Gestion des services Service Location Protocol dans Oracle® Solaris 11.1

Référence : E36527–01
Octobre 2012

ORACLE®

130327@25097

Table des matières

Liste des figures

Liste des tableaux

Liste des exemples

Préface

Le manuel *Gestion des services Service Location Protocol dans Oracle Solaris 11.1* fait partie d'un ensemble de plusieurs volumes couvrant une part importante des informations d'administration du système Oracle Solaris. Ce manuel suppose que vous avez déjà installé le système d'exploitation Oracle Solaris 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.

Utilisateurs de ce manuel

Ce manuel s'adresse aux personnes chargées de l'administration d'un ou de plusieurs systèmes fonctionnant sous Oracle Solaris. 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.

Accès au support technique Oracle

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

Conventions typographiques

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

TABLEAU P–1 Conventions typographiques

Type de caractères	Description	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*.
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
Bash shell, korn shell et bourne shell	`$`
Bash shell, korn shell et bourne shell pour superutilisateur	`#`
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`

◆ ◆ ◆ CHAPITRE 1

1 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 Oracle 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.

- Sollicitation par l'application client des informations nécessaires pour accéder à un service
- 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 le fonctionnement 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 4, “Intégration des services hérités”.

Les applications client s'appuient sur les bibliothèques SLP qui envoient des demandes directement aux agents qui annoncent les services.

Agents et processus SLP

Le tableau suivant décrit les agents SLP.

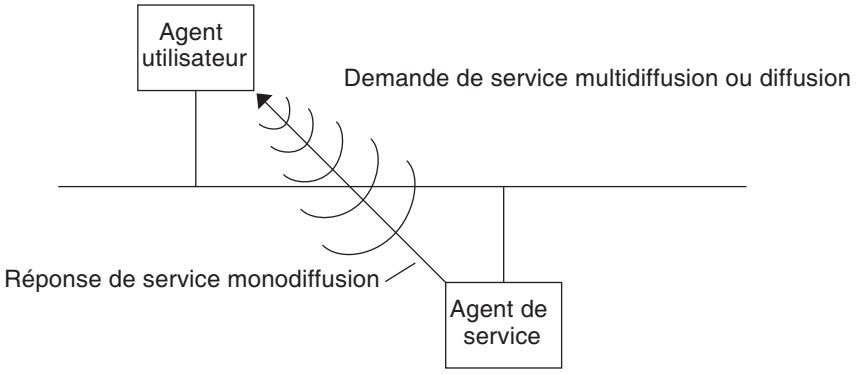
TABLEAU 1–1 Agents SLP

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 oeuvre 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 demandes multidiffusion de service au SA. Ce dernier envoie une réponse monodiffusion à l'UA. Par exemple, lorsque l'UA envoie un message de demande de service, le SA répond avec un message de réponse de service. La réponse de service contient l'emplacement des services qui

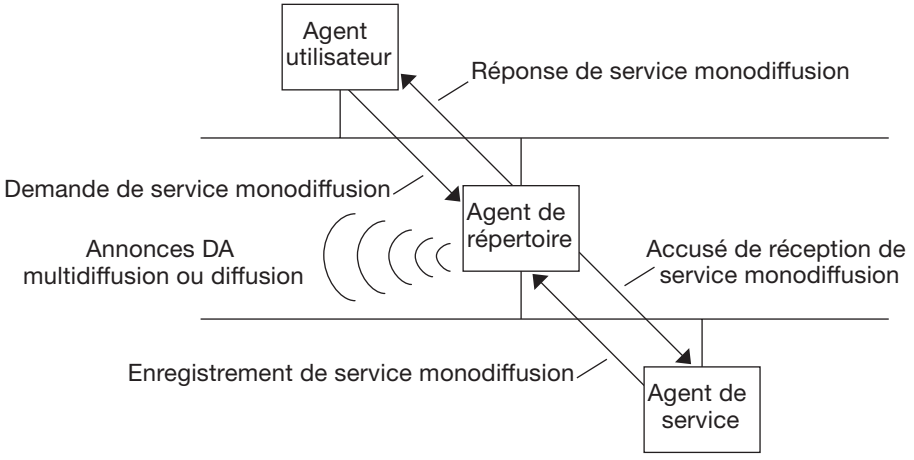
répondent aux besoins du client. D'autres demandes et réponses sont possibles pour les attributs et types de service. Pour plus d'informations, reportez-vous au Chapitre 5, “SLP (références)”.

FIGURE 1–1 Agents et processus SLP de base



La figure ci-dessous montre les agents et processus de base qui mettent en oeuvre l'architecture SLP lorsqu'un DA est déployé dans la structure.

FIGURE 1–2 Agents et processus d'architecture SLP mis en oeuvre 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 demande monodiffusion au DA plutôt que d'envoyer des demandes multidiffusion aux SA.

