



Sun Java Desktop System Configuration Manager, version 1 - Guide d'installation

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Référence : 819-0679-10
Septembre 2004

Copyright 2004 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

Le présent produit ou document est protégé par copyright et sa distribution est soumise à des licences en restreignant l'utilisation, la copie, la distribution et la décompilation. Toute reproduction, même partielle, du produit ou du présent document est formellement interdite, quelle qu'en soit la forme, sans autorisation préalable écrite en ce sens, de Sun et de ses concédants de licences. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et une licence des fournisseurs de Sun.

Il est possible que des parties du produit soient dérivées des systèmes Berkeley BSD, concédés en licence par la University of California. UNIX est une marque déposée aux États-Unis et dans d'autres pays, exclusivement concédée en licence par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, docs.sun.com, AnswerBook, AnswerBook2, et Solaris sont des marques commerciales ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays. Toutes les marques déposées SPARC sont utilisées sous licence et sont des marques commerciales ou déposées de SPARC International, Inc. aux États-Unis et dans d'autres pays. Les produits portant les marques déposées SPARC sont constitués selon une architecture développée par Sun Microsystems, Inc.

OPEN LOOK et l'interface graphique utilisateur Sun™ sont développés par Sun Microsystems, Inc. pour ses utilisateurs et ses concessionnaires. Sun reconnaît les efforts pionniers de Xerox en recherche et développement du concept des interfaces utilisateur visuelles ou graphiques dans l'industrie informatique. Sun détient une licence non-exclusive de Xerox pour l'interface utilisateur graphique Xerox, laquelle licence couvre également les titulaires de licence Sun mettant en œuvre les IUG OPEN LOOK et se conformant par ailleurs aux accords écrits de Sun.

Logiciel commercial déposé aux États-Unis. Les utilisateurs gouvernementaux sont soumis au contrat de licence standard de Sun Microsystems, Inc. et aux clauses applicables du FAR et de ses compléments.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTES LES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



040928@9495



Table des matières

1	Introduction	9
	Introduction	9
2	Serveur LDAP	11
	Concepts	11
	Configuration	12
	Outils de déploiement	12
	Extension de schéma	13
	Mappage organisationnel	13
	Mappage de profils utilisateur	14
	Déploiement	15
	Autres considérations	17
3	Sun Web Console	19
	Configuration système requise	19
	Client	20
	Serveur	20
	Installation de la Sun Web Console	20
	▼ Installation de la Sun Web Console	20
	Exécution de la console	22
	Désinstallation de la Sun Web Console	22
	Informations sur les ports de la Sun Web Console	23
4	Sun Java Desktop System Configuration Manager, version 1	25
	Installation de Configuration Manager	25

▼ Installation de Configuration Manager	25
Exécution de Configuration Manager	26
▼ Démarrage de Configuration Manager	26
Désinstallation de Configuration Manager	27
5 Composants de bureau - Linux	29
Accès aux données / Authentification des utilisateurs	29
Configuration Agent	30
Informations d'initialisation	30
Paramètres de fonctionnement	32
Propagation des changements de données de configuration	33
Informations relatives aux ports de Configuration Agent	33
Adaptateur GConf	34
Adaptateur Mozilla	34
Adaptateur StarOffice	34
6 Composants de bureau - Solaris	35
Configuration Agent	35
Informations d'initialisation	36
Paramètres de port	38
Intervalle de détection des changements	39
Paramètres de fonctionnement	40
Application des paramètres de l'agent	42
Adaptateur GConf	43
Adaptateur Mozilla	43
Adaptateur StarOffice	43
A Packages de la Sun Web Console	45
Problèmes connus	45
Sécurité	45
Utilisation du script d'installation	45
Packages de la Sun Web Console	46
Packages Solaris	46
RPM Linux	46
B Packages de Configuration Manager	49
Packages de Configuration Manager	49

Packages Solaris 49
RPM Linux 49

C Utilisation d'OpenLDAP et d'Active Directory avec Configuration Manager 51
Utilisation d'un serveur OpenLDAP avec Configuration Manager 51
Utilisation d'un serveur Active Directory avec Configuration Manager 52

Liste des figures

FIGURE 5-1	Java Desktop System Configuration Agent dans YaST	30
FIGURE 6-1	Configuration Agent, référentiel de configuration	36
FIGURE 6-2	Configuration Agent, mécanisme d'authentification	37
FIGURE 6-3	Configuration Agent, paramètres de port	38
FIGURE 6-4	Configuration Agent, répertoire de données	40
FIGURE 6-5	Configuration Agent, gestion des demandes et enregistrement	40
FIGURE 6-6	Configuration Agent, résumé	42

Introduction

Offre une brève présentation de Sun Java™ Desktop System Configuration Manager, version 1.

