccess`. Pour obtenir une liste complète des cookies de message pris en charge, reportez-vous à la page de manuel `ftpaccess(4)`.

Remarque – Si le nom d'hôte n'est pas défini dans le fichier `ftpaccess`, le nom d'hôte par défaut pour la machine locale est utilisée.

▼ Personnalisation des fichiers de message

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2. **Modifiez votre fichier de message pour inclure les cookies magiques comme approprié.**

   Pour obtenir la liste des cookies utilisables, reportez-vous à la page de manuel `ftpaccess(4)`.

Exemple 28–9 Personnalisation des fichiers de message

Ci-dessous, l'exemple d'un fichier de message qui comprend des cookies magiques :

```
Welcome to %L -- local time is %T.

You are number %N out of a maximum of %M.
All transfers are logged.

If your FTP client crashes or hangs shortly after login
please try
using a dash (-) as the first character of your password.
This will
turn off the informational messages that may be confusing
your FTP
client.

Please send any comments to %E.
```

▼ Création de messages à envoyer aux utilisateurs

Une fois que l'utilisateur est connecté, les messages associés au système ou à une application sont affichés à l'écran. Le fichier `ftpaccess` répertorie les événements qui déclenchent les instructions `message` associées.

1. **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

   Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess` :

`message` *message-file* `[`*when* `[`*class* ...`]]`

`message`	Mot-clé qui est utilisé pour spécifier le fichier de message à afficher lorsqu'un utilisateur se connecte ou exécute la commande pour modifier le répertoire de travail.
message-file	Nom du fichier de message à afficher.
when	Paramètre qui est défini sur `login` ou `cwd=` *dir*. Voyez l'exemple suivant :
class	La spécification `class` indique l'affichage du message uniquement pour les membres d'une classe particulière.

Exemple 28–10 Création de messages à envoyer aux utilisateurs

```
message    /etc/ftpd/Welcome    login   anon guest
message    .message    cwd=*
```

L'exemple précédent indique que le fichier `/etc/ftpd/Welcome` s'affiche au moment de la connexion pour les utilisateurs de la classe `anon` ou `guest`. La deuxième ligne indique que le fichier `.message` dans le répertoire de travail en cours s'affiche pour tous les utilisateurs.

Les fichiers de message sont créés par rapport au répertoire `chroot` pour les utilisateurs invités et anonymes.

▼ Configuration de l'option README

La première fois qu'un répertoire est visité, le fichier `README` peut être répertorié. Pour configurer l'option README, ajoutez les entrées suivantes dans le fichier `ftpaccess`.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess`.

`readme` *message-file* `[when [`*class*`...]]`

`readme`	Mot-clé qui est utilisé pour spécifier un fichier de message à vérifier lorsqu'un utilisateur se connecte ou modifie le répertoire de travail. Si le fichier de message existe, l'utilisateur est averti et est donné la date à laquelle le fichier a été modifié.
message-file	Nom du fichier de message à vérifier.

when Paramètre qui est défini sur `login` ou `cwd=` *dir*. Voyez l'exemple suivant :

class La spécification `class` indique l'affichage du message uniquement pour les membres d'une classe particulière.

Remarque – Les mots-clés `greeting` et `banner` peuvent également être utilisés pour envoyer des messages aux utilisateurs. Reportez-vous à la page de manuel `ftpaccess(4)`.

Exemple 28–11 Configuration de l'option README

```
readme  README*     login
readme  README*     cwd=*
```

L'exemple précédent indique que tous les fichiers correspondant à `README*` sont répertoriés au moment de la connexion ou lorsqu'un répertoire est modifié. Voici l'extrait d'une connexion, qui est basée sur les paramètres utilisés dans cet exemple.

```
% ftp earth
Connected to earth.
220 earth FTP server ready.
Name (earth:rimmer): ftp
331 Guest login ok, send your complete e-mail address as password.
Password:
230-
230-Welcome to earth -- local time is Thu Jul 15 16:13:24
1999.
230-
230-You are number 1 out of a maximum of 10.
230-All transfers are logged.
230-
230-If your FTP client crashes or hangs shortly after login
please try
230-using a dash (-) as the first character of your
password.  This will
230-turn off the informational messages that may be
confusing your FTP
230-client.
230-
230-Please send any comments to ftpadmin@earth.
230-
230 Guest login ok, access restrictions apply.
ftp> cd pub
250-Please read the file README
250-  it was last modified on Thu Jul 15 16:12:25 1999 - 0
days ago
250 CWD command successful.
ftp> get README /tmp/README
200 PORT command successful.
150 Opening ASCII mode data connection for README (0
bytes).
226 ASCII Transfer complete.
ftp> quit
```

```
221 Goodbye.
```

Contrôle de l'accès à des fichiers sur le serveur FTP

Les contrôles d'accès au serveur FTP de cette section complètent les contrôles d'accès aux répertoires et aux fichiers standard disponibles avec la version. Utilisez les commandes standard pour restreindre l'accès, la modification ou le chargement des fichiers. Reportez-vous aux pages de manuel `chmod(1)`, `chown(1)` et `chgrp(1)`.

▼ Contrôle des commandes d'accès aux fichiers

Pour utiliser les capacités d'autorisation dans `ftpaccess` pour spécifier quel type d'utilisateur est autorisé à exécuter des commandes particulières, procédez de la façon suivante :

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Ajoutez les entrées suivantes au fichier `ftpaccess` :**

command `yes|no` *typelist*

command Commandes `chmod`, `delete`, `overwrite`, `rename` ou `umask`.

`yes|no` Autorise ou empêche un utilisateur d'émettre une commande.

typelist Liste d'un type de mots-clés `anonymous`, `guest` et `real` séparés par des virgules.

Exemple 28–12 Contrôle des commandes d'accès aux fichiers

Les éléments suivants sont des exemples d'autorisations qui sont définies pour l'accès aux fichiers sur le serveur FTP.

```
chmod no anonymous, guest
delete    no anonymous
overwrite no anonymous
rename    no anonymous
umask     no guest, anonymous
```

L'exemple précédent indique ce qui suit :

- Les utilisateurs anonymes ne sont pas autorisés à supprimer, remplacer ou renommer les fichiers.
- Les invités et les utilisateurs anonymes ne sont pas autorisés à modifier de modes d'accès et à réinitialiser umask.

Contrôle des chargements et téléchargements sur le serveur FTP

Vous pouvez contrôler les chargements et téléchargements qui sont lancés à partir de et vers le serveur FTP en définissant les droits d'accès aux répertoires du serveur. Par défaut, les chargements ne sont pas autorisés pour les utilisateurs anonymes. Soyez très prudent lorsque vous autoriser les chargements anonymes.

▼ Contrôle des chargements vers le serveur FTP

Ajoutez les directives dans le fichier `ftpaccess` pour spécifier les autorisations de chargement et les messages d'erreur relatifs aux échecs de chargement.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess`.

Pour permettre aux utilisateurs de charger des fichiers, ajoutez l'entrée suivante :

```
upload [absolute|relative] [class=<classname>]... [-] root-dir \
dirglob yes|no owner group mode [dirs|nodirs] [<d_mode>]

path-filter typelist mesg allowed-charset {disallowed regexp...}
```

`upload`	Mot-clé qui est appliqué aux utilisateurs qui ont un répertoire personnel (l'argument pour `chroot()`) de *root-dir*. *root-dir* peut être spécifié en tant que "*" pour correspondre à un répertoire personnel.
`absolute|relative`	Paramètre qui indique si les chemins du répertoire *root-dir* sont interprétés en tant que chemin absolu ou relatif au répertoire `chroot` actuel.

`class`	Mot-clé qui est utilisé pour spécifier n'importe quel nombre de restrictions `class=<classname>`. Si des restrictions sont spécifiées, la clause de chargement entre en vigueur uniquement si l'utilisateur actuel est membre de l'une des classes spécifiées.
root-dir	Répertoire racine de l'utilisateur et répertoire personnel pour les utilisateurs anonymes.
dirglob	Motif de correspondance pour un nom de répertoire. Un astérisque peuvent être utilisé n'importe où, ou seul, pour signifier n'importe quel répertoire.
`yes|no`	Variable qui autorise ou interdit le chargement vers le serveur FTP.
owner	Propriétaire des fichiers qui sont chargés dans `dirnames`.
group	Groupe qui est associé aux fichiers chargés dans `dirnames`.
mode	Ce paramètre est utilisé pour définir des autorisations d'accès aux fichiers chargés. Le mode par défaut `0440` empêche le compte anonyme de lire les fichiers chargés.
`dirs|nodirs`	Mot-clé qui autorise ou interdit aux utilisateurs de créer des sous-répertoires dans un répertoire qui est répertorié dans `dirnames`.
`d_mode`	Mode facultatif qui détermine les autorisations pour un répertoire nouvellement créé.
`path-filter`	Mot-clé qui contrôle les noms des fichiers chargés.
typelist	Liste d'un type de mots-clés `anonymous`, `guest` et `real` séparés par des virgules.
mesg	Le fichier de message qui s'affiche ne parvient pas à correspondre aux critères `regexp`.
allowed-charset {disallowed regexp...}	Les caractères alphanumériques autorisés ou non dans les noms de fichiers.

Exemple 28–13 Contrôle des chargements vers le serveur FTP

```
upload /export/home/ftp /incoming yes ftpadm ftpadmin 0440 nodirs
path-filter anonymous /etc/ftpd/filename.msg ^[-A-Za-z0-9._]*$ ^[.-]
```

L'exemple précédent indique ce qui suit :

- Les comptes utilisateur FTP qui utilisent `chroot` dans `/export/home/ftp` peuvent charger des fichiers vers le répertoire `/incoming`. Les fichiers chargés sont possédés par l'utilisateur `ftpadm` et le groupe `ftpadmin`. Le mode est défini sur `0440` avec le mot-clé `nodirs` pour empêcher les utilisateurs anonymes de créer des sous-répertoires.
- Pour les utilisateurs anonymes, un nom de fichier est une séquence de caractères A à Z, a à z, 0-9, . (point), - (tiret), ou _ (trait de soulignement). Les noms de fichiers ne peuvent pas commencer par un . (point) ou - (tiret). Si un nom de fichier ne répond pas à ce filtre, le message `/etc/ftpd/filename.msg` s'affiche si l'administrateur FTP a créé le fichier de message. Ce message est suivi d'un message d'erreur de serveur FTP.

La propriété et les autorisations liées à un répertoire pour lequel les chargements anonymes sont autorisés doivent faire l'objet d'un contrôle rigoureux. L'administrateur FTP doit être le propriétaire de tous les fichiers chargés vers le serveur FTP. Vous devez créer un administrateur FTP lorsque les utilisateurs anonymes sont autorisés à charger des fichiers. Le répertoire doit être détenu par l'utilisateur `ftpadm` et le groupe `ftpadm` avec des autorisations définies sur `3773`.

Le mode d'accès pour les fichiers chargés vers le serveur FTP doit être `0440`. Le mode `0440` empêche le compte anonyme de lire les fichiers chargés. Cette restriction protège votre serveur de devenir une zone intermédiaire pour la distribution de fichiers tiers.

Pour rendre les fichiers chargés disponibles pour la distribution, l'administrateur FTP peut déplacer les fichiers vers un répertoire public.

▼ Contrôle des téléchargements depuis le serveur FTP

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess` pour empêcher les utilisateurs de récupérer des fichiers.

`noretrieve [absolute|relative] [class=`*classname*`]... [-]` *filename* `...`

`noretrieve`	Mot-clé qui est utilisé pour refuser la récupération d'un ou plusieurs fichiers.
`absolute|relative`	Paramètre qui indique si les chemins du répertoire *root-dir* sont interprétés en tant que chemin absolu ou relatif au répertoire `chroot` actuel.

`class`	Mot-clé qui est utilisé pour spécifier la `class=<classname>` d'utilisateurs auxquels des restrictions `noretrieve` s'appliquent.
filename	Nom de fichier que l'utilisateur n'est pas autorisé à récupérer.

Exemple 28–14 Contrôle des téléchargements depuis le serveur FTP

```
noretrieve /etc/passwd
```

L'exemple précédent indique que tous les utilisateurs sont dans l'impossibilité de récupérer le fichier `/etc/passwd`.

Hébergement virtuel

L'hébergement virtuel permet au serveur FTP de prendre en charge plusieurs domaines sur la même machine. Chaque hôte virtuel nécessite une interface logique et une adresse IP distinctes.

