



Guide d'administration de Solaris for ISPs

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303
U.S.A.

Référence : 805-5393
Novembre 1998

Copyright 1998 Sun Microsystems, Inc. 901 San Antonio Road, Palo Alto, Californie 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées du système Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd. Parties Copyright 1993, 1994 Washington Université de Saint Louis. Tous droits réservés. Parties Copyright 1985, 1988, 1990 Regents de l'Université de Californie. Tous droits réservés.

Sun, Sun Microsystems, le logo Sun, SunSoft, SunDocs, SunExpress, HotJava, Java, Java Development Kit, JDK, SunScreen SKIP, Sun WebServer, Ultra, Solaris for ISPs, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc. Netscape et Netscape Navigator sont marques de Netscape Communications Corporation.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

CETTE PUBLICATION EST FOURNIE TELLE QUELLE ET AUCUNE GARANTIE, EXPRESSE OU IMPLICITE, N'EST ACCORDÉE, Y COMPRIS DES GARANTIES CONCERNANT LA VALEUR MARCHANDE, L'APTITUDE DE LA PUBLICATION A RÉPONDRE A UNE UTILISATION PARTICULIÈRE, OU LE FAIT QU'ELLE NE SOIT PAS CONTREFAISANTE DE PRODUIT DE TIERS. CE DENI DE GARANTIE NE S'APPLIQUERAIT PAS, DANS LA MESURE OU IL SERAIT TENU JURIDIQUEMENT POUR NUL ET NON AVENU.



Sommaire

Préface xi

1. Présentation de Solaris for ISPs 1

Architecture de Solaris for ISPs 1

Extensions de plate-forme Solaris for ISPs 2

Sun Internet Administrator 2

Logiciel de configuration d'hôte 3

Sun Internet Services Monitor 3

Sun Directory Services 4

Sunscreen SKIP 5

Serveur de licence FlexLM 5

Navigateur HotJava 5

Kit de développement Java 6

Services ISP 6

SWS 7

Sun Internet News Server 7

Sun Internet FTP Server 8

Installation de Solaris for ISPs 8

Modèle de configuration hôte 9

Configuration répétable 10

Gestion de services avec Sun Internet Administrator	10
Fonctions pour un environnement sécurisé	10
Architecture d'application trois couches	11
Architecture d'application deux couches	13
2. Planification de l'installation	15
Le processus d'installation	15
Présentation du processus d'installation	16
Planification de l'installation	18
Préparation d'installation	20
Installation de Solaris for ISPs	22
Configuration de Sun Directory Services	23
Configuration de Sun Internet Administrator	24
Tâches de post-installation	25
3. Recommandations pour l'installation	27
Scénario d'installation	27
Configuration réseau	27
Problèmes de sécurité	30
Risques pour la sécurité Internet standard	30
Risques relatifs à la sécurité dans Solaris for ISPs	31
Comment renforcer la sécurité?	32
Eléments à prendre en compte	32
Modifications dans Solaris	33
Gestion de fichier journal	39
Création de scripts définis par l'utilisateur	40
Restauration des paramètres AWS par défaut	41
4. Configuration requise	43
Prérequis d'installation	43
Configuration minimale du système d'exploitation	44

Configuration matérielle minimale	46
Navigateur Web supporté	47
Dépendance des composants	47
5. Utilisation des services de répertoire	49
Structure de répertoires Solaris for ISPs	50
Structure d'arborescence OSI	50
Structure arborescente DC	52
Création d'entrées de répertoire depuis la ligne de commande	53
Création d'entrées de répertoire : Procédure générale	53
Structure d'un fichier ldif(4)	54
Création d'entrées de domaine	55
Création d'entrées d'abonné	57
Création d'entrées de groupe	62
Contrôle d'accès Solaris for ISPs	63
Règles d'activation des fonctionnalités de Sun Internet Administrator	63
Règles activant les fonctionnalités de service	64
Règles d'activation de l'accès utilisateur approprié	64
6. Schéma des services de répertoire Solaris for ISPs	65
Maintenance du schéma	65
Que faut-il sauvegarder?	66
Restauration du schéma	66
▼ Restauration du schéma Solaris for ISPs	67
Classes d'objet Solaris for ISPs	68
Classe ispAdministrator	68
Classe ispManagedService	70
Classe ispService	71
Classe ispSubscriber	74

Attributs Solaris for ISPs 75

Attribut associatedDomain	76
Attribut associatedName	76
Attribut commonName	76
Attribut description	77
Attribut gidNumber	77
Attribut homeDirectory	77
Attribut host	77
Attribut ispAdministeredService	77
Attribut ispAuthorizedServices	77
Attribut ispCategory	78
Attribut ispContentDirectory	78
Attribut ispDirectoryRoot	78
Attribut ispImageFile	78
Attribut ispPrivateData	79
Attribut ispServiceContext	79
Attribut ispServiceLocation	79
Attribut ispServlets	79
Attribut ispServletClasspath	80
Attribut ispParameterizedOperation	80
Attribut ispSupplementaryInformation	80
Attribut ispSupportedOperation	80
Attribut ispVersion	81
Attribut labeledURI	81
Attribut mail	81
Attribut objectClass	81
Attribut ou	81
Attribut surname	82

Attribut uidNumber 82

Attribut userCertificate 82

Attribut userid 82

Attribut userPassword 82

7. Intégration d'applications de service existantes 83

Généralités concernant l'intégration d'un service existant 83

Intégration des services X 84

Intégration de programmes de ligne de commande 85

Intégration d'applications Web deux couches 86

Enregistrement d'informations pour une application Web à deux couches 87

Configuration pour coordination des comptes d'administrateur 88

Index 91

Figures

Figure 1–1	Architecture de base de Solaris for ISPs	1
Figure 1–2	Processus de configuration d'hôte de Solaris for ISPs	9
Figure 1–3	Architecture de service ISP trois couches	12
Figure 1–4	Architecture de service ISP deux couches	13
Figure 2–1	Processus d'installation	16
Figure 2–2	Planification de l'installation	18
Figure 2–3	Préparation de l'installation	20
Figure 2–4	Installation de Solaris for ISPs	22
Figure 2–5	Configuration de Sun Directory Services	23
Figure 2–6	Configuration de Sun Internet Administrator	24
Figure 2–7	Tâches de post-installation	25
Figure 3–1	Configuration de base	28
Figure 3–2	Configuration étendue	29
Figure 5–1	Arborescence OSI de Solaris for ISPs	50
Figure 5–2	Entrées d'arborescence OSI	51
Figure 5–3	Structure de domaine dans l'arborescence OSI	52
Figure 5–4	Arborescence DC de Solaris for ISPs	52
Figure 5–5	Arborescence de répertoire avec un domaine ajouté	57

Préface

Le Guide d'administration de Solaris for ISPs présente des informations sur les extensions de plate-forme et les services Solaris™ for ISPs™. Il aborde une grande variété de sujets, fournissant une présentation générale du logiciel et examinant le schéma des services de répertoire, les besoins de pré-installation et les scripts de post-installation.

A qui s'adresse ce manuel?

Ce manuel est destiné aux administrateurs système, aux personnes chargées de la maintenance de systèmes informatiques multi-utilisateurs ou de réseaux, et à tous ceux amenés à ajouter et configurer de nouvelles stations de travail, définir des comptes utilisateur et installer des logiciels à l'échelle d'un système.

Structure de ce manuel

Ce manuel contient les chapitres suivants :

Le chapitre 1, "Présentation de Solaris for ISPs", présente les caractéristiques des extensions de plate-forme et les services Solaris for ISPs.

Le chapitre 2, "Planification de l'installation", étudie les diverses étapes d'installation des extensions de plate-forme et des services Solaris for ISPs.

Le chapitre 3, "Recommandations pour l'installation", présente les directives de configuration d'hôte pour l'installation des extensions de plate-forme et des services Solaris for ISPs.

Le chapitre 4, "Configuration requise", précise la configuration minimale du serveur pour l'installation des extensions de plate-forme et des services Solaris for ISPs.

Le chapitre 5, "Utilisation des services de répertoire", décrit la structure de répertoire requise et la création d'entrées dans le répertoire depuis la ligne de commande.

Le chapitre 6, "Schéma des services de répertoire Solaris for ISPs", constitue un matériel de référence sur les classes et attributs d'objets ajoutés au schéma Sun™ Directory Services.

Le chapitre 7, "Intégration d'applications de service existantes", étudie les besoins pour l'intégration d'applications de service existantes avec Sun™ Internet Administrator™.

Manuels Solaris™ for ISPs™ complémentaires

La documentation associée à Solaris for ISPs inclut des manuels imprimés, des AnswerBooks et des pages de manuel. Ces éléments de documentation sont présentés ci-dessous.

Manuels

Les documents indiqués ici sont fournis en version papier dans la version anglaise du produit. Ces manuels sont également disponibles sous forme d'AnswerBooks™ et de fichiers d'aide en ligne sur le CD.

- *Solaris for ISPs Administration Guide*, référence # 805-4874
- *Solaris for ISPs Installation Guide*, référence # 805-4875
- *Solaris for ISPs Command Reference*, référence # 805-4876

AnswerBook

Ces documents sont fournis sous forme d'AnswerBook™ sur le CD.

- *Guide d'administration de Solaris for ISPs*, référence # 805-5032
- *Guide d'installation de Solaris for ISPs*, référence # 805-5075

- *Sun Directory Services 3.1 Administration Guide*
- *Sun Directory Services 3.1 User's Guide*

Ces documents sont fournis en version française sous forme d'AnswerBook™ sur l'Internet à l'adresse suivante : <http://docs.sun.com>

- *Guide d'administration de Solaris for ISPs*, référence # 805-5963-10
- *Guide d'installation de Solaris for ISPs*, référence # 805-5393-10

Pages de manuel

Chaque page de manuel, "man" page, aborde un sujet tel qu'une commande utilisateur ou une fonction de bibliothèque.

L'emplacement des pages de manuel des extensions de plate-forme et des services Solaris for ISPs est indiqué ci-dessous :

- Les pages de manuel JDK 1.1.5™ se trouvent dans `/usr/share/man`.
- Les pages de manuel FLEXLm se trouvent dans `/opt/SUNWste/license_tools/man`.
- Les pages de manuel de la console de Sun™ Internet Administrator™ se trouvent dans `/opt/SUNWixamc/man`.
- Les pages de manuel Sun™ Directory Services se trouvent dans `/opt/SUNWconn/man`.
- Les pages de manuel de Sunscreen™ SKIP se trouvent dans `/opt/SUNWicg/man`.
- Les pages de manuel de configuration d'hôte se trouvent dans `/opt/SUNWisp/man`.
- Les pages de manuel de Sun™ Internet FTP Server™ se trouvent dans `/opt/SUNWixfta/1.0/man`.
- Les pages de manuel de Sun™ Internet News Server™ se trouvent dans `/opt/SUNWsns/man`.
- Les pages de manuel de Sun™ WebServer™ (SWS) se trouvent dans `/usr/share/man`.

Le fichier README

Le fichier `README.1st` de Solaris for ISPs est un petit fichier sur le CD du produit contenant les toutes dernières informations, les erreurs, les informations de diffusion et divers pointeurs vers des fichiers `readme` et documents du logiciel relatifs à l'installation.

Autres documents complémentaires

Vous pouvez également consulter les manuels suivants complétant les informations fournies dans ce manuel.

- *Automating Solaris Installations (A Custom JumpStart Guide)*, par Paul Anthony Kasper and Alan L. McClellan, SunSoft Press, 1995.
- *Solaris Advanced Installation Guide*, référence # 802-5740-10.

Sites Web associés

Vous pouvez consulter les sites Web suivants pour obtenir des informations sur les sujets abordés dans ce manuel.

- <http://access1.sun.com/Products/ISP/> pour les patches (logiciels) requis et recommandés.
- <http://skip.incog.com/spec/SKIP.html> pour la documentation SKIP.
- <http://www.javasoft.com/products/jdk/1.1/index115.html> pour la documentation de la trousse d'outils JDK 1.1.5.
- http://www.nai.com/default_pgp.asp pour les informations PGP.
- <http://www.isc.org/> pour une référence sur la mise en oeuvre des principaux protocoles Internet.
- http://www.sun.com/servers/ultra_enterprise/sw/webstart/ pour l'installation de JumpStart.
- <http://sunsolve1.sun.com/> pour des patches (logiciels) publics.

Commande de documents Sun

Le programme SunDocsSM fournit plus de 250 manuels produits par Sun Microsystems, Inc. Si vous vivez aux États-Unis, au Canada, en Europe ou au Japon, vous pouvez acheter des jeux de documentation ou des manuels individuels au moyen de ce programme.

Pour obtenir une liste des documents et la procédure permettant de les commander, reportez-vous à la section du catalogue de SunExpressTM à l'adresse Web <http://www.sun.com/sunexpress>.

Définitions des polices de caractères

Le tableau suivant présente la typographie utilisée dans ce manuel.

Police de caractère ou symbole	Signification	Exemple
AaBbCc123	Les noms de commande, de fichier et de répertoire.	Editez votre fichier <code>.login</code> . Utilisez <code>ls -a</code> pour afficher la liste de tous les fichiers.
AaBbCc123	Espace réservé de ligne de commande : à remplacer par un nom ou une valeur réelle.	Pour supprimer un fichier, tapez <code>rm nomfichier</code> .
AaBbCc123	Titres de manuel, nouvelles expressions ou nouvelle terminologie, ou mots à mettre en évidence.	Lisez le chapitre 6 dans le <i>User's Guide</i> . Il s'agit d'options de <i>classe</i> . Vous <i>devez</i> être un utilisateur racine pour effectuer cette intervention.

Présentation de Solaris for ISPs

Bienvenue dans Solaris™ for ISPs™. Ce produit Solaris repose sur l'architecture ouverte et la dimensionnabilité du système d'exploitation Solaris pour fournir un environnement d'exploitation optimal aux fournisseurs de service Internet et à leurs clients.

Architecture de Solaris for ISPs

Solaris for ISPs est structuré en deux groupes de logiciels. Le logiciel de plate-forme étend la base Solaris, en ajoutant des fonctions qui activent des services ISP, mais qui ne sont pas directement accessibles par les abonnés des ISP. Les services ISP fournissent aux abonnés des fonctionnalités telles que les groupes de discussion Internet (News), FTP et l'accès Web, tout en tirant parti de l'environnement Solaris étendu.

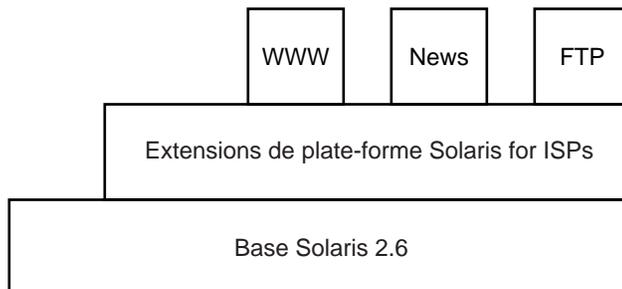


Figure 1-1 Architecture de base de Solaris for ISPs

Extensions de plate-forme Solaris for ISPs

Solaris for ISPs apporte les améliorations suivantes au système d'exploitation Solaris :

- Sun™ Internet Administrator™
- Logiciel de configuration d'hôte
- Sun™ Internet Services Monitor™
- Sun™ Directory Services
- Sunscreen™ SKIP
- Serveur de licence FlexLM
- Navigateur HotJava™
- Kit de développement Java

Sun Internet Administrator

Sun Internet Administrator assure une gestion centrale sécurisée pour les services ISP répartis. Il offre aux administrateurs ISP les fonctions suivantes :

- *Ouverture de session unique pour les administrateurs.* Les administrateurs ISP se connectent à Sun Internet Administrator une seule fois pour accéder à toutes les fonctions pour lesquelles il ont une autorisation. Les services développés conformément aux directives des ISP et gérés depuis Sun Internet Administrator reçoivent des informations d'ouverture de session de celui-ci ; l'utilisateur n'est plus sollicité par la suite.
- *Communications sécurisées entre machines client de l'administrateur et hôtes de service distants.* Le logiciel SKIP en option peut être installé et configuré sur toutes les connexions à la console, et de la console aux machines hôtes de service, mettant ces communications à l'abri des intrusions.
- *Enregistrement des actions d'administrateur pour traçabilité.* Chaque action administrateur, de la tentative de connexion initiale à la déconnexion, est enregistrée par l'intermédiaire de l'utilitaire `syslog`. Cette fonction fournit des informations de dépannage et de comptabilisation.
- *Gestion à distance de services ISP existants.* Les composants de service fournis avec Solaris for ISPs peuvent être gérés depuis Sun Internet Administrator, quelle que soit leur position sur le réseau. En outre, Sun™ Internet FTP Server™ et Sun™ Internet News Server™ sont des composants à trois couches et bénéficient de tous les avantages de sécurité intégrés dans Sun Internet Administrator. Pour plus

d'informations sur l'interaction des services avec Sun Internet Administrator, reportez-vous à "Gestion de services avec Sun Internet Administrator" , page 10.

- *Extensibilité pour services existants.* Les ISP peuvent intégrer leurs propres applications dans Sun Internet Administrator et les gérer de la même manière que les services fournis avec Solaris for ISPs. Pour consulter des instructions sur l'intégration d'applications dans Sun Internet Administrator, reportez-vous au Chapitre 7.

Logiciel de configuration d'hôte

Le logiciel de configuration d'hôte Solaris for ISPs offre les fonctionnalités suivantes :

- *Installation du logiciel.* Les administrateurs installent et désinstallent tout le logiciel Solaris for ISPs à l'aide du logiciel de configuration d'hôte. Les administrateurs peuvent enregistrer des scénarios d'installation en vue d'une utilisation dans le script final JumpStart pour répéter les installations automatiquement.
- *Configuration de base Solaris.* Pour améliorer la sécurité et économiser les ressources, les services Solaris non requis sont désactivés. Les composants associés à la sécurité de Solaris sont adaptés à un environnement ISP.
- *Détection d'intrusion.* De façon périodique, le détecteur d'intrusion vérifie son fichier journal, déterminant si des tentatives de connexion ayant échoué se sont produites depuis la dernière vérification. Si une tentative d'intrusion s'est produite, le détecteur collecte les données consignées et les passe au mécanisme de notification spécifié par l'utilisateur, tel que courrier électronique.
- *Gestion de processus de serveur.* Ce travail `cron` garantit l'exécution effective des processus du serveur (tels que les serveurs de groupes de discussion). Si un serveur s'est arrêté prématurément, le gestionnaire de processus de serveur démarre ce serveur.
- *Gestion de fichier journal.* Des journaux d'audit et système sont recyclés quotidiennement. Le démon de gestion de fichier journal archive les journaux toutes les semaines et supprime les archives datant de plus d'un mois.

Le logiciel de configuration d'hôte est un composant logiciel obligatoire. Il est installé sur chaque machine hôte Solaris for ISPs.

Sun Internet Services Monitor

Le logiciel de surveillance de performances permet à un ISP de configurer des machines client spéciales émulant une expérience d'abonné avec les services ISP. L'applet de surveillance des performances peut être configuré pour se connecter à n'importe quel serveur de services Web, messagerie, groupe de discussion et répertoire, et recueillir des informations sur leurs performances dans une perspective

d'abonné. Les données sont recueillies sur la machine hôte surveillante et consultables au moyen d'un navigateur Web.

Sun Internet Services Monitor est une application deux couches. Elle est gérable par l'intermédiaire de Sun Internet Administrator, mais ne tire pas parti des avantages de l'ouverture de session unique ou de l'authentification de l'administrateur. Pour plus d'informations sur l'architecture deux couches, consultez "Gestion de services avec Sun Internet Administrator", page 10.

Sun Directory Services

Cette mise en oeuvre LDAP (Lightweight Directory Access Protocol) fournit un référentiel partagé pour l'utilisateur (administrateur) et des informations de configuration de service. Les administrateurs stockent également des informations d'abonné dans le référentiel. Les fonctions de cette version de Sun Directory Services incluent notamment :

- Conformité aux normes Internet LDAP v3.
- Un serveur RADIUS (Remote Access Dialup User Service) fournissant une authentification pour des utilisateurs distants se connectant au réseau par l'intermédiaire d'un serveur d'accès réseau (NAS, Network Access Server).
- Un serveur NIS (Network Information System) s'intégrant dans un environnement NIS existant pour fournir un service de noms intégré.
- Une suite complète d'outils d'administration, incluant l'éditeur de répertoire Deja, une console d'administration à implémentation Java, pour la gestion du répertoire, et une passerelle Web permettant un accès depuis n'importe quel navigateur.

Sun Directory Services est gérable depuis Sun Internet Administrator comme application X.

Sun Directory Services s'installe avec une restriction en l'absence de licence de 1K (mille) entrées dans le répertoire. Un certificat de licence pour 5K (cinq mille) entrées est fourni avec Solaris for ISPs et doit être racheté et enregistré avec le serveur de licence FlexLM avant d'entrer en vigueur. Consultez les instructions du manuel *Guide d'installation de Solaris for ISPs* pour plus de détails sur le rachat et l'installation du certificat de licence.

Consultez le Chapitre 5 et le Chapitre 6 du présent manuel pour obtenir des informations sur le rôle de Sun Directory Services dans Solaris for ISPs. La documentation Sun Directory Services est composée de deux manuels, *Sun Directory Services 3.1 Administration Guide* et *Sun Directory Services 3.1 User's Guide*, tous deux livrés comme progiciels AnswerBook2™. L'outil Sun Directory Services Deja comporte également une aide en ligne complète.

Sunscreen SKIP

Sunscreen™ SKIP est basé sur la norme SKIP (Simple Key-management for Internet Protocols) de gestion de clé pour cryptage IP. Les caractéristiques de SKIP incluent notamment :

- Des échanges de certificat automatiques
- Des protocoles sans session
- Des protocoles de paquet multidestinataire et monodestinataire pour IPv4 et IPv6
- Un protocole de découverte de certificat (CDP)

La technologie SKIP complète est disponible uniquement en Amérique du Nord, mais une version existe pour l'exportation vers d'autres parties du monde. Lorsque SKIP est installé, ses pages manuelles se trouvent dans le répertoire `/opt/SUNWicp/man`.

Serveur de licence FlexLM

Le serveur de licence FlexLM est utilisé par Sun Directory Services pour gérer les licences de diverses tailles. Si votre réseau comporte déjà un serveur de licence (version 4.1 ou version ultérieure), vous pouvez l'utiliser pour servir des licences Sun Directory Services.

Sun Directory Services autorise 1K (mille) entrées avant de nécessiter une licence. Cela est suffisant pour installer et initialiser le répertoire. Cependant, dans n'importe quelle application ISP raisonnable, un nombre plus grand d'entrées sera rapidement requis. Suivez les instructions du manuel *Guide d'installation de Solaris for ISPs* pour acquérir une clé de licence et configurer le serveur.

Après son installation, les pages de manuel FlexLM se trouvent dans `/opt/SUNWste/licene_tools/man`.

