



# Sun Java™ Desktop System Configuration Manager, Release 1 Guide d'installation

---

Sun Microsystems, Inc.  
4150 Network Circle  
Santa Clara, CA 95054,  
États-Unis 650-960-1300

Référence 817-5590-10

Avril 2004, révision A

# Copyrights and Trademarks

**Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.**

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.sun.com/patents> and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

This product is based in part on the work of the Independent JPEG Group and The FreeType Project.

Portions Copyright 2000 SuSE, Inc. Word for Word Copyright © 1996 Inso Corp. International CorrectSpell spelling correction system Copyright © 1995 by Lernout & Hauspie Speech Products N.V. All rights reserved.

Sun, Sun Microsystems, the Sun logo, Java, Solaris, StarOffice, the Butterfly logo, the Solaris logo, and the StarOffice logo are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd. Screen Beans and Screen Beans clipart characters are registered trademarks of A Bit Better Corporation.

Federal Acquisitions: Commercial Software - Government Users Subject to Standard License Terms and Conditions.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

**Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, Etats-Unis. Tous droits réservés.**

Sun Microsystems, Inc. a les droits de propriété intellectuelle relatants à la technologie incorporée dans ce produit. En particulier, et sans la limitation, ces droits de propriété intellectuelle peuvent inclure un ou plus des brevets américains énumérés à <http://www.sun.com/patents> et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et les autres pays.

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.

Ce produit repose en partie sur le travail de l'Independent JPEG Group et de The FreeType Project.

Portions Copyright 2000 SuSE, Inc. Word for Word Copyright © 1996 Inso Corp. Système de correction orthographique International CorrectSpell Copyright © 1995 de Lernout & Hauspie Speech Products N.V. Tous droits réservés.

Sun, Sun Microsystems, le logo Sun, Java, Solaris, StarOffice, le logo Butterfly, le logo Solaris et le logo StarOffice sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Les Screen Beans et les objets graphiques prédessinés Screen Beans sont des marques déposées de A Bit Better Corporation.

Acquisitions fédérales : logiciel commercial ; les utilisateurs gouvernementaux sont soumis aux conditions générales standard de la licence.

LA DOCUMENTATION est fournie « TELLE QUELLE » et TOUTES LES CONDITIONS, REPRÉSENTATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS TOUTE GARANTIE TACITE CONCERNANT LA QUALITÉ MARCHANDE, L'APTITUDE À UN USAGE PARTICULIER OU LA NON-VIOLATION DE DROITS DE TIERS SERONT REJETÉES, EXCEPTÉ DANS LE CAS OÙ L'EXCLUSION OU LA LIMITATION DE TELLES GARANTIES NE SERAIT PAS AUTORISÉE PAR LA LÉGISLATION EN VIGUEUR.

# Table des matières

---

<b>1 Introduction.....</b>	<b>5</b>
<b>2 Serveur LDAP.....</b>	<b>7</b>
Concepts.....	7
Configuration.....	8
Autres considérations.....	12
<b>3 Console Web de Sun™.....</b>	<b>13</b>
Configuration système requise.....	13
Installation de la Console Web de Sun.....	14
Exécution de la console.....	15
Désinstallation de la Console Web de Sun.....	15
Informations sur les ports de la Console Web de Sun .....	16
<b>4 Sun Java™ Desktop System Configuration Manager, Release 1.....</b>	<b>17</b>
Installation de Configuration Manager.....	17
Exécution de Configuration Manager.....	18
Désinstallation de Configuration Manager.....	18
<b>5 Composants de bureau.....</b>	<b>19</b>
Accès aux données / Authentification des utilisateurs.....	19
Configuration Agent.....	20
Adaptateur GConf.....	22
Adaptateur Mozilla.....	23
Adaptateur StarOffice.....	23
<b>6 Annexe A - Console Web de Sun.....</b>	<b>25</b>
Problèmes connus.....	25
Utilisation du script d'installation.....	25
Packages de la Console Web de Sun.....	26
<b>7 Annexe B - Configuration Manager.....</b>	<b>27</b>
Packages de Configuration Manager.....	27
<b>8 Annexe C.....</b>	<b>29</b>
Utilisation d'un serveur OpenLDAP avec Configuration Manager.....	29
Utilisation d'un serveur Active Directory avec Configuration Manager.....	30



## Introduction

---

Sun Java™ Desktop System Configuration Manager, Release 1 a été conçu pour fournir une configuration centralisée pour les hôtes de bureau exécutant Sun Java™ Desktop System. Les paramètres peuvent être assignés à différents éléments d'une structure organisationnelle, ce qui permet à l'administrateur de gérer facilement plusieurs groupes d'utilisateurs ou d'hôtes. Ses principaux composants sont les suivants :

- Un serveur LDAP comportant la structure organisationnelle des utilisateurs et des hôtes à gérer, destiné à recevoir les données de configuration ;
- Un outil de gestion Web permettant aux administrateurs de définir des données de configuration et d'assigner celles-ci aux éléments de la structure organisationnelle ;
- Des composants de bureau installés sur l'hôte du client qui extraient des données de configuration au nom de l'utilisateur actuellement connecté et les exposent aux diverses applications formant le système Java Desktop System.

L'outil de gestion est une application Web qui est exécutée dans la Console Web de Sun. Il permet à l'administrateur de parcourir la structure organisationnelle du serveur LDAP et d'assigner des stratégies à ses éléments. Les stratégies sont affichées et éditées en fonction de modèles de stratégies qui définissent les paramètres que l'outil de gestion manipulera.

Les composants de bureau sont organisés autour de l'agent Sun Java™ Desktop System Configuration Agent qui extrait les données de configuration du serveur LDAP au nom des utilisateurs et les met à disposition d'un certain nombre d'adaptateurs de système de configuration, qui complètent la configuration locale (paramètres par défaut fournis par les applications et paramètres d'utilisateur) avec les paramètres de stratégie. Les systèmes de configuration actuellement pris en charge sont GConf (qui gère la configuration des applications Gnome comme le bureau Gnome ou Evolution), les Préférences de Mozilla et StarRegistry (système de configuration de StarOffice).



## Serveur LDAP

---

### Concepts

Dans la structure de Java Desktop System Configuration Manager, les données de configuration sont associées à des entités qui constituent des entrées du référentiel LDAP et correspondent aux éléments de la structure organisationnelle de la société.

Les entités reconnues sont indiquées ci-dessous.

- Organisation : désigne généralement une unité organisationnelle (division, groupe, équipe) ou géographique (continent, pays, site) de la structure globale.
- Utilisateur : désigne un nœud terminal de la structure globale et, comme le nom le suggère, généralement un utilisateur.
- Domaine : désigne une unité de structure logique pour l'organisation du réseau.
- Hôte : désigne également un nœud terminal de la structure globale, mais fait référence à un ordinateur sur le réseau.
- Rôle : désigne des propriétés, généralement une distinction en termes de fonction (administrateur, gestion du site), appliquées à un ensemble d'utilisateurs.