Le serveur FTP prend en charge deux types d'hébergement virtuel : *limité* et *complet*. Avec l'hébergement virtuel limité, les mêmes fichiers de configuration sont utilisés pour tous les hôtes virtuels. Avec l'hébergement virtuel complet, des fichiers de configuration distincts peuvent être utilisés pour chaque hôte virtuel.

Remarque – Par défaut, les utilisateurs réel et invités ne sont pas autorisés à se connecter à des hôtes virtuels. Vous pouvez définir les directives `ftpaccess` suivantes pour remplacer la valeur par défaut.

```
To allow access to specific users:
virtual address allow username
To deny access to anonymous users:
virtual address private username
```

Pour plus d'informations, reportez-vous à la page de manuel `ftpaccess(4)`.

▼ Activation de l'hébergement virtuel limité

L'hébergement virtuel limité assure une prise en charge partielle de serveurs FTP virtuels. Vous pouvez activer la prise en charge pour l'hébergement virtuel limité en spécifiant le répertoire racine virtuel. Si nécessaire, vous pouvez également définir les paramètres suivants pour l'hôte virtuel dans le fichier `ftpaccess` :

- `banner`
- `logfile`

- `email`
- `hostname`

Toutes les directives du fichier `ftpaccess` sont partagées globalement sur tous les serveurs virtuels.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess`.

```
virtual address root|banner|logfile path
virtual address hostname|email string
```

`virtual`	Mot-clé qui est utilisé pour activer les fonctions du serveur virtuel.
address	Adresse IP du serveur virtuel.
`root`	Répertoire racine du serveur virtuel.
`banner`	Fichier banner qui s'affiche lorsqu'une connexion est établie avec le serveur virtuel.
`logfile`	Enregistrement des transferts de fichiers qui sont effectués depuis et vers le serveur virtuel.
path	Variable qui est utilisée pour indiquer l'emplacement des répertoires et des fichiers sur le serveur virtuel.
`email`	Adresse e-mail qui est utilisée dans des fichiers de message et dans la commande `HELP`.
`hostname`	Nom de l'hôte qui est indiqué dans le message d'accueil ou la commande d'état.
string	Variable qui est utilisée pour spécifier les paramètres `email` ou `hostname`.

Remarque – Bien qu'il soit possible d'utiliser `hostname` en tant qu'*address* du serveur virtuel, il est fortement recommandé d'utiliser l'adresse IPv4 à la place. Le DNS doit être disponible lorsque la connexion FTP est reçue pour la correspondance avec `hostname`. Pour un hôte IPv6, utilisez le nom d'hôte à la place de l'adresse IPv6.

Exemple 28–15 Activation de l'hébergement virtuel limité dans le fichier `ftpaccess`

```
virtual 10.1.2.3 root    /var/ftp/virtual/ftp-serv
virtual 10.1.2.3 banner  /var/ftp/virtual/ftp-serv/banner.msg
virtual 10.1.2.3 logfile /var/log/ftp/virtual/ftp-serv/xferlog
```

L'exemple précédent définit l'emplacement du répertoire `root`, de `banner` et `logfile` sur un serveur FTP virtuel.

Exemple 28–16 Activation de l'hébergement virtuel limité sur la ligne de commande

Le script `ftpaddhost(1M)` avec l'option `-l` est fourni pour configurer des hôtes virtuels limités.

Dans l'exemple suivant, `ftpaddhost` est exécuté avec les options `-l -b -x` pour configurer l'hébergement virtuel limité avec une bannière test et le fichier journal `/var/ftp/virtual/10.1.2.3/xferlog` sous une racine virtuelle `/var/ftp/virtual/10.1.2.3`.

```
# ftpaddhost -l -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

▼ Activation de l'hébergement virtuel complet

L'hébergement virtuel complet permet d'avoir des fichiers de configuration distincts pour chaque domaine virtuel. Pour activer la prise en charge complète de l'hébergement virtuel sur le serveur FTP, vous pouvez créer ou modifier les fichiers de configuration FTP suivants pour des domaines spécifiques :

- `ftpaccess`
- `ftpusers`
- `ftpgroups`
- `ftphosts`
- `ftpconversions`

Pour plus d'informations, reportez-vous aux pages de manuel `ftpaccess(4)`, `ftpusers(4)`, `ftpgroups(4)`, `ftphosts(4)` et `ftpconversions(4)`.

Remarque – Si des versions distinctes des fichiers de configuration ne sont pas disponibles, les versions maître des fichiers dans le répertoire `/etc/ftpd` sont utilisées.

---

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez l'entrée suivante au fichier `/etc/ftpd/ftpservers`.

address */config-file-dir*

address Adresse IP du serveur virtuel.

config-file-dir Répertoire qui contient les fichiers de configuration qui sont personnalisés pour l'hôte virtuel.

Remarque – Bien qu'il soit possible d'utiliser `hostname` en tant qu'*address* du serveur virtuel, il est fortement recommandé d'utiliser l'adresse IPv4 à la place. Le DNS doit être disponible lorsque la connexion FTP est reçue pour la correspondance avec `hostname`. Pour un hôte IPv6, utilisez le nom d'hôte à la place de l'adresse IPv6.

---

3 **Pour créer une version personnalisée d'un fichier de configuration du serveur FTP pour l'hôte virtuel, copiez la version maître du fichier de `/etc/ftpd` vers le répertoire `/config-file-dir`.**

Pour plus d'informations, reportez-vous à la page de manuel `ftpservers(4)`.

Exemple 28–17 Activation de l'hébergement virtuel complet dans le fichier `ftpservers`

```
#
# FTP Server virtual hosting configuration file
#

10.1.2.3 /net/inet/virtual/somedomain/
10.1.2.4 /net/inet/virtual/anotherdomain/
```

L'exemple précédent spécifie les adresses IP de deux domaines différents sur le serveur virtuel.

Exemple 28–18 Activation de l'hébergement virtuel complet depuis la ligne de commande

Le script `ftpaddhost(1M)` avec l'option `-c` est fourni pour configurer des hôtes virtuels complets.

Dans l'exemple suivant, `ftpaddhost` est exécuté avec les options `-c -b -x` pour configurer l'hébergement virtuel complet avec une bannière test et le fichier journal `/var/ftp/virtual/10.1.2.3/xferlog` sous une racine virtuelle `/var/ftp/virtual/10.1.2.3`.

```
# ftpaddhost -c -b -x /var/ftp/virtual/10.1.2.3/xferlog \
/var/ftp/virtual/10.1.2.3
```

Démarrage du serveur FTP automatiquement

Le serveur FTP peut être démarré selon l'une des trois manières suivantes :

- En tant que serveur `nowait` qui est démarré par `inetd`
- En tant que serveur autonome exécuté en arrière-plan
- En tant que serveur autonome exécuté au premier plan depuis le fichier `inittab`

Un serveur autonome offre toujours le temps de réponse le plus rapide et est destiné aux serveurs de grande taille dédiés à fournir un service FTP. Il offre en outre une faible latence de connexion pour les serveurs dédiés car le système autonome n'a jamais à être redémarré. Il reste en effet toujours en fonctionnement, même pendant les heures creuses, et attend indéfiniment des connexions.

▼ Démarrage d'un serveur FTP à l'aide de SMF

Par défaut, le service SMF est configuré pour démarrer le serveur FTP à l'aide du mode `nowait`. Si le site gère de nombreuses connexions, le serveur FTP peut également être exécuté en mode autonome. Pour plus d'informations sur les autres options de ligne de commande, reportez-vous à la page de manuel `in.ftpd(1M)`.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Vérifiez la propriété `wait` pour le serveur FTP.

La ligne affichant `wait=FALSE` indique que le serveur est démarré en mode `nowait`.

```
# inetadm -l network/ftp
SCOPE    NAME=VALUE
         name="ftp"
         endpoint_type="stream"
         proto="tcp6"
         isrpc=FALSE
         wait=FALSE
         exec="/usr/sbin/in.ftpd -a"
         user="root"
default  bind_addr=""
default  bind_fail_max=-1
default  bind_fail_interval=-1
default  max_con_rate=-1
default  max_copies=-1
default  con_rate_offline=-1
default  failrate_cnt=40
default  failrate_interval=60
default  inherit_env=TRUE
default  tcp_trace=FALSE
default  tcp_wrappers=FALSE
```

3 Démarrez le serveur FTP.

```
# svcadm enable network/ftp
```

▼ Démarrage d'un serveur FTP autonome en arrière-plan

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le serveur FTP.**

```
# svcadm disable network/ftp
```

3 **Démarrez le serveur FTP autonome.**

```
# /usr/sbin/in.ftpd -a -S
```

Ajouter la ligne à un script de démarrage du serveur FTP. Pour plus d'informations sur la création d'un script de démarrage système, reportez-vous à la rubrique "Utilisation de scripts de contrôle d'exécution" du *Guide d'administration système : administration de base*.

▼ Démarrage d'un serveur FTP autonome au premier plan

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Désactivez le serveur FTP.**

```
# svcadm disable network/ftp
```

3 **Ajoutez une entrée au fichier `inittab` pour démarrer le service.**

La nouvelle entrée dans `/etc/inittab` doit se présenter comme suit :

```
ftpd:3:respawn:/usr/sbin/in.ftpd -a -s
```

4 **Demandez à `init` de réexaminer `/etc/inittab`.**

Cette commande doit démarrer le service FTP.

```
# init q
```

Arrêt du serveur FTP

La commande `ftpshut(1M)` arrête le serveur FTP à un moment précis.

Lorsque vous exécutez `ftpshut`, un fichier est généré à partir des options de la ligne de commande pour indiquer à quel moment l'arrêt se produit, le point auquel les nouvelles connexions sont refusées et le moment auquel les connexions existantes sont rejetées. Les utilisateurs sont informés de l'arrêt du serveur sur la base de ces informations. L'emplacement du fichier créé par `ftpshut` est spécifié par la directive `shutdown` dans le fichier `ftpaccess`.

▼ Arrêt du serveur FTP

Suivez les étapes de cette procédure pour exécuter `ftpshut` et ajouter la directive `shutdown` au fichier `ftpaccess`.

1 Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 Ajoutez les entrées suivantes au fichier `ftpaccess`.

`shutdown` *path*

`shutdown`	Mot-clé utilisé pour spécifier le *path* vers un fichier qui est vérifié régulièrement pour contrôler si le serveur FTP est programmé pour être arrêté.
path	Emplacement du fichier qui a été créé par la commande `ftpshut`.

3 Exécutez la commande `ftpshut`.