Navigateur HotJava

Le navigateur HotJava est fourni avec Solaris for ISPs pour supporter Sun Internet Administrator et d'autres interfaces utilisateur d'administration dans le produit. Il prend en charge les normes et protocoles Internet suivants :

- Kit de développement Java 1.1.6
- Protocole HTTP 1.1
- HTML 3.2
- Tableaux et cadres
- Cookies persistants
- Formats de support GIF et JPEG

- Format audio AU
- Protocoles de transfert de fichier FTP et Gopher
- Protocoles de courrier électronique SMTP MIME
- Protocole SOCKS
- Secure Sockets Layer (SSL) 3.0
- Format d'archive Java (JAR)

Kit de développement Java

Le kit de développement Java (JDK) est fourni avec Solaris for ISPs pour supporter l'utilisation de Java dans le produit. JDK version 1.1.5 inclut les nouvelles possibilités suivantes :

- Internationalisation
- Applets signés
- Format de fichier JAR
- Améliorations AWT (boîte à outils de fenêtre)
- Modèle de composant JavaBeans™
- Améliorations réseau
- Progiciel mathématique pour grands nombres
- Invocation de méthode distante (RMI)
- Réflexion
- Connectivité aux bases de données (JDBC)

Services ISP

Les services de cette version de Solaris for ISPs incluent notamment :

- Sun™ WebServer™ (SWS)
- Sun™ Internet News Server™
- Sun™ Internet FTP Server™

Outre les interfaces utilisateur graphiques, tous les services ISP fournissent également un accès par ligne de commande pour l'écriture de scripts.

SWS

SWS est un serveur Web très fiable, sécurisé, répondant aux normes, pour accéder aux informations, les gérer et les distribuer sur l'Internet, des extranets ou des intranets. Les fonctions ajoutées à cette version de SWS incluent notamment :

- *Support pour HTTP/1.1.* SWS supporte la dernière version du protocole de transfert hypertexte, notamment les hôtes virtuels nommés et leur négociation de contenu.
- *Dimensionnabilité améliorée.* Plusieurs instances du processus de serveur peuvent s'exécuter sur une machine spécifique et peuvent être gérées par l'intermédiaire de la même interface utilisateur graphique d'administration. Le nombre d'hôtes virtuels disponibles est ainsi augmenté géométriquement.
- *Support de servlet Java.* L'utilisation de servlets à la place de scripts CGI plus fréquemment employés permet de bénéficier des avantages inter-plate-formes de Java côté serveur, tout en améliorant la vitesse de traitement.
- *Communications HTTP sécurisées.* SWS inclut une fonctionnalité SSL (secure-socket layer) et supporte les certificats Verisign pour des communications sûres et cryptées.
- *Support de Microsoft FrontPage.* SWS supporte les extensions FrontPage dans les secteurs de la création, de l'administration et du contenu dynamique.

SWS est une application deux couches. Il est gérable par l'intermédiaire Sun Internet Administrator, mais ne bénéficie pas de l'ouverture de session unique. Il a été configuré pour partager des données d'administrateur avec Sun Internet Administrator. Reportez-vous au Chapitre 7 pour obtenir plus de détails sur cette configuration et au "Gestion de services avec Sun Internet Administrator", page 10 pour plus d'informations sur l'architecture deux couches.

Sun Internet News Server

Sun Internet News Server est un serveur de groupes de discussion hautes performances et dimensionnable. Les principales fonctions incluent :

- *Hautes performances et dimensionnabilité de connexion client.* Un démon à unités d'exécution multiples, multiprocesseur gère les connexions client, tirant parti de la possibilité qu'offrent les serveurs Solaris multiprocesseur d'assurer une dimensionnabilité par la gestion d'un grand nombre de connexions de lecteurs de groupes de discussions simultanées.
- *Gestion complète d'alimentation de groupes de discussion.* Basé sur INN issu du consortium de logiciel Internet (INN version 1.5 sec. 2), Sun Internet News Server maintient toutes les améliorations d'utilisation offertes par cette mise en oeuvre pour la gestion des groupes de discussion.
- *Fonctionnalités séparées pour la gestion d'alimentation et les fonctionnalités du service pour lecteurs de groupes de discussion.* Ce service pour lecteurs de groupes de discussion peut être séparé des fonctions de gestion d'alimentation pour permettre

une dimensionnabilité horizontale dans le traitement des connexions de lecteurs de groupes de discussion.

- *Gestion centralisée, basée sur un navigateur.* Sun Internet News Server est un service trois couches qui s'intègre à Sun Internet Administrator pour assurer l'administration centralisée et offrir des avantages de sécurité étendus. Pour plus d'informations sur l'architecture trois couches, consultez "Gestion de services avec Sun Internet Administrator", page 10.

Sun Internet FTP Server

Ce serveur FTP dimensionnable hautes performances offre les améliorations suivantes :

- *Domaines multiples sur hôte unique.* Sun Internet FTP Server supporte la gestion d'hôte virtuel IP. Chaque hôte virtuel possède ses propres fichiers de configuration qui règlent le serveur pour le domaine particulier.
- *Authentification utilisateur configurable.* Sun Internet FTP Server peut utiliser des comptes ou des entrées UNIX dans le registre SunDS pour authentifier des administrateurs.
- *Gestion centralisée, basée sur un navigateur.* Sun Internet FTP Server est un service trois couches qui s'intègre avec Sun Internet Administrator pour assurer une administration centralisée et offrir de réels avantages en matière de sécurité. Pour plus d'informations sur l'architecture trois couches, consultez "Gestion de services avec Sun Internet Administrator", page 10.

Installation de Solaris for ISPs

Le serveur UNIX typique devant exécuter une variété d'applications, l'installation de Solaris par défaut part du principe que la plupart des services UNIX sont requis. Les ISP se concentrent sur la fourniture de services spécifiques dans un environnement public. Ils ont des besoins importants en matière de performances et de sécurité.

Pour configurer Solaris en fonction de leurs besoins, les administrateurs ISP effectuent généralement des tâches de durcissement et de réglage. Ils arrêtent les services Solaris non requis et changent les autorisations aux fichiers pour éliminer les vulnérabilités à la sécurité. Ce processus peut prendre des heures.

Le logiciel de configuration d'hôte dans Solaris for ISPs automatise ce processus de durcissement et de réglage pour l'administrateur. Outre la copie des progiciels nécessaires aux emplacements appropriés, il durcit la base Solaris 2.6 sous-jacente, changeant les propriétaires et les modes de fichier lorsque cela est approprié et configurant les mécanismes de sécurité et de connexion Solaris. Une étape finale

dans ce processus consiste à désactiver sélectivement les services Solaris standard (tels que `finger` ou `rlogin`) lorsqu'ils ne supportent pas la fonction d'une machine hôte donnée.

La configuration d'hôte Solaris for ISPs peut être effectuée de façon interactive en utilisant son interface utilisateur graphique ou, de façon répétée et non interactive, à l'aide de JumpStart.

Modèle de configuration hôte

Le processus de configuration fonctionne en construisant un scénario de l'état courant du système, en déterminant les composants logiciels disponibles à installer, et en identifiant ce que l'utilisateur a sélectionné pour installer ou désinstaller.

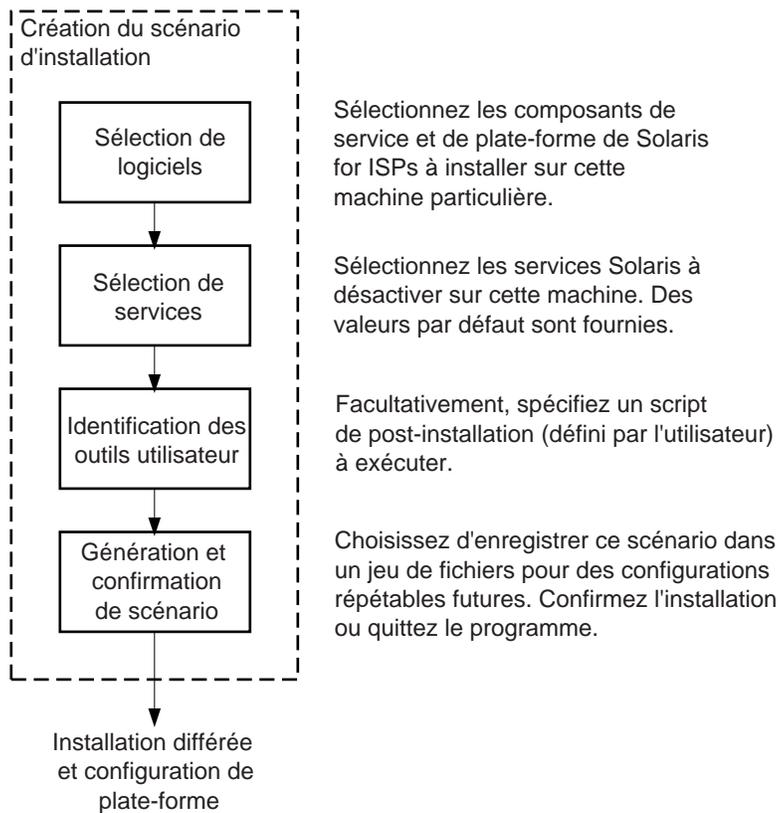


Figure 1-2 Processus de configuration d'hôte de Solaris for ISPs

Le logiciel de configuration d'hôte peut également être utilisé, le cas échéant, pour reconfigurer un hôte après l'installation, l'ajout et le retrait de services.

Configuration répétable

Une configuration d'hôte interactive (utilisant l'interface utilisateur graphique) offre la possibilité d'enregistrer un scénario de configuration (sous la forme d'un fichier binaire et de fichiers associés). En créant et en enregistrant un scénario, l'administrateur ISP peut l'utiliser dans un script JumpStart™ formant une installation non interactive, en une seule étape. De telles installations JumpStart sont répétables et peuvent être employées pour configurer des systèmes de façon identique.

JumpStart fait partie du système d'exploitation Solaris pouvant effectuer des installations personnalisées répétables de Solaris à la fois localement et à distance. Pour la procédure de création d'une installation JumpStart personnalisée, consultez le manuel *Solaris Advanced Installation Guide*. Pour plus d'informations sur l'emploi d'un fichier de scénario dans un script final pour une installation JumpStart personnalisée, reportez-vous au chapitre 2 du présent manuel.

Gestion de services avec Sun Internet Administrator

Sun Internet Administrator assure une gestion centralisée sécurisée pour tous les services ISP, à la fois localement et sur un réseau d'hôtes. Il lance les IUG d'administration (lorsqu'elles sont présentes) de services individuels sur demande d'un administrateur autorisé. Des interfaces à ligne de commande peuvent également être employées lorsque cela est approprié.

Fonctions pour un environnement sécurisé

Sun Internet Administrator offre les fonctions de sécurité suivantes :

- *Authentification d'administrateur.* Les administrateurs doivent fournir un nom d'utilisateur et un mot de passe valides lors de l'accès à l'interface utilisateur graphique.
- *Contrôle d'accès de l'administrateur.* L'accès est contrôlé par un service ISP. Un administrateur autorisé à gérer des serveurs FTP sur le réseau peut ou non avoir également accès aux serveurs de groupes de discussion. Les administrateurs de console (ceux pouvant gérer des processus Sun Internet Administrator) ont accès à tous les services gérés par Sun Internet Administrator.
- *Audit centralisé.* Les actions des administrateurs sont consignées pour une traçabilité et une comptabilisation.

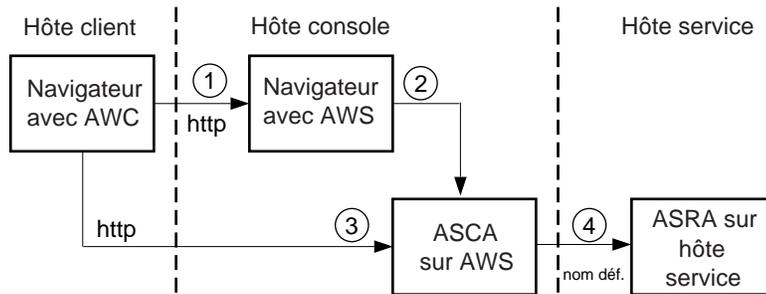
- *Protection de vue privée et d'intégrité pour tout le trafic réseau.* Le logiciel SKIP facultatif peut être configuré pour protéger toutes les connexions vers et depuis Sun Internet Administrator. SSL peut également être employé pour un trafic HTTP sécurisé.

Sun Internet Administrator supporte des services dans deux architectures : trois couches et deux couches. Seule l'architecture trois couches bénéficie de tous les avantages liés à la sécurité indiqués ci-dessus. Quatre types d'IU de service sont pris en charge :

- *Les applications trois couches reposant sur un navigateur* bénéficient de tous les avantages de sécurité offerts par Sun Internet Administrator.
- *Les applications deux couches basées sur un navigateur* ne peuvent pas exploiter la fonction d'ouverture de session unique, mais sont gérables par l'intermédiaire de Sun Internet Administrator. Si elles utilisent SWS pour supporter l'application d'administration, elles peuvent le configurer pour assurer l'authentification de l'administrateur. Pour plus de détails, reportez-vous au Chapitre 7. L'architecture deux couches est incluse pour supporter les anciennes applications.
- *Les applications X* bénéficient de tous les avantages d'une application trois couches.
- *Les fonctions de ligne de commande* (scripts, programmes ou toutes combinaisons) bénéficient de tous les avantages des applications trois couches. Ces applications peuvent être toutes enregistrées pour un service donné et gérées par Sun Internet Administrator, qui construit une interface Web aux programmes de ligne de commande.

Architecture d'application trois couches

L'architecture d'application trois couches basée sur un navigateur recommandé bénéficie de tous les avantages de sécurité de Sun Internet Administrator.



Légende

AWC : Administration Web Client. La partie de l'interface graphique de Sun Internet Administrator qui est téléchargée dans le navigateur de l'administrateur.

AWS : Administration Web Server. Le serveur Web qui sert l'interface graphique de Sun Internet Administrator et les ASCA présents pour les services gérés.

ASCA : Administration Server Client Agent. La partie d'une interface utilisateur d'un service géré co-résident avec AWS.

ASRA : Administration Server Remote Agent. La partie d'une interface utilisateur d'un service géré co-résident avec le service.

Figure 1-3 Architecture de service ISP trois couches

Tel qu'illustré dans la Figure 1-3, un administrateur exécute les opérations suivantes pour accéder aux fonctions d'administration des services :

1. A partir d'un navigateur, l'administrateur demande une URL spécifique (l'emplacement de la page d'interface utilisateur graphique principale de Sun Internet Administrator).

L'AWC est téléchargé dans le navigateur client, où l'administrateur peut choisir un service à gérer.

2. Sun Internet Administrator invite l'administrateur à entrer un nom d'utilisateur et un mot de passe. L'administrateur n'a pas besoin d'utiliser un compte UNIX pour accéder à l'interface graphique utilisateur de la console ; un référentiel de services de répertoire (Sun Directory Services) gère les informations d'administrateur pour Sun Internet Administrator. Cette connexion doit être sécurisée à l'aide d'un protocole HTTP sécurisé.

Le service sélectionné est traduit en une URL qui désigne l'ASCA du service. En réponse, l'interface utilisateur graphique de l'agent du serveur est téléchargée. A ce stade, le contrôle passe au programme d'administration de service.

3. Tout accès ultérieur est effectué directement entre le navigateur client et l'agent serveur du composant sur l'AWS.

L'AWS authentifie l'administrateur par rapport aux services de répertoire et consigne chaque requête de l'administrateur. Si l'administrateur a un accès approprié, les requêtes sont passées à l'ASRA.

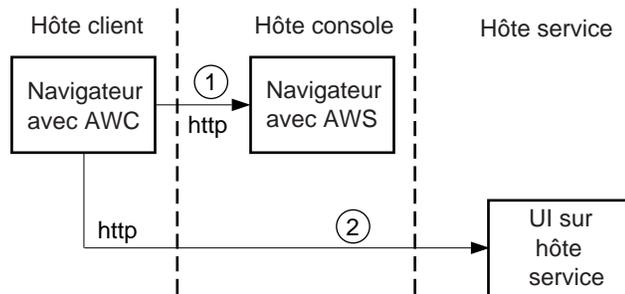
4. L'ASCA communique avec l'ASRA par l'intermédiaire d'un protocole choisi par le développeur du service. Des mesures de sécurité de niveau IP appropriées doivent être prises pour protéger cette connexion et son trafic.

L'ASRA authentifie et consigne de nouveau chaque action de l'administrateur. Pour protéger les communications réseau, l'ISP peut ajouter un cryptage de niveau IP, si cela est désiré, en utilisant SKIP.

Les modules ASCA et ASRA pour programmes de ligne de commande et X sont fournis dans Solaris for ISPs. Sun Internet Administrator les utilise automatiquement lorsque vous enregistrez ces applications.

Architecture d'application deux couches

Pour certaines applications, surtout en ce qui concerne les services existants, une architecture deux couches garantissant l'accès par l'intermédiaire de Sun Internet Administrator est plus pratique. Ces services peuvent être gérés depuis Sun Internet Administrator, mais ne bénéficient pas des avantages de sécurité d'une ouverture de session et d'une connexion uniques.



Légende

AWC : Administration Web Client. La partie de l'interface graphique de Sun Internet Administrator qui est téléchargée dans le navigateur de l'administrateur.

AWS : Administration Web Server. Le serveur Web qui sert l'interface graphique de Sun Internet Administrator et les ASCA présents pour les services gérés.

Figure 1-4 Architecture de service ISP deux couches

Tel qu'illustré dans la Figure 1-4, un administrateur exécute les opérations suivantes pour accéder aux fonctions d'administration des services :

1. A partir d'un navigateur, l'administrateur demande une URL spécifique (l'emplacement de la page d'interface graphique de la console principale).

Cette étape est la même pour l'architecture trois couches. L'AWC est téléchargé dans le navigateur client, où l'administrateur peut choisir un service à gérer.

2. Le service sélectionné est traduit en une URL, désignant l'ASRA du composant. Si l'interface utilisateur d'administration du service n'est pas basée sur le navigateur, d'autres protocoles peuvent être employés au choix du développeur.
3. Tout accès ultérieur s'effectue directement entre le navigateur client et l'agent distant du service. Des mesures de sécurité de niveau IP appropriées doivent être prises pour protéger cette connexion et son trafic.

Dans une architecture deux couches, les services ne peuvent pas tirer parti de la fonction d'ouverture de session unique.

Planification de l'installation

Pour l'installation de Solaris™ for ISPs™, une planification méthodique s'impose. Ce chapitre présente une vue d'ensemble des diverses opérations nécessaires pour procéder à l'installation des extensions de plate-forme et services Solaris for ISPs. Pour des instructions détaillées sur l'installation du logiciel, consultez le manuel *Guide d'installation de Solaris for ISPs*.

Le processus d'installation

Cette section décrit les opérations du processus d'installation dans des organigrammes séquentiels :

- Planification de l'installation.
- Préparation d'installation.
- Installation de Solaris™ for ISPs™.
- Configuration de Sun™ Directory Services.
- Configuration de Sun™ Internet Administrator™.
- Tâches de post-installation

Remarque - Pour chaque opération du processus, veuillez vous reporter au chapitre indiqué.

Présentation du processus d'installation

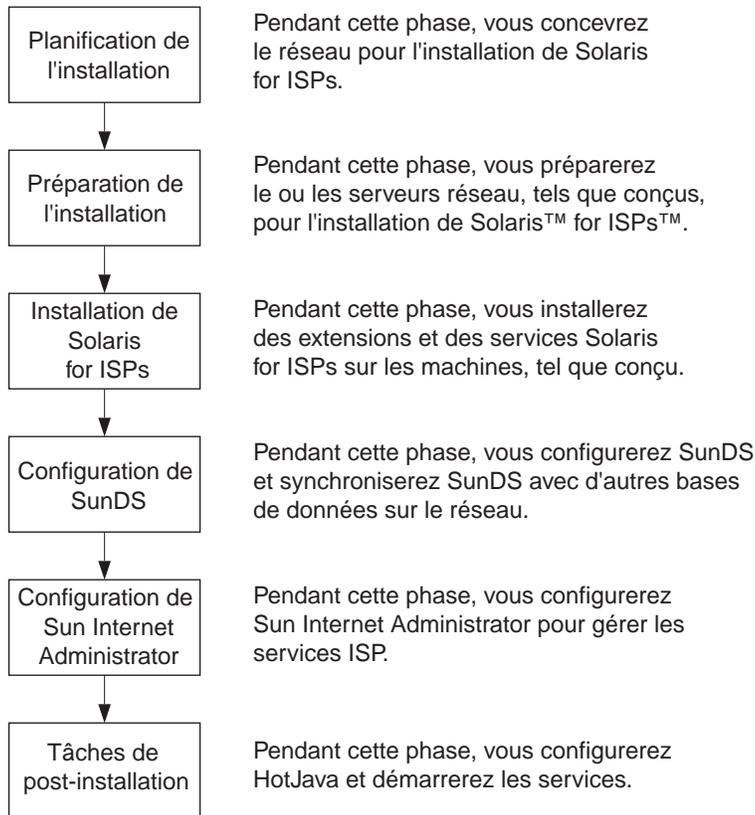


Figure 2-1 Processus d'installation

Vous devez effectuer les opérations décrites ici. Cette section examine les diverses interventions du processus d'installation illustré dans la Figure 2-1.

- **Etape 1** : Pendant cette phase du processus, vous lisez le Chapitre 1 et le Chapitre 3 pour planifier l'installation de Solaris for ISPs.

Cette étape vise à :

- Comprendre les fonctions des composants de Solaris for ISPs.
- Concevoir la configuration de l'hôte réseau et désigner un rôle pour le serveur hôte Solaris for ISPs.
- **Etape 2** : Pendant cette phase du processus, vous vous reporterez à "*Extensions de plate-forme Solaris for ISPs*", page 46 pour préparer des hôtes réseau, comme vous l'aviez prévu dans la phase de planification.

L'objectif de cette opération est de garantir que vos hôtes réseau répondent aux :

- Configuration minimale matérielle spécifiée.
- Configuration minimale de système d'exploitation spécifié.

Remarque - Vous répétez ces opérations pour préparer tous les hôtes sur le réseau afin d'installer les extensions de plate-forme et les services Solaris for ISPs.

- *Etape 3* : Pendant cette phase de processus, vous vous reporterez au "*Guide d'installation de Solaris for ISPs*" et installerez les extensions de plate-forme et services Solaris for ISPs sur les hôtes réseau, comme vous l'aviez prévu dans la phase de planification.

L'objectif de cette opération est de garantir :

- L'installation des extensions de plate-forme Solaris for ISPs.
- L'installation des services Solaris for ISPs.

Remarque - Vous devez installer le logiciel de plate-forme Solaris for ISPs sur chaque machine. Au moins une installation de Sun Internet Administrator et de Sun Directory Services est requise pour supporter les services Solaris for ISPs.

- *Etape 4* : Pendant cette phase de processus, consultez *Sun Directory Services Administration Guide* et configurez Sun Directory Services.

Cette étape vise à :

- Démarrer Sun Directory Services.
- Synchroniser Sun Directory Services avec les autres bases de données d'abonné indépendantes sur le réseau.

- *Etape 5* : Pendant cette phase du processus, consultez l'aide en ligne et configurez Sun Internet Administrator.

Cette étape vise à :

- Personnaliser Sun Internet Administrator en fonction de votre environnement.
- Enregistrer et gérer des services depuis Sun Internet Administrator.

- *Etape 6* : Pendant cette phase de processus, vous consulterez *Guide d'installation de Solaris for ISPs*, configurerez le navigateur HotJava™ et démarrerez les services.

Cette étape vise à :

- Configurer HotJava pour prendre en charge les besoins en matière de sécurité d'applet pour Sun Internet Administrator et Sun™ Internet Services Monitor™.
- Accéder aux services par l'intermédiaire de Sun Internet Administrator ou directement à partir d'un navigateur et démarrer les services.