Les entités d'organisation et d'utilisateur permettent de définir une arborescence d'utilisateurs, tandis que les entités de domaine et d'hôte définissent une arborescence d'hôtes. Ces deux arborescences sont indépendantes, mais sont manipulées de façon similaire dans la structure.

Le lien entre les entités d'organisation et de domaine et les autres entrées est défini par l'emplacement physique des entrées dans le référentiel. En d'autres termes, les entités d'organisation et de domaine peuvent inclure toute entrée située sous elles dans l'arborescence. Le lien entre les rôles et les utilisateurs ou hôtes est défini par les attributs des entrées d'utilisateur et d'hôte.

Les données de configuration associées à une entité sont stockées dans des entrées spéciales qui sont gérées par la structure. Ces entrées sont identifiées par le nom de service et le container de service associés aux entrées.

# Configuration

Pour pouvoir utiliser un serveur LDAP existant avec Configuration Manager, vous devez effectuer les opérations suivantes :

- Étendre le schéma du serveur afin qu'il prenne en charge les classes d'objet personnalisées et les attributs utilisés par Configuration Manager pour stocker les données de configuration ;
- Personnaliser et stocker sur le serveur les informations de mappage des entrées du référentiel ainsi que les entités prises en charge par Configuration Manager.

## Outils de déploiement

Les outils de déploiement suivants (fournis sur le CD-ROM d'installation) sont nécessaires pour utiliser un serveur LDAP existant avec Configuration Manager :

- `88apoc-registry.ldif` - Fichier de schéma introduisant les classes d'objet et les attributs nécessaires au stockage des données de configuration.
- `OrganizationMapping` - Fichier de propriétés par défaut décrivant le mappage entre les entrées LDAP et les entités de Configuration Manager.
- `UserProfileMapping` - Fichier de propriétés par défaut décrivant le mappage entre les attributs d'entrées d'utilisateur LDAP et les attributs de profils utilisateur de Configuration Manager.
- `createServiceTree` - Script stockant les fichiers de mappage dans le référentiel LDAP.
- `deployApoc` - Script étendant le schéma du serveur LDAP et stockant les fichiers de mappage dans le référentiel LDAP.

## Extension de schéma

Les données de configuration sont stockées dans des arborescences d'entrées qui sont liées aux entrées auxquelles les données sont associées. Avant de pouvoir stocker sur un serveur LDAP les classes d'objet et les attributs utilisés par ces arborescences, vous devez ajouter les objets et les classes au schéma du serveur LDAP. Par exemple, le fichier d'extension de schéma qui est fourni utilise le format LDIF pour ajouter ces objets et classes au serveur d'annuaire Sun Java System. Pour ajouter ces objets et classes à d'autres serveurs LDAP, vous devez utiliser un format reconnu par les serveurs.

## Mappage organisationnel

Le fichier de mappage organisationnel doit être édité pour définir le mappage entre les entrées LDAP et les entités de Configuration Manager. Il est nécessaire de fournir des valeurs correspondant au format du référentiel LDAP pour les différentes clés.

Les entités d'utilisateur sont identifiées par une classe d'objet que toutes les entités utilisent ainsi que par un attribut dont la valeur doit être unique dans tout le référentiel. Il est possible de fournir un format de nom d'affichage qui détermine la façon dont les utilisateurs seront affichés dans l'application de gestion. Le cas échéant, une entrée de container peut également être définie si une telle



entrée est utilisée par les entrées d'utilisateur d'une organisation. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# Classe d'objet utilisée par toutes les entrées d'utilisateur
User/ObjectClass=inetorgperson
# Attribut dont la valeur dans les entrées d'utilisateur est unique dans le référentiel
User/UniqueIdAttribute=uid
# Container facultatif dans les entrées d'organisation des entrées d'utilisateur ligne à supprimer s'il n'est pas utilisé)
User/Container=ou=People
# Format de nom d'affichage dans l'application de gestion
User/DisplayNameFormat=sn, givenname
```

Les entités de rôle sont identifiées par une liste de classes d'objet possibles qu'elles utilisent et par les attributs d'affectation de nom correspondants. Ces listes sont au format <élément1>,<élément2>,...,<élémentN> et doivent être alignées. Elles doivent en effet comporter le même nombre d'éléments et l'éniesième classe d'objet doit être utilisée avec l'éniesième attribut d'affectation de nom. Deux clés définissent le lien entre les rôles et les utilisateurs ainsi qu'entre les rôles et les hôtes. La clé VirtualMemberAttribute doit spécifier un attribut dont les valeurs peuvent être obtenues à partir d'une entrée d'utilisateur ou d'hôte. Elle doit également contenir les DN complets des rôles auxquels l'entrée appartient. La clé MemberAttribute doit spécifier un attribut d'une entrée d'utilisateur ou d'hôte pour le filtre de recherche. Elle doit également contenir les DN complets des rôles auxquels l'utilisateur ou l'hôte appartient. La clé VirtualMemberAttribute peut être un attribut virtuel de classe de service, tandis que la clé MemberAttribute doit être un attribut physique pouvant être utilisé dans un filtre. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# Liste des classes d'objet pour les rôles
Role/ObjectClass=nsRoleDefinition
# Liste alignée des attributs d'affectation de nom correspondants
Role/NamingAttribute=cn
# Attribut physique (utilisable dans un filtre) contenant les DN des rôles d'un utilisateur ou d'un hôte
Role/MemberAttribute=nsRoleDN
# Attribut dont l'interrogation sur un utilisateur ou un hôte renvoie aux DN des rôles auxquels il appartient
Role/VirtualMemberAttribute=nsRole
```

Les entités d'organisation sont identifiées d'une manière similaire aux rôles, avec deux listes alignées de classes d'objet et d'attributs d'affectation de nom correspondants. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# Liste des classes d'objet pour les organisations
Organization/ObjectClass=organization
# Liste alignée des attributs d'affectation de nom correspondants
Organization/NamingAttribute=o
```

Les entités de domaine sont identifiées d'une manière similaire aux entités d'organisation. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# Liste des classes d'objet pour les domaines
Domain/ObjectClass=ipNetwork
# Liste alignée des attributs d'affectation de nom correspondants
Domain/NamingAttribute=cn
```