```
ftpshut [ -V ] [ -l min] [ -d min] time [warning-message...]
```

`ftpshut`	Commande qui propose une procédure pour avertir les utilisateurs que le serveur FTP est en cours d'arrêt.
`-V`	Option qui est spécifiée pour afficher le copyright et les informations sur la version, puis s'arrêter.
`-l`	Indicateur qui est utilisé pour régler l'heure à laquelle les nouvelles connexions au serveur FTP sont refusées.
`-d`	Indicateur qui est utilisé pour régler l'heure à laquelle les connexions existantes au serveur FTP sont déconnectées.
`time`	L'heure d'arrêt qui est spécifiée par le mot `now` pour un arrêt immédiat, ou dans l'un des deux formats (+ *number* ou *HHMM*) pour un arrêt ultérieur.

`[warning-message...]` Message de notification d'arrêt.

4 **Utilisez la commande `ftprestart` pour redémarrer le serveur FTP après son arrêt.**

Pour plus d'informations, reportez-vous aux pages de manuel `ftpshut(1M)`, `ftpaccess(4)` et `ftprestart(1M)`.

Débogage du serveur FTP

Cette section décrit des méthodes pour déboguer les problèmes avec le serveur FTP.

Vérification de `syslogd` pour les messages du serveur FTP

Le serveur FTP écrit des messages qui sont utiles pour le débogage à l'emplacement spécifié pour les messages du démon dans le fichier `/etc/syslog.conf`. Si un problème survient avec le serveur FTP, consultez d'abord la partie de ce fichier pour de tels messages.

Les messages du serveur FTP sont contrôlés par le démon de l'utilitaire et les informations sur le niveau. Pour envoyer des messages à partir du serveur FTP à `/var/adm/message` et demander à `syslogd` de relire son fichier de configuration, suivez les instructions ci-dessous :

1 **Ajoutez une entrée, telle que celle à continuation, au fichier `/etc/syslog.conf`.**

```
daemon.info /var/adm/message
```

2 **Signalez à `syslogd` de relire sa configuration.**

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

Cette action entraîne l'écriture des messages d'information du serveur FTP sur `/var/adm/messages`.

Utilisation de `greeting text` pour vérifier `ftpaccess`

Pour utiliser la fonction `greeting text` pour vérifier que le bon fichier `ftpaccess` est utilisé, procédez de la façon suivante :

1 **Ajoutez la directive suivante au fichier ftpaccess.**

`greeting text` *message*

2 **Connectez-vous au serveur FTP.**

3 **Si le message ne s'affiche pas, effectuez les opérations suivantes :**

a. **Confirmez que le fichier `ftpaccess` se trouve à l'emplacement correct. Utilisez la commande `strings(1)` pour obtenir l'emplacement du fichier à partir du binaire du serveur FTP.**

```
# strings /usr/sbin/in.ftpd | grep "^/.*ftpaccess"
```

b. **Vérifiez le fichier `ftpservers` pour voir si l'hébergement virtuel a été configuré.**

Pour plus d'informations, reportez-vous aux pages de manuel `ftpaccess(4)`, `ftpservers(4)`, `strings(1)`, `syslog.conf(4)` et `pgrep(1)`.

▼ Vérification des commandes exécutées par les utilisateurs FTP

Pour voir quelles sont les commandes exécutées par les utilisateurs FTP, utilisez la fonction de journalisation `log commands` dans `ftpaccess`.

1 **Ajoutez la directive suivante au fichier `ftpaccess` pour consigner les commandes individuelles lancées par des utilisateurs qui sont spécifiés dans *typelist*.**

```
log commands typelist
```

2 **Vérifiez les messages qui sont écrits à l'emplacement spécifié dans `/etc/syslog.conf`.**

Une aide à la configuration des sites occupés

La liste ci-après fournit quelques suggestions pour améliorer les performances des sites FTP occupés.

1. Les sites qui prennent en charge de nombreuses connexions simultanées doivent exécuter le serveur FTP en mode autonome (voir "Démarrage du serveur FTP automatiquement" à la page 647).
2. Utilisez `vmstat` et d'autres utilitaires système afin de surveiller le système qui héberge le serveur FTP. Si le système arrive à court de ressources, placez une limite pour le nombre de connexions simultanées (voir "Définition de limites de connexions d'utilisateurs" à la page 628). Pour plus d'informations sur le contrôle du système, reportez-vous au Chapitre 13, "Surveillance des performances du système (tâches)" du *Guide d'administration système : Administration avancée*.
3. Si vous imposez une limite de connexions, pensez à utiliser les fonctions `limit-time` et `timeout idle` dans le fichier `ftpaccess` pour empêcher les utilisateurs à monopoliser les connexions. Si vous n'imposez pas de limite de connexions, définissez l'option `-Q` sur `inftpd`.

4. Si vous n'avez pas besoin d'enregistrements des connexions et déconnexions FTP dans `/var/adm/wtmpx`, définissez l'option `-W` sur `in.ftpd`.
5. Afin de réduire la charge sur le système qui héberge le serveur FTP, augmentez la taille des mémoires tampon de transfert à l'aide des fonctions `recvbuf` et `sendbuf` dans le fichier `ftpaccess`. Si de grandes tailles de mémoire tampon sont sélectionnées, il peut être nécessaire d'augmenter le délai d'attente d'activité de données à l'aide de la fonction `timeout data` dans le fichier `ftpaccess`.
6. Le serveur FTP lit à partir de différentes bases de données, y compris hosts, passwd, group et services. Les recherches lentes risquent d'entraîner un délai important de connexion au serveur FTP ; pour y remédier, la configuration de la source `files` d'abord dans `nsswitch.conf` minimise les temps de recherche. Pour plus d'informations, reportez-vous à la page de manuel `nsswitch.conf(4)`.
7. Par défaut, le serveur FTP tente d'effectuer une recherche du nom d'hôte, qui peut être lente et ralentir également la connexion. La fonction `rhostlookup` du fichier `ftpaccess` peut être utilisée pour arrêter cette recherche. Cependant, rappelez-vous que si le nom de l'hôte distant n'est pas recherché, seule son adresse IP est mise en correspondance lors de l'utilisation d'autres fonctions dans le fichier `ftpaccess` et lors de la correspondance avec les entrées du fichier `ftphosts`. En outre, l'adresse IP de l'hôte distant sera utilisée dans les messages, à la place du cookie magique %R. Pour plus d'informations, reportez-vous à la description de la fonction `rhostlookup` à la page de manuel `ftpaccess(4)`.
8. La récupération des informations sur les quotas peut également entraîner un retard important lors de la connexion au serveur FTP ; par conséquent, utilisez la fonction `quota-info` dans le fichier `ftpaccess` uniquement si vous utilisez des cookies magiques de quotas. Pour obtenir la liste des cookies magiques de quotas, reportez-vous à la page de manuel `ftpaccess(4)`.

◆ ◆ ◆ CHAPITRE 29

Accès aux systèmes distants (tâches)

Ce chapitre décrit toutes les tâches qui sont requises pour la connexion aux systèmes distants et l'utilisation de leurs fichiers. Voici la liste des instructions détaillées, contenues dans ce chapitre.

Accès aux systèmes distants (liste des tâches)

Ce chapitre présente les tâches qui sont décrites dans le tableau ci-après pour vous connecter et copier des fichiers à partir des systèmes distants.

TABLEAU 29–1 Liste des tâches : Accès aux systèmes distants

Tâche	Description	Voir
Connexion à un système distant (`rlogin`)	■ Supprimez les fichiers `.rhosts`. ■ Utilisez la commande `rlogin` pour accéder à un système distant.	"Recherche et suppression des fichiers `.rhosts`" à la page 661 "Vérification du fonctionnement d'un système distant" à la page 661 "Identification des utilisateurs connectés à un système distant" à la page 662 "Connexion à un système distant (`rlogin`)" à la page 663 "Déconnexion d'un système distant (`exit`) " à la page 664

TABLEAU 29–1 Liste des tâches : Accès aux systèmes distants *(Suite)*

Tâche	Description	Voir
Connexion à un système distant (ftp)	■ Ouvrez et fermez une connexion ftp. ■ Copiez des fichiers sur et à partir d'un système distant.	"Ouverture d'une connexion ftp à un système distant" à la page 666 "Fermeture d'une connexion ftp à un système distant " à la page 666 "Copie de fichiers à partir d'un système distant (ftp) " à la page 667 "Copie de fichiers vers un système distant (ftp) " à la page 669
Copie de fichiers à distance avec rcp	Utilisez la commande rcp pour copier des fichiers vers et à partir d'un système distant.	"Copie de fichiers entre un système local et un système distant (rcp) " à la page 673

Connexion à un système distant (rlogin)

La commande rlogin vous permet de vous connecter à un système distant. Une fois que vous vous êtes connecté, vous pouvez naviguer dans le système de fichiers à distance et manipuler son contenu (à condition de disposer de l'autorisation nécessaire), copier des fichiers ou exécuter des commandes à distance.

Si le système auquel vous vous connectez est dans un domaine distant, assurez-vous d'ajouter le nom de domaine au nom du système. Dans cet exemple, SOLAR est le nom du domaine distant :

```
rlogin pluto.SOLAR
```

En outre, vous pouvez à tout moment interrompre une opération de connexion à distance en appuyant sur Ctrl-d.

Authentification pour les connexions à distance (rlogin)

Pour les opérations rlogin, l'authentification (votre identification) peut être effectuée par le système distant ou l'environnement réseau.

La principale différence entre ces formes d'authentification se trouve dans le type d'interaction dont elles ont besoin de votre part et la manière dont elles sont établies. Si un système distant essaie de vous authentifier, vous êtes invité à fournir un mot de passe, sauf si vous avez configuré le fichier /etc/hosts.equiv ou .rhosts. Si le réseau tente de vous authentifier, vous n'êtes pas invité à fournir un mot de passe, car le réseau sait déjà qui vous êtes.

Lorsque le système distant tente de vous authentifier, il s'appuie sur les informations contenues dans ses fichiers locaux, en particulier si l'une des conditions suivantes est remplie :

- Votre nom de système et le nom de l'utilisateur s'affichent dans le fichier `/etc/hosts.equiv` du système distant.
- Le nom de votre système et votre nom d'utilisateur s'affichent dans le fichier `.rhosts` de l'utilisateur distant, sous le répertoire personnel de cet utilisateur.

L'authentification réseau s'appuie sur l'une des deux méthodes suivantes :

- Environnement réseau fiable qui a été configuré avec votre service d'information réseau local et l'agent de montage automatique.
- L'un des services d'information réseau qui est désigné par le fichier `/etc/nsswitch.conf` du système distant contient des informations vous concernant.

Remarque – L'authentification réseau remplace généralement l'authentification système.

Fichier `/etc/hosts.equiv`

Le fichier `/etc/hosts.equiv` contient une liste des hôtes de confiance pour un système distant (un par ligne). Si un utilisateur tente de se connecter à distance (à l'aide de `rlogin`) à partir de l'un des hôtes qui est répertorié dans ce fichier, et si le système distant peut accéder au mot de passe de l'utilisateur, le système distant permet à l'utilisateur de se connecter sans mot de passe.

Un fichier `hosts.equiv` standard présente la structure suivante :