Planification de l'installation

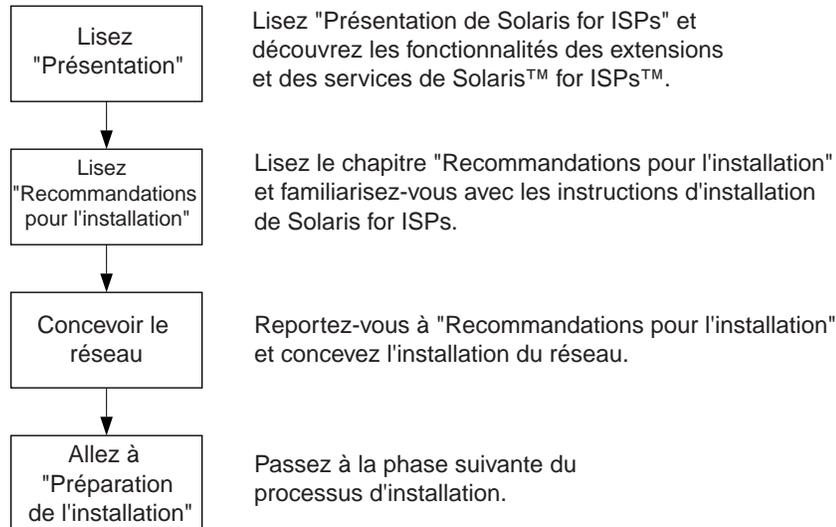


Figure 2-2 Planification de l'installation

Vous devez effectuer les opérations décrites ci-après. Cette section examine les diverses opérations présentées dans la phase de planification du processus d'installation illustré dans Figure 2-2.

- **Étape 1** : Lisez Chapitre 1. Cette étape a pour but de garantir que :
 - Vous comprenez les diverses fonctions des extensions de plate-forme et services Solaris for ISPs.
 - Vous comprenez le mode d'installation de Solaris for ISPs.

La documentation de présentation générale de Solaris for ISPs est disponible en plusieurs formats.

- Dans le répertoire racine de votre support d'installation, la documentation de présentation générale se trouve dans *racine_support/docs/README.1st*.
 - Dans la documentation imprimée, vous trouverez ces informations dans les chapitres 1 à 4 de ce manuel.
 - Sur le Web, vous pouvez accéder à ces informations à l'adresse <http://access1.sun.com/Products/ISP>.
- **Étape 2** : Lisez Chapitre 3. Cette étape vous aidera à :
 - Planifier l'installation.
 - Préparer l'installation.

- *Etape 3* : Concevez votre réseau Solaris for ISPs. Consultez “Scénario d’installation” , page 27 pour concevoir le réseau. Cette étape vise à garantir que :
 - Vous concevez votre configuration réseau.
 - Vous désignez les serveurs hôtes réseau pour les extensions de plate-forme Solaris for ISPs.
 - Vous désignez les serveurs hôtes réseau pour les services Solaris for ISPs.
- *Etape 4* : Commencez à préparer l’installation de Solaris for ISPs.

Préparation d'installation

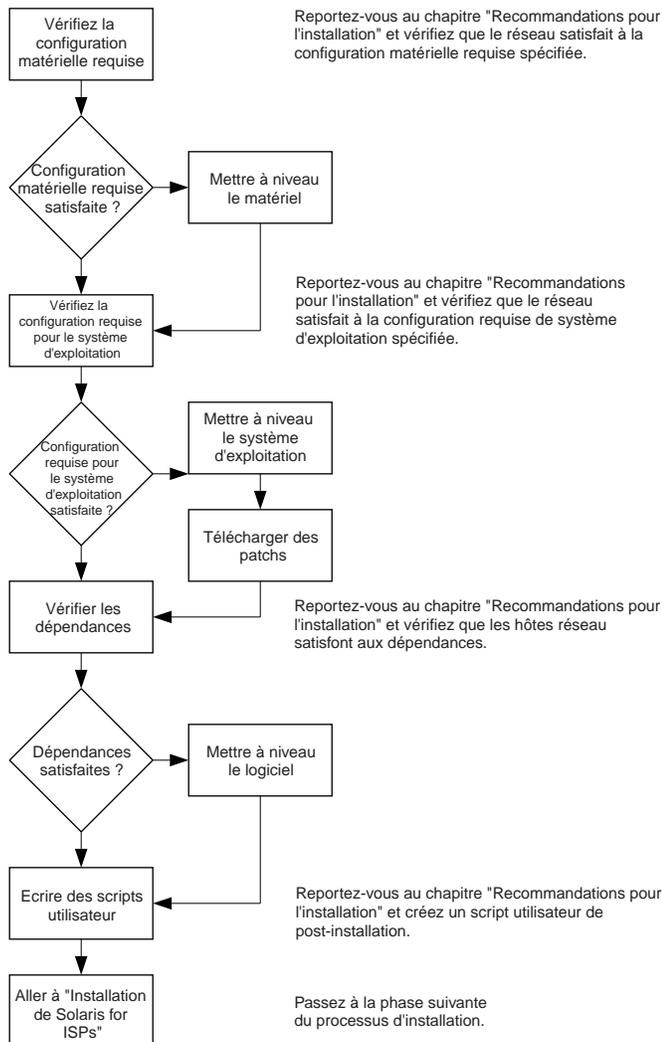


Figure 2-3 Préparation de l'installation

Vous devez effectuer les opérations décrites ci-après. Cette section étudie les opérations de la phase de préparation du processus d'installation illustré dans la Figure 2-3.

Remarque - Vous devez répéter ces opérations pour préparer tous les hôtes sur le réseau afin d'installer les extensions de plate-forme et les services Solaris for ISPs.

- *Etape 1* : Vérifiez la configuration matérielle minimale du système pour les extensions de plate-forme et les services Solaris for ISPs. Consultez “Configuration matérielle minimale” , page 46 dans “*Extensions de plate-forme Solaris for ISPs*” , page 46.

L’objectif de cette étape est de garantir que vos serveurs hôtes réseau Solaris for ISPs répondent :

- aux normes CPU spécifiées,
 - aux besoins en espace disque spécifiés,
 - aux besoins en RAM spécifiés,
 - aux exigences SWAP spécifiées.
- *Etape 2* : Vérifiez la configuration minimale du système d’exploitation pour les extensions de plate-forme et les services Solaris for ISPs. Consultez “Prérequis d’installation” , page 43 dans “*Extensions de plate-forme Solaris for ISPs*” , page 46.

Cette étape vise à garantir que :

- Vous disposez de la configuration minimale du système d’exploitation spécifiée.
 - Vous téléchargez les patches (logiciels) du système d’exploitation spécifiés.
- *Etape 3* : Vérifiez les dépendances d’extensions de plate-forme et de services Solaris for ISPs. Consultez “Dépendance des composants” , page 47 dans le Chapitre 4.

Cette étape vise à garantir que, pour l’installation et l’utilisation efficaces du logiciel Solaris for ISPs,

- toutes les dépendances intégrées et de logiciels indépendants spécifiées sont satisfaites.
- toutes les dépendances interlogiciel ont été notées. Cela vous permettra d’installer et de configurer les extensions de plate-forme et services Solaris for ISPs en fonction de leur interdépendance.

Remarque - Si vous utilisez le navigateur, les dépendances de composant sont affichées dans l’interface utilisateur graphique. Si vous installez le produit depuis la ligne de commande, reportez-vous au *Guide d’installation de Solaris for ISPs*.

- *Etape 4* : Ecrivez un script de post-installation à exécuter après l’installation de Solaris for ISPs. Cette intervention est facultative. Pour les instructions d’écriture du script, consultez “Création de scripts définis par l’utilisateur” , page 40 dans le Chapitre 3.

Cette étape vise à :

- Ecrire un script de post-installation.
 - Fournir un chemin au script.
- *Etape 5* : Procédez à l'installation d'extensions de plate-forme et services Solaris for ISPs sur les hôtes réseau respectifs.

Installation de Solaris for ISPs



Figure 2-4 Installation de Solaris for ISPs

Vous devez effectuer les opérations décrites ci-après. Cette section étudie les opérations de la phase d'installation du processus illustré dans la Figure 2-4.

- *Etape 1* : Exécutez `hcsstartup` et démarrez l'outil de configuration d'hôte. Consultez le *Guide d'installation de Solaris for ISPs* pour démarrer l'outil de configuration d'hôte :
- *Etape 2* : Installez le produit à partir de l'interface d'utilisateur graphique. Pour installer :
 - Sélectionnez la ou les extensions et le ou les services à installer sur l'hôte dans la liste d'extensions de plate-forme et de services Solaris for ISPs.

Remarque - Vous devez installer le composant de plate-forme Solaris for ISPs. Vérifiez les dépendances de composant sur d'autres composants Solaris for ISPs pour les services que vous avez sélectionnés.

Remarque - Lors de la sélection d'extension de plate-forme ou de service, vous pouvez personnaliser le composant sélectionné en fonction de votre environnement. Si vous ne personnalisez pas, vous acceptez les valeurs par défaut.

- Sélectionnez les services Solaris à activer ou à désactiver dans la liste de services Solaris. Pour plus d'informations sur l'activation ou la désactivation de services Solaris, consultez "Paramètres reconfigurables" , page 34 dans le Chapitre 3.

- Spécifiez le chemin du script de post-installation que vous avez écrit lors de la préparation de l'installation. Ce script sera exécuté pendant l'installation différée.
- Facultativement, enregistrez le scénario configuré. Si vous choisissez d'enregistrer le scénario, vous pouvez utiliser ce scénario enregistré pour l'installation JumpStart™ d'extensions de plate-forme et de services Solaris for ISPs sur d'autres hôtes sur le réseau. Pour plus d'informations sur les installations répétables, consultez le Chapitre 1.
- Installez des extensions de plate-forme et des services Solaris for ISPs. Reportez-vous au *Guide d'installation de Solaris for ISPs* ou à l'aide en ligne.

Configuration de Sun Directory Services

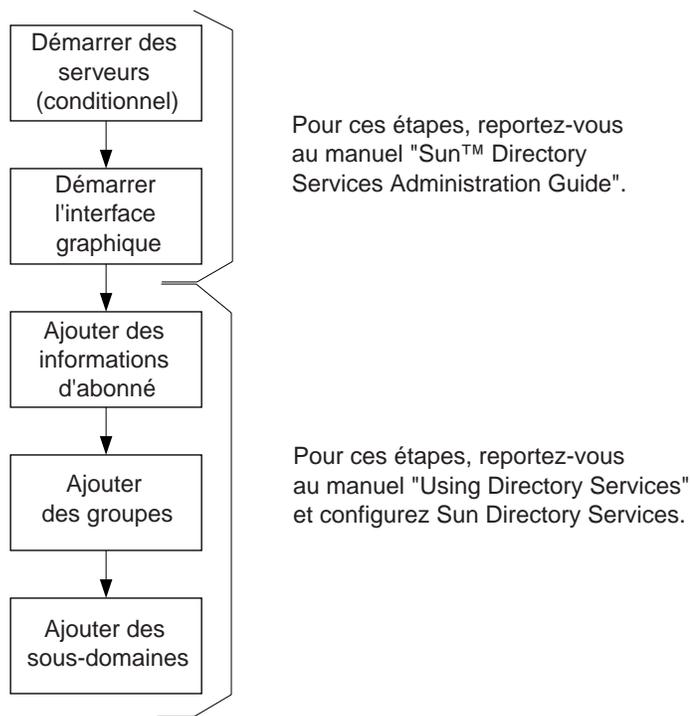


Figure 2-5 Configuration de Sun Directory Services

Vous devez effectuer les opérations décrites ci-après. Cette section étudie les opérations de la phase de configuration du processus d'installation. Vous devez d'abord configurer Sun Directory Services tel qu'illustré dans la Figure 2-5.

- **Étape 1** : Démarrez Sun Directory Services RADIUS, l'administration et les serveurs de passerelle Web. Pour démarrer, reportez-vous au chapitre 3 du manuel *Guide d'installation de Solaris for ISPs*.

Remarque - Vous ne devez démarrer manuellement les services que si les serveurs n'ont pas déjà été démarrés après le réamorçage de la machine suite à l'installation.

- *Etape 2* : Démarrez le navigateur.
- *Etape 3* : Ajoutez des informations d'abonné dans Sun Directory Services. Synchronisez les informations d'abonné dans Sun Directory Services avec toute autre base de données d'abonné indépendante sur le réseau. Reportez-vous à "Création d'entrées d'abonné" , page 57.
- *Etape 4* : Ajoutez des entrées de groupe dans Sun Directory Services. Consultez le Chapitre 5.
- *Etape 5* : Ajoutez les domaines requis sous le domaine racine. Consultez "Création d'entrées de domaine" , page 55.

Remarque - Vous pouvez également vous référer à l'aide en ligne de Sun Internet Administrator pour connaître les étapes de création de domaine et d'ajout d'entrées d'abonné et de groupe.

Configuration de Sun Internet Administrator

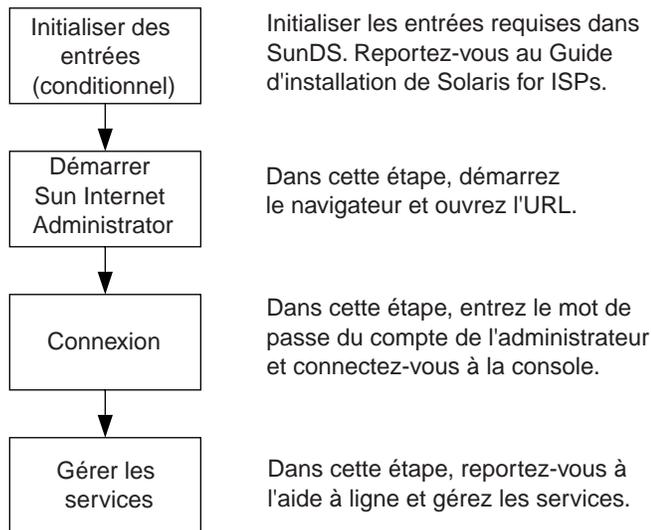


Figure 2-6 Configuration de Sun Internet Administrator

Vous devez effectuer les opérations décrites ci-après. Cette section étudie les opérations de la phase de configuration du processus d'installation. Après la configuration de Sun Directory Services, vous devez configurer Sun Internet Administrator tel qu'illustré dans la Figure 2-6.

- *Etape 1* : Exécutez `mcdsinit` pour initialiser les entrées requises dans Sun Directory Services. Pour créer les entrées initiales, consultez le chapitre 3 du manuel *Guide d'installation de Solaris for ISPs*.

Remarque - Vous devez exécuter cette commande après l'installation, uniquement si les entrées n'ont pas déjà été automatiquement créées.

- *Etape 2* : Démarrez l'interface utilisateur graphique de la console de Sun Internet Administrator. Pour démarrer la console, accédez au site `http://nom d'hôte de la console:50080/ispmc`. Spécifiez le nom d'hôte et le numéro de port Sun Internet Administrator, si vous avez installé le produit sur un autre port que le port par défaut.
- *Etape 3* : Entrez le mot de passe de compte Sun Internet Administrator et connectez-vous à la console.
- *Etape 4* : Gérez et administrez les services. Pour gérer des services, vous devez :
 - Enregistrer des services Solaris for ISPs. Reportez-vous à l'aide en ligne.
 - Créer des comptes administrateur. Cette intervention est facultative. Pour créer des comptes administrateur, consultez l'aide en ligne.

Tâches de post-installation

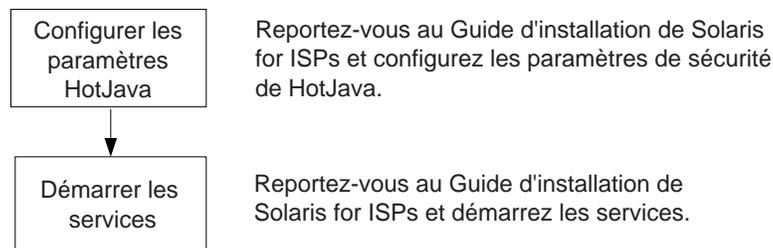


Figure 2-7 Tâches de post-installation

Vous devez effectuer les opérations décrites ci-après. Cette section étudie les tâches de post-installation à effectuer.

- *Etape 1* : Configurez les paramètres de sécurité HotJava. Consultez le *Guide d'installation de Solaris for ISPs* et configurez les paramètres de sécurité HotJava pour prendre en charge :

- Les exigences de sécurité de navigateur pour les applets d'administration à distance de Sun Internet Administrator.
- Les paramètres de définition de sécurité de navigateur pour les applets Java Sun™ Internet Services Monitor™.
- *Etape 2* : Démarrez les services. Consultez le chapitre 3 du manuel *Guide d'installation de Solaris for ISPs* et accédez aux services :
 - Depuis Sun Internet Administrator. Si vous souhaitez accéder aux services depuis Sun Internet Administrator, enregistrez d'abord les services et suivez les instructions de la section Starting Sun Internet Administrator au chapitre 3 du manuel *Guide d'installation de Solaris for ISPs*.
 - En utilisant directement un navigateur. Si vous souhaitez accéder à l'interface utilisateur des services directement à partir d'un navigateur, vérifiez le navigateur supporté par le service et référez-vous au service dans l'aide en ligne pour démarrer l'exécution du service. Pour accéder à l'interface utilisateur du service, reportez-vous au chapitre 3 du manuel *Guide d'installation de Solaris for ISPs* pour connaître l'URL du service.

Recommandations pour l'installation

Solaris™ for ISPs™ fournit une infrastructure principale avec un jeu d'extensions de plate-forme et de services pour ISP. Ce chapitre présente des directives de configuration d'hôte réseau pour l'installation d'extensions et de services Solaris for ISPs. Ces informations de configuration sont essentielles pour réussir l'installation. Veuillez les lire attentivement.

Scénario d'installation

Vous *devez* concevoir le réseau avant d'installer Solaris for ISPs. Cette section traite deux exemples testés de configuration d'hôtes réseau Solaris for ISPs. Vous pouvez utiliser l'exemple de configuration d'hôtes réseau correspondant le mieux à votre environnement.

Configuration réseau

Cette section décrit un exemple de configuration de réseau de base et étendu, et les caractéristiques et recommandations relatives à la configuration du matériel.

Remarque - Nous ne partons pas du principe qu'il existe un pare-feu dans nos exemples de configuration réseau. Si vous utilisez un produit pare-feu Internet pour contrôler le trafic réseau vers ou depuis n'importe quel hôte Solaris for ISPs, vous devez étudier la politique de sécurité contrôlant cet hôte pour vous assurer que les types de communication appropriés sont autorisés. Ce document *ne* présente *pas* de recommandations relatives aux pare-feu Internet.

Configuration de base

Cette figure illustre un exemple de configuration de base.

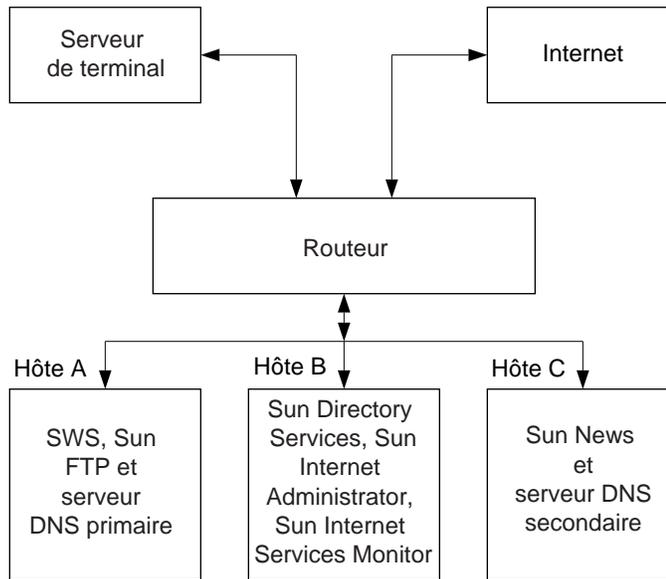


Figure 3-1 Configuration de base

Caractéristiques matérielles de base

- Trois stations de travail haut de gamme.
- Serveurs DNS primaires et secondaires.
- Les hôtes *doivent* se trouver sur un réseau connecté à l'Internet.
- Vous pouvez choisir n'importe quel serveur sur le réseau devant agir comme hôte client.
- Vous avez besoin d'un navigateur Web sur le client hôte pour Sun Internet Administrator et le logiciel client Sun Internet Services Monitor.

Exemple de conception de configuration de base

Les trois serveurs sont qualifiés d'hôte A, hôte B et hôte C. Par exemple, les serveurs hôte peuvent être configurés de la façon suivante :

- *Hôte A* : Configurez ce serveur pour qu'il agisse comme hôte de service. Installez SWS et Sun Internet FTP Server, et configurez l'hôte comme serveur DNS primaire.
- *Hôte B* : Configurez ce serveur pour qu'il agisse comme hôte console. Installez Sun Internet Administrator, Sun Directory Services et Sun Internet Services Monitor.

- *Hôte C* : Configurez ce serveur pour qu'il agisse comme hôte de service. Installez Sun Internet News Server et configurez l'hôte comme serveur DNS secondaire.

Remarque - Les configurations de serveur DNS décrites dans cet exemple de configuration ne sont présentées qu'à titre indicatif. Vous ne devez pas installer d'extensions et de services Solaris for ISPs sur un hôte agissant comme serveur DNS. La plupart des extensions et des services nécessitent uniquement la possibilité d'effectuer régulièrement des recherches de noms.

Configuration étendue

Cette figure illustre un exemple de configuration réseau étendue.

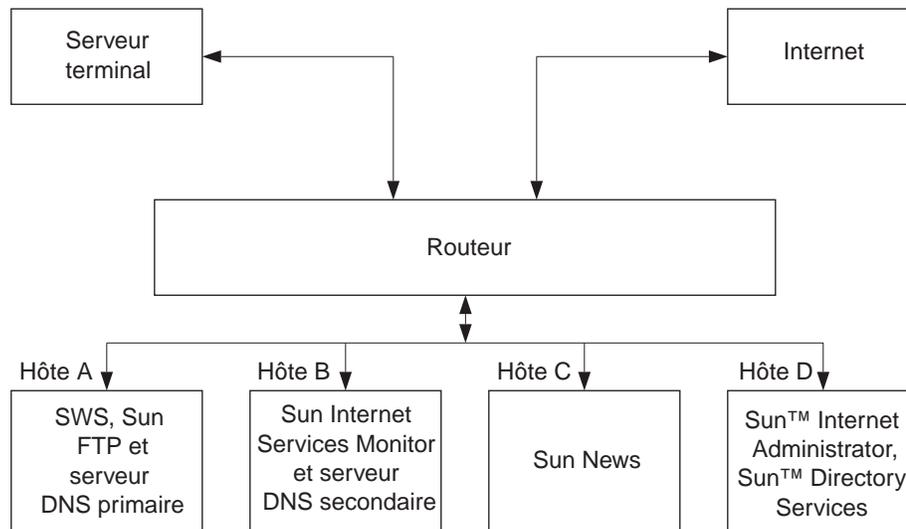


Figure 3-2 Configuration étendue

Caractéristiques matérielles étendues

- Quatre stations de travail haut de gamme.
- Serveurs DNS primaires et secondaires.
- Les hôtes *doivent* se trouver sur un réseau connecté à l'Internet.
- Vous pouvez choisir n'importe quel serveur sur le réseau devant agir comme hôte client.
- Vous avez besoin d'un navigateur Web sur le client hôte pour Sun Internet Administrator et le logiciel client Sun Internet Services Monitor.