Les entités d'hôte sont identifiées d'une manière similaire aux entités d'utilisateur. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# Classe d'objet utilisée par toutes les entrées d'hôte
Host/ObjectClass=ipHost
# Attribut dont la valeur dans les entrées d'hôte est unique dans le
référentiel
Host/UniqueIdAttribute=cn
# Container facultatif dans les entrées de domaine des entrées
d'hôte (ligne à supprimer s'il n'est pas utilisé)
Host/Container=ou=Hosts
```

## Mappage de profils utilisateur

Le fichier de mappage de profils utilisateur doit être édité pour définir le mappage entre les attributs d'entrées d'utilisateur LDAP et les attributs d'entités d'utilisateur de Configuration Manager. Chaque clé correspond à un attribut d'utilisateur de Configuration Manager. Une clé peut être assignée en tant que valeur au nom d'un attribut dans une entrée d'utilisateur, comme identifié par le mappage organisationnel. Les attributs utilisés dans le paramètre User/DisplayNameFormat doivent être assignés dans le mappage de profils utilisateur. Le nom des clés et leurs valeurs par défaut sont les suivants :

```
# inetOrgPerson.givenName
org.openoffice.UserProfile/Data/givenname = givenname
# person.sn
org.openoffice.UserProfile/Data/sn = sn
# inetOrgPerson.initials
org.openoffice.UserProfile/Data/initials = initials
# organizationalPerson.street
org.openoffice.UserProfile/Data/street =
street,postalAddress,streetAddress
# organizationalPerson.l (ville)
org.openoffice.UserProfile/Data/l = l
# organizationalPerson.st (État)
org.openoffice.UserProfile/Data/st = st
# organizationalPerson.postalCode
org.openoffice.UserProfile/Data/postalcode = postalcode
# country.c (pays)
org.openoffice.UserProfile/Data/c =
# organizationalPerson.o (société)
org.openoffice.UserProfile/Data/o = o,organizationName
# désapprouvé -- aucun corollaire LDAP
org.openoffice.UserProfile/Data/position =
# organizationalPerson.title
org.openoffice.UserProfile/Data/title = title
# inetOrgPerson.homePhone
org.openoffice.UserProfile/Data/homephone = homephone
# organizationalPerson.telephoneNumber
org.openoffice.UserProfile/Data/telephonenumber = telephonenumber
```

```
# organizationalPerson.facsimileTelephoneNumber
org.openoffice.UserProfile/Data/facsimiletelephonenumber =
facsimiletelephonenumber,officeFax
# inetOrgPerson.mail
org.openoffice.UserProfile/Data/mail = mail
```

## Déploiement

Une fois que les fichiers de mappage ont été personnalisés pour refléter l'état du référentiel LDAP, ils peuvent être déployés. Si le schéma du serveur LDAP contient déjà les classes d'objet et attributs requis, le script `createServiceTree` peut directement être exécuté ; sinon, le script `deployApoc` doit être exécuté.

Le script `deployApoc` est destiné à être utilisé avec les serveurs d'annuaire Sun Java System. Il copie dans le répertoire adéquat le fichier d'extension de schéma fourni et procède à une itération du serveur LDAP, puis appelle le script `createServiceTree`. Le script doit être exécuté par un utilisateur disposant des autorisations pour copier les fichiers dans le référentiel de schéma et redémarrer le serveur ; il est appelé avec la commande suivante :

```
./deployApoc <répertoire du serveur d'annuaire>
```

Le paramètre `<répertoire du serveur d'annuaire>` doit correspondre au chemin d'accès au sous-répertoire `slapd-<nom du serveur>` d'une installation de serveur d'annuaire. Si les répertoires par défaut ont été utilisés pour l'installation et que le serveur se nomme `monserveur.mondomaine`, ce répertoire correspond à `/var/Sun/mps/slapd-monserviceur.mondomaine`.

Qu'il soit appelé directement ou à partir du script `deployApoc`, le script `createServiceTree` demande à l'utilisateur d'indiquer l'emplacement du serveur LDAP (nom d'hôte, numéro de port et DN de base) ainsi que la définition d'un utilisateur disposant de droits d'administration (DN complet et mot de passe). Le script crée ensuite une arborescence de service d'initialisation sur le serveur LDAP afin d'y stocker les fichiers de mappage. Il peut être exécuté par n'importe quel utilisateur et est appelé avec la commande suivante :

```
./createServiceTree
```

L'utilisateur est ensuite invité à indiquer les éléments suivants :

- Nom d'hôte (valeur par défaut : `localhost`) : nom d'hôte du serveur LDAP ;
- Numéro de port (valeur par défaut : `389`) : numéro de port du serveur LDAP ;
- DN de base : DN de base du référentiel LDAP ;
- DN de l'utilisateur (valeur par défaut : `cn=Directory Manager`) : DN complet d'un utilisateur disposant des autorisations suffisantes pour créer de nouvelles entrées sous le DN de base ;
- Mot de passe : mot de passe de l'utilisateur en question ;

Une entrée avec le DN :