```
host1
host2 user_a
+@group1
-@group2
```

Lorsqu'une entrée unique est effectuée pour un hôte dans `hosts.equiv`, telle que l'entrée précédente pour `host1`, cela signifie que l'hôte est approuvé et que tout utilisateur de cette machine l'est également.

Si le nom d'utilisateur est également mentionné, comme dans la deuxième entrée de l'exemple, l'hôte est de confiance uniquement si l'utilisateur spécifié effectue une tentative d'accès.

Un nom de groupe qui est précédé d'un signe plus (+) indique que toutes les machines de ce groupe réseau sont considérées comme de confiance.

Un nom de groupe qui est précédé d'un signe moins (–) signifie qu'aucune des machines de ce groupe réseau n'est considérée comme de confiance.

Risques liés à la sécurité lors de l'utilisation du fichier /etc/hosts.equiv

Le fichier /etc/hosts.equiv présente un risque pour la sécurité. Si vous mettez à jour un fichier /etc/hosts.equiv sur votre système, vous devez inclure uniquement des hôtes de confiance sur votre réseau. Le fichier ne doit inclure aucun hôte appartenant à un autre réseau, ou à des machines qui se trouvent dans des lieux publics. Par exemple, n'incluez pas d'hôte qui se trouve dans une salle de terminal.

L'utilisation d'hôtes non approuvés peut créer un grave problème de sécurité. Remplacez le fichier /etc/hosts.equiv par un fichier correctement configuré ou supprimez le fichier purement et simplement.

Une seule ligne de + dans le fichier /etc/hosts.equiv indique que chaque hôte connu est de confiance.

Fichier .rhosts

Le fichier .rhosts est l'équivalent utilisateur du fichier /etc/hosts.equiv. Ce fichier contient une liste de combinaisons hôte-utilisateur, plutôt que d'hôtes en général. Si une combinaison hôte-utilisateur est répertoriée dans ce fichier, l'utilisateur spécifié est autorisé à se connecter à distance depuis l'hôte spécifié sans avoir à fournir un mot de passe.

Notez qu'un fichier .rhosts doit se trouver au niveau supérieur du répertoire personnel d'un utilisateur. Les fichiers .par qui se trouvent dans des sous-répertoires ne sont pas consultés.

Les utilisateurs peuvent créer des fichiers .rhosts dans leurs répertoires personnels. L'utilisation du fichier .rhosts est une autre façon de permettre l'accès sécurisé aux propres comptes des utilisateurs sur les différents systèmes sans utiliser le fichier /etc/hosts.equiv.

Risques de sécurité lors de l'utilisation du fichier .rhosts

Malheureusement, le fichier .rhosts présente un grave problème de sécurité. Tandis que le fichier /etc/hosts.equiv est sous le contrôle de l'administrateur système et peut être géré efficacement, n'importe quel utilisateur peut créer un fichier .rhosts qui accorde l'accès à la personne choisie par lui sans que l'administrateur système n'en soit informé.

Dans une situation dans laquelle tous les répertoires personnels des utilisateurs se trouvent sur un seul serveur, auquel seules certaines personnes peuvent accéder en tant que superutilisateur, un bon moyen d'empêcher un utilisateur d'utiliser un fichier .rhosts est de créer un fichier vide en tant que superutilisateur dans leur répertoire personnel. Ensuite, vous devez modifier les autorisations de ce fichier en 000 afin qu'il soit difficile de modifier ce dernier, même en tant que superutilisateur. Cette modification a pour effet d'empêcher un utilisateur de compromettre la sécurité du système en utilisant un fichier .rhosts de manière irresponsable. Cependant, la modification ne résout rien si l'utilisateur est en mesure de changer le chemin d'accès à son répertoire personnel.

Le seul moyen de gérer les fichiers .rhosts de manière sécurisée est de les interdire complètement. Reportez-vous à la section "Recherche et suppression des fichiers .rhosts" à la page 661 pour obtenir des instructions détaillées. En tant qu'administrateur système, vous pouvez vérifier souvent le système à la recherche d'éventuelles violations de cette stratégie. Une exception possible à cette stratégie concerne le compte root ; vous pouvez avoir besoin d'un fichier .rhosts pour effectuer les sauvegardes réseau et d'autres services à distance.

Liaison des connexions à distance

Si votre système est configuré correctement, vous pouvez lier des connexions à distance. Par exemple, un utilisateur d'earth se connecte à jupiter et décide, à partir de là, de se connecter à pluto.

L'utilisateur peut également se déconnecter de jupiter, puis se connecter directement à pluto, mais ce type de liaison peut être plus pratique.

Pour lier des connexions à distance sans avoir à fournir un mot de passe, vous devez avoir configuré le fichier /etc/hosts.equiv ou .rhosts correctement.

Connexions à distance directes ou indirectes

La commande rlogin vous permet de vous connecter à un système distant de manière directe ou indirecte.

Une connexion à distance directe est tentée avec le nom d'utilisateur par défaut, c'est-à-dire le nom d'utilisateur de la personne qui est actuellement connectée au système local. Il s'agit du type de connexion à distance le plus commun.

Une connexion à distance indirecte est lancée avec un autre nom d'utilisateur, qui est fourni pendant l'opération de connexion à distance. Il s'agit du type de connexion à distance que vous pouvez essayer à partir d'une station de travail que vous avez empruntée temporairement. Par exemple, si vous êtes dans le bureau d'un collègue de travail et avez besoin d'examiner les fichiers dans votre répertoire personnel, vous pouvez vous connecter à votre système à distance, à partir du système de votre collègue. Cependant, vous devez effectuer une connexion à distance indirecte en indiquant votre propre nom d'utilisateur.

Les dépendances entre les connexions directes et indirectes et les méthodes d'authentification sont résumées dans le tableau suivant.

TABLEAU 29–2 Dépendances entre la méthode de connexion et la méthode d'authentification (rlogin)

Type de connexion	Nom d'utilisateur fourni par	Authentification	Mot de passe
Directe	Système	Réseau	Aucune

TABLEAU 29–2 Dépendances entre la méthode de connexion et la méthode d'authentification (rlogin) *(Suite)*

Type de connexion	Nom d'utilisateur fourni par	Authentification	Mot de passe
Indirecte	Utilisateur	Système	Requis
		Réseau	Aucune
		Système	Requis

Que se passe-t-il après que vous vous êtes connecté à distance ?

Lorsque vous vous connectez à un système distant, la commande `rlogin` recherche votre répertoire personnel. Si la commande `rlogin` n'est pas en mesure de trouver votre répertoire personnel, elle vous affecte le répertoire root (`/`) du système distant. Par exemple :

```
Unable to find home directory, logging in with /
```

Toutefois, si la commande `rlogin` trouve votre répertoire personnel, elle se procure vos fichiers `.cshrc` et `.login`. Par conséquent, après une connexion à distance, l'invite de connexion standard s'affiche, et le répertoire en cours est le même que lorsque vous vous connectez localement.

Par exemple, si votre invite habituelle affiche le nom de votre système et de votre répertoire de travail, et lorsque vous vous connectez, votre répertoire de travail est votre répertoire personnel, votre invite de connexion ressemble à la suivante :

```
earth(/home/smith):
```

Ensuite, lorsque vous vous connectez à un système distant, vous voyez une invite similaire, et votre répertoire de travail est votre répertoire personnel, quel que soit le répertoire à partir duquel vous avez saisi la commande `rlogin` :

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/smith):
```

La seule différence est que le nom du système distant se substitue à votre système local au début de l'invite. Le système de fichiers distant est parallèle à votre répertoire personnel.

En fait, si vous changez le répertoire en `/home`, puis exécutez `ls`, la sortie suivante s'affiche :

```
earth(home/smith): cd ..
earth(/home): ls
smith  jones
```

▼ Recherche et suppression des fichiers .rhosts

1 **Connectez-vous en tant que superutilisateur ou endossez un rôle équivalent.**

Les rôles contiennent des autorisations et des commandes privilégiées. Pour plus d'informations sur les rôles, reportez-vous à la section "Configuring RBAC (Task Map)" du *System Administration Guide: Security Services*.

2 **Recherchez et supprimez les fichiers .rhosts à l'aide de la commande find(1).**

```
# find home-directories -name .rhosts -print -exec rm {} \;
```

home-directories	Identifie le chemin d'accès à un répertoire dans lequel se trouvent les répertoires personnels des utilisateurs. Notez que vous pouvez saisir plusieurs chemins d'accès pour rechercher plusieurs répertoires personnels à la fois.
`-name .rhosts`	Identifie le nom du fichier.
`-print`	Imprime le chemin d'accès en cours.
`-exec rm {} \;`	Indique à la commande `find` d'appliquer la commande `rm` à tous les fichiers qui sont identifiés à l'aide du nom de fichier correspondant.

La commande `find` démarre au répertoire désigné et recherche tous les fichiers nommés `.rhosts`. Si `find` trouve un fichier de ce type, elle affiche le chemin d'accès à l'écran et supprime le fichier.

Exemple 29–1 Recherche et suppression des fichiers .rhosts

L'exemple suivant recherche et supprime les fichiers `.rhosts` de tous les répertoires personnels de l'utilisateur qui se trouvent dans le répertorie `/export/Home` .

```
# find /export/home -name .rhosts -print | xargs -i -t rm {} \;
```

Vérification du fonctionnement d'un système distant

Déterminez si un système distant fonctionne en utilisant la commande `ping`.

```
$ ping system-name | ip-address
```

system-name	Nom du système distant
adresse_ip	Adresse IP du système distant

La commande `ping` renvoie l'un des trois messages suivants :

Message d'état	Explication
system-name is alive	Le système est accessible sur le réseau.
ping: unknown host *system-name*	Le nom du système est inconnu.
ping: no answer from *system-name*	Le système est connu, mais n'est pas en cours de fonctionnement.

Si le système faisant l'objet de la commande ping est situé dans un autre domaine, le message de retour peut également contenir les informations de routage, que vous pouvez ignorer.

Le délai de la commande ping est de 20 secondes. En réalité, si elle ne reçoit pas de réponse dans les 20 secondes, elle renvoie le troisième message. Vous pouvez forcer ping à attendre plus longtemps (ou moins) en tapant une valeur *time-out*, en secondes :

```
$ ping system-name | ip-address time-out
```

Pour plus d'informations, reportez-vous à la commande ping(1M).

Identification des utilisateurs connectés à un système distant

Identifiez les utilisateurs connectés à un système distant à l'aide de la commande rusers(1).

```
$ rusers [-l] remote-system-name
```

rusers	(Pas d'options) Affiche le nom du système, suivi par le nom des utilisateurs qui sont actuellement connectés à celui-ci, y compris root
-l	Affiche des informations supplémentaires à propos de chaque utilisateur : la fenêtre de connexion de l'utilisateur, l'heure, la date et la durée de la connexion, et le nom du système distant à partir duquel l'utilisateur s'est connecté

EXEMPLE 29–2 Recherche des utilisateurs connectés à un système distant

L'exemple ci-dessous présente la sortie brève de rusers.

```
$ rusers pluto
pluto    smith  jones
```

Dans l'exemple suivant, la version longue de rusers indique que deux utilisateurs sont connectés au système distant starbug. Le premier utilisateur s'est connecté à partir de la console système le 10 septembre et est resté connecté 137 heures et 15 minutes. Le deuxième utilisateur s'est connecté à partir d'un système distant, mars, le 14 septembre.

EXEMPLE 29–2 Recherche des utilisateurs connectés à un système distant *(Suite)*

```
$rusers -l starbug
root         starbug:console           Sep 10 16:13  137:15
rimmer       starbug:pts/0             Sep 14 14:37         (mars)
```

Connexion à un système distant (`rlogin`)

Connectez-vous à un système distant en utilisant la commande `rlogin(1)`.

`$ rlogin [-l` *user-name*`]` *system-name*

`rlogin`	(Pas d'options) Permet de vous connecter au système distant *directement*, efficacement, avec votre nom d'utilisateur en cours
`-l` *user-name*	Permet de vous connecter au système distant *indirectement*, efficacement, avec le nom d'utilisateur que vous avez fourni

Si le réseau tente de vous authentifier, vous n'êtes pas invité à saisir un mot de passe. Si le système distant tente de vous authentifier, vous êtes invité à fournir un mot de passe.

Si l'opération réussit, la commande `rlogin` affiche des informations succinctes sur votre dernière connexion à distance à ce système, la version du système d'exploitation qui est en cours d'exécution sur le système distant, et si vous avez du courrier en attente dans votre répertoire personnel.

EXEMPLE 29–3 Connexion à un système distant (`rlogin`)

L'exemple ci-dessous présente la sortie d'une connexion à distance directe à `pluto`. L'utilisateur a été authentifié par le réseau.

```
$ rlogin starbug
Last login: Mon Jul 12 09:28:39 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
starbug:
```

L'exemple suivant présente la sortie d'une connexion à distance indirecte à `pluto`, avec l'authentification de l'utilisateur par le système distant.

```
$ rlogin -l smith pluto
password: user-password
Last login: Mon Jul 12 11:51:58 from venus
Sun Microsystems Inc.   SunOS 5.8       February 2000
starbug:
```

Déconnexion d'un système distant (exit)

Déconnexion d'un système distant à l'aide de la commande exit(1).

```
$ exit
```

EXEMPLE 29–4 Déconnexion d'un système distant (exit)

Cet exemple illustre l'utilisateur smith se déconnectant du système pluto.

```
$ exit
pluto% logout
Connection closed.
earth%
```

Connexion à un système distant (ftp)

La commande ftp ouvre l'interface utilisateur du protocole de transfert de fichiers (FTP). Cette interface utilisateur, appelée l'interpréteur de commandes, permet de vous connecter à un système distant et d'effectuer de nombreuses opérations avec son système de fichiers. Les principales activités sont résumées dans le tableau ci-dessous.

Le principal avantage de ftp sur rlogin et rcp est que ftp n'a pas besoin que le système distant exécute UNIX. Le système distant, cependant, doit être configuré pour les communications TCP/IP. Cependant, rlogin fournit l'accès à un nombre plus important de commandes de manipulation de fichiers que ftp.

Authentification pour les connexions à distance (ftp)

L'authentification des opérations de connexion à distance ftp peut être effectuée selon l'une des méthodes suivantes :

- Indication de votre mot de passe dans le fichier /etc/passwd du système distant ou la liste ou table des services d'information réseau équivalente
- Création d'un compte ftp anonyme sur le système distant

Commandes ftp de base

TABLEAU 29–3 Commandes ftp de base

Commande	Description
`ftp`	Accède à l'interpréteur de commandes `ftp`.
`ftp` *remote-system*	Établit une connexion `ftp` à un système distant. Pour plus d'instructions, consultez la section "Ouverture d'une connexion `ftp` à un système distant" à la page 666.
`open`	Permet de se connecter au système distant à partir de l'interpréteur de commandes.
`close`	Permet de se déconnecter du système distant et renvoie à l'interpréteur de commandes.
`bye`	Ferme l'interpréteur de commandes `ftp`.
`help`	Affiche la liste de toutes les commandes `ftp` ou, si un nom de commande est fourni, décrit brièvement l'action de la commande.
`reset`	Resynchronisez le séquencement commande-réponse avec le serveur `ftp` distant.
`ls`	Répertorie le contenu du répertoire de travail distant.
`pwd`	Affiche le nom du répertoire de travail distant.
`cd`	Modifie le répertoire de travail distant.
`lcd`	Modifie le répertoire de travail local.
`mkdir`	Crée un répertoire sur le système distant.
`rmdir`	Supprime un répertoire sur le système distant.
`get, mget`	Copie un fichier (ou plusieurs fichiers) à partir du répertoire de travail distant vers le répertoire de travail local.
`put, mput`	Copie un fichier (ou plusieurs fichiers) à partir du répertoire de travail local vers le répertoire de travail distant.
`delete, mdelete`	Supprime un fichier (ou plusieurs fichiers) à partir du répertoire de travail distant.