Exemple de conception de configuration étendue

Les quatre serveurs sont qualifiés d'hôte A, hôte B, hôte C et hôte D. Par exemple, les serveurs hôte peuvent être configurés de la façon suivante :

- *Hôte A* : Configurez ce serveur pour qu'il agisse comme hôte de service. Installez SWS et Sun Internet FTP Server, et configurez l'hôte comme serveur DNS primaire.
- *Hôte B* : Configurez ce serveur pour qu'il agisse comme hôte console. Installez Sun Internet Services Monitor et configurez l'hôte comme serveur DNS secondaire.
- *Hôte C* : Configurez ce serveur pour qu'il agisse comme hôte de service. Installez Sun Internet News Server.
- *Hôte D* : Configurez ce serveur pour qu'il agisse comme hôte console. Installez Sun Internet Administrator et Sun Directory Services sur cet hôte.

Remarque - Les configurations de serveur DNS illustrées dans cet exemple de configuration ne sont présentées qu'à titre indicatif. Vous ne devez pas installer d'extensions et de services Solaris for ISPs sur un hôte agissant comme serveur DNS. La plupart des extensions et des services nécessitent uniquement la possibilité d'effectuer régulièrement des recherches de noms.

Remarque - Après la conception de la configuration d'hôtes réseau, préparez les hôtes pour l'installation de Solaris for ISPs. Reportez-vous à "*Extensions de plate-forme Solaris for ISPs*", page 46 pour préparer les hôtes selon la conception définie.

Problèmes de sécurité

Tout réseau avec accès Internet est exposé à certains risques concernant la sécurité. En outre, certaines fonctions de Solaris for ISPs introduisent d'autres risques. Dans chaque cas, plusieurs mesures de sécurité peuvent être mises en oeuvre pour protéger votre réseau. Les sections suivantes présentent certaines pratiques d'administration système adaptées et des fonctions de Solaris for ISPs vous permettant de sécuriser votre réseau et de le mettre à l'abri de ce risque.

Risques pour la sécurité Internet standard

La connexion du réseau à d'autres réseaux sur l'Internet l'expose à des interruptions de service potentiels, à une intrusion illicite et à des dommages importants. Cette section vous fait prendre conscience de ce type de risque. Les protections contre ces risques sont décrites dans "*Comment renforcer la sécurité?*", page 32.

- **Attaques refus de services** : Ces attaques interdisent au système de servir les clients et rend un service non disponible pour les clients. Par exemple, les attaques peuvent encombrer le réseau avec un trafic inutile compromettant la qualité du service aux clients. Très souvent, de telles attaques peuvent bloquer le système ou le ralentir considérablement.
- **Exploits (piratage) de dépassement de capacité de tampon** : Ces événements incluent l'exploitation des faiblesses logicielles pour ajouter des données arbitraires dans un programme qui, lorsqu'il est exécuté comme racine, peut donner à l'exploiteur un accès racine dans votre système. Cela peut également entraîner une attaque refus de services.
- **Attaques usurpation et écoute** : Les attaques usurpation impliquent une intrusion d'écoute du trafic entre deux machines sur votre réseau. Le trafic peut inclure l'échange de mots de passe cryptés lors de l'utilisation de `telnet`, `rlogin` ou `ftp`. Cela peut permettre à un individu de s'introduire illicitement dans votre réseau ou de lire des données confidentielles.
- **Usurpation IP** : Les attaques basées sur l'usurpation IP impliquent un accès non autorisé à des ordinateurs. L'intrus écoutant le trafic de votre réseau trouve une adresse IP d'un hôte de confiance et envoie des messages indiquant que le message provient de cet hôte de confiance.
- **Exposition interne** : La plupart des intrusions illicites dans des réseaux sont le fait d'un employé actuel ou d'un ancien employé malveillant utilisant à mauvais escient l'accès à des informations ou s'introduisant de façon illicite dans votre réseau.

Risques relatifs à la sécurité dans Solaris for ISPs

Cette section traite de certaines fonctions de Solaris for ISPs pouvant créer des risques de sécurité pour le logiciel. Veuillez vous reporter à "Comment renforcer la sécurité?", page 32 pour plus de détails concernant la protection contre ces risques.

- **Administration de produits** : Les produits d'administration Solaris for ISPs pour services individuels, tels que `ftp` ou groupes de discussion, offrent de nouvelles possibilités d'accès à des opérations privilégiées. Cet intrus, en connaissant, en devinant ou en déplaçant le mot de passe de l'administrateur, peut modifier le comportement des services en exploitant l'interface d'administrateur à travers le réseau. Cependant, `Sunscreen™ SKIP`, intégré dans Solaris for ISPs, authentifie le trafic entrant et garantit que les données sortantes ne sont pas visualisées par d'autres personnes en cours de transit.
- **Mécanisme d'exécution d'une commande distante** : Sun Internet Administrator donne accès à toutes les commandes d'administration de ligne de commande par l'intermédiaire de son mécanisme d'exécution distante de console administrateur. Un intrus peut s'introduire dans ce mécanisme et avoir accès à ces commandes. Cependant, l'accès à ces commandes peut être limité, par racine, uniquement aux administrateurs système enregistrés.

- Sun Directory Services : Ce logiciel Solaris for ISPs peut être utilisé pour stocker et gérer des mots de passe et des informations sur d'autres extensions et services Solaris for ISPs. Un intrus peut s'introduire illicitement et exploiter l'accès à de telles informations privilégiées. Cependant, la plupart des mots de passe dans Sun Directory Services sont cryptés. Les mots de passe non cryptés dans Sun Directory Services nécessitent un accès racine.

Comment renforcer la sécurité?

Pour protéger votre système contre tout accès illicite, corruption ou modification des informations, et pour rendre le réseau disponible pour les utilisateurs autorisés :

- Changez régulièrement les mots de passe et encouragez l'utilisation de mots de passe difficiles à deviner. Le logiciel Solaris for ISPs impose le changement des mots de passe périodiquement si des fichiers locaux sont employés pour la gestion des mots de passe.
- Utilisez une cryptographie à clé publique pour crypter tout le trafic effectué entre hôtes de confiance au niveau IP. SKIP, livré avec Solaris for ISPs, authentifie le trafic IP entrant et s'assure que les données sortantes ne sont ni modifiées ni visualisées par d'autres en cours de transit.
- Utilisez des routeurs pouvant identifier des hôtes de confiance et bloquer les adresses IP usurpées.
- Réparez les vulnérabilités et renforcez la sécurité de votre logiciel.
- Désactivez les services non désirés créant des risques pour la sécurité de votre réseau. Le logiciel de configuration d'hôte de Solaris for ISPs, partie intégrante du processus d'installation initial, peut désactiver certaines commandes 'r' pour assurer une protection pour les mots de passe et pour limiter l'accès aux hôtes pour les individus non autorisés.
- Donnez aux employés uniquement l'accès aux données ou aux informations dont ils ont besoin pour leur travail.
- Mettez en oeuvre des mécanismes de sécurité tels que la surveillance du réseau et des pare-feu.

Eléments à prendre en compte

Cette section traite de certaines fonctions par défaut de Solaris for ISPs que vous devez envisager pendant la configuration d'hôte. Dans cette section, les rubriques incluent notamment :

- Modifications dans Solaris—Fichiers système modifiés par Solaris for ISPs.
- Gestion de fichier journal—Démon résident de Solaris for ISPs.
- Script utilisateur—Création de scripts de post-installation.
- Paramètre de serveur Web d'administration par défaut—Restauration des valeurs par défaut AWS.

Modifications dans Solaris

Cette section traite des modifications exécutées une seule fois et des modifications reconfigurables pouvant être apportées aux services Solaris pendant la configuration d'hôte. Si vous acceptez les paramètres d'installation par défaut, ces modifications seront apportées à l'hôte où Solaris for ISPs est installé.

Remarque - Vous *devez* réviser et pouvez modifier, si nécessaire, ces modifications dans Solaris pendant la configuration d'hôte. Ces modifications ne peuvent pas être incorporées dans des versions futures de Solaris for ISPs.

Paramètres définis une seul fois

Solaris for ISPs est composé d'une unité de configuration de base s'exécutant seulement une fois pour assurer la sécurité des mots de passe et pour attribuer des autorisations fichier au propriétaire des fichiers. Il effectue un ensemble de modifications par défaut lors du processus d'installation initiale. La fonctionnalité de cette unité est similaire à celle du script dans `ftp://ftp.wins.uva.nl:/pub/solaris/fix-modes.tar.gz`. Pour annuler ces modifications, passez à "Annulation des modifications", page 38.

Cette section examine les opérations d'installation initiale exécutées automatiquement une seule fois dans le progiciel de base. Vous *devez* étudier cette section avant d'installer Solaris for ISPs.

Remarque - Le script *sera* exécuté. Cependant, ces modifications seront uniquement effectuées si des modifications aux fichiers en conflit n'ont pas déjà été effectuées par vous.

- Il exécute un script qui accroît la sécurité des modes de fichier installés avec les progiciels Solaris. Ces modifications sont les suivantes :
 - Il retire les autorisations de groupe et universelle pour `setuid` et `setgid`.
 - Il retire les autorisations d'écriture de groupe et universelle sur tous les fichiers non- `setuid` répondant à l'un des critères suivants :

- Le fichier a une autorisation de lecture de groupe et universelle, mais aucune permission d'écriture universelle.
 - Le fichier a une autorisation d'exécution universelle.
 - Le fichier a des autorisations de propriétaire, de groupe et universelle identiques.
 - C'est un répertoire binaire ou un fichier non volatile. Il a des autorisations de lecture et d'exécution de groupe et universelle..
- Il retire les autorisations d'écriture pour les propriétaires sur les exécutables non possédés par racine.
- Il ajoute `umask 077` à `/.cshrc` et `/.profile`. Cela rend lisible et inscriptible uniquement par racine les fichiers créés sous un interpréteur de commandes de racine interactif.
 - Il ajoute une racine à `/etc/ftpusers` pour désactiver la possibilité de la racine d'effectuer un accès ftp à l'hôte.
 - Il choisit noshell par défaut pour `sys`, `uucp`, `nuucp` et écoute les comptes pour consigner les tentatives de connexion illicites. Cela simplifie la détection d'intrusion dans le système.
 - Il définit `MAXWEEKS=12` dans `/etc/default/passwd`. Si des fichiers locaux sont employés pour la gestion des messages, cela impose un changement de mot de passe périodique.
 - Il crée `S35umask` pour attribuer par défaut l'autorisation d'écriture uniquement au propriétaire pour les fichiers créés par des démons système.
 - Il interdit les attaques refus de services en ajoutant la ligne `ndd-set/dev/ipip_respond_to_echo_broadcast 0` dans le fichier `/etc/rc2.d/S69inet`.
 - Il remplace `/etc/syslog.conf` par une nouvelle version pour garantir un enregistrement plus granulaire et pour détecter d'éventuelles intrusions. Cette nouvelle version isole des messages par un niveau de facilité et de consignation, et envoie les messages de haut niveau à un serveur d'enregistrement central.
 - Il exécute `bsmconv` et configure `/etc/security` pour consigner les actions administratives, ainsi que les connexions et les déconnexions. Cela autorise un audit C2, pouvant intercepter des événements omis par `syslog`.
 - Toutes les modifications apportées par cette unité sont consignées par `/var/sadm/install/contents`. Cela permettra l'installation ultérieure de patchs (logiciels).

Paramètres reconfigurables

L'installation d'extensions de plate-forme et de services Solaris for ISPs avec leur configuration par défaut outrepassera le comportement des services par défaut sur

les hôtes où ils sont installés. Cette procédure crée un serveur plus sécurisé en désactivant les utilitaires réseau Solaris qui ne sont pas essentiels au logiciel Solaris for ISPs installé sur le système.

Remarque - Vous *devez* réviser et pouvez modifier, si nécessaire, la configuration par défaut pendant la configuration de l'hôte.

Si vous acceptez la configuration d'installation par défaut, ces services Solaris seront désactivés, sauf indication contraire. La désactivation de ce service n'est pas requise, mais nous la recommandons pour éviter d'éventuelles brèches à la sécurité et pour conserver les ressources. Pour changer la valeur de ces services, `inetd.conf` sera modifié, sauf indication contraire. Pour annuler ces modifications, passez à "Annulation des modifications", page 38

Fermeture de brèches éventuelles à la sécurité

Nous recommandons de désactiver les services suivants pour assurer la protection des mots de passe et pour empêcher quiconque d'accéder sans autorisation aux hôtes.

Remarque - Si vous acceptez la valeur par défaut, vous ne pourrez plus accéder à l'hôte avec ces commandes "r" désactivées.

- `rexecd`: Désactivez ce service pour arrêter le support d'exécution de commande distante par l'intermédiaire de la fonction `rexec(3N)`, qui passe les mots de passe en clair.
- `rlogind`: Désactivez ce service pour assurer la sécurité des mots de passe parce qu'il repose sur `.rhosts` et `hosts.equiv` pour l'authentification sans mot de passe pendant la connexion à distance.
- `rshd`: Désactivez ce service pour protéger le mot de passe parce qu'il repose sur `.rhosts` et `hosts.equiv` pour une authentification sans mot de passe pendant l'exécution d'une commande à distance.

Remarque - Si vous acceptez la valeur par défaut, les services suivants seront activés. Vous *devez* réviser et pouvez modifier le paramètre.

- `telnetd`: Si vous acceptez la valeur d'installation par défaut, sachez que ce service est activé et autorise les mécanismes de connexion distante.
- `ftpd`: Si vous acceptez la valeur d'installation par défaut, sachez que ce service est activé et assure le support du transfert de fichier vers et depuis les sites réseau distants dans un mode plus sécurisé. Ce service sera désactivé si vous sélectionnez Sun Internet FTP Server pour l'installation.

Remarque - Si vous avez besoin de mécanismes de sécurité pour les services telnet et FTP, configurez votre réseau de façon à ce que les demandes de transfert de fichier soient effectuées à l'intérieur du réseau.

Nous vous recommandons de désactiver les services suivants pour protéger les informations contre tout utilisateur non autorisé. La désactivation de ces services améliore la sécurité du système et interdit l'accès aux informations du système en empêchant des réponses d'hôte à ces demandes réseau.

- **fingerd**: Désactivez ce service pour protéger les informations contre les demandes finger réseau.
- **netstat**: Désactivez ce service pour assurer que le contenu des diverses structures de données associées au réseau ne sont pas exposées à une invocation distante de `netstat`.
- **rstatd**: Désactivez ce service pour empêcher l'accès aux statistiques système.
- **rusersd**: Désactivez ce service pour protéger les informations sur les utilisateurs connectés.
- **sysstat**: Désactivez ce service pour arrêter le support de l'exécution à distance de `ps` sur l'hôte.
- **routing**: Désactivez ce service pour assurer que l'hôte ne fonctionne pas comme un routeur. Si ce service est désactivé, le fichier `/etc/notrouter` est créé.
- **sendmail**: Désactivez ce service pour le protéger contre les attaques refus de services et pour désactiver le support de réception et d'envoi de courrier électronique. `S88sendmail` est modifié.
- **sprayd**: Désactivez ce service pour arrêter le support du test du réseau et de l'enregistrement de progiciels envoyés par `spray`.

Conservation de ressources

Nous recommandons de désactiver les services CDE et OpenWindows suivants, sauf s'ils sont requis dans votre environnement. La désactivation de ces services améliore les performances du système.

- **cmsd**: Désactivez ce service puisqu'il est requis uniquement si des calendriers CDE se trouvent sur l'hôte.
- **dtspcd**: Désactivez ce service pour arrêter le support de sessions CDE.
- **kcms_server**: Désactivez ce service pour arrêter le support d'accès distant aux profils OpenWindows KCMS.
- **ttldbserverd**: Désactivez ce service pour arrêter le support du serveur de base de données Tooltalk requis pour un fonctionnement correct de CDE.

Nous recommandons la désactivation des services (`inetd`) réseau suivants, sauf s'ils sont requis dans votre environnement. La désactivation de ces services libérera

des ressources et améliorera les performances du système. Modifiez la configuration par défaut si vous avez besoin des utilitaires réseau indiqués ci-dessous.

- `chargen`: Désactivez ce service pour arrêter le support du test d'`inetd` et de génération de caractères.
- `discard`: Désactivez ce service pour arrêter le rejet de toutes les entrées issues du test d'`inetd`.
- `echo`: Désactivez ce service pour arrêter le support de l'écho de toutes les entrées du test `inetd`.
- `fs.auto`: Désactivez ce service pour désactiver le serveur de polices.

Remarque - Si vous acceptez la valeur par défaut, le service suivant sera activé. Vous devez réviser et pouvez modifier la valeur.

- `time`: Si vous acceptez la valeur d'installation par défaut, sachez que ce service sera activé et que personne ne pourra interroger l'heure du système à distance. Il renvoie l'heure machine.
- `cachedfsd`: Si vous acceptez la valeur d'installation par défaut, sachez que ce service sera activé. Cela correspond au démon `cacheFS`.

Nous recommandons la désactivation des services suivants, sauf s'ils sont essentiels pour votre environnement. La désactivation de ces services améliore les performances du système. Veuillez modifier la configuration par défaut si vous avez besoin des services indiqués ci-dessous.

- `automountd`: Désactivez ce service puisqu'il supporte uniquement le montage automatique et non des montages NFS normaux. Pour changer sa valeur, `S74autofs` sera modifié.
- `comsat`: Désactivez ce service pour arrêter la notification `biff(1)` de nouveaux messages sur l'hôte.
- `daytime`: Désactivez ce service pour arrêter le support de renvoi de l'heure du jour.
- `rquotad`: Désactivez ce service pour garantir que l'hôte n'est pas utilisé comme un serveur NFS supportant des quotas de disque sur son système de fichiers.
- `sadmind`: Désactivez ce service pour arrêter le support d'exécution d'opérations d'administration système réparties utilisant Solstice AdminSuite.
- `talkd`: Désactivez ce service pour arrêter le support d'exécution du programme de parole interactive.
- `tnamed`: Désactivez ce service pour arrêter le support du protocole de serveur de noms DARPA.
- `lpd`: Désactivez ce service pour garantir que l'hôte n'est pas utilisé comme un serveur d'impression BSD. Cela ne désactive pas le serveur d'impression système V.

- `uucpd`: Désactivez ce service et arrêtez le support de copie de fichiers nommés par les arguments de fichier source dans l'argument de fichier destination.
- `walld`: Désactivez ce service et arrêtez le support d'envoi de message par wall.
- `xaserver`: Désactivez ce service et arrêtez le support pour les fonctions audio X.

Remarque - Vous pouvez également consulter l'aide en ligne pendant la configuration de l'hôte pour obtenir de l'aide sur l'activation ou la désactivation des services Solaris.

Annulation des modifications

Les modifications apportées pendant la configuration d'hôte, pour durcir et régler le système afin d'accroître sa sécurité et ses performances, peuvent ne pas être incorporées dans la version suivante de Solaris for ISPs. Cette section indique les opérations à effectuer pour annuler les modifications apportées à la configuration de base de Solaris pendant la configuration d'hôte.

Connectez-vous à l'ordinateur où vous souhaitez annuler les modifications et attribuez-vous un accès racine. Déterminez les modifications à annuler et suivez les instructions de la liste de procédure :

- Les services Solaris de base sont réglés pour une sécurité et des performances optimales à partir de l'interface utilisateur graphique de configuration d'hôte. Ces modifications sont reconfigurables et vous pouvez réinitialiser les valeurs en utilisant l'interface utilisateur graphique de configuration d'hôte. Reportez-vous au manuel *Guide d'installation de Solaris for ISPs* et à l'aide en ligne concernant la configuration d'hôte pour réinitialiser les valeurs de service Solaris.
- Les deux fichiers d'amorçage supplémentaires `S35umask` et `S68echo` dans `/etc/rc2.d`, créés après l'installation, sont automatiquement retirés lors de la désinstallation du composant de plate-forme Solaris for ISPs.

Remarque - Vous devez annuler manuellement certaines modifications exécutées une seule fois et apportées à la configuration du système. Pour annuler les modifications de durcissement :

- Entrez : `# /opt/SUNWfixm/bin/fixmodes -u` pour annuler les modifications exécutées une seule fois.
- Entrez : `# bsmunconv` pour passer du mode audit C2 au mode C1. Cela désactive les fonctions d'audit activées pour intercepter les événements omis par `syslog`.
- Comparez la version courante de `/.cshrc`, `/.profile`, `/.zshenv`, `/etc/ftpusers`, `/etc/default/passwd`, `/etc/syslog.conf` avec la version *fichier.pre-hcfconfig* du fichier. Le fichier actuel contient les modifications de durcissement et toute autre modification qui peut avoir été apportée après l'exécution du durcissement. Déterminez les modifications apportées par le logiciel

de configuration d'hôte et utilisez un éditeur de texte pour annuler ces modifications.

Remarque - Ne copiez pas le *fichier.pre-hcfconfig* dans la version en cours du *fichier* sans déterminer les modifications apportées par et après la configuration d'hôte.

Gestion de fichier journal

Cette section décrit le démon résident, *hclfmd*, qui effectue la gestion des fichiers journaux. Ce démon résident fonctionne comme racine. Il démarre lors de l'amorçage et effectue les fonctions suivantes :

- Il analyse la liste de fichiers journaux dans */etc/syslog.conf* à la recherche de chemins de fichiers qui ne démarrent pas avec */dev* (fichiers associés aux dispositifs système) et réalise un nettoyage, un journal et une exploration quotidienne.

Pour chaque fichier journal écrit par *syslogd*, il effectue les fonctions suivantes :

- Il renomme le fichier journal existant et crée un nouveau journal quotidien.
 - Il envoie le signal de redémarrage (*-HUP*) au démon *syslog* pour créer un nouveau journal quotidien.
 - Il génère un archive hebdomadaire en compressant des fichiers journaux quotidiens chaque semaine et stocke ces informations dans *nom.AAAAMMJJ-AAAAMMJJ.tar.z*.
 - Il supprime les archives hebdomadaires datant de plus d'un mois.
- Il obtient l'emplacement des journaux d'audit à partir de */etc/security/audit_control* et effectue un nettoyage, un journal et une exploration quotidienne.

Il effectue les fonctions suivantes pour chaque répertoire d'audit monté localement :

- Il exécute *audit -n* pour créer un nouveau journal quotidien. Cela indique au répertoire d'audit de fermer le fichier d'audit courant et d'ouvrir un nouveau fichier d'audit dans le répertoire d'audit courant.
 - Il génère un archive hebdomadaire en compressant des fichiers journaux quotidiens chaque semaine et les stocke dans *nom.AAAAMMJJ-AAAAMMJJ.tar.z*.
 - Il supprime les archives hebdomadaires datant de plus d'un mois.
- Il effectue un contrôle de détection d'intrusion toutes les 10 minutes.

- Il détecte et signale tous les échecs d'entrée d'autorisation dans les fichiers syslog.
- Par défaut, `/etc/opt/SUNWisp/hc/hclfm.d.conf` est configuré pour envoyer du courrier électronique à la racine pour chaque échec de tentative d'autorisation entrée dans syslog.

Remarque - Vous pouvez reconfigurer ce fichier. Par défaut, il est configuré de la façon suivante :

`/var/log/badauth:/usr/bin/mailx -s ``%f' ' root < %c` où :

- `/var/log/badauth` est le fichier où les entrées sont effectuées.
 - `/usr/bin/mailx -s` est la commande à envoyer à root.
 - “%f” est la ligne de sujet du message, contenant le nom de fichier où les entrées ont été détectées, et
 - “%c” est le nouveau contenu du fichier `syslog`.
-

Création de scripts définis par l'utilisateur

Cette section décrit certaines mises à jour d'installation et/ou de configuration dont vous pouvez prévoir l'exécution après l'installation de Solaris for ISPs. Ces paramètres peuvent être écrits sous forme de script Shell. Par exemple, vous pouvez écrire une commande similaire à : `echo "foo" >> /etc/ftpusers`

Le chemin à ce script que vous créez peut être enregistré lors de la configuration de l'hôte (écran `Post-Configuration Command`) pour l'installation de Solaris for ISPs. Vous pouvez également chaîner ces commandes. Cette commande de post-configuration que vous fournissez sera exécutée par un script de post-installation de Solaris for ISPs pendant l'installation en différé.