```
ou=ApocRegistry,ou=default,ou=OrganizationConfig,ou=1.0,ou=ApocService,ou=services,<DN de base>
```

est créée et remplie avec le contenu des deux fichiers de mappage.

Comme indiqué plus haut, les opérations effectuées par le script `deployApoc` supposent que les répertoires d'installation, le format et la procédure d'extension de schéma du serveur LDAP correspondent à ceux du serveur d'annuaire Sun Java System. Une extension manuelle du schéma est nécessaire pour les

autres répertoires avant de pouvoir exécuter le script `createServiceTree`. Pour plus d'informations sur l'utilisation de OpenLDAP et ActiveDirectory, reportez-vous à l'Annexe C.

L'arborescence créée, qui correspond à celle qui contiendra les données de configuration associées aux entités, est alignée avec la structure des arborescences utilisées pour la gestion des services sur le serveur d'identité Sun Java System.

## Autres considérations

La structure de Configuration Manager nécessite qu'une connexion au serveur LDAP avec les autorisations de lecture et de recherche puisse être créée pour identifier le DN complet qui est associé à un identificateur d'utilisateur ou d'hôte donné provenant du bureau. À ce titre, le référentiel doit être configuré de manière à autoriser les connexions anonymes ou un utilisateur spécial disposant d'un accès en lecture et en recherche doit être créé à cet effet.

L'application de gestion crée des arborescences de service sous les entrées mappées vers des entités pour y stocker les données de configuration de celles-ci. Les entrées d'utilisateur employées à des fins de gestion doivent donc être autorisées à créer des sous-entrées sous les entrées qu'elles gèrent.

Deux méthodes permettent l'authentification des utilisateurs de la structure à partir des clients de bureau : anonyme et GSSAPI. La méthode anonyme nécessite qu'un accès anonyme soit activé pour la lecture et la recherche dans le référentiel dans la mesure où les clients de bureau ne fourniront pas d'informations d'identification lorsqu'ils tenteront d'extraire des données du serveur LDAP. Pour utiliser la méthode GSSAPI (en employant Kerberos pour l'authentification), le serveur LDAP doit être configuré selon les instructions fournies dans le chapitre "Implémentation de la sécurité" du "Guide d'administration du serveur d'annuaire Sun Java System".

## Console Web de Sun™

---

La Console Web de Sun est destinée à fournir une solution de gestion du système commune basée sur le Web pour Sun Microsystems. Cette console est le point à partir duquel les utilisateurs peuvent accéder aux applications de gestion du système, qui ont toutes une interface utilisateur cohérente.

La console est conçue sur un modèle Web pour de nombreuses raisons, notamment afin de permettre aux administrateurs système d'utiliser un navigateur Web pour accéder à leurs applications de gestion du système.

La Console Web de Sun offre les avantages suivants :

- Une authentification et une autorisation communes ;
- Un enregistrement des événements commun ;
- Un point d'entrée unique pour toutes les applications de gestion du système par l'intermédiaire du même port HTTPS ;
- Un aspect et un comportement similaires.

La console présente un avantage majeur puisqu'il suffit à l'administrateur de se connecter une seule fois pour utiliser ensuite n'importe quelle application de la console.

## Configuration système requise

La Console Web de Sun prend en charge plusieurs systèmes d'exploitation client et serveur ainsi que plusieurs navigateurs.

### Client

- Netscape 4.7x, 6.2x et 7.x sur Solaris 8 ou version ultérieure
- Netscape 4.7x, 6.2x et 7.x sur Windows 98, 98 Deuxième Édition, ME, 2000 et XP
- Internet Explorer 5.x et 6.x sur Windows 98, 98 Deuxième Édition, ME, 2000 et XP
- Mozilla sur Linux et Solaris

## Serveur

- Solaris 8 ou version ultérieure
- Redhat 8 ou version ultérieure, Redhat Enterprise Linux 2.1
- SuSE Linux 2.1 ou version ultérieure
- J2SE version 1.4.1\_03 ou version ultérieure
- Si J2SE 1.4.1 ou une version antérieure est détectée sur votre serveur, le programme d'installation vous demande de mettre l'installation à niveau avec la version de J2SE fournie sur le CD-ROM Java Desktop System Management Tools.
- Tomcat : 4.0.3 ou version ultérieure

Tomcat est inclus sur le CD-ROM Java Desktop System Management Tools.

## Installation de la Console Web de Sun

Avant d'installer la Console Web de Sun, lisez les sections de description des packages et des problèmes connus dans l'annexe A du présent guide.

Les fichiers binaires d'installation de la Console Web de Sun pour les systèmes d'exploitation Solaris SPARC (version 8 ou ultérieure) et Linux sont disponibles sur le CD-ROM Java Desktop System Management Tools.

Pour installer la Console Web de Sun :

1. Sur le CD-ROM Java Desktop System Management Tools, accédez au répertoire de la Console Web de Sun qui correspond au système d'exploitation sur lequel vous voulez installer la console.

Sur les systèmes Linux, accédez au répertoire `/linux/swc` et pour Solaris SPARC, accédez au répertoire `/solsparc/swc`.

2. Tapez `./setup`.

Par défaut, la Console Web de Sun ne crée pas de fichier journal d'installation. Pour en créer un portant le nom "fichierjournal", tapez `./setup | tee fichierjournal`.

**Remarque :** la majeure partie du processus d'installation et de configuration de la console Web est automatiquement effectuée par l'application d'installation `setup`. Pour plus d'informations sur l'application `setup` de la Console Web de Sun, reportez-vous à l'annexe A.

3. Si vous voulez localiser la Console Web de Sun, vous devez installer deux packages supplémentaires pour chaque langue. Recherchez dans le tableau ci-dessous le nom du package correspondant à la langue voulue, puis effectuez une des opérations suivantes :
  - Sur Solaris, tapez `pkgadd -d path/pkgname.pkg pkgname`, où *pkgname* est le nom du package de langue à ajouter.
  - Sur Linux, tapez `rpm -i path/pkgname<...>.rpm`, où *pkgname* est le nom du package à ajouter.

Nom du package	Description
SUNWcmcon, SUNWcmctg	Console Web 2.0 de Sun™ en chinois simplifié
SUNWdmcon, SUNWdmctg	Console Web 2.0 de Sun™ en allemand
SUNWemcon, SUNWemctg	Console Web 2.0 de Sun™ en espagnol
SUNWfmcon, SUNWfmctg	Console Web 2.0 de Sun™ en français
SUNWhmcon, SUNWhmctg	Console Web 2.0 de Sun™ en chinois traditionnel
SUNWimcon, SUNWimctg	Console Web 2.0 de Sun™ en italien
SUNWjmcon, SUNWjmctg	Console Web 2.0 de Sun™ en japonais
SUNWkmcon, SUNWkmctg	Console Web 2.0 de Sun™ en coréen
SUNWsmcon, SUNWsmctg	Console Web 2.0 de Sun™ en suédois

## Exécution de la console

Il n'est généralement nécessaire d'arrêter et de redémarrer le serveur de la Console Web de Sun que lorsque vous voulez enregistrer une nouvelle application.

Avant le premier démarrage de la Console Web de Sun, vérifiez que l'installation de Configuration Manager est terminée.

- Pour démarrer la Console Web de Sun, tapez `smcwebserver start`.
- Pour arrêter la Console Web de Sun, tapez `smcwebserver stop`.
- Pour accéder à la Console Web de Sun, saisissez l'URL suivante dans votre navigateur :  
`https://<nomhôte>.<nomdomaine>:6789`

Telle qu'elle est livrée, la console Web de Sun prend en charge l'authentification Unix et le contrôle d'accès basé sur les rôles (RBAC). Vous pouvez toutefois également configurer d'autres méthodes d'authentification comme l'authentification LDAP.

**Remarque :** le délai d'expiration de session par défaut est de 15 minutes. Vous pouvez configurer ce délai avec la commande `smreg`. Par exemple, pour définir un délai d'expiration de 5 minutes, tapez `smreg add -p -c session.timeout.value=5`.

Pour plus d'informations sur les commandes de la Console Web de Sun, reportez-vous aux pages `man smcwebserver` et `smreg`.

## Désinstallation de la Console Web de Sun

Pour désinstaller la Console Web de Sun, exécutez `/usr/lib/webconsole/setup -u`.

**Remarque :** n'exécutez pas cette commande si vous vous trouvez dans le répertoire `/usr/lib/webconsole` ou un de ses sous-répertoires, car elle provoquerait l'échec de `pkgrm`.

# Informations sur les ports de la Console Web de Sun

Configuration Manager utilise les ports de la Console Web de Sun :

- 8005 pour l'arrêt du service, et
- 6789 pour l'accès https.

Vous pouvez changer les deux ports dans `/etc/opt/webconsole/server.xml`. Une fois les ports changés, vous devez redémarrer la Console Web de Sun à l'aide de la commande `/usr/sbin/smcwebserver restart`.



# Sun Java™ Desktop System Configuration Manager, Release 1

---

Configuration Manager fournit un outil d'administration qui s'exécute sur la Console Web de Sun. Cette interface utilisateur Web permet à un administrateur de parcourir la hiérarchie d'une organisation afin de définir des stratégies pour les applications bureautiques. Ces stratégies peuvent être définies pour chaque élément de la hiérarchie, notamment pour les organisations, rôles, utilisateurs, domaines et hôtes. Configuration Manager utilise plusieurs modèles de configuration pour afficher les paramètres spécifiques à différentes applications bureautiques telles que Gnome, Mozilla, StarOffice et Evolution.

## Installation de Configuration Manager

L'installation de Configuration Manager nécessite une installation fonctionnelle de la Console Web de Sun.

1. Sur le CD-ROM Java Desktop System Management Tools, accédez au répertoire de Configuration Manager correspondant.

Sur les systèmes Linux, accédez au répertoire `/linux/apoc`. Sur Solaris SPARC, accédez au répertoire `/solsparc/apoc`.

2. Tapez `./setup`.
3. Saisissez le nom d'hôte du serveur LDAP.  
Le nom par défaut est `localhost` (hôte local).
4. Saisissez le numéro de port du serveur LDAP (valeur par défaut : 389).
5. Saisissez le DN de base du référentiel LDAP.

6. Saisissez le nom de la classe d'objet utilisée pour l'identification des entités d'utilisateur. La classe d'objet par défaut est `inetorgperson`.

Pour plus de détails, reportez-vous à la section Mappage organisationnel du chapitre Serveur LDAP.

7. Saisissez un nom d'attribut unique dans tout le référentiel LDAP. L'attribut par défaut est `uid`.

Pour plus de détails, reportez-vous à la section Mappage organisationnel du chapitre Serveur LDAP.

8. Saisissez le DN complet d'un utilisateur disposant des droits d'accès nécessaires pour effectuer des requêtes sur le serveur LDAP.

Utilisez n'importe quel DN complet ayant un accès en lecture et en recherche. Pour un accès anonyme, n'indiquez rien dans le champ.

9. Saisissez un mot de passe pour l'utilisateur auquel vous avez assigné les droits d'accès LDAP.

Si vous avez configuré un accès anonyme au serveur LDAP, ignorez cette étape.

Au cours de l'installation, un module de connexion supplémentaire est ajouté à la Console Web de Sun ; il vous permet d'authentifier les utilisateurs par le biais du protocole LDAP.

À la fin de l'installation, la Console Web de Sun redémarre automatiquement pour vous permettre d'accéder à Configuration Manager.

**Remarque :** Vous pouvez à tout moment modifier les paramètres précédents de Configuration Manager en utilisant le script `/usr/share/webconsole/apoc/configure`. Vous pouvez par exemple modifier le script afin d'employer un serveur LDAP différent sans avoir à réinstaller Configuration Manager.

## Exécution de Configuration Manager

1. Pour accéder à Configuration Manager, saisissez l'URL suivante dans votre navigateur :