Pour plus d'informations, reportez-vous à la page de manuel `ftp(1)`.

▼ Ouverture d'une connexion ftp à un système distant

1 **Assurez-vous que vous disposez de l'authentification ftp.**

Vous devez disposer de l'authentification ftp, comme décrit dans la section "Authentification pour les connexions à distance (ftp) " à la page 664.

2 **Ouvrez une connexion à un système distant en utilisant la commande ftp.**

```
$ ftp remote-system
```

Si la connexion est établie, un message de confirmation et une invite sont affichés.

3 **Tapez votre nom d'utilisateur.**

```
Name (remote-system:user-name): user-name
```

4 **Si vous y êtes invité, tapez votre mot de passe.**

```
331 Password required for user-name:
Password: password
```

Si le système auquel vous accédez dispose d'un compte ftp anonyme établi, vous êtes invité à indiquer une adresse e-mail pour le mot de passe. Si l'interface ftp accepte votre mot de passe, elle affiche un message de confirmation et l'invite (ftp>).

Vous pouvez maintenant utiliser l'une ou l'autre des commandes qui sont fournies par l'interface ftp, y compris help. Les principales commandes sont récapitulées dans le Tableau 29–3.

Exemple 29–5 Ouverture d'une connexion ftp à un système distant

Cette session ftp a été établie par l'utilisateur smith sur le système distant pluto :

```
$ ftp pluto
Connected to pluto.
220 pluto FTP server ready.
Name (pluto:smith): smith
331 Password required for smith:
Password: password
230 User smith logged in.
ftp>
```

Fermeture d'une connexion ftp à un système distant

Fermez une connexion ftp à un système distant en utilisant la commande bye.

```
ftp> bye
221-You have  transferred 0 bytes in 0 files.
221-Total traffic for this sessions was 172 bytes in 0 transfers.
221-Thanks you for using the FTP service on spdev.
221 Goodbye.
```

Un message de fermeture s'affiche, suivi de l'invite de shell habituelle.

▼ Copie de fichiers à partir d'un système distant (ftp)

1. **Modifiez un répertoire sur le système local où vous souhaitez que les fichiers d'un système distant soient copiés.**

   $ **cd** *target-directory*

2. **Établissez une connexion ftp.**

   Reportez-vous à la section "Ouverture d'une connexion ftp à un système distant" à la page 666.

3. **Passez au répertoire source.**

   ftp> **cd** *source-directory*

   Si votre système utilise l'agent de montage automatique, le répertoire personnel de l'utilisateur du système distant s'affiche parallèlement au vôtre, sous /home.

4. **Assurez-vous que vous disposez de l'autorisation de lecture pour les fichiers source.**

   ftp> **ls -l**

5. **Définissez le type de transfert sur binary (binaire).**

   ftp> **binary**

6. **Pour copier un fichier unique, utilisez la commande get.**

   ftp> **get** *filename*

7. **Pour copier plusieurs fichiers à la fois, utilisez la commande mget.**

   ftp> **mget** *filename* [*filename* ...]

   Vous pouvez fournir une série de noms de fichier et utiliser des caractères génériques. La commande mget copie chaque fichier individuellement, en vous demandant confirmation à chaque fois.

8. **Fermez les connexions ftp.**

   ftp> **bye**

Exemple 29–6 Copie de fichiers à partir d'un système distant (ftp)

Dans cet exemple, l'utilisateur kryten ouvre une connexion ftp au système pluto et utilise la commande get pour copier un fichier unique à partir du répertoire /tmp.

```
$ cd $HOME
ftp pluto
Connected to pluto.
```

```
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34344)
(0 bytes).
filea
files
ps_data
226 ASCII Transfer complete.
53 bytes received in 0.022 seconds (2.39 Kbytes/s)
ftp> get filea
200 PORT command successful.
150 ASCII data connection for filea (129.152.221.238,34331)
(0 bytes).
221 Goodbye.
```

Dans cet exemple, le même utilisateur `kryten` utilise la commande `mget` pour copier un ensemble de fichiers à partir du répertoire `/tmp` dans son répertoire personnel. Notez que `kryten` peut accepter ou rejeter les fichiers individuels de l'ensemble.

```
$ ftp> cd /tmp
250 CWD command successful.
ftp> ls files
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34345)
(0 bytes).
fileb
filec
filed
remote: files
21 bytes received in 0.015 seconds (1.36 Kbytes/s)
ftp> cd files
250 CWD command successful.
ftp> mget file*
mget fileb? y
200 PORT command successful.
150 ASCII data connection for fileb (129.152.221.238,34347)
(0 bytes).
226 ASCII Transfer complete.
mget filec? y
200 PORT command successful.
150 ASCII data connection for filec (129.152.221.238,34348)
(0 bytes).
226 ASCII Transfer complete.
mget filed? y
200 PORT command successful.
150 ASCII data connection for filed (129.152.221.238,34351)
(0 bytes).
226 ASCII Transfer complete.200 PORT command successful.
ftp> bye
221 Goodbye.
```

▼ Copie de fichiers vers un système distant (ftp)

1. **Passez au répertoire source sur le système local.**

   Le répertoire à partir duquel vous tapez la commande ftp est le répertoire de travail local, et donc le répertoire source pour cette opération.

2. **Établissez une connexion ftp.**

   Reportez-vous à la section "Ouverture d'une connexion ftp à un système distant" à la page 666.

3. **Passez au répertoire cible.**

   ```
   ftp> cd target-directory
   ```

   N'oubliez pas que si votre système utilise l'agent de montage automatique, le répertoire personnel de l'utilisateur du système distant s'affiche parallèlement au vôtre, sous /home.

4. **Assurez-vous que vous disposez d'une autorisation d'écriture sur le répertoire cible.**

   ```
   ftp> ls -l target-directory
   ```

5. **Définissez le type de transfert sur binary.**

   ```
   ftp> binary
   ```

6. **Pour copier un fichier unique, utilisez la commande put.**

   ```
   ftp> put filename
   ```

7. **Pour copier plusieurs fichiers à la fois, utilisez la commande mput.**

   ```
   ftp> mput filename [filename ...]
   ```

   Vous pouvez fournir une série de noms de fichier et utiliser des caractères génériques. La commande mput copie chaque fichier individuellement, en vous demandant confirmation à chaque fois.

8. **Pour fermer la connexion ftp, tapez bye.**

   ```
   ftp> bye
   ```

Exemple 29–7 Copie de fichiers vers un système distant (ftp)

Dans cet exemple, l'utilisateur kryten ouvre une connexion ftp au système pluto et utilise la commande put pour copier un fichier à partir de son système vers le répertoire /tmp du système pluto.

```
$ cd /tmp
ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
```

```
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> put filef
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> ls
200 PORT command successful.
150 ASCII data connection for /bin/ls (129.152.221.238,34357) (0 bytes).
filea
filef
files
ps_data
226 ASCII Transfer complete.
60 bytes received in 0.058 seconds (1.01 Kbytes/s)
ftp> bye
221 Goodbye.
```

Dans cet exemple, le même utilisateur `kryten` utilise la commande `mput` pour copier un ensemble de fichiers à partir de son répertoire personnel vers le répertoire `/tmp` de `pluto`. Notez que `kryten` peut accepter ou rejeter les fichiers individuels de l'ensemble.

```
$ cd $HOME/testdir
$ ls
test1   test2   test3
$ ftp pluto
Connected to pluto.
220 pluto FTP server (SunOS 5.8) ready.
Name (pluto:kryten): kryten
331 Password required for kryten.
Password: xxx
230 User kryten logged in.
ftp> cd /tmp
250 CWD command successful.
ftp> mput test*
mput test1? y
200 PORT command successful.
150 ASCII data connection for test1 (129.152.221.238,34365).
226 Transfer complete.
mput test2? y
200 PORT command successful.
150 ASCII data connection for test2 (129.152.221.238,34366).
226 Transfer complete.
mput test3? y
200 PORT command successful.
150 ASCII data connection for filef (129.152.221.238,34356).
226 Transfer complete.
ftp> bye
221 Goodbye.
```

Copie à distance avec rcp

La commande rcp copie les fichiers ou les répertoires entre un système local et un système distant ou entre deux systèmes distants. Vous pouvez utiliser cette commande à partir d'un système distant (après la connexion avec la commande rlogin) ou à partir du système local (sans vous connecter à un système distant).

À l'aide de rcp, vous pouvez effectuer les opérations de copie à distance suivantes :

- Copie d'un fichier ou d'un répertoire de votre système vers un système distant
- Copie d'un fichier ou d'un répertoire à partir d'un système distant vers votre système local
- Copie d'un fichier ou d'un répertoire entre des systèmes distants à partir de votre système local

Si l'agent de montage automatique est en cours d'exécution, vous pouvez effectuer ces opérations à distance avec la commande cp. Toutefois, la plage de cp est limitée au système de fichiers virtuel créé par l'agent de montage automatique et aux opérations relatives au répertoire personnel de l'utilisateur. Dans la mesure où rcp effectue les mêmes opérations sans ces limitations, cette section décrit uniquement les versions rcp de ces tâches.

Considérations en matière de sécurité pour les opérations de copie

Pour copier des fichiers ou des répertoires d'un système à un autre, vous devez avoir l'autorisation de vous connecter et de copier des fichiers.

Attention – Les commandes cp et rcp peuvent écraser les fichiers sans avertissement. Assurez-vous que les noms de fichier sont corrects avant d'exécuter la commande.

Indication de la source et de la cible

À l'aide de la commande rcp dans le shell C, vous pouvez spécifier la source (fichier ou répertoire à copier) et la cible (emplacement de copie du fichier ou répertoire) avec les noms de chemins absolus ou abrégés.

	Noms de chemins absolus	Noms de chemins abrégés
Depuis le système local	`mars:/home/jones/monfichier.txt`	`~jones/monfichier.txt`
Après une connexion à distance	`/home/jones/monfichier.txt`	`~jones/monfichier.txt`

Les noms de chemins absolus identifient les fichiers ou répertoires qui sont montés sur un système particulier. Dans l'exemple précédent, le premier nom de chemin absolu identifie un fichier (`monfichier.txt`) sur le système `mars`. Les noms de chemins abrégés identifient les fichiers ou répertoires par rapport au répertoire personnel de l'utilisateur, où qu'il se trouve. Dans le premier exemple, le nom de chemin abrégé identifie le même fichier, `monfichier.txt`, mais utilise le symbole « ~ » pour indiquer le répertoire personnel `jones` :

```
~ = mars:/home/jones
```

Les exemples de la deuxième ligne illustre l'utilisateur des noms de chemins absolus et abrégés après une connexion à distance. Aucune différence n'apparaît pour le nom de chemin abrégé. Toutefois, étant donné que l'opération de connexion à distance a monté le répertoire personnel `jones` sur le système local (parallèle au répertoire personnel de l'utilisateur local), le nom de chemin absolu ne nécessite plus le nom de système `mars`. Pour plus d'informations sur la manière dont une opération de connexion à distance monte le répertoire personnel d'un autre utilisateur, reportez-vous à la section “Que se passe-t-il après que vous vous êtes connecté à distance ?” à la page 660.

Le tableau suivant fournit des exemples de noms de chemins absolus et abrégés qui sont reconnus par le shell C. L'exemple utilise la terminologie suivante :

- Répertoire de travail : répertoire à partir duquel la commande `rcp` est saisie. Peut être local ou distant.
- Utilisateur en cours : nom d'utilisateur sous lequel est entrée la commande `rcp`.