Remarque - La création de ce script est facultative.

Certains exemples de configuration système post-installation dont vous pouvez prévoir l'exécution dans votre script après l'installation sont illustrés dans les paragraphes suivants. Par exemple :

- Ecrivez un programme pour vérifier et confirmer les modifications apportées à la configuration système.
- Ecrivez un programme pour notifier ou imprimer la disponibilité d'espace disque après l'installation.
- Ecrivez un programme pour reconfigurer les messages de notification depuis syslog pour les échecs d'entrée d'autorisation. Reportez-vous à “Gestion de fichier journal” , page 39.
- Ecrivez un programme pour configurer d'autres logiciels indépendants.

- Ecrivez un programme pour configurer un hôte DNS :
 - Entrer des adresses IP de serveur DNS dans `/etc/hosts`.
 - Configurer `/etc/resolv.conf`.
 - Modifier `/etc/nsswitch.conf`.

Remarque - Les configurations de serveur DNS traitées dans cette section sont présentées uniquement à titre indicatif. Vous ne devez pas reconfigurer votre serveur DNS existant. Veuillez vous reporter à un document approprié pour reconfigurer votre serveur DNS afin de supporter la demande d'extensions et de services Solaris for ISPs pour des recherches de noms régulières.

Restauration des paramètres AWS par défaut

Sun Internet Administrator utilise un serveur Web pour les fonctions d'administration effectuées à partir de son interface utilisateur. Ce serveur Web est qualifié d'AWS (Administration Web Server). Vous pouvez, si nécessaire, reconfigurer le serveur Web d'administration en fonction de vos besoins. Reportez-vous à l'aide en ligne pour cette tâche. Pour garantir que vous ne perdez pas la configuration par défaut, cette section décrit l'emplacement des fichiers de configuration de serveur Web d'administration et la méthode permettant de restaurer les valeurs par défaut.

Les fichiers de configuration par défaut du serveur Web d'administration se trouvent dans `/etc/opt/SUNWixamc/awsconf/default/*` et `/var/opt/SUNWixamc/awsconf`. Lors de la reconfiguration du serveur Web d'administration, seules les configurations de fichier `/var/opt/SUNWixamc/awsconf` doivent être changées.

Pour restaurer les valeurs par défaut, copiez `/etc/opt/SUNWixamc/awsconf/default/*` dans `/var/opt/SUNWixamc/awsconf`.

Remarque - Pour assurer le fonctionnement effectif de la console Sun Internet Administrator, *ne modifiez pas* les valeurs par défaut dans `aws.conf`, `site.conf`, `map.conf`, `realms.conf` et `access.acl`.

Configuration requise

Ce chapitre décrit les conditions préalables à la pré-installation de Solaris for ISPs. Veuillez lire attentivement ces informations et vous assurer que les hôtes réseau remplissent tous les prérequis spécifiés.

Prérequis d'installation

Cette section présente la configuration minimale pour la pré-installation d'extensions de plate-forme et de services Solaris for ISPs.

- configuration minimale du système d'exploitation
 - Version de Solaris
 - Patches de système d'exploitation
- Configuration matérielle minimale
 - UC
 - Espace disque
 - RAM
 - Espace d'échange
- Navigateur Web supporté
- Dépendance des composants
 - Dépendance sur les logiciels
 - Ports de composants par défaut

Configuration minimale du système d'exploitation

Cette section décrit la configuration minimale du système d'exploitation telle que la version de Solaris requise pour l'installation et le fonctionnement des extensions de plate-forme et des services Solaris for ISPs, et les patchs de système d'exploitation que vous devez télécharger.

Version de Solaris

La version de Solaris requise pour l'installation et l'utilisation des extensions de plate-forme et des services Solaris for ISPs est *Solaris 2.6 et versions ultérieures*.

Patchs à télécharger

Cette section décrit les patchs de système d'exploitation pour SPARC et x86. Reportez-vous au numéro de patch approprié à votre système et téléchargez-le. Veuillez lire cette section lors de la préparation du ou des serveurs hôte pour l'installation de Solaris for ISPs.

Mettez à niveau le système d'exploitation en téléchargeant les patchs suivants à partir de <http://www.access1.sun.com/Products/ISP/>.

Remarque - *Ces patchs Solaris 2.6 pour le système d'exploitation sont requis pour le bon fonctionnement des extensions de plate-forme et des services Solaris for ISPs.*

TABLEAU 4-1 Patchs de système d'exploitation requis

Description du patch	Patch SPARC #	Patch x86 #
SunOS 5.6 : patch libc & watchmalloc	105210-03	105211-03
SunOS 5.6 : patch /kernel/fs/hsfs	105486-02	105487-02
SunOS 5.6 : patch /kernel/drv/glm	105580-03	ND
SunOS 5.6 : patch /usr/lib/nfs/mountd	105615-03	105616-03
SunOS 5.6 : patch adb & kadb	106031-02	ND
SunOS 5.6 : patch de mise à jour du noyau	105181-06	105182-06
SunOS 5.6 : patch /usr/sbin/rpcbind	105216-02	105217-02
SunOS 5.6 : patch /kernel/drv/ssd	105356-01	ND

TABLEAU P-1 Patches de système d'exploitation requis *(suite)*

Description du patch	Patch SPARC #	Patch x86 #
SunOS 5.6 : patch /kernel/drv/ses	105357-01	ND
SunOS 5.6 : patch de pilote sf et social	105375-04	ND
SunOS 5.6 : patch /kernel/misc/nfssrv	105379-01	105380-01
SunOS 5.6 : patch /usr/bin/at	105393-01	105394-01
SunOS 5.6 : patch /usr/bin/volrmmount	105407-01	105408-01
SunOS 5.6 : patch /usr/bin/vacation	105518-01	105519-01
SunOS 5.6 : patch /kernel/fs/fifofs	ND	105581
SunOS 5.6 : patch /usr/lib/nfs/mountd	105615-03	105616-03
SunOS 5.6 : patch libbsm	105621-01	105662-01
SunOS 5.6 : patch /usr/bin/login	105665-01	105666-01
SunOS 5.6 : patch /usr/bin/rdist	105667-01	105668-01
SunOS 5.6 : patch /kernel/drv/ip	105786-01	105787-01

Remarque - Ces patches Solaris 2.6 pour le CDE 1.2 et les pages de manuel sont requis pour le bon fonctionnement des extensions de plate-forme et des services Solaris for ISPs.

TABLEAU 4-2 Patches de système d'exploitation recommandés

Description du patch	Patch SPARC #	Patch x86 #
CDE 1.2 : patch dtlogin	105703-03	ND
CDE 1.2 : patch dtpad	105558-01	ND
CDE 1.2 : patch libDtSvc	105669-02	ND
SCDE 1.2 : patch dtappgather	105837-01	ND
Patch de bibliothèque d'exécution Motif 1.2.7 ¹	105284-08	105285-08
Patch de page manuelle pour la bibliothèque client LDAP	106497-01	106498-01
Patch de page manuelle ²	105390-02	106061-02
Patch SGML ²	106123-02	106124-01

1. Ce patch améliore le gestionnaire de fenêtre Motif pour assurer la compatibilité avec la trousse d'outils JDK 1.1.5.

TABLEAU P-2 Patches de système d'exploitation recommandés (suite)

2. Vous aurez besoin de ces patches pour afficher les pages de manuel Solaris for ISPs.

Configuration matérielle minimale

Cette section décrit le matériel tel que l'UC, l'espace disque, la RAM et l'espace d'échange requis pour l'installation de Solaris for ISPs.

Extensions de plate-forme Solaris for ISPs

Cette section traite de la configuration matérielle minimale pour l'installation d'extensions de plate-forme Solaris for ISPs.

TABLEAU 4-3 Configuration matérielle minimale pour les extensions de plate-forme

Extensions de plate-forme Solaris for ISPs	UC	Espace disque	RAM	Espace d'échange
	Recommandé	Minimum	Recommandé	Recommandé
Solaris for ISPs ¹	Système biprocesseur haut de gamme	4 Go	256 Mo	1 Go
Plate-forme Solaris for ISPs ²		3 Mo	ND	ND
Sun Internet Administrator		1 Mo	64 Mo	64 Mo
Sun Directory Services		50 Mo	64 Mo	
Serveur de licence FlexLM	Station de travail haut de gamme	3 Mo	NA	NA
Sun Internet Services Monitor		5 Mo	64 Mo	1 Mo
Sunscreen™ SKIP1.1.1 ³		10 Mo	32 Mo	
JDK 1.1.5		3 Mo		
HotJava 1.1.4		9 Mo	32 Mo	

1. La configuration minimale spécifiée ici concerne une installation de tous les composants Solaris for ISPs sur une seule machine.
2. Ce composant *devant* être installé sur chaque machine et exécutant un composant Solaris for ISPs, assurez-vous que cette configuration minimale est satisfaite par chaque machine Solaris for ISPs sur le réseau.
3. Allez à <http://www.sun.com/security/skip/> pour plus d'informations.

Services Solaris for ISPs

Cette section décrit la configuration matérielle minimale pour l'installation de services Solaris for ISPs.

TABLEAU 4-4 Configuration matérielle minimale pour Services

Services Solaris for ISPs	UC	Espace disque	RAM
	Recommandé	Minimum	Minimum
Sun Internet FTP Server		23,1 Mo	64 Mo
Sun Internet News Server		2-20 Go ¹	64 Mo
SWS	Station de travail haut de gamme	4 Mo + fichiers de documents et de journaux	64 Mo

1. Cette spécification s'étend en fonction de l'extension de la base de données des groupes de discussion.

Navigateur Web supporté

Le navigateur web supporté par les extensions de plate-forme et services Solaris for ISPs est Sun Microsystems HotJava 1.1.4.

Dépendance des composants

Cette section décrit les dépendances de composant sur les progiciels et les ports de composant par défaut.

Dépendance sur les progiciels

Cette section décrit les dépendances des extensions de plate-forme et des services Solaris for ISPs sur les progiciels requis et recommandés intégrés et indépendants.

TABLEAU 4-5 Dépendance des composants de Solaris for ISPs

Progiciels requis et recommandés	Pour extensions et services Solaris for ISPs	Où les trouver?
JDK/JRE 1.1.5	Tous les composants Solaris for ISPs nécessitent ce progiciel.	Fourni en standard
SSL	SWS, Sun Internet Administrator, Sun Internet FTP Server, Sun Internet News Server	Fourni en standard
SKIP	Sun Internet Administrator ¹	Fourni en standard
JavaIDL	Sun Internet FTP Server, Sun Internet News Server	Fourni en standard
PGP 5.0	Sun Internet News Server ²	Allez à http://www.nai.com/default_pgp.asp ³

1. SKIP est recommandé côté serveur pour ce composant.

2. Ce progiciel est *recommandé* pour l'authentification du message de contrôle.

3. Pour plus d'informations sur les clés publiques PGP spécifiques des groupes de discussion, allez à <http://www.isc.org/inn.html>

Ports de composants par défaut

Solaris for ISPs utilise les ports suivants :

- 8000 est le port par défaut pour le serveur Web temporaire utilisé pour l'installation par le logiciel de configuration d'hôte.
- 50080 est le port par défaut pour le serveur Web d'administration utilisé par SunTM Internet AdministratorTM.
- 1760 est le port par défaut pour SunTM Directory Services.
- 2380 est le port par défaut pour SunTM WebServerTM (SWS).
- 2381 est le port par défaut pour SunTM Internet Services MonitorTM.

Utilisation des services de répertoire

Solaris™ for ISPs™ utilise Sun™ Directory Services pour stocker des informations de composant logiciel et des informations de connexion pour Sun™ Internet Administrator™ et certains services. Ces informations incluent des classes d'objet standard et de nouveaux objets définis supportant les fonctionnalités de Solaris for ISPs.

Ce chapitre présente des informations sur la structure arborescente des informations de Solaris for ISPs, sur la création d'entrées dans l'arborescence, depuis la ligne de commande, et sur les contrôles d'accès requis. Pour plus d'informations sur l'extension de schéma proprement dite, consultez le Chapitre 6.

Sun Directory Services fournit les outils suivants pour utiliser et administrer le répertoire :

- L'outil Deja, éditeur de répertoire Java, fournit, ajoute, modifie et supprime des possibilités.
- La console d'administration Sun Directory Services offre une administration locale et distante du serveur.
- La passerelle Web autorise un accès par navigateur depuis n'importe quel navigateur.
- Un jeu complet de programmes de ligne de commande.

Vous trouverez dans les manuels Sun Directory Services, *Sun Directory Services 3.1 Administration Guide* et *Sun Directory Services 3.1 User's Guide*, des informations complètes sur le démarrage et l'emploi de ces outils. Ils sont présentés dans le format AnswerBook2 sur le CD-ROM du produit. Les programmes de ligne de commande sont documentés dans des pages de manuel à la section 1 (/opt/SUNWconn/man).

Structure de répertoires Solaris for ISPs

Solaris for ISPs nécessite une structure spécifique dans l'arborescence d'informations de répertoires (DIT), qui est créée pendant l'installation et la configuration. La structure requise est composée de deux contextes de noms, qualifiés d'arborescence OSI (Open Systems Interconnection) et d'arborescence DC (Domain Component). Des parties de ces deux arborescences sont parallèles. Cette structure parallèle simplifie le mappage des noms de domaine d'une requête DNS aux entrées de contenu réelles dans l'arborescence OSI, en passant par l'arborescence DC.

Structure d'arborescence OSI

L'arborescence OSI contient les entrées réelles de Solaris for ISPs, ses services de composant, les administrateurs de ses services et les abonnés de ces services. La structure requise est illustrée dans la Figure 5-1.

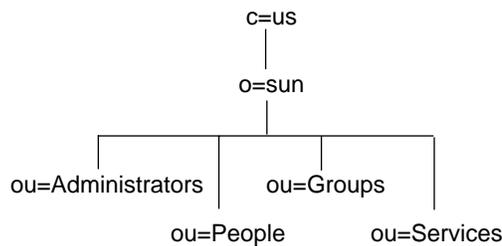


Figure 5-1 Arborescence OSI de Solaris for ISPs

Dans l'arborescence OSI, l'entrée du domaine sun.com est représentée par l'entrée portant le nom distinctif o=sun,c=us. Cette entrée est qualifiée de *domaine racine* et représente l'entreprise du client de Solaris for ISPs. Vous spécifiez le nom du domaine racine pendant l'installation des services de répertoire.

Sous le domaine racine, on retrouve quatre entrées `organizationalUnit` obligatoires :

- *Administrators* contient les entrées des administrateurs Sun™ Internet Administrator™. Ces entrées sont créées par le produit lors de la création d'administrateurs à l'aide de l'interface utilisateur graphique.
- *People* contient les entrées des abonnés aux services ISP. Vous créez des entrées pour vos clients, sur la ligne de commande ou en utilisant l'outil Deja.
- *Groups* contient des entrées regroupant des entrées d'abonné à des fins de contrôle d'accès. Vous créez des entrées de groupe adaptées à vos besoins, sur la ligne de commande ou à l'aide de l'outil Deja.

- *Services* contient des entrées créées pour des services Solaris for ISPs. Vous devez créer des entrées sous cette unité uniquement lorsque vous intégrez un nouveau service ou que vous effectuez une configuration d'hôte virtuelle spéciale de Sun™ Internet FTP Server™. Reportez-vous à l'aide en ligne de Sun Internet FTP Server et de Sun Internet Administrator pour plus d'informations sur cette caractéristique.

Les *noeuds People*, *Groups* et *Services* sont requis sous chaque entrée de domaine que vous définissez. Le noeud *Administrators* existe uniquement sous le domaine racine.

La Figure 5-2 illustre un jeu d'entrées classiques sous chaque unité organisationnelle.

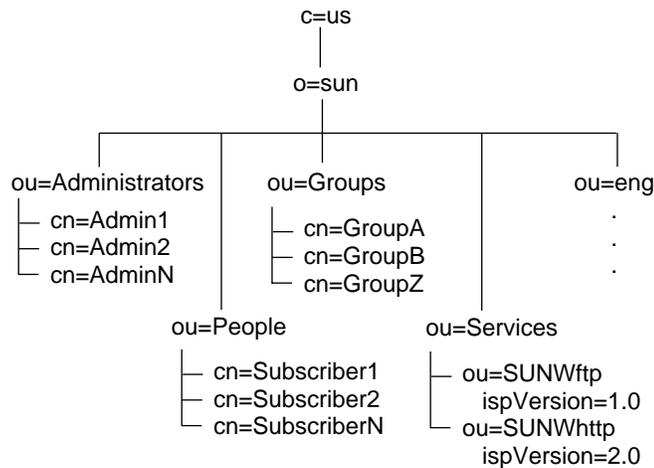
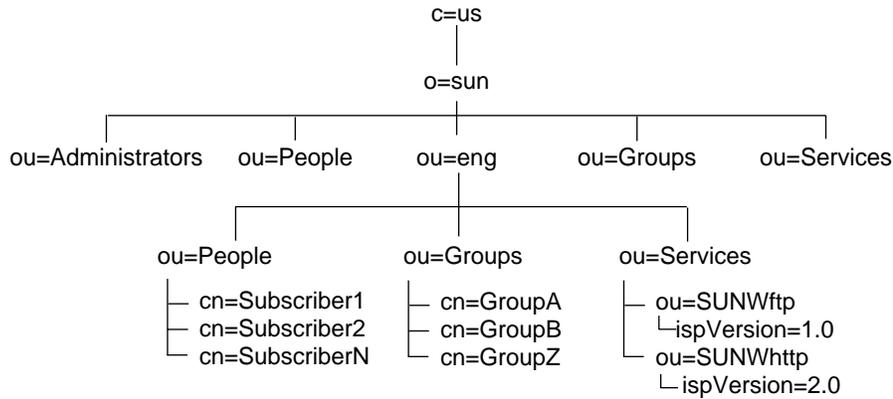


Figure 5-2 Entrées d'arborescence OSI

L'entrée `organizationalUnit eng` est un exemple d'une entrée *domain*. Elle peut correspondre à un client entreprise de l'ISP ou à quiconque ayant des services d'hébergement de domaine virtuel chez l'ISP. Les domaines doivent avoir deux entrées : une ici dans l'arborescence OSI et une autre dans l'arborescence DC pour le mappage de nom de domaine. Reportez-vous à "Création d'entrées de domaine", page 55 pour plus d'informations sur la création de ces deux entrées.

Les domaines, le domaine racine par exemple, nécessitent certaines entrées `organizationalUnit`. Tel qu'illustré dans la Figure 5-3, les entrées *People*, *Groups* et *Services* sont également requises dans un domaine sous la racine.



Remarque : les entrées de données dans le domaine racine sont omises pour plus de clarté.

Figure 5-3 Structure de domaine dans l'arborescence OSI

Lors de la création d'une entrée de domaine dans l'arborescence OSI, vous devez également créer des entrées pour *People*, *Groups* et *Services*. Lors de la configuration de services pour ce domaine, les entrées de service sont effectuées sous l'unité organisationnelle *Services*. Les informations d'abonné pour ce domaine forment les entrées `ispSubscriber` sous l'unité organisationnelle *People*.

Remarque - Les entrées Administrator sont effectuées sous le domaine racine dans cette version de Solaris for ISPs. Ces entrées sont créées par Sun Internet Administrator lors de leur spécification par l'intermédiaire de l'interface utilisateur graphique.

Structure arborescente DC

L'arborescence DC (composant de domaine) mappe le format de nom de domaine (par exemple sun.com) au nom distinctif de l'entrée correspondante dans l'arborescence OSI. Tel qu'illustré dans la Figure 5-4, la DC est généralement relativement plate et plus simple que l'arborescence OSI.

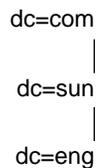


Figure 5-4 Arborescence DC de Solaris for ISPs

Dans la Figure 5-4, l'entrée `dc=sun,dc=com` correspond à l'entrée `o=sun,c=us` dans l'arborescence OSI. Le domaine `eng` est mappé ici à la forme de serveur de nom de domaine (DNS) `eng.sun.com`.

Pour plus de détails sur la création des deux entrées de domaine, reportez-vous à "Création d'entrées de domaine", page 55.

Création d'entrées de répertoire depuis la ligne de commande

Vous trouverez des informations générales sur la création d'entrées de service de répertoire au chapitre 5, "Loading and Maintaining Directory Information," du manuel *Sun Directory Services 3.1 Administration Guide*. Vous trouverez dans cette section des instructions sur la création des entrées spécifiques requises par Solaris for ISPs.

Pour plus d'informations sur la création d'entrées de répertoire à l'aide de l'outil *Deja*, reportez-vous à l'aide en ligne de Sun™ Internet Administrator™.

Création d'entrées de répertoire : Procédure générale

Sun Directory Services possède les utilitaires de ligne de commande suivants pour créer et modifier les entrées de répertoire :

- `ldapadd`
- `ldapmodify`
- `ldapdelete`

Ces utilitaires de ligne de commande de service de répertoire nécessitent un accès racine. Ils sont entièrement documentés dans les pages de manuel de référence (section 1).

`ldapadd` et `ldapmodify` peuvent prendre une entrée de la ligne de commande ou d'un fichier spécifié. Les informations pour une entrée pouvant être relativement longues et complexes, les sections qui suivent décrivent la forme nécessitant un fichier texte.

Dans chaque cas, la création d'une entrée (ou de plusieurs entrées) implique les interventions suivantes :

1. **Ecrire un fichier spécifiant l'entrée ou les entrées à effectuer dans le répertoire. Le format de ce fichier est spécifié dans la page de manuel de référence `ldif(4)`.**
2. **Obtenir un accès racine et créer l'entrée à l'aide de `ldapadd`, spécifiant le fichier contenant les informations de l'entrée.**

Dans chaque cas, la forme de la commande `ldapadd` doit être la suivante :

```
# ldapadd -D "BindDN" -w password -f file
```

Où *BindDN* est le nom distinctif (DN) de la liaison au répertoire avec un accès en écriture à cette partie de l'arborescence de répertoire, et *password* le mot de passe de la liaison. Remplacez l'option *file* par le nom du fichier `ldif` que vous avez créé.

Structure d'un fichier `ldif(4)`

Pour chaque entrée que vous ajoutez dans la ligne de commande, vous créez un fichier de format `ldif` pour contenir les informations sur l'entrée. Ces fichiers sont de simples fichiers texte avec une ou plusieurs entrées de répertoire, chacune étant séparée par une ligne vierge. Chaque entrée a la structure de l'exemple suivant.

Remarque - Seuls les attributs obligatoires sont indiqués dans l'exemple. La plupart des classes d'objet ont plusieurs attributs facultatifs pouvant être définis en fonction de votre utilisation particulière de l'entrée.

```
dn: ou=wgate1,ou=eng,o=sun,c=US
ou: wgate1
associateddomain: wgate1.eng.sun.com
objectclass: organizationalUnit
objectclass: domainRelatedObject
```

Où

dn	Indique le nom distinctif de l'entrée créée.
ou	Est l'attribut de nom de l'entrée créée. Les attributs de nom commun incluent <code>commonName</code> , <code>organizationalUnit (ou)</code> et <code>domainComponent (dc)</code> .
associatedDomain	Contient le nom de domaine (en note point) de l'entrée correspondante dans l'arborescence DC. Pour plus d'informations sur l'interaction entre l'arborescence OSI et l'arborescence DC, reportez-vous à "Structure de

répertoires Solaris for ISPs” , page 50. Pour plus d’informations sur la création des deux entrées de référence croisée d’un domaine, consultez “Création d’entrées de domaine” , page 55.