```
https://<nomhôte>.<nomdomaine>:6789
```

2. À l'invite, saisissez le nom d'utilisateur (ID utilisateur, UID) et le mot de passe d'un utilisateur LDAP existant.

La Console Web de Sun s'ouvre.

3. Dans la fenêtre de la console, cliquez sur **Sun Java™ Desktop System Configuration Manager, Release 1**.

**Remarque :** si vous voulez ignorer la page de lancement de la Console Web de Sun pour accéder directement à Configuration Manager, saisissez l'URL suivante dans votre navigateur :

```
https://<nomhôte>.<nomdomaine>:6789/apoc
```

## Désinstallation de Configuration Manager

Pour désinstaller Configuration Manager de la Console Web de Sun, accédez au répertoire de Configuration Manager correspondant sur le CD-ROM Java Desktop System Management Tools, puis exécutez `./setup -u`.

**Remarque :** lorsque vous désinstallez Configuration Manager, le module de connexion LDAP est supprimé de la Console Web de Sun.

## Composants de bureau

---

Pour accéder aux données de configuration à partir de Configuration Manager, un client de bureau a besoin de l'agent Sun Java™ Desktop System Configuration Agent. Configuration Agent communique avec le référentiel des données de configuration distantes ainsi qu'avec les adaptateurs, et il intègre les données dans des systèmes de configuration spécifiques. Les systèmes de configuration actuellement pris en charge sont GConf, les Préférences de Mozilla et le registre de StarOffice.

Tous ces composants sont livrés et installés avec Java Desktop System.

## Accès aux données / Authentification des utilisateurs

Configuration Agent extrait des informations du serveur LDAP en fonction de l'ID de connexion d'un utilisateur de bureau. Le paramètre User/UniqueIdAttribute du fichier de mappage organisationnel associe l'ID de connexion à une entité d'utilisateur sur le serveur LDAP. Configuration Agent extrait également des informations relatives à l'hôte, par exemple son nom ou son adresse IP. Ces informations sont associées à une entrée d'hôte sur le serveur LDAP par le biais du paramètre Host/UniqueIdAttribute du fichier de mappage organisationnel.

Il existe deux méthodes d'accès au serveur LDAP, à savoir la méthode anonyme et la méthode GSSAPI. Aucune action n'est requise sur le bureau pour un accès anonyme. Pour la méthode GSSAPI, des informations d'identification Kerberos doivent être obtenues sur le bureau. Pour intégrer l'obtention des informations d'identification Kerberos à la connexion de l'utilisateur, le module pam\_krb5 doit être installé et configuré sur l'hôte Java Desktop System. Vous trouverez des exemples de configuration pour le module pam dans le répertoire `/usr/share/doc/packages/pam_krb5/README.SuSE` sur le CD-ROM Java Desktop System. Vous pouvez également utiliser gdm pour intégrer Kerberos à la connexion de l'utilisateur, par exemple en utilisant le fichier `/etc/pam.d/gdm` suivant :