Pour plus d'informations sur les messages SLP Oracle Solaris, reportez-vous au chapitre Chapitre 5, “SLP (références)”.

Implémentation SLP

Dans une implémentation SLP Oracle Solaris, les SA, UA, DA et serveurs SA SLP, les étendues et autres composants d'architecture décrits dans le Tableau 1–1 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 de répertoire 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 de configurer également `slpd` pour qu'il agisse comme un DA. Reportez-vous au Chapitre 3, “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 :

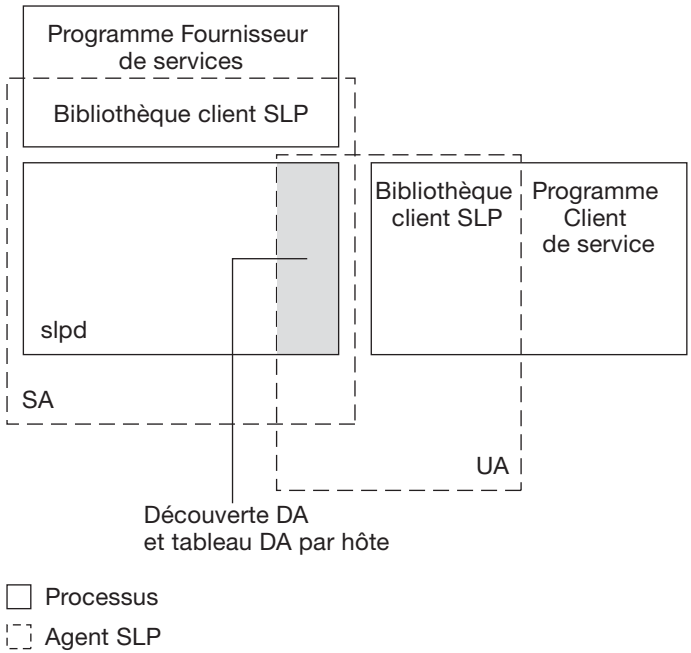
- Logiciel qui offre des services réseau capables d'enregistrer ou annuler l'enregistrement d'annonces de services
- Logiciel client qui peut demander des services en émettant des requêtes d'annonces de services
- Liste des étendues SLP disponibles pour l'enregistrement et les demandes

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 de 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 demandes. La bibliothèque client SLP envoie des demandes multidiffusion aux SA ou des demandes 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 3, “Administration de SLP (tâches)”. Le processus `slpd` gère toutes les fonctionnalités SA, telles que la réponse aux demandes multidiffusion et l'enregistrement avec les DA.

FIGURE 1–3 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 2

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.

Eléments 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`, qui est placé dans le répertoire `/etc/inet`. Si vous souhaitez modifier les paramètres par défaut de la propriété, reportez-vous au Chapitre 3, "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 médias 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 qu'administrateur.

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

2 Exécutez snoop avec l'argument de ligne de commande slp.

```
Brief Mode:
# snoop slp
```

Lorsque vous exécutez snoop en mode *brief* (bref), le mode 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 *verbose* (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* en mode par défaut en tant que 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 demande 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 demande, 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 l'hôte *slphost2* répondant à l'hôte *slphost1* `SrvReg` avec un accusé de réception de service (`SrvAck`) indiquant 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`) indiquant 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.

Etape 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 3, “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 5, “SLP (références)”.

◆ ◆ ◆ CHAPITRE 3

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 3–1 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 à la documentation suivante : 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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 de manière appropriée les paramètres de la propriété dans le fichier `/etc/inet/slp.conf`.**

   Reportez-vous à la section "Propriétés de configuration" à la page 28 pour obtenir des informations générales sur les paramètres de propriétés SLP. Reportez-vous aux sections qui suivent cette procédure pour consulter des exemples de situations dans lesquelles vous pouvez être amené à 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 3–1 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 demandes 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 3–2 Propriétés de synchronisation d'annonces DA et de demandes de découverte

Propriétés	Description
`net.slp.passiveDADetection`	Booléen spécifiant si `slpd` est à l'écoute des annonces DA non sollicitées
`net.slp.DAActiveDiscoveryInterval`	Valeur spécifiant la fréquence à laquelle `slpd` effectue la découverte DA active pour un nouveau DA

TABLEAU 3–2 Propriétés de synchronisation d'annonces DA et de demandes de découverte *(Suite)*

Propriétés	Description
`net.slp.DAHeartBeat`	Valeur spécifiant 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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` pour 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 demandes 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 31.