Il peut y avoir plusieurs paires attribut:valeur dans cette position, une par ligne.

objectClass Est la classe d’objet (type) de l’entrée. Il peut y avoir plusieurs entrées `objectClass` ; cet exemple en illustre deux.

Pour des informations plus détaillées sur les classes d’objet et les attributs disponibles, reportez-vous au Chapitre 6 de ce guide et au chapitre 8, “Configuring the Directory Schema” du manuel *Sun Directory Services 3.1 Administration Guide*.

Création d’entrées de domaine

Pour créer un domaine dans le répertoire, vous devez créer deux entrées de domaine parallèles, l’une dans l’arborescence OSI et l’autre dans l’arborescence DC, puis créer les entrées `organizationalUnit` sous l’entrée de domaine dans l’arborescence OSI.

Pour créer le domaine `wcgate1` sous `eng.sun.com`, procédez comme suit :

1. Editez un fichier texte (par exemple, `domain.ldif`) et entrez les données de l’entrée d’arborescence OSI :

```
dn: ou=wcgate1,ou=eng,o=sun,c=US
ou: wcgate1
associateddomain: wcgate1.eng.sun.com
objectclass: organizationalUnit
objectclass: domainRelatedObject
```

Sachez que l’attribut `associatedDomain` de l’entrée contient le nom de l’entrée d’arborescence DC en note point (style DNS).

2. Ajoutez à `domain.ldif` les données de l’entrée d’arborescence DC :

```
dn: dc=wcgate1,dc=eng,dc=sun,dc=com
dc: wcgate1
associatedname: ou=wcgate1,ou=eng,o=sun,c=US
description: DNS-to-DN Mapping for wcgate1.eng.sun.com
labeleduri: ldap:///ou=wcgate1,ou=eng,o=sun,c=US??sub
objectclass: domain
objectclass: labeledURIObject
```

Sachez que l'attribut `associatedName` de l'entrée contient le nom distinctif de l'entrée d'arborescence OSI. L'attribut `labeledURI` contient les mêmes informations (telles que spécifiées dans RFC 2255).

3. Ajoutez à `domain.ldif` les données de l'entrée d'unité organisationnelle Services requises :

```
dn: ou=Services,ou=wcgate1,ou=eng,o=sun,c=US
ou: Services
objectclass: organizationalUnit
```

4. Ajoutez à `domain.ldif` les données de l'entrée d'unité organisationnelle People requises :

```
dn: ou=People,ou=wcgate1,ou=eng,o=sun,c=US
ou: People
objectclass: organizationalUnit
```

5. Ajoutez à `domain.ldif` les données de l'entrée d'unité organisationnelle Groups requises :

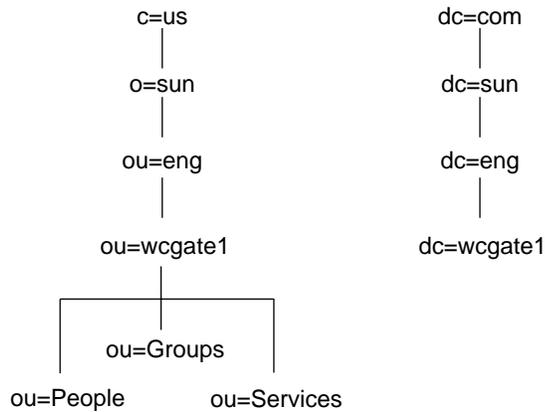
```
dn: ou=Groups,ou=wcgate1,ou=eng,o=sun,c=US
ou: Groups
objectclass: organizationalUnit
```

6. Enregistrez et fermez `domain.ldif`.

7. Obtenez un accès racine et ajoutez les entrées au répertoire avec la commande suivante, en remplaçant le DN et le mot de passe de liaison par les vôtres :

```
# ldapadd -D "cn=admin,o=sun,c=US" -w password -f domain.ldif
```

Lorsque votre `ldapadd` est terminé, le répertoire a l'aspect présenté dans la Figure 5-5.



Remarque : certaines entrées sont omises pour plus de clarté.

Figure 5-5 Arborecence de répertoire avec un domaine ajouté

Création d'entrées d'abonné

Il existe plusieurs variétés d'abonnés de Solaris for ISPs :

- L'abonné général (de base)
- L'abonné qui utilise les services FTP ou Web à hôte virtuel
- L'abonné qui a accès aux services par l'intermédiaire d'un serveur RADIUS
- L'abonné qui utilise les deux et dont l'entrée de répertoire nécessite à la fois des informations RADIUS et FTP

Dans les sections qui suivent, des instructions sont fournies pour construire l'entrée d'abonné complexe en créant l'entrée simple et en procédant par ajouts dans celle-ci.

Création d'une entrée d'abonné de base

Avant de créer des entrées d'abonné, les entrées de domaine et d'unité organisationnelle *People* doivent exister. Une fois que vous avez créé ces entrées, vous pouvez éditer un fichier texte (par exemple `people.ldif`) et entrer les données pour l'abonné. L'entrée d'abonné de base a la classe d'objet unique `ispSubscriber` et quelques attributs obligatoires. Le fichier pour un abonné de base a l'aspect suivant :

```

dn: cn=Jane Doe (jldoe),ou=People,ou=wcgate1,ou=eng,o=sun,c=US
commonname: Jane Doe (jldoe)
sn: Doe
uid: jldoe
  
```

(suite)

userpassword: hidden
objectclass: ispSubscriber

Où

dn	Est le nom distinctif de l'entrée d'abonné.
commonName	Est l'attribut de nom d'une entrée d'abonné (classe d'objet <code>ispSubscriber</code>). Pour les abonnés et les administrateurs Solaris for ISPs, la valeur de l'attribut <code>commonName</code> prend la forme Prénom Nom (userid) .
sn	Est le nom de l'abonné.
uid	Est le nom de connexion de l'abonné.
userPassword	Est le mot de passe, limité à huit caractères si vous partagez des informations de mot de passe avec des comptes UNIX. Cette valeur est générée avec la méthode de cryptage que vous avez définie dans la console d'administration des services de répertoire.

objectClass: ispSubscriber Est le type de classe d'objet de l'entrée d'abonné.

Vous pouvez créer n'importe quel nombre d'entrées d'abonné en ajoutant des blocs de données avec différentes valeurs d'attribut au fichier. Une fois cette opération terminée, enregistrez et fermez `people.ldif`. Obtenez un accès racine et ajoutez les entrées de l'abonné dans le répertoire avec la commande suivante, en remplaçant le lien DN et le mot de passe par les vôtres :

```
# ldapadd -D "cn=admin,o=sun,c=US" -w password -f people.ldif
```

Ajout d'informations d'hôte virtuel FTP et Web

Les informations requises pour l'hébergement virtuel spécialement configuré avec Sun™ Internet FTP Server™ et Sun™ WebServer™ (SWS) ajoutent uniquement trois attributs au fichier de données :

gidnumber: 60001
uidnumber: 60001
ispcontentdirectory: jldoe

Où

gidNumber	Est l'ID de groupe UNIX spécifié pour cet utilisateur dans le domaine à hôte virtuel pour les services FTP et Web.
uidNumber	Est l'ID utilisateur UNIX spécifié pour cet utilisateur dans le domaine hébergé virtuellement pour les services FTP et Web.
ispContentDirectory	Est l'emplacement (par rapport à la racine de document du domaine associé) où se trouve le fichier de contenu de cet abonné.

Remarque - La définition des valeurs des attributs `uidNumber` et `gidNumber` impliquent que les comptes UNIX existants soient correctement configurés pour partager l'accès au domaine FTP virtuel. Reportez-vous à l'aide en ligne de Sun Internet FTP Server pour obtenir des informations sur la définition d'une configuration d'hôte virtuel.

Vous pouvez créer n'importe quel nombre d'entrées d'abonné en ajoutant des blocs de données au fichier. Une fois cette opération terminée, enregistrez et fermez `people.ldif`. Obtenez un accès racine et ajoutez les entrées de l'abonné dans le répertoire avec la commande suivante, en remplaçant le lien DN et le mot de passe par les vôtres :

```
# ldapadd -D "cn=admin,o=sun,c=US" -w password -f people.ldif
```

Si vous avez déjà créé ces entrées, vous pouvez effectuer une opération `ldapmodify`. Localisez la page de manuel de `ldapmodify(1)` et suivez ces instructions.

Ajout d'informations utilisateur distant

Une entrée pour un abonné ayant accès aux services ISP par l'intermédiaire d'un serveur RADIUS doit supporter une classe d'objet supplémentaire (`remoteUser`) et a plusieurs attributs ajoutés aux informations de l'entrée.

Remarque - La configuration Solaris for ISPs par défaut désigne le domaine racine comme base de recherche pour les entrées d'abonné RADIUS. Si votre configuration est différente, utilisez la console d'administration des services de répertoire pour configurer RADIUS et entrez les valeurs adaptées à votre base de recherche.

Les lignes supplémentaires dans le fichier `ldif` sont les suivantes :

```
objectclass: remoteUser
authsuffixname: @ispexpress
grpcheckinfo: authSuffixName
grpcheckinfo: userPassword
authserviceprotocol: Framed-User
framedrouting: None
framedprotocol: PPP
grpreplyinfo: authServiceProtocol
grpreplyinfo: framedProtocol
grpreplyinfo: framedRouting
```

Où

objectClass: remoteUser	Est une classe d'objet obligatoire pour l'abonné accédant aux services à l'aide d'un serveur RADIUS.
authsuffixname: @ispexpress	Est un suffixe ajouté au nom d'utilisateur de l'abonné pour permettre au serveur RADIUS d'établir une distinction entre les entrées portant le même <code>uid</code> dans différents domaines. Entrez le suffixe approprié pour l'entrée d'utilisateur spécifique.
grpcheckinfo: authSuffixName	Indique que le serveur RADIUS doit vérifier la valeur d'attribut <code>authSuffixName</code> avant de sélectionner l'entrée pour authentification.
grpcheckinfo: userPassword	Indique que le serveur RADIUS doit vérifier la valeur d'attribut <code>userPassword</code> avant de sélectionner l'entrée à authentifier.
authserviceprotocol: Framed-User	Si vous utilisez la configuration RADIUS par défaut, entrez cet attribut tel qu'indiqué. La valeur correcte est déterminée par la configuration de votre serveur d'accès réseau.
framedrouting: None	Si vous utilisez la configuration RADIUS par défaut, entrez cet attribut tel quel. La valeur correcte est déterminée par la configuration de votre serveur d'accès réseau.

framedprotocol: PPP	Si vous utilisez la configuration RADIUS par défaut, entrez cet attribut tel qu'indiqué. La valeur correcte est déterminée par la configuration de votre serveur d'accès réseau.
grpreplyinfo: authServiceProtocol	Demande au serveur RADIUS d'inclure la valeur de l'attribut <code>authServiceProtocol</code> dans son message de réponse.
grpreplyinfo: framedProtocol	Demande au serveur RADIUS d'inclure la valeur de l'attribut <code>framedProtocol</code> dans son message de réponse.
grpreplyinfo: framedRouting	Demande au serveur RADIUS d'inclure la valeur de l'attribut <code>framedRouting</code> dans son message de réponse.

Vous pouvez créer n'importe quel nombre d'entrées d'abonné en ajoutant des blocs de données au fichier. Une fois cette opération terminée, enregistrez et fermez `people.ldif`. Obtenez un accès racine et ajoutez les entrées de l'abonné dans le répertoire avec la commande suivante, remplaçant le DN de liaison et le mot de passe par les vôtres :

```
# ldapadd -D "cn=admin,o=sun,c=US" -w password -f people.ldif
```

Si vous avez déjà créé ces entrées, vous pouvez effectuer une opération `ldapmodify`. Localisez la page de manuel de `ldapmodify(1)` et suivez ces instructions.

Le fichier `ldif` terminé

Le fichier `ldif` terminé pour un utilisateur complexe a l'aspect suivant :

```
dn: cn=Jane Doe (jldoe),ou=People,ou=wcgate1,ou=eng,o=sun,c=US
commonname: Jane Doe (jldoe)
sn: Doe
uid: jldoe
userpassword: hidden
gidnumber: 60001
uidnumber: 60001
objectclass: ispSubscriber
objectclass: remoteUser
ispcontentdirectory: /home/users/jldoe
authsuffixname: @ispexpress
grpcheckinfo: authSuffixName
grpcheckinfo: userPassword
authserviceprotocol: Framed-User
```

(suite)

```

framedrouting: None
framedprotocol: PPP
gpreplayinfo: authServiceProtocol
gpreplayinfo: framedProtocol
gpreplayinfo: framedRouting

```

Création d'entrées de groupe

Avant de pouvoir créer des entrées de groupe, un certain nombre d'entrées doit déjà exister :

- Les deux entrées de domaine (arborescences OSI et DC)
- L'entrée d'unité organisationnelle *Group*
- Les entrées d'abonné (sous le noeud *People*) qui deviendront les membres du groupe.

Une fois que vous avez créé ces entrées, vous pouvez démarrer un fichier texte (par exemple, `groups.ldif`) et entrer les entrées pour le groupe. Un jeu de données typique a l'aspect suivant :

```

dn: cn=isp-gp1,ou=Groups,ou=wcgate1,ou=eng,o=sun,c=US
cn: isp-grp1
objectclass: groupOfNames
member: cn=Ed Anchor (anchor),ou=People,ou=wcgate1,ou=eng,o=sun,c=US
member: cn=April Shower (showers),ou=People,ou=wcgate1,ou=eng,o=sun,c=US
member: cn=Chili Jones (relleno),ou=People,ou=wcgate1,ou=eng,o=sun,c=US

```

Où

dn	Est le nom distinctif du groupe à créer.
cn	Est le nom distinctif relatif de l'entrée de groupe.
objectClass	La classe d'objet <code>groupOfNames</code> distingue ce type d'entrée.
member	Chaque attribut <code>member</code> prend comme valeur le nom distinctif d'une entrée d'abonné existante.

Vous pouvez créer n'importe quel nombre d'entrées de groupe en ajoutant des données au fichier. Une fois qu'il est terminé, enregistrez et fermez `groups.ldif`. Obtenez un accès racine et ajoutez les groupes au répertoire avec la commande suivante, en remplaçant le DN de liaison et le mot de passe par les vôtres :

```
# ldapadd -D "cn=admin,o=sun,c=US" -w password -f groups.ldif
```

Contrôle d'accès Solaris for ISPs

Solaris for ISPs définit un contrôle d'accès pour les services de répertoire, pour garantir un accès approprié par les parties du logiciel qui le nécessitent, tout en assurant la sécurité et en empêchant l'accès par d'autres. Le principe général de ces contrôles d'accès veut que toutes les entités ont des accès en lecture tandis que l'accès en écriture est restreint. Il est très important que vous ne changiez pas les contrôles d'accès existants, car vous pourriez introduire des risques concernant la sécurité ou provoquer le blocage de Solaris for ISPs.

Souvenez-vous que les règles de contrôle d'accès sont tributaires de l'ordre d'utilisation. Lorsque Sun Directory Services procède à des vérification d'accès, la première règle qui s'applique à la requête est employée. Toutes les règles suivantes sont ignorées. Par conséquent, ne changez pas l'ordre des règles dans le fichier. Lors de la création d'une nouvelle règle, veillez à ce qu'elle ne s'applique pas accidentellement à des informations de Solaris for ISPs existantes et annule certaines règles de contrôle d'accès déjà mises en oeuvre.

Remarque - Le contrôle d'accès est désactivé si vous effectuez une liaison au répertoire comme administrateur.

Généralement, les informations spécifiques de Solaris for ISPs sont stockées dans des entrées prenant en charge des classes d'objet définies dans l'extension de schéma Solaris for ISPs. Chacune de ces classes est nommée en commençant par la chaîne "isp." Toute règle dans le fichier de configuration d'accès qui contient une telle classe d'objet (ou attribut) est probablement une règle Solaris for ISPs et, en tant que telle, est soumise aux modifications. Les règles de contrôle d'accès sont définies dans `/etc/opt/SUNWconn/ldap/current/dsserv.acl.conf`.

Pour terminer les informations sur les contrôles d'accès Sun Directory Services, reportez-vous au chapitre 1, "Introduction to Directory Concepts," et au chapitre 4, "Configuring a Directory Server," du manuel *Sun Directory Services 3.1 Administration Guide*.

Les sections qui suivent décrivent le comportement général assuré par les contrôles d'accès Solaris for ISPs. La phrase "a accès" indique qu'une liaison au répertoire avec le DN et le mot de passe de cette entrée donnera la forme d'accès indiquée.

Règles d'activation des fonctionnalités de Sun Internet Administrator

Sun Internet Administrator a besoin des types d'accès suivants pour effectuer son travail :

- Il doit créer et supprimer des administrateurs. Par conséquent, Sun Internet Administrator a un accès en écriture à la partie du DIT définie par l'entrée d'unité organisationnelle `Administrators`.
- Il doit être en mesure de changer certains attributs d'administrateur (notamment les attributs `userPassword` et `ispAuthorizedServices`).
- Il doit être capable de contrôler la création d'entrées de service géré (`ispManagedService`). Par conséquent, Sun Internet Administrator possède sa propre partie de l'arborescence, sous l'entrée de niveau supérieur `SUNWixamc` (par exemple, `ispVersion=1.0,ou-SUNWixamc,ou-Services,o=sun,c=us`).
- Il doit créer des entrées de service de niveau supérieur pour les services qu'il enregistre et gère. Par conséquent, Sun Internet Administrator a l'accès et les informations dont il a besoin pour écrire dans cette partie du DIT (par exemple, `ou-Services,o=sun,c=us`).
- Il doit également définir la valeur de l'attribut `ispPrivateData` protégé sur les entrées `ispService`. Par conséquent, Sun Internet Administrator a un accès en lecture/écriture à cet attribut des entrées de service existant. En fait, aucune autre entité n'a accès à l'attribut `ispPrivateData`.

Règles activant les fonctionnalités de service

Les divers services Solaris for ISPs doivent enregistrer et accéder à des informations de configuration stockées sous leurs entrées de service (celles situées sous le noeud `Services` dans les sous-domaines et les domaines virtuels). Par conséquent, chacun a l'accès et les informations qu'il doit écrire pour créer et modifier des entrées dans cette partie du DIT, notamment sa propre entrée de service.

Règles d'activation de l'accès utilisateur approprié

Les utilisateurs (abonnés et administrateurs) ont un accès en écriture à leur propre attribut `password`, mais ne peuvent pas changer d'autres parties de leur entrée. Cependant, n'importe quel administrateur avec un accès de gestion à Sun Internet Administrator a un accès global et peut changer n'importe quoi.

Schéma des services de répertoire Solaris for ISPs

Solaris™ for ISPs™ étend le schéma standard défini dans Sun™ Directory Services. Le schéma de base est défini au chapitre 8, “Configuring the Directory Schema” du manuel *Sun Directory Services 3.1 Administration Guide*. Les extensions au schéma de base, classes et attributs sont décrites dans ce chapitre.

Remarque - Le schéma défini par Solaris for ISPs est instable dans cette première version du produit. Les définitions de classe et d’attribut d’objet faisant partie de l’extension du schéma peuvent changer sans avertissement dans les versions ultérieures.

Maintenance du schéma

En général, vous ne devez pas changer les classes ou les attributs d’objet dans le schéma, mais plutôt les utiliser ou y apporter des ajouts en fonction de vos besoins. Si vous changez un attribut ou une classe d’objet de telle sorte que le logiciel Solaris for ISPs ne peut pas l’utiliser, vous devrez éventuellement réinstaller le répertoire. Dans ce cas, toute entrée non sauvegardée sera perdue. Pour plus d’informations sur la sauvegarde du répertoire, reportez-vous aux pages de manuel Sun Directory Services pour `ldbmcats` et `ldif2ldb`.

Si vous décidez d’apporter des ajouts au schéma, reportez-vous au chapitre 8, “Configuring the Directory Schema,” du manuel *Sun Directory Services 3.1 Administration Guide* pour plus de détails.

Que faut-il sauvegarder?

Pour assurer l'intégrité du répertoire, vous devez périodiquement sauvegarder les fichiers de configuration du schéma. Il convient de sauvegarder le schéma avant de commencer à travailler pour l'étendre à vos propres utilisations.

Tel que décrit de façon détaillée au chapitre 4, "Configuring Directory Services," du manuel *Sun Directory Services 3.1 Administration Guide*, les fichiers suivants sont critiques pour la fonction des services de répertoire :

- `dsserv.conf` contient les informations de configuration principales.
- `dsserv.oc.conf` contient les définitions de classes d'objet.
- `dsserv.at.conf` contient les définitions d'attribut.
- `dsserv.acl.conf` contient les informations de contrôle d'accès.

Des copies de ces fichiers sont stockées à trois endroits dans le système :

- `/etc/opt/SUNWconn/ldap/current` contient les fichiers de configuration courants.
- `/etc/opt/SUNWconn/ldap/default` contient les fichiers de configuration par défaut qui ont été installés avec le logiciel. Ces fichiers sont en lecture seule.
- `/etc/opt/SUNWconn/ldap/previous` contient les fichiers de configuration précédents.

Avant de commencer à travailler sur le schéma, sauvegardez les fichiers de configuration dans `/etc/opt/SUNWconn/ldap/current` et ceux contenus dans `/etc/opt/SUNWconn/ldap/previous`. Lorsque vous modifiez les fichiers, Sun Directory Services copie les fichiers non modifiés dans `~/current` à `~/previous`. Il n'effectue cette intervention qu'une seule fois par session d'édition (jusqu'à ce que vous redémarriez `dsservd`). Si vous apportez des modifications de schéma, vous souhaitez éventuellement créer des sauvegardes manuelles de vos modifications pendant votre travail.

Des informations sur la sauvegarde sont présentées de façon détaillée au chapitre 4, "Configuring Directory Services," du manuel *Sun Directory Services 3.1 Administration Guide*.

Restauration du schéma

Pour restaurer votre configuration de services de répertoire à une version précédente, arrêtez `dsservd`, remplacez les fichiers de configuration désirés dans `/etc/opt/SUNWconn/ldap/current` et redémarrez le démon. Des informations détaillées sont présentées au chapitre 4, "Configuring Directory Services," du manuel *Sun Directory Services 3.1 Administration Guide*.

▼ Restauration du schéma Solaris for ISPs

Lors de l'installation de Solaris for ISPs, les fichiers de configuration de schéma d'origine sont sauvegardés dans `/etc/opt/SUNWisp/SUNWconn/ldap/backup`. Ces fichiers sont personnalisés lors de l'installation avec votre domaine racine et vos informations d'administrateur. Si vous travaillez sur le schéma et si vous trouvez dans une situation où Solaris for ISPs ne fonctionne pas, restaurez le schéma par défaut de la façon suivante :

1. **Connectez-vous à la machine où s'exécutent les services de répertoire.**
2. **Attribuez-vous un accès racine.**
3. **Pour arrêter le serveur de services de répertoire, entrez :**
`# /etc/init.d/dsserv stop`

Remarque - Vous pouvez également arrêter et démarrer le serveur par l'intermédiaire de la console d'administration.