```
##PAM-1.0
auth    required    pam_unix2.so  nullok #set_secrpc
auth    optional    pam_krb5.so  use_first_pass missing_keytab_ok
ccache=SAFE putenv_direct
account required    pam_unix2.so
password required    pam_unix2.so  #strict=false
session required    pam_unix2.so  # trace or none
session required    pam_devperm.so
session optional    pam_console.so
```

# Configuration Agent

Configuration Agent fait partie du package `apoc`. Lorsque vous installez le RPM correspondant, les fichiers requis pour cette API sont installés et enregistrés avec `inetd`. Vous pouvez installer le RPM manuellement ou par le biais de l'installation Java Desktop System.

## Informations d'initialisation

Pour accéder aux données de configuration distantes, l'emplacement du serveur LDAP doit être fourni à Configuration Agent. Vous pouvez ajouter cet emplacement avec l'outil de configuration autoYaST de YaST2 ou en éditant manuellement le fichier de propriétés `policymgr.properties` figurant dans le répertoire `/opt/apoc/lib`. Dans YaST2, vous pouvez ajouter ces données dans la section Réseau/Options avancées.

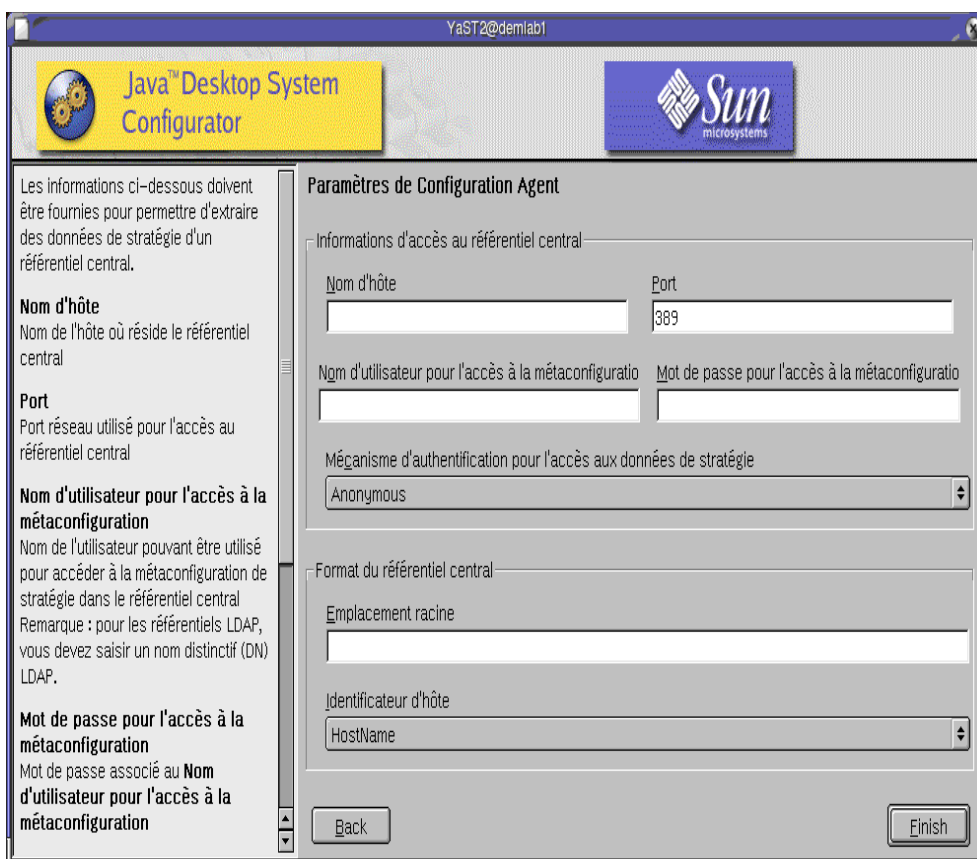


Figure 1 Java Desktop System Configuration Agent dans YaST

Les informations ci-dessous sont nécessaires pour exécuter Configuration Agent :

- Nom d'hôte (Server) : nom d'hôte du serveur LDAP ;
- Port (Port) : numéro de port du serveur LDAP ;
- Nom d'utilisateur pour l'accès aux métadonnées (AuthDn) : DN complet d'un utilisateur ayant des droits d'accès en lecture et en recherche dans le référentiel ;

**Remarque :** si l'accès anonyme est activé dans le répertoire, ce paramètre peut rester vide.

- Mot de passe pour l'accès aux métadonnées (Password) : mot de passe d'un utilisateur LDAP enregistré ;

**Remarque :** si l'accès anonyme est activé dans le répertoire, ce paramètre peut rester vide.

- Méthode d'authentification pour l'accès aux données de stratégie (AuthType) : anonyme ou GSSAPI selon le mode d'authentification des utilisateurs employé par le serveur LDAP ;
- Emplacement racine (BaseDn) : DN de base du référentiel LDAP ;
- Identificateur d'hôte (HostIdentifier) : peut être HostName ou IPAddress et doit être configuré pour correspondre au contenu de l'attribut LDAP utilisé pour identifier les hôtes ; cet attribut est défini dans les fichiers de mappage sous la forme Host/UniqueIdAttribute.
- Expiration du délai de connexion (Connect Timeout) : indique le délai d'expiration (en secondes) des tentatives de connexion au serveur LDAP. La valeur par défaut est 1 seconde.

**Remarque :** Configuration Agent doit être redémarré lorsque vous modifiez ces paramètres.

Pour redémarrer Configuration Agent sur le bureau, vérifiez au préalable qu'aucune des applications clientes associées n'est en cours d'exécution, connectez-vous en tant que racine et entrez la commande `/opt/apoc/bin/apocd restart`.

## Paramètres de fonctionnement

Vous pouvez configurer les paramètres de fonctionnement de Configuration Agent localement ou à distance. Pour configurer ces paramètres localement, éditez le fichier `apocd.properties` dans le répertoire `/opt/apoc/lib`. Pour configurer ces paramètres à distance, utilisez la stratégie Configuration Agent dans Configuration Manager. Les paramètres suivants peuvent être configurés dans le fichier de propriétés :

- `DaemonPort` : port sur lequel Configuration Agent écoute les communications provenant de ses clients sur le bureau ;
- `MaxClientThreads` : nombre maximal de demandes des clients pouvant être traitées simultanément ;
- `MaxClientConnections` : nombre maximal de connexions des clients ;
- `MaxRequestSize` : taille maximale de demandes des clients ;
- `DaemonChangeDetectionInterval` : intervalle en minutes entre les cycles de détection des changements pour cette liste de paramètres de configuration ;
- `ChangeDetectionInterval` : intervalle en minutes entre les cycles de détection des changements pour les données de configuration des clients ;
- `GarbageCollectionInterval` : intervalle en minutes entre les cycles de libération de la mémoire dans la base de données de configuration locale ;
- `TimeToLive` : intervalle en minutes pendant lequel les données de configuration qui ne sont pas hors ligne demeurent dans la base de données locale ;
- `LogLevel` : niveau de détail dans les fichiers journaux de l'agent.

Le paramètre `DaemonPort` peut uniquement être modifié localement et nécessite un redémarrage de l'agent pour que les modifications soient prises en compte. Tous les autres paramètres sont pris en compte au prochain cycle de détection des changements de la configuration de l'agent. Le niveau de détail d'enregistrement spécifié dans le paramètre `LogLevel` doit être une valeur cohérente avec les niveaux d'enregistrement des événements Java. Par ordre décroissant de gravité, ces niveaux sont : GRAVE, AVERTISSEMENT, INFO, CONFIG, FIN, PLUS FIN et LE PLUS FIN.

## Propagation des changements de données de configuration

Vous pouvez utiliser le paramètre `ChangeDetectionInterval` décrit dans la section Paramètres de fonctionnement pour définir la propagation des changements de données de configuration à distance sur les applications côté client. La valeur que vous indiquez pour ce paramètre correspond à la durée maximale en minutes s'écoulant avant que les changements effectués à distance ne soient reflétés dans les applications clientes. Si vous indiquez des valeurs peu élevées pour `ChangeDetectionInterval`, l'activité de Configuration Agent et du serveur LDAP est augmentée. Vous devez donc ajuster avec précaution la valeur de ce paramètre. Par exemple, dans une phase de déploiement initial, vous pouvez définir une valeur égale à une minute de manière à pouvoir tester facilement l'impact de la configuration distante sur les applications clientes. Une fois le test terminé, rétablissez la valeur initiale du paramètre.

## Informations sur les ports utilisés par Configuration Agent

L'agent de configuration utilise deux ports :

1. Le port du démon (par défaut, 38900), utilisé par le démon pour communiquer avec les applications clientes.