TABLEAU 29–4 Syntaxes autorisées pour les noms de répertoire et de fichier

Connecté à	Syntaxe	Description
Système local	.	Répertoire de travail local
	path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) dans le répertoire de travail local
	~	Répertoire personnel de l'utilisateur en cours
	~/path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) sous le répertoire personnel de l'utilisateur en cours
	~user	Répertoire personnel de l'utilisateur (*user*)
	~user/path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) sous le répertoire personnel de l'utilisateur (*user*)
	remote-system:path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) dans le répertoire de travail distant
Système distant	.	Répertoire de travail distant

TABLEAU 29–4 Syntaxes autorisées pour les noms de répertoire et de fichier *(Suite)*

Connecté à	Syntaxe	Description
	filename	Nom du fichier (*filename*) dans le répertoire de travail distant
	path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) dans le répertoire de travail distant
	~	Répertoire personnel de l'utilisateur en cours
	~/path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) dans le répertoire personnel de l'utilisateur en cours
	~user	Répertoire personnel de l'utilisateur (*user*)
	~/user/path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) sous le répertoire personnel de l'utilisateur (*user*)
	local-system:path/filename	Chemin d'accès (*path*) et nom de fichier (*filename*) dans le répertoire de travail local

▼ Copie de fichiers entre un système local et un système distant (`rcp`)

1 Assurez-vous que vous êtes autorisé à copier.

Vous devez au moins disposer de l'autorisation de lecture sur le système source et de l'autorisation d'écrire sur le système cible.

2 Déterminez l'emplacement de la source et de la cible.

Si vous ne connaissez pas le chemin d'accès de la source ou de la cible, vous pouvez d'abord vous connecter au système distant avec la commande `rlogin`, comme décrit dans la section "Connexion à un système distant (`rlogin`)" à la page 663. Ensuite, parcourez le système distant jusqu'à ce que vous trouviez l'emplacement. Vous pouvez ensuite exécuter l'étape suivante sans vous déconnecter.

3 Copiez le fichier ou répertoire.

`$ rcp [-r]` *source-file|directory target-file|directory*

`rcp` (Pas d'options) Copie un fichier unique à partir de la source vers la cible.

`-r` Copie un répertoire de la source vers la cible.

Cette syntaxe s'applique que vous soyez connecté au système distant ou au système local. Seul le nom de chemin du fichier ou répertoire change, comme décrit dans le Tableau 29–4 et comme l'illustrent les exemples suivants.

Vous pouvez utiliser les caractères « ~ » et « . » pour indiquer les parties des chemins d'accès des noms de fichiers ou répertoires. Notez, cependant, que le caractère « ~ » s'applique à l'utilisateur en cours, et non au système distant, et que le caractère « . » s'applique au système auquel vous êtes connecté. Pour obtenir des explications sur ces symboles, reportez-vous au Tableau 29–4.

Exemple 29–8 Utilisation de `rcp` pour copier un fichier distant sur un système local

Dans cet exemple, `rcp` est utilisée pour copier le fichier `letter.doc` à partir du répertoire `/home/jones` du système distant `pluto` dans le répertoire de travail (`/home/smith`) du système local `earth` :

```
earth(/home/smith): rcp pluto:/home/jones/letter.doc .
```

Dans cette instance, l'opération `rcp` est effectuée sans connexion à distance. Ici, le symbole « . » à la fin de la ligne de commande fait référence au système local, et non au système distant.

Le répertoire cible est également le répertoire personnel de l'utilisateur local, de sorte qu'il peut également être spécifié avec le symbole « ~ ».

Exemple 29–9 Utilisation de `rlogin` et `rcp` pour copier un fichier distant sur un système local

Dans cet exemple, l'opération `rcp` est exécutée après la commande `rlogin` pour copier un fichier à partir d'un système distant sur un système local. Bien que le flux de l'opération soit le même que celui de l'exemple précédent, les chemins d'accès sont modifiés pour permettre la connexion à distance :

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp letter.doc ~
```

L'utilisation du symbole « . » à la fin de la ligne de commande n'est pas appropriée dans ce cas. En raison de la connexion à distance, ce symbole ferait simplement référence au système distant, en dirigeant principalement `rcp` pour créer un fichier en double. Le symbole « ~ », cependant, fait référence au répertoire personnel de l'utilisateur actuel, même lorsqu'il s'agit d'une connexion à un système distant.

Exemple 29–10 Utilisation de `rcp` pour copier un fichier local sur un système distant

Dans cet exemple, `rcp` est utilisée pour copier le fichier `notice.doc` à partir du répertoire personnel (`/home/smith`) du système local `earth` sur le répertoire `/home/jones` du système distant `pluto` :

```
earth(/home/smith): rcp notice.doc pluto:/home/jones
```

Étant donné qu'aucun nom de fichier distant n'est fourni, le fichier `notice.doc` est copié dans le répertoire `/home/jones` avec le même nom.

Dans ce cas, l'opération `rcp` de l'exemple précédent est répétée, mais `rcp` est saisie à partir d'un autre répertoire de travail sur le système local (`/tmp`). Notez l'utilisation du symbole « ~ » pour désigner le répertoire personnel de l'utilisateur en cours :

```
earth(/tmp): rcp ~/notice.doc pluto:/home/jones
```

Exemple 29–11 Utilisation de `rlogin` et `rcp` pour copier un fichier local sur un système distant

Dans cet exemple, l'opération `rcp` est exécutée après la commande `rlogin` pour copier un fichier local sur un répertoire distant. Bien que le flux de l'opération soit le même que celui de l'exemple précédent, les chemins d'accès sont modifiés pour permettre la connexion à distance.

```
earth(/home/smith): rlogin pluto
.
.
.
pluto(/home/jones): rcp ~/notice.doc .
```

Dans cette instance, le symbole « ~ » peut être utilisé pour indiquer le répertoire personnel de l'utilisateur en cours, même s'il se trouve sur le système local. Le symbole « `.` » fait référence au répertoire de travail sur le système distant car l'utilisateur est connecté à ce dernier. Voici une syntaxe alternative qui effectue la même opération :

```
pluto(/home/jones): rcp earth:/home/smith/notice.doc /home/jones
```

PARTIE VII

Sujets relatifs au contrôle des services réseau

Cette section fournit des instructions détaillées concernant le contrôle des services réseau.

◆ ◆ ◆ CHAPITRE 30

Contrôle des performances du réseau (tâches)

Ce chapitre décrit comment contrôler les performances de votre réseau. Vous trouverez ci-après une liste des instructions relatives à chaque étape décrite dans ce chapitre.

Contrôle des performances du réseau

Le Tableau 30–1 décrit les commandes disponibles pour le contrôle des performances réseau.

TABLEAU 30–1 Commandes de contrôle du réseau

Commande	Description
`ping`	Examinez la réponse des hôtes sur le réseau.
`spray`	Vérifiez la fiabilité des tailles de vos paquets. Cette commande peut vous indiquer si le réseau retarde ou abandonne des paquets.
`snoop`	Capturez des paquets à partir du réseau et suivez les appels de chaque client à chaque serveur.
`netstat`	Affichez l'état du réseau, notamment l'état des interfaces utilisées pour le trafic TCP/IP, la table de routage IP et les statistiques de chaque protocole (`UDP`, `TCP`, `ICMP` et `IGMP`).
`nfsstat`	Affichez un récapitulatif des statistiques relatives au serveur et au client, que vous pouvez utiliser pour identifier les problèmes NFS.

Vérification de la réponse des hôtes sur le réseau

Vérifiez la réponse des hôtes sur le réseau à l'aide de la commande `ping`.

```
$ ping hostname
```

Lorsque vous rencontrez un problème physique, la commande `ping` peut indiquer le temps de réponse de plusieurs hôtes sur le réseau. Si la réponse d'un hôte n'est pas celle attendue, vérifiez la configuration de l'hôte. Les éléments suivants peuvent être à l'origine de problèmes physiques :

- Câbles ou connecteurs mal branchés
- Mise à la terre incorrecte
- Aucun raccordement
- Réflexion du signal

Pour plus d'informations sur cette commande, reportez-vous à `ping(1M)`.

EXEMPLE 30–1 Vérification de la réponse d'hôtes sur le réseau

La version la plus simple de `ping` envoie un paquet unique à un hôte sur le réseau. Si `ping` reçoit la réponse correcte, elle imprime le message *host* `is alive`.

```
$ ping elvis
elvis is alive
```

Avec l'option `-s`, `ping` envoie un datagramme par seconde vers un hôte. Elle imprime alors chaque réponse et le temps qui a été nécessaire à la transmission aller-retour Reportez-vous à l'exemple ci-dessous.

```
$ ping -s pluto
64 bytes from pluto (123.456.78.90): icmp_seq=0. time=3.82 ms
64 bytes from pluto (123.456.78.90): icmp_seq=5. time=0.947 ms
64 bytes from pluto (123.456.78.90): icmp_seq=6. time=0.855 ms
^C
----pluto PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss

round-trip (ms) min/avg/max/sttdev = 0.855/1.87/3.82/1.7
```

Envoi de paquets à des hôtes sur le réseau

Vérifiez la fiabilité des tailles de vos paquets à l'aide de la commande `spray`.

```
$ spray [ -c count -d interval -l packet-size] hostname
```

`-i` *count* — Nombre de paquets à envoyer.

`-d` *interval* — Nombre de microsecondes de la pause entre l'envoi de paquets. Si vous n'utilisez pas de délai, vous pouvez réduire les tampons.

`-l` *packet-size* Taille de paquet.

hostname Système d'envoi de paquets.

Pour plus d'informations sur cette commande, reportez-vous à `spray(1M)`.

EXEMPLE 30–2 Envoi de paquets à des hôtes sur le réseau

L'exemple suivant envoie 100 paquets d'une taille de 2 048 octets (`-l 2048`) à l'hôte `-l 2048`. Les paquets sont envoyés avec un délai de 20 microsecondes entre chaque rafale (`-d 20`).

```
$ spray -c 100 -d 20 -l 2048 pluto
sending 100 packets of length 2048 to pluto ...
no packets dropped by pluto
279 packets/sec, 573043 bytes/sec
```

Capture de paquets sur le réseau

La commande `snoop` permet de capturer des paquets sur le réseau et de suivre les appels entre chaque client et chaque serveur. Cette commande fournit des horodatages précis qui permettent d'isoler rapidement des problèmes liés aux performances du réseau. Pour plus d'informations, reportez-vous à `snoop(1M)`.

```
# snoop
```

Un espace tampon insuffisant ou une CPU surchargée peuvent être à l'origine de l'abandon de paquets.

Vérification de l'état du réseau

Pour afficher les informations sur l'état du réseau, telles que les statistiques sur l'état des interfaces réseau, les tables de routage et divers protocoles, utilisez la commande `netstat`.

```
$ netstat [-i] [-r] [-s]
```

`-i` Affiche l'état des interfaces TCP/IP

`-r` Affiche la table de routage IP

`-s` Affiche les statistiques sur les protocoles `UDP`, `TCP`, `ICMP` et `IGMP`

Pour plus d'informations, reportez-vous à `netstat(1M)`.

Exemples : vérification de l'état du réseau

L'exemple suivant illustre la sortie de la commande `netstat -i`, qui affiche l'état des interfaces utilisées pour le trafic TCP/IP.

```
$ netstat -i
Name  Mtu  Net/Dest    Address      Ipkts  Ierrs Opkts  Oerrs Collis Queue
lo0   8232 software    localhost     1280   0     1280     0       0    0
eri0   1500 loopback    venus      1628480   0   347070    16   39354    0
```

Cet affichage indique le nombre de paquets qu'une machine a transmis et a reçus sur chaque interface. Pour une machine dont le trafic réseau est actif, `Ipkts` et `Opkts` doivent augmenter continuellement.

Pour calculer le taux de collision sur le réseau, divisez le nombre de collisions (`Collis`) par le nombre de paquets sortants (`Opkts`). Dans l'exemple précédent, le taux de collision est de 11 %. À l'échelle du réseau, un taux de collision supérieur à 5 ou 10 % peut indiquer un problème.

Pour calculer le taux d'erreur des paquets entrants, divisez le nombre d'erreurs d'entrée par le nombre total de paquets entrants (`Ierrs/Ipkts`). Le taux d'erreur des paquets sortants correspond au nombre d'erreurs de sortie divisé par le nombre total de paquets sortants (`Oerrs/Opkts`). Lorsque le taux d'erreur d'entrée est élevé (supérieur à 0.25 %), l'hôte risque d'abandonner des paquets.

L'exemple suivant illustre la sortie de la commande `netstat -s`, qui affiche des statistiques pour chacun des protocoles `UDP`, `TCP`, `ICMP` et `IGMP`.