Introduction

Sun Java™ Desktop System Configuration Manager, version 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 Sun Java Desktop System.

L'outil de gestion est une application Web qui est exécutée dans la Sun Web Console. 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 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

Ce chapitre fournit des informations sur la configuration et le déploiement d'un serveur LDAP devant être utilisé avec Configuration Manager.

Concepts

Dans la structure de Java Desktop System Configuration Manager, les données de configuration sont associées à des entités, qui sont des entrées du référentiel LDAP correspondant aux éléments de la structure organisationnelle de l'entreprise.

Les entités reconnues sont les suivantes :

- 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.

La relation des entités d'organisation et de domaine avec les autres entrées est définie par l'emplacement physique des entrées dans le référentiel. Par conséquent, les entités d'organisation et de domaine peuvent comprendre n'importe quelle entrée située sous ces deux entités dans l'arborescence. La relation des rôles avec les utilisateurs ou les hôtes est définie par les attributs des entrées des utilisateurs et des hôtes.

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 utiliser un serveur LDAP existant avec Configuration Manager, vous devez :

- étendre le schéma du serveur afin de prendre en charge les classes d'objet et les attributs personnalisés utilisés par Configuration Manager pour stocker les données de configuration.
- personnaliser et enregistrer sur le serveur les informations de mappage des entrées dans le référentiel, ainsi que les entités prises en charge par Configuration Manager.

Outils de déploiement

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

- `88apoc-registry.ldif` : fichier de schéma présentant les classes d'objet et les attributs requis pour stocker les 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'entrée 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 qui étend le schéma du serveur LDAP et qui stocke 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 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

Pour définir le mappage entre les entrées LDAP et les entités de Configuration Manager, vous devez modifier le fichier de mappage nommé *Organization*. 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 utilisent le format <item1>, <item2>, . . . , <itemN> 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

Pour définir le mappage entre les attributs d'entrées d'utilisateur LDAP et les attributs d'entités d'utilisateur de Configuration Manager, vous devez modifier le fichier de mappage de profils utilisateur. 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 (city)
org.openoffice.UserProfile/Data/l = l
# organizationalPerson.st (state)
org.openoffice.UserProfile/Data/st = st
# organizationalPerson.postalCode
org.openoffice.UserProfile/Data/postalcode = postalcode
# country.c (country)
org.openoffice.UserProfile/Data/c =
# organizationalPerson.o (company)
org.openoffice.UserProfile/Data/o = o,organizationName
# deprecated -- no LDAP corollary
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-monserveur.mondomaine`.