2. Le port admin du démon (par défaut, 38901), utilisé par le programme de contrôle du démon, `apocdctl`, lorsqu'il communique avec le démon.

Changement du port du démon :

Pour changer le port du démon, vous devez modifier la propriété `DaemonPort` dans le fichier `apocd.properties` du démon, ainsi que les entrées `apocd` dans `/etc/services` et `/etc/inetd.conf`. Vous devez ensuite redémarrer le démon et recharger `inetd`.

Changement du port admin du démon :

Pour changer le port admin du démon, vous devez modifier la propriété `DaemonAdminPort` dans le fichier `apocd.properties`. Vous devez ensuite redémarrer le démon.

## Adaptateur GConf

L'adaptateur GConf fait partie du package `apoc-adapter-gconf`. Lorsque vous installez l'adaptateur à partir du RPM correspondant, le chemin d'accès des sources de données GConf dans `/etc/gconf/2/path` est mis à jour pour inclure les sources de Configuration Manager. Une sauvegarde de l'ancien chemin d'accès est stockée dans `/etc/gconf/2/path.apocBackup`. Si l'ancien chemin d'accès fait référence à des sources de données personnalisées, vous devrez mettre à jour le chemin d'accès en fusionnant les changements du chemin d'accès par défaut avec le chemin d'accès de Manager nouvellement installé. Les deux sources de données fournies par l'adaptateur sont les suivantes :

- `"apoc:readonly:"` : fournit un accès à des paramètres non protégés à partir des stratégies. Insérez cette source de données après les paramètres de l'utilisateur et avant les paramètres par défaut locaux.
- `"apoc:readonly:mandatory@"` : fournit un accès à des paramètres protégés à partir des stratégies. Insérez cette source de données après les paramètres obligatoires locaux et avant les paramètres de l'utilisateur.

## Adaptateur Mozilla

L'adaptateur Mozilla fait partie du package `mozilla-apoc-integration`. Lorsque vous installez l'adaptateur à partir du RPM correspondant, les fichiers requis sont ajoutés à une installation existante de Mozilla et sont automatiquement enregistrés.

## Adaptateur StarOffice

L'adaptateur StarOffice est inclus dans une installation StarOffice standard et permet d'accéder aux données de configuration de stratégie sans que des modifications spéciales ne soient nécessaires.





## Annexe A – Console Web de Sun

---

### Problèmes connus

#### Sécurité

Sans que l'utilisateur ne s'en aperçoive, une session peut être laissée dans un état actif du fait de certaines de ses actions. Par exemple, lorsqu'un utilisateur ferme une fenêtre de navigateur, il n'est pas automatiquement déconnecté de la Console Web de Sun. L'utilisateur doit explicitement se déconnecter d'une session dans la Console Web de Sun avant de fermer une fenêtre d'application.

### Utilisation du script d'installation

Synopsis : `setup [-h] | [-n] | [-d <ver>,<arch>[,client1,client2,...]] [-u [-f]]`

-h = Imprime l'instruction d'utilisation

-n = Ne démarre pas le serveur à la fin de l'installation

-u = Désinstalle la Console Web de Sun

-f = Désinstalle les packages Tomcat et Java 1.4 s'ils étaient installés avec l'application d'installation. Vous ne pouvez utiliser ce paramètre qu'avec le paramètre -u.

Pour avoir une description complète des paramètres d'installation disponibles, exécutez `setup -h`.

Pour désinstaller la Console Web de Sun, exécutez `/usr/lib/webconsole/setup -u`.

**Remarque :** n'exécutez pas cette commande si vous vous trouvez dans le répertoire `/usr/lib/webconsole` ou un de ses sous-répertoires, car elle provoquerait l'échec de `pkgrm`.

# Packages de la Console Web de Sun

## Packages Solaris

<i>Nom du package</i>	<i>Description</i>
SUNWmctag	Bibliothèque de balises de l'interface utilisateur de la Console Web de Sun
SUNWmcon	Console Web de Sun
SUNWmcos	Services Solaris communs pour la Console Web de Sun
SUNWmcosx	Services spécifiques à la version Solaris pour la Console Web de Sun
SUNWmconr	Racine de la Console Web de Sun
SUNWjato	Exécution de Sun One Application Framework
SUNWtcatu	Tomcat

## RPM Linux

<i>Nom du package</i>	<i>Description</i>
SUNWmctag	Bibliothèque de balises de l'interface utilisateur de la Console Web de Sun
SUNWmcon	Console Web de Sun
SUNWmcos	Services Linux communs pour la Console Web de Sun
SUNWmcosx	Services spécifiques à la version Linux pour la Console Web de Sun
SUNWmconr	Racine de la Console Web de Sun
SUNWjato	Exécution de Sun One Application Framework
tomcat4	Tomcat

## Annexe B – Configuration Manager

### Packages de Configuration Manager

#### Packages Solaris

<i>Nom du package</i>	<i>Description</i>
SUNWapm	Configuration Manager
SUNWapmca	Modèles de Configuration Agent
SUNWapmev	Modèles d'Evolution
SUNWapmgo	Modèles de Gnome
SUNWapmmo	Modèles de Mozilla
SUNWapmso	Modèles de StarOffice

#### RPM Linux

<i>Nom du package</i>	<i>Description</i>
apoc-manager	Configuration Manager
apoc-agent-templates	Modèles de Configuration Agent
apoc-evolution-templates	Modèles d'Evolution
apoc-gnome-templates	Modèles de Gnome
apoc-mozilla-templates	Modèles de Mozilla
apoc-staroffice-templates	Modèles de StarOffice



## Annexe C

---

### Utilisation d'un serveur OpenLDAP avec Configuration Manager

Pour utiliser un serveur OpenLDAP comme référentiel pour les données de Configuration Manager, son schéma doit être étendu pour présenter les classes d'objet et attributs utilisés pour le stockage des données de configuration. Un fichier de schéma personnalisé nommé `apoc.schema` se trouve dans le sous-répertoire `openldap` de l'outil de déploiement de Configuration Manager, fourni sur le CD-ROM Java Desktop System Management Tools.

Ce fichier doit être copié dans le sous-répertoire `schema` du répertoire de configuration OpenLDAP (`/etc/openldap`) et être ajouté au schéma OpenLDAP en l'incluant dans le fichier `slapd.conf` se trouvant dans ce répertoire. Cette opération est effectuée en insérant la ligne `include /etc/openldap/schema/apoc.schema` à la fin de la séquence d'inclusions de schéma présente dans ce fichier. Pour plus d'informations sur l'extension du schéma d'un serveur OpenLDAP, reportez-vous à son manuel.