```
UDP
    udpInDatagrams      =196543    udpInErrors         =     0
    udpOutDatagrams     =187820

TCP
    tcpRtoAlgorithm     =     4    tcpRtoMin           =   200
    tcpRtoMax           = 60000    tcpMaxConn          =    -1
    tcpActiveOpens      = 26952    tcpPassiveOpens     =   420
    tcpAttemptFails     =  1133    tcpEstabResets      =     9
    tcpCurrEstab        =    31    tcpOutSegs          =3957636
    tcpOutDataSegs      =2731494   tcpOutDataBytes     =1865269594
    tcpRetransSegs      = 36186    tcpRetransBytes     =3762520
    tcpOutAck           =1225849   tcpOutAckDelayed    =165044
    tcpOutUrg           =     7    tcpOutWinUpdate     =   315
    tcpOutWinProbe      =     0    tcpOutControl       = 56588
    tcpOutRsts          =   803    tcpOutFastRetrans   =   741
    tcpInSegs           =4587678
    tcpInAckSegs        =2087448   tcpInAckBytes       =1865292802
    tcpInDupAck         =109461    tcpInAckUnsent      =     0
    tcpInInorderSegs    =3877639   tcpInInorderBytes   =-598404107
    tcpInUnorderSegs    = 14756    tcpInUnorderBytes   =17985602
    tcpInDupSegs        =    34    tcpInDupBytes       = 32759
    tcpInPartDupSegs    =   212    tcpInPartDupBytes   =134800
    tcpInPastWinSegs    =     0    tcpInPastWinBytes   =     0
    tcpInWinProbe       =   456    tcpInWinUpdate      =     0
```

```
    tcpInClosed         =    99    tcpRttNoUpdate      =  6862
    tcpRttUpdate        =435097    tcpTimRetrans       = 15065
    tcpTimRetransDrop   =    67    tcpTimKeepalive     =   763
    tcpTimKeepaliveProbe=     1    tcpTimKeepaliveDrop =     0

IP
    ipForwarding        =     2    ipDefaultTTL        =   255
    ipInReceives        =11757234  ipInHdrErrors       =     0
    ipInAddrErrors      =     0    ipInCksumErrs       =     0
    ipForwDatagrams     =     0    ipForwProhibits     =     0
    ipInUnknownProtos   =     0    ipInDiscards        =     0
    ipInDelivers        =4784901   ipOutRequests       =4195180
    ipOutDiscards       =     0    ipOutNoRoutes       =     0
    ipReasmTimeout      =    60    ipReasmReqds        =  8723
    ipReasmOKs          =  7565    ipReasmFails        =  1158
    ipReasmDuplicates   =     7    ipReasmPartDups     =     0
    ipFragOKs           = 19938    ipFragFails         =     0
    ipFragCreates       =116953    ipRoutingDiscards   =     0
    tcpInErrs           =     0    udpNoPorts          =6426577
    udpInCksumErrs      =     0    udpInOverflows      =   473
    rawipInOverflows    =     0

ICMP
    icmpInMsgs          =490338    icmpInErrors        =     0
    icmpInCksumErrs     =     0    icmpInUnknowns      =     0
    icmpInDestUnreachs  =   618    icmpInTimeExcds     =   314
    icmpInParmProbs     =     0    icmpInSrcQuenchs    =     0
    icmpInRedirects     =   313    icmpInBadRedirects  =     5
    icmpInEchos         =   477    icmpInEchoReps      =    20
    icmpInTimestamps    =     0    icmpInTimestampReps =     0
    icmpInAddrMasks     =     0    icmpInAddrMaskReps  =     0
    icmpInFragNeeded    =     0    icmpOutMsgs         =   827
    icmpOutDrops        =   103    icmpOutErrors       =     0
    icmpOutDestUnreachs =    94    icmpOutTimeExcds    =   256
    icmpOutParmProbs    =     0    icmpOutSrcQuenchs   =     0
    icmpOutRedirects    =     0    icmpOutEchos        =     0
    icmpOutEchoReps     =   477    icmpOutTimestamps   =     0
    icmpOutTimestampReps=     0    icmpOutAddrMasks    =     0
    icmpOutAddrMaskReps =     0    icmpOutFragNeeded   =     0
    icmpInOverflows     =     0

IGMP:
        0 messages received
        0 messages received with too few bytes
        0 messages received with bad checksum
        0 membership queries received
        0 membership queries received with invalid field(s)
        0 membership reports received
        0 membership reports received with invalid field(s)
        0 membership reports received for groups to which we belong
        0 membership reports sent
```

L'exemple suivant illustre la sortie de la commande `netstat - r`, qui affiche la table de routage IP.

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

```
------------------ -------------------- ----- ----- ------ ---------
localhost          localhost            UH       0   2817  lo0
earth-bb           pluto                U        3  14293  eri0
224.0.0.0          pluto                U        3      0  eri0
default            mars-gate            UG       0  14142
```

Les champs du rapport `netstat - r`sont décrits dans le tableau suivant.

TABLEAU 30–2 Sortie de la commande `netstat - r`

Nom du champ		Description
`Flags`	`U`	La route est active.
	`G`	La route transite par une passerelle.
	`H`	La destination de la route est un hôte.
	`D`	La route a été créée de façon dynamique à l'aide d'une redirection.
`Ref`		Affiche le nombre actuel de routes partageant une couche de liaison.
`Use`		Indique le nombre de paquets envoyés.
`Interface`		Indique l'interface réseau utilisée pour la route.

Affichage des statistiques relatives au client et au serveur NFS

Le service de fichier distribué NFS utilise un utilitaire RPC (Remote Procedure Call, appel de procédure à distance) qui convertit les commandes locales en demandes pour l'hôte distant. Les appels de procédure à distance sont synchrones. L'application cliente est bloquée ou suspendue jusqu'à ce que le serveur termine l'appel et renvoi les résultats. L'un des principaux facteurs ayant une incidence sur les performances NFS est le taux de retransmission.

Si le serveur de fichiers ne peut pas répondre à la demande d'un client, ce dernier retransmet la demande un nombre de fois spécifique avant d'arrêter. Chaque retransmission inflige une surcharge au système et augmente le trafic du réseau. Des retransmissions excessives risquent de provoquer des problèmes de performances. Si la vitesse de retransmission est élevée, vous pouvez effectuer les vérifications suivantes :

- Serveurs saturés qui exécutent les requêtes trop lentement
- Interface Ethernet qui abandonne des paquets
- Congestion du réseau, qui ralentit la transmission des paquets

Le tableau suivant décrit les options `nfsstat` qui permettent d'afficher les statistiques du serveur et du client.

TABLEAU 30–3 Commandes d'affichage des statistiques client/serveur

Commande	Affichage
`nfsstat -c`	Statistiques relatives au client
`nfsstat -s`	Statistiques relatives au serveur
`netstat -m`	Statistiques du réseau pour chaque système de fichiers

Utilisez les commandes `nfsstat -c` et `nfsstat -s` pour afficher les statistiques relatives au client et au serveur, respectivement. Utilisez la commande `netstat -m` pour afficher les statistiques réseau pour chaque système de fichiers. Pour plus d'informations, reportez-vous à `nfsstat(1M)`.

Exemples : affichage des statistiques du client et du serveur NFS

L'exemple suivant affiche les données RPC et NFS pour le client `pluto`.

```
$ nfsstat -c

Client rpc:
Connection oriented:
calls    badcalls  badxids  timeouts newcreds  badverfs   timers
1595799  1511      59       297      0         0          0
cantconn nomem     interrupts
1198      0         7
Connectionless:
calls    badcalls  retrans  badxids  timeouts  newcreds   badverfs
80785    3135      25029    193      9543      0          0
timers   nomem     cantsend
17399    0         0

Client nfs:
calls    badcalls  clgets   cltoomany
1640097  3112      1640097  0
Version 2: (46366 calls)
null     getattr   setattr  root     lookup     readlink  read
0 0%     6589 14%  2202 4%  0 0%     11506 24%  0 0%      7654 16%
wrcache  write     create   remove   rename     link      symlink
0 0%     13297 28% 1081 2%  0 0%     0 0%       0 0%      0 0%
mkdir    rmdir     readdir  statfs
24 0%    0 0%      906 1%   3107 6%
Version 3: (1585571 calls)
null    getattr    setattr  lookup     access     readlink  read
0 0%    508406 32% 10209 0% 263441 16% 400845 25% 3065 0%  117959 7%
write    create     mkdir    symlink    mknod    remove   rmdir
69201 4% 7615 0%    42 0%    16 0%      0 0%     7875 0%  51 0%
rename   link       readdir  readdir+   fsstat   fsinfo   pathconf
929 0%   597 0%     3986 0%  185145 11% 942 0%   300 0%   583 0%
commit
4364 0%

Client nfs_acl:
```

```
Version 2: (3105 calls)
null       getacl     setacl     getattr    access
0 0%       0 0%       0 0%       3105 100%  0 0%
Version 3: (5055 calls)
null       getacl     setacl
0 0%       5055 100%  0 0%
```

La sortie de la commande `nfsstat -c` est décrite dans le tableau suivant.

TABLEAU 30–4 Sortie de la commande `nfsstat -c`

Champ	Description
`calls`	Nombre total d'appels envoyés
`badcalls`	Nombre total d'appels rejetés par RPC
`retrans`	Nombre total de retransmissions. Pour ce client, le nombre de retransmissions est inférieur à 1 %, soit environ 10 délais d'attente sur 6 888 appels. Ces retransmissions peuvent être provoquées par des pannes temporaires. Des taux plus élevés peuvent indiquer un problème.
`badxid`	Nombre de fois qu'un accusé de réception en double a été reçu pour une demande NFS
`timeout`	Nombre d'appels ayant dépassé le délai imparti
`wait`	Nombre de fois qu'un appel a dû attendre, car aucun identificateur client n'était disponible
`newcred`	Nombre de fois que les informations d'authentification ont dû être actualisées
`timers`	Nombre de fois que la valeur d'expiration a été supérieure ou égale à la valeur d'expiration spécifiée pour un appel
`readlink`	Nombre de fois que la commande `read` a été exécutée sur un lien symbolique. Si ce nombre est élevé (supérieur à 10 %), il est possible qu'il y ait trop de liens symboliques.

L'exemple suivant illustre la sortie de la commande `nfsstat -m`.