4. **Copiez chacun des fichiers de configuration de la sauvegarde dans le répertoire courant :**
 - a. `cp /etc/opt/SUNWisp/SUNWconn/ldap/backup/ispdsserv.conf /etc/opt/SUNWconn/ldap/current/dsserv.conf`
 - b. `cp /etc/opt/SUNWisp/SUNWconn/ldap/backup/ispdsserv.at.conf /etc/opt/SUNWconn/ldap/current/dsserv.at.conf`
 - c. `cp /etc/opt/SUNWisp/SUNWconn/ldap/backup/ispdsserv.oc.conf /etc/opt/SUNWconn/ldap/current/dsserv.oc.conf`
 - d. `cp /etc/opt/SUNWisp/SUNWconn/ldap/backup/ispdsserv.acl.conf /etc/opt/SUNWconn/ldap/current/dsserv.acl.conf`
 - e. `cp /etc/opt/SUNWisp/SUNWconn/ldap/backup/mapping/radius.mapping /etc/opt/SUNWconn/ldap/current/mapping/radius.mapping`
5. **Pour démarrer le serveur de services de répertoire, entrez :**
`# /etc/init.d/dsserv start`

Classes d'objet Solaris for ISPs

Cette section contient une liste de classes d'objet ajoutées au schéma de base de support de Solaris for ISPs. Il faut obligatoirement entrer une valeur pour les attributs indiqués comme obligatoires lors de la création de l'entrée. Les classes d'objet sont indiquées par ordre alphabétique.

Classe `ispAdministrator`

Objet : Définit une entrée représentant un administrateur de services et de réseaux ISP. Le nom distinctif relatif de `ispAdministrator` est l'attribut `commonName` et sa valeur. Son objet supérieur est `ispSubscriber`.

TABLEAU 6-1 Attributs `ispAdministrator`

Nom d'attribut	Obligatoire ?	Schéma	Objet
<code>associatedDomain</code>	Non	Base	Le domaine auquel cet administrateur est associé. Réserve pour une future fonctionnalité de Solaris for ISPs.
<code>commonName</code>	Oui	Base	Le nom de l'administrateur décrit par l'entrée, sous la forme Prénom Nom (id utilisateur).
<code>description</code>	Non	Base	Une description arbitraire de l'administrateur.
<code>gidNumber</code>	Non	Base	Un ID de groupe UNIX. Pour les services FTP ou Web à hôte virtuel, l'ID de groupe spécifié pour le domaine virtuel.
<code>homeDirectory</code>	Non	Base	L'emplacement du système de fichiers du répertoire d'origine de l'administrateur décrit par l'entrée. (Inutilisé par Solaris for ISPs).
<code>ispAdministeredService</code>	Non	Extension	Les noms distinctifs de services que cet administrateur est autorisé à gérer.

TABLEAU P-1 Attributs ispAdministrator (suite)

Nom d'attribut	Obligatoire ?	Schéma	Objet
ispContentDirectory	Non	Extension	Un emplacement de répertoire où se trouve le contenu appartenant à l'administrateur. Pour les services FTP ou Web à hôte virtuel, le chemin au contenu utilisateur relatif à ispRootDirectory.
labeledURI	Non	Base	L'URL (Uniform Resource Identifier) et l'étiquette associées à la page Web de cet administrateur.
mail	Non	Base	L'adresse de courrier électronique annoncée de l'administrateur.
objectClass	Oui	Base	La classe d'objet de l'entrée (ispAdministrator).
ou	Non	Base	L'unité organisationnelle à laquelle l'entrée appartient. Dans cette version de Solaris for ISPs, le noeud <i>Administrator</i> sous le domaine racine.
surname	Oui	Base	Le nom de famille de l'administrateur
userCertificate	Non	Base	Un certificat contenant la clé publique de l'administrateur.
userid	Oui	Base	Le nom de connexion de l'administrateur.
userPassword	Oui	Base	Le mot de passe de l'administrateur.
uidNumber	Non	Base	Un ID utilisateur UNIX. Pour les services FTP ou Web à hôte virtuel, l'ID utilisateur spécifié pour le domaine virtuel.

Classe `ispManagedService`

Objet : Définit une entrée représentant un service ISP géré par Sun Internet Administrator. Cette classe d'objet est réservée pour une utilisation par Sun Internet Administrator. Le nom distinctif relatif de `ispManagedService` est l'attribut `host` et sa valeur.

TABLEAU 6-2 Attributs `ispManagedService`

Nom d'attribut	Obligatoire ?	Schéma	Objet
<code>associatedName</code>	Non	Base	Le nom distinctif de l'entrée de service de niveau supérieur pour ce service.
<code>commonName</code>	Non	Base	Le nom convivial d'un service, pour affichage dans l'interface utilisateur graphique de Sun Internet Administrator.
<code>host</code>	Oui	Base	Le nom entièrement qualifié de l'hôte où le service est installé.
<code>ispCategory</code>	Non	Base	Le type d'interface utilisateur pris en charge par ce service. Reportez-vous à la section de l'attribut <code>ispCategory</code> pour plus de détails.
<code>ispImageFile</code>	Non	Extension	Le nom d'un fichier graphique GIF contenant l'icône de ce service.
<code>ispServiceLocation</code>	Non	Extension	Le chemin à l'application d'administration X pour ce service.
<code>ispParameterizedOperation</code>	Non	Extension	Informations sur un utilitaire de ligne de commande pris en charge acceptant les paramètres.

TABLEAU P-2 Attributs `ispManagedService` (suite)

Nom d'attribut	Obligatoire ?	Schéma	Objet
<code>ispServlets</code>	Non	Extension	Le nom de classe Java entièrement qualifié d'un servlet utilisé dans cette interface utilisateur d'administration du service.
<code>ispServletClasspath</code>	Non	Extension	Le chemin de classe Java pour les classes requises par cette interface utilisateur d'administration du service.
<code>ispSupportedOperation</code>	Non	Extension	Informations sur un utilitaire de ligne de commande supporté n'acceptant aucun paramètre.
<code>ispVersion</code>	Non	Extension	Le numéro de version (majeur.mineur) du service décrit par l'entrée.
<code>labeledURI</code>	Non	Base	Le chemin à la page d'interface utilisateur graphique principale d'un service. Pour un service à 3 couches, entrez le chemin relatif à la racine du document. Pour un service à 2 couches, entrez l'URL complète.
<code>objectClass</code>	Oui	Base	La classe d'objet de l'entrée (<code>ispManagedService</code>).

Classe `ispService`

Objet : Définit une entrée représentant un composant logiciel Solaris for ISPs. Le nom distinctif relatif d'`ispService` est l'attribut `ispVersion` et sa valeur.

TABLEAU 6-3 Attributs `ispService`

Nom d'attribut	Obligatoire ?	Schéma	Objet
<code>associatedDomain</code>	Non	Base	Le domaine auquel ce service est associé.
<code>commonName</code>	Oui	Base	Le nom du service (inutilisé dans Solaris for ISPs).
<code>description</code>	Non	Base	Une description arbitraire du service.
<code>host</code>	Non	Base	Le nom entièrement qualifié de l'hôte où le service est installé.
<code>ispDirectoryRoot</code>	Non	Extension	Un préfixe de répertoire vers un emplacement dans le système de fichiers où un contenu de domaine est hébergé virtuellement. Utilisé par Sun Internet FTP Server et SWS dans une configuration d'hôte virtuelle.
<code>ispPrivateData</code>	Non	Extension	Informations de mot de passe du composant logiciel à utiliser par Sun Internet Administrator. Cet attribut est protégé par des ACL contre tout accès par un utilisateur autre que la racine du répertoire et Sun Internet Administrator.
<code>ispServiceContext</code>	Non	Extension	Un contexte de nom CORBA employé par Sun Internet FTP Server et Sun Internet News Server.

TABLEAU P-3 Attributs `ispService` (suite)

Nom d'attribut	Obligatoire ?	Schéma	Objet
<code>ispServiceLocation</code>	Non	Extension	Une référence d'objet CORBA au serveur d'administration de services. (Utilisée par Sun Internet FTP Server et Sun Internet News Server.)
<code>ispSupplementaryInformation</code>	Non	Extension	Informations arbitraires sur le service. Réservee pour les besoins spécifiques des services Solaris for ISPs.
<code>ispVersion</code>	Oui	Extension	Le numéro de version (majeur.mineur) du service décrit par l'entrée.
<code>labeledURI</code>	Non	Base	Le chemin aux servlets d'une interface utilisateur graphique à trois couches.
<code>mail</code>	Non	Base	L'adresse de courrier électronique annoncée de l'utilisateur. Inutilisée par Solaris for ISPs.
<code>objectClass</code>	Oui	Base	La classe d'objet de l'entrée (<code>ispService</code>).
<code>userCertificate</code>	Non	Base	Un certificat contenant la clé publique de l'utilisateur.
<code>userPassword</code>	Non	Base	Le mot de passe de l'entrée, utilisé pour la liaison au répertoire.

Classe ispSubscriber

Objet : Définit une entrée représentant un abonné (client) de l'ISP. Le nom distinctif relatif d'ispSubscriber est l'attribut commonName et sa valeur. Son objet supérieur est inetOrgPerson.

Si vous utilisez le serveur RADIUS fourni avec Sun Directory Services, recouvrez les objets ispSubscriber avec la classe d'objet remoteUser.

TABLEAU 6-4 Attributs ispSubscriber

Nom d'attribut	Obligatoire ?	Schéma	Objet
associatedDomain	Non	Base	Le domaine auquel cet abonné est associé.
commonName	Oui	Base	Le nom de l'abonné décrit par l'entrée, sous la forme Prénom Nom (id utilisateur).
gidNumber	Non	Base	Un ID de groupe UNIX. Pour les services FTP et Web à hôte virtuel, l'ID de groupe spécifiée pour le domaine virtuel.
homeDirectory	Non	Base	L'emplacement dans le système de fichiers du répertoire de connexion de l'abonné décrit par l'entrée (inutilisé par Solaris for ISPs).
host	Non	Base	Le nom entièrement qualifié de l'hôte. Inutilisé par Solaris for ISPs.
ispAuthorizedServices	Non	Extension	Les noms distinctifs des services que l'abonné est autorisé à employer.
ispContentDirectory	Non	Extension	Un emplacement de répertoire où se trouve le contenu appartenant à un abonné. Pour les services FTP et Web à hôte virtuel, le chemin relatif à ispRootDirectory.
labeledURI	Non	Base	L'URL et l'étiquette associées à la page Web de cet abonné.

TABLEAU P-4 Attributs ispSubscriber (suite)

Nom d'attribut	Obligatoire ?	Schéma	Objet
mail	Non	Base	L'adresse de courrier électronique annoncée de l'abonné.
objectClass	Oui	Base	La classe d'objet de l'entrée (ispSubscriber).
ou	Non	Base	L'unité organisationnelle à laquelle l'abonné appartient (dans Solaris for ISPs, le noeud <i>People</i> sous une entrée de domaine).
surname	Oui	Base	Le nom de l'abonné.
uidNumber	Non	Base	Un ID utilisateur UNIX. Pour les services FTP et Web à hôte virtuel, l'ID utilisateur spécifié pour le domaine virtuel.
userCertificate	Non	Base	Un certificat contenant la clé publique de l'abonné.
userid	Oui	Base	Le nom de connexion de l'abonné.
userPassword	Oui	Base	Le mot de passe de l'abonné.

Attributs Solaris for ISPs

Cette section décrit les attributs utilisés par les classes d'objet ajoutées au schéma de base de Solaris for ISPs. Certains de ces attributs font partie du schéma de base, mais sont inclus ici pour simplifier les choses. Les attributs créés par l'extension de schéma de Solaris for ISPs commencent par "isp."

Les attributs définis dans le schéma ont l'une des syntaxes suivantes :

- bin : binaire
- ces: chaîne respectant la casse (case-exact string)
Une chaîne alphanumérique respectant la casse.
- cis: chaîne ne respectant pas la casse (case-ignore string)

Une chaîne alphanumérique ne respectant pas la casse.

- dn: nom distinctif
- protected: crypté
Valeur qui a été cryptée à l'aide de crypt(1)
- int ou long: entier
- tel: numéro de téléphone
- utctime: heure UTC

La liste suivante présente les attributs par ordre alphabétique.

Attribut associatedDomain

Résumé : cis, valeurs multiples, schéma de base

Objet : Spécifie le domaine auquel l'objet décrit par l'entrée est associé. Pour l'entrée d'arborescence OSI d'un domaine, doit contenir le nom (en note point, par exemple, eng.sun.com) de l'entrée d'arborescence DC correspondante.

Attribut associatedName

Résumé : dn, schéma de base

Objet : Spécifie le nom distinctif d'une entrée associée à cette entrée. Pour l'entrée d'arborescence DC d'un domaine, doit contenir le nom distinctif de l'entrée d'arborescence OSI correspondante.

Attribut commonName

Nom secondaire : cn

Résumé : cis, valeurs multiples, schéma de base

Objet : Spécifie le nom complet de l'objet décrit par l'entrée.

Les entrées d'abonné et d'administrateur utilisent la forme *Prénom Nom (uid)*. Par exemple, l'utilisateur John Smith qui utilise le nom de connexion jsmith aurait une entrée dans le répertoire. Son attribut commonName prendrait la valeur John Smith (jsmith).

La classe d'objet ispManagedService utilise cet attribut pour le nom convivial affiché dans l'interface utilisateur graphique de Sun Internet Administrator GUI.

Attribut description

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Spécifie une description arbitraire de l'objet d'entrée.

Attribut gidNumber

Résumé : `long`, valeur unique, schéma de base

Objet : Spécifie un ID de groupe UNIX. Pour un abonné avec des services FTP à hôte virtuel, doit correspondre à l'ID de groupe spécifié pour le domaine virtuel.

Attribut homeDirectory

Résumé : `ces`, valeur unique, schéma de base

Objet : Spécifie l'emplacement dans le système de fichiers du répertoire de connexion de l'utilisateur décrit par l'entrée. Cet attribut n'est pas employé par Solaris for ISPs, mais est laissé pour des informations générales requises par le client.

Attribut host

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Spécifie le nom de la machine associée à ou gérée par l'objet décrit par l'entrée. Lorsqu'utilisé avec des entrées d'objet Solaris for ISPs, l'attribut `host` doit contenir le nom d'hôte entièrement qualifié.

Attribut ispAdministeredService

Résumé : `dn`, valeurs multiples, extension de schéma Solaris for ISPs

Objet : Spécifie les services (par noms distinctifs des entrées de service de niveau supérieur) qu'un administrateur peut gérer. L'entrée de niveau supérieur d'un service est l'objet `ispService` sous l'entrée de domaine racine. Par exemple, sous `ou=services,o=sun,c=us` où `sun.com` est l'entrée de domaine racine.

Attribut ispAuthorizedServices

Résumé : `dn`, valeurs multiples, extension de schéma Solaris for ISPs

Objet : Spécifie les services (par nom distinctif) qu'un `ispSubscriber` est autorisé à employer.

Attribut `ispCategory`

Résumé : `cis`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie la catégorie d'une interface utilisateur graphique supportée par le service décrit par l'entrée. Les valeurs acceptables sont les suivantes :

- `2tier`, indiquant que l'interface utilisateur est basée sur le Web et utilise l'architecture deux couches supportée par Sun Internet Administrator.
- `3tier`, indiquant que l'interface utilisateur est basée sur le Web et utilise l'architecture trois couches supportée par Sun Internet Administrator.
- `CLI`, indiquant que l'interface utilisateur est un utilitaire de ligne de commande.
- `X`, indiquant que l'interface utilisateur est un programme X.

Attribut `ispContentDirectory`

Résumé : `ces`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie un emplacement de répertoire (pouvant être différent de celui contenu dans l'attribut `homeDirectory`) où se trouve du contenu appartenant à un utilisateur. Utilisé par les classes `ispAdministrator` et `ispSubscriber`. Pour un utilisateur avec des services FTP à hôte virtuel, doit contenir le chemin (relatif à `ispDirectoryRoot` du domaine) au contenu FTP de l'utilisateur.

Attribut `ispDirectoryRoot`

Résumé : `ces`, valeur unique, extension de schéma de Solaris for ISPs

Objet : Spécifie un répertoire racine pour un service ISP, généralement par domaine.

Attribut `ispImageFile`

Résumé : `cis`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie le nom d'un fichier contenant l'image décrite par l'entrée. La classe d'objet `ispManagedService` utilise cet attribut pour spécifier son fichier d'icône au format GIF.

Attribut `ispPrivateData`

Résumé : `ces`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie les informations de mot de passe de composant logiciel employé par Sun Internet Administrator. Cet attribut est protégé par des ACL contre tout accès par des utilisateurs autres que l'administrateur racine Sun Directory Services.

Attribut `ispServiceContext`

Résumé : `ces`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie un contexte de service utilisé par un service ISP. Pour Sun Internet FTP Server et Sun Internet News Server, il s'agit ici d'un contexte de nom CORBA.

Attribut `ispServiceLocation`

Résumé : `ces`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie l'emplacement de l'objet `ispService` décrit par l'entrée.

Sun Internet FTP Server et Sun Internet News Server utilisent cet attribut dans un objet `ispService` pour stocker une référence d'objet chaîne CORBA à leurs serveurs d'administration. Sun Internet Administrator utilise cet attribut dans un objet `ispManagedService` pour stocker le chemin à une application d'interface utilisateur X.

Attribut `ispServlets`

Résumé : `ces`, valeurs multiples, extension de schéma Solaris for ISPs

Objet : Spécifie le nom de classe Java entièrement qualifié d'un servlet employé dans une interface utilisateur d'administration `ispManagedService`. Pour chaque servlet employé, affectez un attribut `ispServlets` avec la valeur suivante :

1. Le chemin au servlet, relatif à la racine de document du serveur Web d'administration (partie de Sun Internet Administrator)
2. Le nom de classe Java entièrement qualifié du servlet
3. Tout argument de servlet obligatoire, indiqué par nom et valeur

Attribut `ispServletClasspath`

Résumé : `ces`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie le chemin de classe Java pour les classes requises par une interface utilisateur d'administration `ispManagedService`. Un chemin de classe Java peut contenir plusieurs chemins ; séparez-les par des deux points (:).

Attribut `ispParameterizedOperation`

Résumé : `ces`, valeurs multiples, extension de schéma Solaris for ISPs

Objet : Spécifie des informations sur une fonction de ligne de commande prenant des paramètres. Pour un objet `ispManagedService`, trois champs d'information séparés par des espaces sont requis :

1. Le chemin complet à l'utilitaire de ligne de commande
2. Le chemin complet à un fichier d'aide pour l'utilitaire, ou `NONE`, s'il n'y a aucune information d'aide pour l'utilitaire.
3. Une chaîne arbitraire, contenant les paramètres séparés par des espaces requis par l'utilitaire. Si des paramètres de l'utilisateur sont acceptés sur la ligne de commande, ce champ contient la chaîne `SOME`.

Attribut `ispSupplementaryInformation`

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Contient des informations supplémentaires concernant l'objet décrit par l'entrée. Dans des classes d'objet qui étendent le schéma de base, cet attribut est réservé pour des besoins spécifiques des services Solaris for ISPs.

Attribut `ispSupportedOperation`

Résumé : `ces`, valeurs multiples, extension de schéma Solaris for ISPs

Objet : Stocke des informations sur un utilitaire de ligne de commande n'acceptant aucun paramètre. Pour un objet `ispManagedService`, trois champs d'information séparés par des espaces sont requis :

1. Le chemin complet à l'utilitaire de ligne de commande
2. Le chemin complet à un fichier d'aide pour l'utilitaire, ou `NONE`, s'il n'y a aucune information d'aide pour l'utilitaire.
3. La chaîne `NONE`.

Attribut `ispVersion`

Résumé : `cis`, valeur unique, extension de schéma Solaris for ISPs

Objet : Spécifie la version de diffusion de l'objet `ispService` décrit par cette entrée. Solaris for ISPs utilise la forme `majeur.mineur` pour l'attribut de version.

Attribut `labeledURI`

Nom secondaire : `labeledURL`

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Spécifie un identificateur de ressources uniforme (URI) et une étiquette associés à l'objet décrit par l'entrée.

Attribut `mail`

Nom secondaire : `preferredRfc822Originator`

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Spécifie l'adresse de courrier électronique annoncée, au format RFC822, de l'objet décrit par l'entrée. Sun Internet FTP Server utilise cet attribut comme adresse de rapport d'erreur.

Attribut `objectClass`

Résumé : `cis`, valeurs multiples, schéma de base

Objet : Spécifie la classe d'objet du type d'entrée.

Attribut `ou`

Nom secondaire : `organizationUnitName`

Résumé : `cis`, schéma de base

Objet : Spécifie le nom de l'unité organisationnelle à laquelle l'objet décrit par l'entrée appartient.

Attribut surname

Nom secondaire : sn

Résumé : cis, schéma de base

Objet : Spécifie le nom de la personne décrite par l'entrée.

Attribut uidNumber

Résumé : long, valeur unique, schéma de base

Objet : Spécifie un ID utilisateur UNIX. Pour un abonné avec des services FTP à hôte virtuel, peut être l'ID utilisateur spécifié pour le domaine virtuel.

Attribut userCertificate

Résumé : bin, schéma de base

Objet : Spécifie un certificat contenant la clé publique de l'utilisateur décrit par l'entrée.

Attribut userid

Nom secondaire : uid

Résumé : cis, valeurs multiples, schéma de base

Objet : Spécifie le nom de connexion de l'utilisateur décrit par l'entrée.

Attribut userPassword

Résumé : protected, valeurs multiples, schéma de base

Objet : Spécifie le mot de passe pour l'entité décrite par l'entrée.

Intégration d'applications de service existantes

Solaris™ for ISPs™ est conçu pour permettre l'intégration de vos services existants dans Sun™ Internet Administrator™. Lorsque vous intégrez ces services, ils tirent parti des avantages de l'administration centralisée à distance et de la gestion de compte d'administrateur assurées par ce produit. L'intégration d'une application dans Sun Internet Administrator, gérant l'accès administrateur, permet d'ajouter facilement à une application de service existante la sécurité d'autorisation d'administrateur.

Généralités concernant l'intégration d'un service existant

Pour intégrer et gérer des interfaces d'administration Web, X et ligne de commande avec Sun Internet Administrator, procédez comme suit.

1. Installez l'application de service sur un ordinateur accessible par Sun Internet Administrator par l'intermédiaire du réseau. Le composant de plate-forme Solaris for ISPs (SUNWisp) doit être installé sur cet ordinateur hôte pour fournir des extensions de plate-forme que Sun Internet Administrator utilise.
2. Exécutez la commande `mcreg(1m)` sur l'ordinateur hôte des services avec les paramètres adaptés à ce type de service. La forme de la commande `mcreg` est différente pour chaque type de service et est entièrement décrite ultérieurement dans ce chapitre ainsi que dans la page de manuel de cette commande. Vous devez avoir un accès racine pour exécuter `mcreg`.

Remarque - Vous devez exécuter de nouveau `mcreg` si vous changez l'URL ou d'autres informations de configuration de service (par exemple, si vous changez le port où un serveur Web est exécuté). Si vous exécutez `mcreg` plusieurs fois pour un service (sur une seule et même machine hôte), les informations ultérieures outrepassent les informations enregistrées précédemment.

3. Dans Sun Internet Administrator, gérez l'hôte de service et sélectionnez le nouveau service.
4. Egalement dans Sun Internet Administrator, créez des administrateurs avec un accès au nouveau service ou modifiez les administrateurs existants pour leur attribuer cet accès.