▼ 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 qu'administrateur.**

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

value 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*

value 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 que 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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
   ```

Elimination 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 32. 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 31.

Adaptation d'autres médias 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 3–3 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 demandes de l'UA commencent à expirer et sont abandonnées. L'expiration des demandes 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 5, “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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section “Utilisation de vos droits d’administration” du manuel *Administration d’Oracle Solaris 11.1 : Services de sécurité*.

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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

   value 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 demandes 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 demandes 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

   value 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 propriété `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 55 pour plus d'informations sur le déploiement des DA sur des hôtes multiréseau.

▼ Configuration du routage de diffusion

Utilisez la procédure suivante pour modifier la propriété `net.slp.isBroadcastOnly` sur `True`.

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

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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 demandes de découverte SLP

Deux situations peuvent exiger que vous modifiiez les délais d'attente pour les demandes 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 demande ou un enregistrement. A 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 demandes 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 demandes SLP échouent en raison des délais d'attente des demandes 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 3–4 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 demandes 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

   value 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 demandes 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*

   value Liste de nombres entiers de 32 bits qui spécifient les délais d'attente, en millisecondes, pour la mise en oeuvre 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 demandes 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 qu'administrateur.

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

value 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*

value Liste de nombres entiers de 32 bits qui spécifient les délais d'attente, en millisecondes, pour la mise en oeuvre 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 demandes SLP.

6 Enregistrez les modifications et fermez le fichier.

7 Redémarrez `slpd` pour activer vos modifications.

```
# svcadm enable network/slp
```

Etendues 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 Oracle 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 32. 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`.

Eléments à prendre en compte lors de la configuration d'étendues

Lorsque vous modifiez la propriété `net.slp.useScopes` dans le 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 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 qu'administrateur.

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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 demandes, 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 demandes de service multidiffusion. Les demandes de multidiffusion dans les étendues qui ne sont pas prises en charge par le DA sont cependant toujours directement traitées par le SA.

Les demandes 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 demandes 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 demandes 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 demande à un DA appelé `DA1` et que le SA possède des services enregistrés avec `DA2`, l'UA ne parviendra pas 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 39.

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 Oracle 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 demandes 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 qu'administrateur.

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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 51.

- 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 demandes 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 demandes. 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 demandes UA envoyées à un DA expirent ou sont renvoyées avec l'erreur `DA_BUSY_NOW`.
- Le journal DA indique que de nombreuses demandes 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 demandes UA reviennent avec l'erreur `DA_BUSY_NOW`. Si le nombre de demandes 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 demandes 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 désactivés entre les interfaces.

Généralement, la raison pour laquelle le routage multidiffusion est désactivé entre des interfaces est 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 3–5 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 demandes SLP de monodiffusion et multidiffusion/diffusion sur les interfaces spécifiées.	"Configuration de la propriété `net.slp.interfaces` " à la page 53
Organisation des annonces de services proxy afin que les UA sur les sous-réseaux obtiennent des URL de services avec des adresses accessibles	Limitez l'annonce de proxy à une machine qui exécute `slpd` connecté à un seul sous-réseau plutôt qu'à un hôte multiréseau.	"Annonce de proxy sur les hôtes multiréseau" à la page 54
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 55

Configuration de la propriété net.slp.interfaces

Lorsque la propriété `net.slp.interfaces` est définie, `slpd` écoute les demandes 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 demande 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 demande 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 demandes 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 demandes 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 55.

▼ 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 qu'administrateur.**

   Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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*

   value 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 portant 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 demandes 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 demande 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 appelée `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.

Eléments 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 4

Intégration des services hérités

Les services hérités sont les services réseau qui précèdent le développement et la mise en oeuvre de SLP. Les services tels que le service NFS et le service de noms 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.
- Ecrire 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

Oracle 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 qu'administrateur.**

Pour plus d'informations, reportez-vous à la section "Utilisation de vos droits d'administration" du manuel *Administration d'Oracle Solaris 11.1 : Services de sécurité*.

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 4–1 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.
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.

TABLEAU 4–1 Description du fichier d'enregistrement de proxy SLP *(Suite)*

Numéros de ligne	Description
4	Désignation de l'étendue. La ligne facultative se compose du jeton `scope`, suivi d'un signe égal 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. Lorsqu'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 5

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 demande est reçue (code 0) ou que le récepteur est occupé.

Remarque – Le démon SLP (`slpd`) renvoie des codes d'état pour les messages de monodiffusion uniquement.

Codes d'état SLP

TABLEAU 5–1 Codes d'état SLP

Type d'état	Code d'état	Description
aucune erreur	0	La demande a été traitée sans erreur.
LANGUAGE_NOT_SUPPORTED	1	Pour une demande 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 demande.
AUTHENTICATION_UNKNOWN	5	Le DA ou le SA a reçu une demande pour une SPI SLP non prise en charge.

TABLEAU 5–1 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 reçues.
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 demande 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 5–2 Types de message SLP

Type de message	Abréviation	Code de fonction	Description
Demande de service	`SrvRqst`	1	Emise 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 demande 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 5–2 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 demande de service d'un SA ou à un message d'annulation d'un enregistrement de service.
Demande 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 demandes de service de multidiffusion.
Demande 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 demande 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.

Index

R

S

T

U