L'outil de déploiement fourni avec Configuration Manager doit être utilisé pour préparer la base de données OpenLDAP au stockage des données de configuration. Le schéma ayant déjà été étendu par l'étape précédente de l'installation, seul le script `createServiceTree` doit être exécuté. Ce script doit être démarré à partir du répertoire de l'outil de déploiement par n'importe quel utilisateur, en exécutant la commande suivante : `./createServiceTree`. Le script demande à l'utilisateur d'indiquer des informations sur la base de données OpenLDAP, comme l'indique la section concernant l'outil de déploiement de ce document. Un fichier de mappage par défaut utilisant les classes d'objet et attributs types présentés dans OpenLDAP est fourni dans le sous-répertoire `openldap` de l'outil de déploiement. Ce fichier se nomme `OrganizationalMapping` et peut être déployé en le copiant par-dessus le fichier du même nom se trouvant dans le répertoire principal de l'outil de déploiement avant de lancer le script `createServiceTree`.

Notez que Configuration Manager Agent tentera de se connecter au serveur OpenLDAP de façon anonyme en fournissant le DN de l'utilisateur pour lequel il nécessite des données, mais aucun mot de passe. Il se peut que ce mode d'authentification anonyme soit désactivé par défaut dans certaines versions de serveurs OpenLDAP, auquel cas il doit être activé en ajoutant la ligne `allow bind_anon_cred` dans les paramètres de serveur communs définis dans le fichier `slapd.conf` qui se trouve dans le répertoire de configuration OpenLDAP (`/etc/openldap`). Pour plus d'informations sur ce paramètre, reportez-vous au manuel du serveur en question.

# Utilisation d'un serveur Active Directory avec Configuration Manager

Pour utiliser un serveur Active Directory comme référentiel pour les données de Configuration Manager, son schéma doit être étendu pour présenter les classes d'objet et attributs utilisés pour le stockage des données de configuration. Un fichier d'extension de schéma nommé `apoc-ad.ldf` se trouve dans le sous-répertoire `ad` de l'outil de déploiement de Configuration Manager, fourni sur le CD-ROM Java Desktop System Management Tools. Pour plus d'informations, reportez-vous à la section concernant l'outil de déploiement.

Le fichier `apoc-ad.ldf` doit être importé dans le schéma Active Directory en procédant comme suit :

1. Activez les extensions de schéma. Reportez-vous à la documentation Active Directory pour plus d'informations sur l'exécution de cette opération.
2. Exécutez la commande suivante à partir de l'invite de commande : `ldifde -i -c "DC=Sun,DC=COM" <DN de base> -f apoc-ad-registry.ldf`.

**Remarque :** remplacez `<DN de base>` par le DN de base Active Directory.

L'outil de déploiement doit être utilisé pour préparer le serveur Active Directory au stockage des données de configuration. Le schéma ayant déjà été étendu par l'étape précédente de l'installation, seul le script `createServiceTree` doit être exécuté. Il doit être démarré à partir du répertoire de l'outil de déploiement par n'importe quel utilisateur, en exécutant la commande suivante : `./createServiceTree`. Le script demande à l'utilisateur d'indiquer des informations sur la base de données Active Directory. Un fichier de mappage par défaut utilisant les classes d'objet et attributs types présentés dans Active Directory est fourni dans le sous-répertoire `ad` du répertoire de l'outil de déploiement. Ce fichier se nomme `OrganisationalMapping` et peut être déployé en le copiant par-dessus le fichier du même nom se trouvant dans le répertoire principal de l'outil de déploiement avant de lancer le script `createServiceTree`.

Le serveur Active Directory peut maintenant être utilisé avec Configuration Manager. Lors de l'installation de Configuration Manager, fournissez le DN complet et le mot de passe d'un utilisateur possédant des droits de lecture sur l'arborescence. Il peut s'agir d'un utilisateur ne pouvant pas utiliser Active Directory à d'autres fins. Reportez-vous à la documentation Active Directory pour plus d'informations sur la configuration d'un utilisateur de ce type. En outre, le nom de domaine du serveur Active Directory doit être connu de l'ordinateur exécutant Configuration Manager. Pour ce faire, ajoutez au fichier `/etc/hosts` de l'ordinateur en question une ligne mappant l'adresse IP du serveur Active Directory à son nom de domaine.

Pour pouvoir extraire les données de configuration d'un hôte Java Desktop System (JDS), le nom de domaine du serveur Active Directory doit également être connu de cet hôte. L'authentification de l'utilisateur JDS peut se faire de deux manières, de façon anonyme et à l'aide de GSSAPI.

- Pour effectuer l'authentification à l'aide de connexions anonymes, le serveur Active Directory doit être configuré pour accorder des droits de lecture à tout le monde. Reportez-vous à la documentation Active Directory pour plus d'informations sur l'exécution de cette opération.
- Pour effectuer l'authentification à l'aide de GSSAPI, le fichier `/etc/krb5.conf` spécifiant les paramètres Kerberos doit être modifié pour définir le domaine Active Directory et faire référence au serveur Active Directory en tant que centre de distribution de clés (KDC, Key Distribution Center). Il doit également spécifier, en tant que types de chiffrement par défaut, les types DES pris en charge par Active Directory, à savoir `des-cbc-crc` et `des-cbc-md5`. Reportez-

vous à la documentation Kerberos pour plus d'informations sur l'exécution de cette opération. Avant d'accéder aux données de configuration, il est nécessaire d'obtenir des informations d'identification valides pour l'utilisateur connecté à JDS. Cette opération peut être effectuée manuellement en exécutant la commande `kinit` et en indiquant le mot de passe de l'utilisateur défini dans Active Directory. D'autres schémas peuvent générer automatiquement ces informations d'identification au moment de la connexion. Pour plus d'informations, reportez-vous à la documentation de JDS.