```
pluto$ nfsstat -m
/usr/man from pluto:/export/svr4/man
Flags: vers=2,proto=udp,auth=unix,hard,intr,dynamic,
        rsize=8192, wsize=8192,retrans=5
 Lookups: srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
 All:     srtt=13 (32ms), dev=10 (50ms), cur=6 (120ms)
```

Cette sortie de la commande `nfsstat -m` (affichée en millisecondes) est décrite dans le tableau suivant.

TABLEAU 30–5 Sortie de la commande `nfsstat -m`

Champ	Description
`srtt`	Moyenne lissée du temps de réponse aller-retour
`dev`	Écarts moyens
`cur`	Temps de réponse actuel attendu

Si vous avez des raisons de croire que les composants matériels du réseau sont à l'origine de problèmes, inspectez les câbles et les connecteurs.

Glossaire

adaptateur de terminal RNIS (TA) Périphérique d'adaptation de signal qui fournit une interface de type modem pour une liaison PPP commutée sur un réseau RNIS. Vous pouvez utiliser les mêmes fichiers de configuration Solaris PPP 4.0 pour configurer un TA RNIS que ceux utilisés pour la configuration d'un modem standard.

agent de répertoire (DA) Agent SLP facultatif qui stocke et gère un cache d'annonces de services qui sont envoyées par l'agent de service (SA). Lorsqu'il est déployé, le DA résout les demandes de service de l'agent utilisateur (UA). Le DA répond aux sollicitations actives du SA et de l'UA relatives aux annonces de répertoire. En conséquence, le SA et l'UA découvrent les DA et les *étendues* associés. Un DA envoie des annonces périodiques non sollicitées par l'intermédiaire desquelles les UA et SA découvrent le DA au sein des étendues partagées.

agent de service (SA) Agent SLP qui tient à jour les annonces de services pour les services en réseau. Si aucun DA n'est disponible, le SA répond aux demandes de service de multidiffusion provenant d'UA. Si un DA n'est pas disponible, le SA enregistre et, éventuellement, annule l'enregistrement de services auprès de DA qui prennent en charge ses étendues.

agent utilisateur (UA) Agent SLP qui agit pour le compte de l'application de l'utilisateur. L'agent demande l'identité des étendues, agents de répertoire et annonces de services correspondants.

annonce de service Informations distribuées par un SA qui décrit un service. Une annonce de service se compose d'une URL et d'un ensemble de paires attribut/valeur qui décrivent un service. Toutes les annonces de services ont une durée de vie. Une fois la durée de vie arrivée à expiration, l'annonce n'est plus valide à moins qu'elle soit enregistrée.

`asppp` Version de PPP qui était fournie avec le système d'exploitation à partir des versions Solaris 2.4 à Solaris 8. La commande `asppp` prenait uniquement en charge les communications PPP asynchrones.

Authentification Opération de vérification de l'identité qui est fournie sur le réseau par un utilisateur ou une entité distant(e), telle qu'un programme. Certains protocoles d'authentification permettent de créer des bases de données d'informations d'authentification appartenant à des utilisateurs potentiels. D'autres protocoles d'authentification utilisent des chaînes de certificats de confiance qui sont générées par une autorité de certification à des fins d'authentification. Ces informations permettent d'authentifier les utilisateurs lorsqu'ils tentent de communiquer avec vous ou d'utiliser votre site de services.

channel service unit (CSU) Périphérique de télécommunication synchrone qui fournit une interface locale à une ligne de télécommunication spécialisée et qui termine cette ligne. Aux États-Unis, une CSU (unité de service du réseau) met fin à une ligne T1 et fournit une interface DS1 ou DSX. À l'échelle internationale, la CSU appartient généralement au fournisseur de services téléphoniques.

Voir également CSU/DSU et data service unit (DSU).

CHAP Challenge-Handshake Authentication Protocol est un protocole d'authentification par défi-réponse qui peut être utilisé pour vérifier l'identité d'un programme appelant sur une liaison PPP. L'authentification CHAP utilise les notions de *défi* et de *réponse*, car la machine qui reçoit un appel lance le défi au programme appelant de prouver son identité.

Voir également protocole PAP (password authentication protocol).

comptabilisation étendue Moyen souple d'enregistrer la consommation des ressources sur la base d'une tâche ou d'un processus.

CSU/DSU Périphérique de télécommunication synchrone qui combine les périphériques CSU et DSU et est utilisé sur une liaison PPP de ligne spécialisée. Le périphérique CSU/DSU convertit les signaux provenant d'un pair en une ligne spécialisée. La plupart de ces périphériques n'ont pas besoin de script de discussion pour établir la liaison et sont souvent configurés par le fournisseur de lignes spécialisées.

Voir également channel service unit (CSU) et data service unit (DSU).

data service unit (DSU) Périphérique de télécommunication synchrone qui est utilisé sur une liaison PPP de ligne spécialisée. La DSU (unité de service des données) convertit les formats d'encadrement de données qui sont utilisés sur les lignes de télécommunication et fournit une interface de communication des données standard.

Voir également channel service unit (CSU) et CSU/DSU.

démon SLP (slpd) Processus démon qui agit comme un DA ou un serveur SA dans l'implémentation Oracle Solaris de SLP. Le service s'effectue sur les annonces de services d'enregistrement d'hôte avec `slpd`, évitant la gestion des annonces individuellement. Chaque processus contient une bibliothèque de client SA qui communique avec `slpd` lorsque le démon est configuré en tant que serveur SA. Le démon SLP transmet tous les enregistrements et annulations d'enregistrement aux DA. Le démon temporise les annonces de services expirées et tient à jour une table des DA disponibles en effectuant une détection DA active et passive. Par l'intermédiaire de ces mécanismes, les informations sur les DA sont fournies aux clients UA. Ces derniers utilisent `slpd` sur un hôte uniquement pour les informations DA. Si vous le souhaitez, vous pouvez configurer le démon `slpd` en tant que DA.

Diffusion Procédure de couche de liaison de données qui est utilisée pour transmettre les paquets à chaque machine sur un sous-réseau. Les paquets de diffusion ne sont généralement pas acheminés au-delà du sous-réseau.

Étendue Regroupement de UA et SA qui sont organisés de manière administrative, topologique, ou autre. Vous pouvez utiliser les étendues pour modifier la façon dont vous allouez l'accès aux services dans l'ensemble de l'entreprise.

expect-send Format de script qui est utilisé dans les scripts de discussion PPP et UUCP. Le script de discussion commence par le texte ou l'instruction *expect* (s'attendre à) à partir du pair distant. La ligne suivante contient la réponse à envoyer (*send*) depuis l'hôte local, après qu'il ait reçu la chaîne expect correcte du pair. Les lignes suivantes répètent les instructions expect-send entre l'hôte local et le pair jusqu'à ce que toutes les instructions qui sont nécessaires pour établir la communication soient négociées avec succès.

liaison PPP commutée Connexion PPP qui implique un pair et un modem d'un des côtés d'une ligne téléphonique ou d'un support de communication similaire, tel qu'un support fourni par RNIS. Le terme “commuté” fait référence à la séquence dans la négociation de liaison lorsque le modem local appelle le pair distant en utilisant le numéro de téléphone du pair. La liaison commutée est la configuration du protocole PPP la plus courante et la moins onéreuse.

liaison PPP de ligne spécialisée Connexion PPP qui implique un hôte et un périphérique CSU/DSU qui sont connectés à un support réseau synchrone provenant d'un fournisseur. OC3 et T1 sont des exemples courants de supports de lignes spécialisées. Bien que plus faciles à administrer, les liaisons de ligne spécialisée sont plus coûteuses que les liaisons PPP commutés et, par conséquent, sont moins fréquentes.

lien En PPP, la connexion des communications qui est négociée et établie entre deux pairs. Solaris PPP 4.0 prend en charge deux types de liaisons : ligne commutée et spécialisée.

machine d'appel sortant Pair qui lance l'appel pour établir une liaison PPP commutée. Une fois configurée, la machine d'appel sortant peut appeler un nombre illimité de serveurs d'appel entrant. La machine d'appel sortant fournit généralement les informations d'authentification permettant l'établissement de la liaison commutée.

Microsoft CHAP (MS-CHAP) Protocole d'authentification propriétaire de Microsoft pour PPP. Solaris PPP 4.0 prend en charge les versions 1 et 2 de ce protocole, en mode client et serveur.

Multidiffusion Procédure de couche réseau qui est utilisée pour envoyer des paquets de datagrammes à plusieurs machines sur un réseau IP. Les paquets ne sont pas gérés par chaque machine, comme c'est le cas avec le routage de diffusion. La multidiffusion exige que les routeurs soient configurés par des protocoles de routage spéciaux.

pair En PPP, un ordinateur individuel situé à l'une des extrémités d'une liaison de communication PPP, qui se compose de deux pairs connectés par des supports de communication. Vous avez la possibilité de configurer de nombreux types de matériel informatique en tant que pair, tel qu'une station de travail, un ordinateur personnel, un routeur ou un mainframe.

PPP asynchrone Forme de protocole PPP qui s'exécute sur des lignes série asynchrones, qui transfèrent les données un caractère à la fois. La forme habituelle de configuration du protocole PPP, la liaison commutée, utilise les communications PPP asynchrones.

PPP synchrone Forme de protocole PPP exécuté sur des lignes numériques synchrones, qui transfèrent les données en tant que flux continu de bits bruts. La liaison PPP de ligne spécialisée utilise le protocole PPP synchrone.

programme appelant de confiance En PPP, pairs distants auxquels un serveur d'appel entrant accorde l'accès en incluant les informations de sécurité des pairs dans la base de données PAP ou des clés secrètes CHAP du serveur.

protocole CBCP (Callback Control Protocol) Extension PPP propriétaire de Microsoft qui est utilisée pour négocier une session de rappel. Solaris PPP 4.0 ne prend en charge que le côté client (programme appelant initial) de ce protocole.

protocole CCP (Compression Control Protocol) Sous-protocole de PPP qui négocie l'utilisation de la compression de données sur la liaison. Contrairement à la compression d'en-têtes, le protocole CCP compresse toutes les données contenues dans les paquets envoyés sur la liaison.

protocole IPV6CP (Internet Protocol Version 6 Control Protocol) Voir protocole PCIP (Internet Protocol Control Protocol).

protocole LCP (link control protocol) Sous-protocole de PPP qui sert à négocier l'ensemble initial de paramètres de liaison entre les pairs. L'une des fonctions du protocole LCP est de tester l'intégrité de la liaison, de sorte que les problèmes liés aux liaisons se manifestent en tant que défaillance LCP.

protocole PAP (password authentication protocol) Protocole d'authentification qui peut être utilisé pour vérifier l'identité d'un programme appelant sur une liaison PPP. PAP utilise un mot de passe en clair qui est transmis par la liaison, ce qui permet de stocker ce mot de passe sur l'une des machines d'extrémité. Par exemple, le protocole PAP peut utiliser les entrées de connexion et de mot de passe de la base de données `passwd` UNIX sur la machine qui reçoit un appel pour vérifier l'identité de l'utilisateur.

Voir également CHAP.

protocole PCIP (Internet Protocol Control Protocol) Sous-protocole de PPP qui négocie les adresses IP des pairs sur la liaison. Il négocie également la compression d'en-têtes pour la liaison et permet l'utilisation des protocoles de couche réseau.

protocole PPP (point-to-point protocol) Protocole de couche de liaison de données qui fournit une méthode standard pour le transfert de datagrammes par le biais d'un support point-à-point. Une configuration du protocole PPP se compose de deux ordinateurs d'extrémité, appelés *pairs*, et de lignes téléphoniques ou d'une autre liaison bidirectionnelle que les pairs utilisent pour la communication. La connexion matérielle et logicielle entre les deux pairs est considérée comme étant la *liaison PPP*.

PPP est composé d'un certain nombre de sous-protocoles, y compris PAP, CHAP, LCP et CCP. De nombreuses implémentations PPP sont disponibles.

protocole PPPoE (PPP over Ethernet) Protocole propriétaire de RedBack Networks qui permet aux hôtes d'exécuter des sessions PPP par le biais d'une liaison Ethernet. Ce protocole est couramment utilisé avec les services DSL (Digital Subscriber Line, ligne d'abonné numérique).

script de discussion Instructions qui indiquent à un modem la façon d'établir une liaison de communication entre lui et un pair distant. Les deux protocoles PPP et UUCP utilisent les scripts de discussion pour établir des liaisons commutées et des procédures de rappel.

Secret CHAP Chaîne ASCII ou binaire qui est utilisée à des fins d'identification et qui est connue par les deux pairs sur une liaison PPP. La clé secrète CHAP (CHAP secret) est stockée sous forme de texte en clair dans le fichier `/etc/ppp/chap-secrets` d'un système, mais n'est jamais transmise sur la liaison PPP, pas même dans un format chiffré. Le protocole CHAP vérifie qu'un hachage de la clé secrète CHAP utilisée par un programme appelant correspond à un hachage de l'entrée secrète CHAP pour le programme appelant dans le fichier `/etc/ppp/chap-secrets` du destinataire.

serveur d'appel entrant Pair qui négocie et établit la réception du destinataire d'une liaison PPP commutée après un appel provenant d'une machine d'appel sortant. Bien que le terme “serveur d'appel entrant” soit d'usage commun, ce serveur ne fonctionne pas selon le paradigme client-serveur. Au lieu de cela, il s'agit simplement du pair qui répond à la requête de configuration d'une liaison commutée. Une fois le serveur d'appel entrant configuré, il peut recevoir des appels provenant d'un nombre illimité de machines d'appel sortant.

service hérité Service en réseau qui ne prend pas en charge le protocole SLP. Vous pouvez créer un enregistrement proxy pour enregistrer un service hérité avec SLP. Les clients SLP peuvent alors découvrir les services hérités (voir le Chapitre 10, “Intégration des services hérités”).

URL de service URL qui est utilisé pour annoncer l'emplacement réseau de services. L'URL contient le type de service, le nom d'hôte ou l'adresse réseau de l'hôte de service. Il peut également contenir un numéro de port et d'autres informations nécessaires pour utiliser le service.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X