Vous devez être administrateur avec des droits de gestion de Sun Internet Administrator pour effectuer ces tâches.

Intégration des services X

Une fois que l'application de service est installée sur un ordinateur du réseau, exécutez la commande `mcreg(lm)` pour stocker des informations sur cette application. Ces informations sont utilisées par Sun Internet Administrator pour gérer correctement la présentation et lancer l'interface utilisateur graphique d'administration. Les informations dont vous avez besoin pour la commande `mcreg` sont les suivantes :

- L'identificateur du composant, une chaîne unique identifiant l'application de service. Ces indications étant uniques, Solaris for ISPs recommande l'utilisation de noms de progiciel comme identificateurs de composant. Le développeur d'application de service choisit l'identificateur du composant.
- Un nom convivial, adapté à la présentation de l'administrateur. C'est le nom du service que Sun Internet Administrator affiche dans son écran *Manage Services*, où l'administrateur accède à tous les services. Le développeur d'application de service choisit le nom de l'application.
- Le numéro de version de l'application enregistrée. Le format recommandé pour le numéro de version est *majeur.mineur* (par exemple, 1.2). Le développeur d'application de service choisit le numéro de version.
- Le chemin complet du fichier exécutable d'interface d'administration X sur l'hôte de service dans le système de fichiers.
- Le nom d'utilisateur sous lequel l'interface d'administration s'exécute. Cela identifie l'UID UNIX que Sun Internet Administrator emploie pour invoquer le programme.

- Le nom de groupe sous lequel l'interface d'administration s'exécute. Cela identifie le GID UNIX que Sun Internet Administrator utilise pour invoquer le programme.

Une fois que vous avez toutes les informations requises, obtenez un accès racine et enregistrez les informations telles qu'indiquées ci-dessous. Exécutez cette commande sur l'ordinateur où l'interface d'administration de service est installée.

```
# mcreg -c componentID -n name -vv version -x X_path -u user_name -g group_name
```

Reportez-vous à la page de manuel `mcreg(1m)` pour voir un exemple de cette forme de la commande.

Après l'exécution de `mcreg`, vous pouvez vous connecter à Sun Internet Administrator comme administrateur de console et enregistrer la nouvelle application pour gestion. Si vous souhaitez que d'autres administrateurs aient les droits d'accès nécessaires pour gérer la nouvelle application, modifiez leur accès administrateur pour l'inclure. Vous trouverez dans l'aide en ligne de Sun Internet Administrator des instructions complètes sur l'exécution de ces tâches.

Lorsqu'un administrateur invoque l'application X depuis Sun Internet Administrator, l'affichage est acheminé vers l'écran zéro (`hostname:0`) sur la machine client. Tout message `stdout` ou `stderr` généré par l'application X s'affiche sur l'écran X *Application Output* de Sun Internet Administrator.

Intégration de programmes de ligne de commande

Pour intégrer un programme d'administration de ligne de commande avec Sun Internet Administrator, exécutez la commande `mcreg(1m)` pour stocker des informations sur l'application. Ces informations sont utilisées par Sun Internet Administrator pour gérer correctement la présentation et lancer l'interface utilisateur graphique d'administration. Les informations dont vous avez besoin pour la commande `mcreg` sont les suivantes :

- L'identificateur de composant, chaîne unique identifiant l'application de service. Le développeur d'application de service choisit l'identificateur de composant.
- Un nom convivial, adapté à la présentation à l'administrateur. C'est le nom du service que Sun Internet Administrator affiche sur son écran *Manage Services*, où l'administrateur accède à tous les services. Le développeur d'application de service choisit le nom de l'application.
- Le numéro de version de l'application enregistrée. Le format recommandé pour ce numéro est *majeur.mineur* (par exemple, 1.2). Le développeur d'application de service choisit le numéro de version.

- Le chemin complet au programme de ligne de commande, plus des informations sur ses paramètres et une documentation. Placez cette option de commande entre guillemets (""). Il y a trois champs :
 - Le chemin complet au programme exécutable, avec d'éventuels paramètres statiques. Par exemple, `-p '/usr/bin/ps -ef'`. Ce champ est obligatoire.
 - `-a` indique que cette commande prend des paramètres de l'utilisateur au moment de l'exécution. Ce champ est facultatif.
 - `-h helpfile` indique la documentation en ligne associée à cette commande. Ce champ est facultatif.
- Le nom d'utilisateur sous lequel l'interface d'administration s'exécute. Cela identifie l'UID UNIX que Sun Internet Administrator emploie pour invoquer le programme.
- Le nom de groupe sous lequel l'interface d'administration s'exécute. Cela identifie le GID UNIX que Sun Internet Administrator utilise pour invoquer le programme.

Une fois que vous avez toutes les informations requises, obtenez un accès racine et enregistrez les informations telles qu'indiquées ci-dessous. Exécutez cette commande sur l'ordinateur où l'interface d'administration de service est installée.

```
# mcreg -c componentID -n name -p "prog_path [-a] [-h help_file]"... -vv version -u
    user_name -g group_name
```

Reportez-vous à la page de manuel `mcreg(1m)` pour des exemples sur cet aspect et d'autres formes de la commande.

Pour enregistrer des informations sur des opérations de ligne de commande multiples, entrez multiple `-p` arguments.

Après l'exécution de `mcreg`, vous pouvez vous connecter à Sun Internet Administrator comme administrateur de console et enregistrer la nouvelle application pour gestion. Si vous souhaitez que d'autres administrateurs aient des droits d'accès de gestion de la nouvelle application, modifiez leurs listes d'accès d'administrateur pour les inclure. Vous trouverez dans l'aide en ligne de Sun Internet Administrator des instructions complètes sur l'exécution de ces tâches.

Intégration d'applications Web deux couches

Une application Web deux couches est une application existante dont l'interface d'administration est accessible par l'intermédiaire d'un navigateur Web. Elle peut être mise en oeuvre en HTML, CGI ou Applets et Servlets Java (ou toute

combinaison de ces éléments). Ce type d'interface nécessite un serveur Web installé et s'exécutant sur l'ordinateur où le service est installé.

Cette interface étant accessible par l'intermédiaire d'URL, certains problèmes de sécurité doivent être pris en compte. L'interface doit être protégée par les ACL du serveur Web afin que seuls les administrateurs autorisés puissent y accéder. Pour tirer parti de la gestion d'administrateur assurée par Sun Internet Administrator, vous devez utiliser Sun™ WebServer™ (SWS) et le configurer avec les mêmes ACL que ceux employés par le serveur Web d'administration Sun Internet Administrator (voir "Configuration pour coordination des comptes d'administrateur" , page 88).

Pour sécuriser la connexion entre le navigateur et l'interface d'administration, envisagez l'utilisation d'un protocole HTTP (HTTPS) ou SKIP sécurisé. Reportez-vous à l'aide en ligne SWS et aux pages de manuel SKIP (`/opt/SUNWicp/man`) pour des instructions sur la configuration de ces outils de sécurité.

Enregistrement d'informations pour une application Web à deux couches

Une fois que l'application de service est installée sur un ordinateur du réseau, exécutez la commande `mcreg(1m)` pour stocker des informations sur cette application. Ces informations sont utilisées par Sun Internet Administrator pour gérer correctement la présentation et lancer l'interface utilisateur graphique d'administration. Les informations dont vous avez besoin pour la commande `mcreg` sont les suivantes :

- L'identificateur de composant (*componentID*) chaîne unique identifiant l'application du service. Ces indications étant uniques, Solaris for ISPs recommande l'utilisation de noms de progiciel comme identificateurs de composant. Le développeur d'application de service choisit l'identificateur de composant.
- Un nom convivial, *name*, adapté à la présentation de l'administrateur. Il s'agit du nom de service que Sun Internet Administrator affiche dans son écran *Manage Services*, où l'administrateur accède à tous les services. Le développeur d'application de service choisit le nom de l'application.
- Le numéro de version de l'application enregistrée. Le format recommandé pour le numéro de version est *majeur.mineur* (par exemple, 1.2). Le développeur d'application de service choisit le numéro de version.
- L'*URL* au point d'entrée de l'interface d'application Web. Entrez le chemin absolu (et non relatif).

Une fois que vous avez toutes les informations requises, obtenez un accès racine et enregistrez les informations telles qu'indiquées ci-dessous. Exécutez cette commande sur l'ordinateur où l'interface d'administration de service est installée.

```
# mcreg -c componentID -n name -vv version -w URL
```

Reportez-vous à la page de manuel `mcreg(1m)` pour voir un exemple de cette forme de la commande.

Après l'exécution de `mcreg`, vous pouvez vous connecter à Sun Internet Administrator comme administrateur de console et enregistrer la nouvelle application pour gestion. Si vous souhaitez que d'autres administrateurs aient des droits d'accès de gestion de la nouvelle application, modifiez leurs listes d'accès d'administrateur pour les inclure. Vous trouverez dans l'aide en ligne de Sun Internet Administrator des instructions complètes sur l'exécution de ces tâches.

Configuration pour coordination des comptes d'administrateur

Si l'application de service deux couches utilise SWS pour son interface d'administration, il est possible de configurer les ACL du serveur afin d'utiliser les mêmes informations de connexion d'administrateur que Sun Internet Administrator. Par conséquent, vous pouvez avoir un jeu unique de comptes d'administrateur (dans les services de répertoire) à gérer. Cela simplifie la gestion de ces comptes et améliore vos possibilités de réponse dans des situations pouvant compromettre la sécurité.

Vous devez d'abord installer SWS sur l'hôte de service (l'ordinateur où l'application de service est installée) et arranger les documents et fichiers d'interface dans l'arborescence de documentation du serveur. Ensuite, configurez SWS de la manière suivante :

1. Créez un objet realm dans le site Web par défaut de l'instance SWS :

```
# htrealm add -i instance -h hostname -r realmname -s ISPADMIN -d  
          ComponentID-VersionNo
```

Où

- *instance* est le nom de l'instance httpd configurée.
 - *hostname* est le nom de l'hôte contenant le realm.
 - *realmname* est le nom du realm que vous créez.
 - *ISPAdmin* est la source du realm. Entrez `ISPADMIN`, pour indiquer que ce sont des administrateurs Sun Internet Administrator.
 - *ComponentID-VersionNo* est le répertoire où se trouvent les fichiers d'interface utilisateur graphique d'administration (HTML et autres).
2. Ajoutez une protection ACL à l'URL où réside l'interface utilisateur graphique d'administration de ce service :

```
# htaccess add -i instance -h hostname -U URI -r realname -s BASIC
```

Où

- *instance* est le nom de l'instance httpd configurée.

- *hostname* est le nom de l'ordinateur où le serveur Web est exécuté.
 - *realmname* est le nom de l'objet realm que vous créez.
 - *BASIC* est le schéma d'authentification désiré. Entrez BASIC.
3. Redémarrez le site par défaut, s'il fonctionnait déjà. Utilisez l'interface utilisateur graphique d'administration de SWS pour effectuer cette tâche. Vous trouverez dans l'aide en ligne des instructions complètes.

Index

A

- annulation des modifications à Solaris, 38
- application X
 - intégration, 84
- applications de ligne de commande
 - intégration, 83, 85
- applications ligne de commande
 - spécification ispCategory, 78
- applications Web
 - coordination d'administrateurs, 88
 - enregistrement, 87
 - intégration, 83, 86
 - spécification ispCategory, 78
- applications X
 - intégration, 83
 - spécification ispCategory, 78
- approche d'installation, 8
- arborescence d'information de répertoire, 50
- arborescence d'interconnexion de système
 - ouvert, *Voir* arborescence OSI,
- arborescence DC
 - illustration, 52
 - structure, 52
- arborescence de composants de domaine, *Voir* arborescence DC,
- arborescence OSI
 - illustration d'entrées, 51
 - structure, 50
- architecture
 - applications deux couches, 13
 - applications trois couches, 11
 - Solaris for ISPs, 1
 - architecture deux couches, 10, 13
 - architecture du produit, 1
 - architecture trois couches, 10, 11
 - associatedDomain attribut, 76
 - associatedName attribut, 76
 - attribut (schéma SunDS)
 - ispServlets, 79
 - attributs (schéma SunDS), 75
 - associatedDomain, 76
 - associatedName, 76
 - cn (commonName), 76
 - commonName, 76
 - description, 77
 - définition de syntaxe, 75
 - gidNumber, 77
 - homeDirectory, 77
 - host, 77
 - ispAdministeredService, 77
 - ispAuthorizedServices, 77
 - ispCategory, 78
 - ispContentDirectory, 78
 - ispDirectoryRoot, 78
 - ispImageFile, 78
 - ispParameterizedOperation, 80
 - ispPrivateData, 79
 - ispServiceContext, 79
 - ispServiceLocation, 79
 - ispServletClasspath, 80
 - ispSupplementaryInformation, 80
 - ispSupportedOperation, 80
 - ispVersion, 81
 - labeledURI, 81
 - labeledURL (labeledURI), 81

- mail, 81
- objectClass, 81
- organizationUnitName (ou), 81
- ou, 81
- preferredRfc822Originator (mail), 81
- sn (surname), 82
- surname, 82
- uid (userid), 82
- uidNumber, 82
- userCertificate, 82
- userid, 82
- userPassword, 82

audit, 39

AWS, *Voir* serveur Web d'administration,

C

- caractéristiques matérielles
 - configuration de base, 28
 - configuration étendue, 29
- classes (schéma SunDS)
 - ispAdministrator, 68
 - ispService, 71
 - ispSubscriber, 74
- classes (schéma SunDSa)
 - ispManagedService, 70
- classes (SunDS schéma), 68
- classes d'objet (schéma SunDS), 68
 - ispManagedService, 70
 - ispService, 71
 - ispSubscriber, 74
- classes d'objet (SunDS schéma)
 - ispAdministrator, 68
- cn (commonName) attribut, 76
- commande mcreg, 83, 85 to 87
- commandes de post-configuration, *Voir* scripts définis par l'utilisateur,
- commonName attribut, 76
- conception du réseau, 27
 - exemple de configuration de base, 28
 - exemple de configuration étendue, 30
- configuration
 - AWS (Sun Internet Administrator), 41
 - Sun WebServer, 88
- configuration d'hôte
 - approche, 8
 - fonctions, 3
 - modèle, 9

- renforcement de la sécurité, 33
- réglage des services Solaris, 34
- répétable, 10
- configuration d'un réseau, 27
- configuration de
 - Sun Directory Services, 23
 - Sun Internet Administrator, 24
- configuration hôte
 - Modifications dans Solaris, 33
- configuration matérielle minimale, 46
- configuration minimale du système d'exploitation, 44
- configuration réseau
 - exemple de base, 28
 - exemple étendu, 29
- conservation de ressources, 36
- console de gestion, *Voir* Sun Internet Administrator,
- console, *Voir* Sun Internet Administrator,
- contextes de nom, 52
- contextes de noms, 50
- contrôle d'accès
 - Sun Directory Services, 63
 - SWS, 88
- cryptage, 5
- création d'entrées de répertoire, 53
 - abonnés, 57
 - domaines, 55
 - exemple ldif complet, 61
 - informations d'accès distant, 59
 - informations d'hôte virtuel, 58
 - procédure de ligne de commande, 53
 - unités organisationnelles de groupe, 62

D

- description attribut, 77
- directives d'installation, 27
- disposition d'un réseau, 27
- disposition de réseau
 - exemple de base, 28
 - exemple étendu, 29
- disposition de réseau de base, 28
- disposition réseau étendue, 29
- DIT, *Voir* arborescence d'information de répertoire,
- DNS, 29, 30

- domaine racine, 50
- domaines
 - domaine racine, 50
 - définition, 51
 - entrées de répertoire, 55, 76
 - structure dans DIT, 52
- durcissement et réglage, 32
- durcissement et réglage de Solaris, 3, 8, 33
- dépendance du logiciel, 47
- désinstallation de Solaris for ISPs, *Voir* Guide d'installation de Solaris for ISPs,
- détection d'intrusion, 3, 39

E

- enregistrement, 3, 39
- enregistrement de syslog, 39
- entrées d'abonné (SunDS), 57, 61
 - accès RADIUS, 59
 - entrée de base, 57
 - hôte virtuel, 58
- entrées d'unités organisationnelles, 50
- entrées, *Voir* Sun Directory Services, création d'entrées,
- espace d'échange requis, 46, 47
- espace disque requis, 46, 47
- extensions de plate-forme, 2
 - kit de développement Java, 6
 - logiciel de configuration d'hôte, 3
 - navigateur HotJava, 5
 - serveur de licence FlexLM, 5
 - Sun Directory Services, 4
 - Sun Internet Administrator, 2
 - Sun Internet Services Monitor, 3
 - Sunscreen SKIP, 5
- extensions, *Voir* extensions de plate-forme,

F

- fermeture de brèches de sécurité, 35
- fermeture des brèches de sécurité, 32
- fichier ldif
 - exemple complet, 61
 - structure, 54
- FlexLM, 5
- fonctions
 - FlexLM, 5

- kit de développement Java, 6
- logiciel de configuration hôte, 3
- navigateur HotJava, 5
- Solaris for ISPs, 1
- Sun Directory Services, 4
- Sun Internet Administrator, 2
- Sun Internet FTP Server, 8
- Sun Internet News Server, 7
- Sun Internet Services Monitor, 3
- Sun WebServer, 7
- SunScreen SKIP, 5
- fonctions de logiciel de configuration, 3
- FTP, *Voir* Sun Internet FTP Server,

G

- gestion de fichier journal, 3, 39
- gestion de processus de serveur, 3
- gidNumber attribut, 77
- groupe de discussion, *Voir* Sun Internet News Server,
- groupes (SunDS), 62

H

- homeDirectory attribut, 77
- host attribut, 77
- htaccess command, 88
- htrealm command, 88

I

- information d'hôte virtuel, 77, 82
- informations d'accès distant, 59
- informations d'hôte virtuel, 58
- installation de Solaris for ISPs
 - Voir également* Guide d'installation de Solaris for ISPs,
 - approche, 8
 - configuration matérielle minimale, 46
 - configuration minimale du système d'exploitation, 44
 - configuration requise, 43
 - exemple de scénario, 27
 - exemples de configuration de réseau, 27
 - logiciel de configuration d'hôte, 3
 - phase de planification, 18
 - phase de préparation, 20

- planification, 15
- processus, 15, 16
- présentation, 16
- tâches de post-installation, 25
- intégration d'applications, 83
 - applications de ligne de commande, 85
 - applications Web, 86
 - applications X, 84
- intégration de service
 - applications de ligne de commande, 85
 - applications Web, 86
 - applications X, 84
- intégration de services
 - architecture deux couches, 13
 - architecture trois couches, 11
- ispAdministeredService attribut, 77
- ispAdministrator classe, 63, 68
- ispAuthorizedService attribut, 63
- ispAuthorizedServices attribut, 77
- ispCategory attribut, 78
- ispContentDirectory attribut, 78
- ispDirectoryRoot attribut, 78
- ispImageFile attribut, 78
- ispManagedService classe, 63, 70
- ispParameterizedOperation attribut, 80
- ispPrivateData attribut, 63, 79
- ispService classe, 71
- ispServiceContext attribut, 79
- ispServiceLocation attribut, 79
- ispServletClasspath attribut, 80
- ispServlets attribut, 79
- ispSubscriber classe, 74
- ispSupplementaryInformation attribut, 80
- ispSupportedOperation attribut, 80
- ispVersion attribut, 81

J

JumpStart, xiv, 10

K

kit de développement Java, 6

L

- labeledURI attribut, 81
- labeledURL (labeledURI) attribut, 81
- LDAP, 4, 49

Index-94

Guide d'administration de Solaris for ISPs ♦ Novembre 1998

- ldapadd commande, 53
- ldapdelete commande, 53
- ldapmodify commande, 53

M

- mail attribut, 81
- maintance du schéma (SunDS), 65
- modifications dans Solaris, 33
 - exécutées une seule fois, 33
- modifications exécutées une fois dans Solaris, 33
- modifications reconfigurables dans Solaris, 34
 - conservation de ressources, 36
 - fermeture de brèches de sécurité, 35
- modifications système, 33
- modifications à Solaris
 - annulation de modifications, 38
 - reconfigurables, 34

N

- navigateur HotJava, 5
- Navigateur Web supporté, 47

O

- objectClass attribut, 81
- organizationUnitName (ou) attribut, 81
- ou attribut, 81
- outils d'administration
 - Sun Directory Services, 49
 - Sun Internet Administrator, 2, 10

P

- pages de manuel de patches, 45
- patches requis et recommandés, 44
- Planification de l'installation, 18
- planification du réseau, 27
- ports des composants, 84
- ports par défaut des composants, 48
- ports pour composants, 48
- preferredRfc822Originator (mail) attribut, 81
- Protection du réseau, 31
- protection du réseau, 32

R

RADIUS, 59, 74
RAM requise, 46, 47
recommandations pour l'installation, 27
renforcement de la sécurité, 32, 33
restauration du schéma (SunDS), 66
réglage des services Solaris, 34

S

sauvegarde du schéma, 66
schéma (SunDS), 65
 attributs, 75
 classes d'objet, 68
 maintenance, 65
 restauration, 66
 sauvegarde, 66
scripts (définis par l'utilisateur), 40
scripts de post-installation, *Voir* scripts définis
 par l'utilisateur,
scripts définis par l'utilisateur, 40
scénario, 9, 10
scénario de configuration, 9, 10
serveur de licence, 5
serveur Web d'administration, 41, 88
serveur Web, *Voir* Sun WebServer,
service de nom de domaine, *Voir* DNS,
services, 6
 Sun Internet FTP Server, 8
 Sun Internet News Server, 7
 Sun WebServer, 7
services de gestion, 10
services de répertoire, 4, 49
services Solaris, 34
SKIP, *Voir* SunScreen SKIP,
sn (surname) attribut, 82
Solaris for ISPs
 architecture, 1
 contrôle d'accès, 63
 problèmes de sécurité, 31
SPM, *Voir* gestion de processus de serveur,
structure de répertoire, 50
Sun Directory Services
 configuration après installation, 23
 contrôle d'accès, 63
 création d'entrées, 53, 57
 fonctions, 4
 groupes, 62

 outils d'administration, 49
 programmes de ligne de commande, 53
 rôle dans Solaris for ISPs, 49
 sauvegarde, 66
 schéma, 65
 structure de répertoire, 50
Sun Internet Administrator
 architecture deux couches, 13
 architecture trois couches, 11
 avantages relatifs à la sécurité, 10
 configuration après installation, 24
 fonctions, 2
 opérations, 11, 13
 services de gestion, 10
Sun Internet FTP Server, 8
Sun Internet News Server, 7
Sun Internet Services Monitor, 3
Sun WebServer
 configuration, 88
 fonctions, 7
SunDS, *Voir* Sun Directory Services,
SunScreen SKIP, 5
support FrontPage, 7
support servlet, 7
surname attribut, 82
surveillance, *Voir* Sun Internet Services
 Monitor,
SWS, *Voir* Sun WebServer,
sécurité
 fonctions, 10
 durcissement et réglage, 33
 logiciel de configuration d'hôte, 3
 SKIP, 5
 Sun Internet Administrator, 2
 SWS, 7
 patches, 44
 risques, 30
 Internet standard, 30
 Solaris for ISPs, 31

T

tâches de post-installation, 25

U

UC requise, 46, 47

uid (userid) attribut, 82
uidNumber attribut, 82
userCertificate attribut, 82
userid attribut, 82
userPassword attribut, 63, 82

V

version de Solaris, 44