Le script `createServiceTree`, qu'il soit appelé directement ou à partir du script `deployApoc`, demande à l'utilisateur d'indiquer l'emplacement du serveur LDAP (nom d'hôte, numéro de port et DN de base) et la définition d'un utilisateur disposant de droits d'accès administratifs (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, <baseDN>
```

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

Comme mentionné précédemment, les opérations réalisées par le script `deployApoc` partent du principe que vous utilisez un serveur LDAP dont les répertoires d'installation, la disposition et la procédure d'extension de schéma correspondent étroitement à ceux du serveur d'annuaire Sun Java System. D'autres répertoires nécessitent une extension manuelle du schéma afin de pouvoir exécuter le script `createServiceTree`. Pour plus d'informations concernant l'utilisation d'OpenLDAP et d'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.

L'authentification des utilisateurs de la structure par les clients de bureau peut s'effectuer selon deux méthodes nommées 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 utilisant Kerberos pour l'authentification), le serveur LDAP doit être configuré selon les instructions fournies dans le chapitre "Gestion de l'authentification et du chiffrement" du *Guide d'administration du serveur d'annuaire Sun Java™ System 5 2004Q2*.

Sun™ Web Console

La Sun Web Console 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 Sun Web Console 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 Sun Web Console prend en charge de nombreux 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
- Red Hat 8 ou version ultérieure, Red Hat Enterprise Linux 2.1
- SuSE Linux 2.1 ou version ultérieure
- J2SE™ Version 1.4.1_03 ou ultérieure

Si J2SE version 1.4.1 ou antérieure est détecté sur votre serveur, le programme de configuration vous invite à mettre l'installation à niveau à l'aide de la version J2SE située 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 Sun Web Console

Avant d'installer la Sun Web Console, lisez les sections de description des packages et des problèmes connus dans l'[Annexe A](#) du présent guide.

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

▼ Installation de la Sun Web Console

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

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

2. Tapez `./setup`

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

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 de configuration de Sun Web Console, reportez-vous à l'[Annexe A](#).

3. Si vous souhaitez localiser la Sun Web Console, 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 :

- Sous Solaris, tapez `pkgadd -d path/pkgname.pkg pkgname`, où *pkgname* correspond au nom du package linguistique que vous voulez ajouter.
- Sous Linux, tapez `rpm -i path/pkgname<...>.rpm`, où *pkgname* correspond au package que vous souhaitez ajouter.

Nom	Description
SUNWcmcon, SUNWcmctg	Console Web 2.0 de Sun™ (Chinois simplifié)
SUNWdmcon, SUNWdmctg	Console Web 2.0 de Sun™ (Allemand)
SUNWemcon, SUNWemctg	Console Web 2.0 de Sun™ (Espagnol)
SUNWfmcon, SUNWfmctg	Console Web 2.0 de Sun™ (Français)
SUNWhmcon, SUNWhmctg	Console Web 2.0 de Sun™ (Chinois traditionnel)
SUNWimcon, SUNWimctg	Console Web 2.0 de Sun™ (Italien)
SUNWjmcon, SUNWjmctg	Console Web 2.0 de Sun™ (Japonais)
SUNWkmcon, SUNWkmctg	Console Web 2.0 de Sun™ (Coréen)
SUNWsmcon, SUNWsmctg	Console Web 2.0 de Sun™ (Suédois)

Exécution de la console

Pour enregistrer une nouvelle application, il vous suffit généralement d'arrêter, puis de redémarrer le serveur de la Sun Web Console.

Avant de démarrer la Sun Web Console pour la première fois, vérifiez que Configuration Manager a été correctement installé.

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

Prête à l'emploi, la Sun Web Console prend en charge l'authentification basée sur Unix et le contrôle d'accès basé sur les rôles (Role-Based Access Control ou RBAC). Toutefois, vous pouvez configurer d'autres mécanismes d'authentification, notamment 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 Sun Web Console, reportez-vous aux pages `man smcwebserver` et `smreg`.

Désinstallation de la Sun Web Console

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

Remarque – N'exécutez pas cette commande si vous vous trouvez dans le répertoire `/usr/lib/webconsole` ou l'un de ses sous-répertoires, sans quoi `pkgrm` échouera.

Informations sur les ports de la Sun Web Console

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

- 8005 pour fermer le service et
- 6789 pour l'accès https.

Vous pouvez modifier ces deux ports dans `/etc/opt/webconsole/server.xml`.
Après avoir modifié les ports, redémarrez la Sun Web Console à l'aide de la commande `/usr/sbin/smcwebserver restart`.

Sun Java™ Desktop System Configuration Manager, version 1

Configuration Manager fournit un outil d'administration qui s'exécute sur la Sun Web Console. 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 Sun Web Console.

▼ Installation de Configuration Manager

- Étapes**
1. **Accédez au répertoire de Configuration Manager correspondant sur le CD-ROM Java Desktop System Management Tools.**
Pour les systèmes Linux, accédez à `/linux/apoc`. Pour Solaris SPARC, accédez à `/solsparc/apoc`.
 2. **Tapez `./setup`.**
 3. **Saisissez le nom d'hôte du serveur LDAP.**
Le nom par défaut est `localhost`.
 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" à la page 13 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" à la page 13 du chapitre Serveur LDAP.
8. Saisissez le DN complet d'un utilisateur disposant des droits d'accès nécessaires pour interroger 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 Sun Web Console. Ce module vous permet d'authentifier les utilisateurs par le biais du protocole LDAP.
À la fin de l'installation, la Sun Web Console redémarre automatiquement pour vous permettre d'accéder à Configuration Manager.

Remarque – Vous pouvez modifier les paramètres précédents de Configuration Manager à tout moment à l'aide du script `/usr/share/webconsole/apoc/configure`. Par exemple, vous pouvez utiliser ce script pour changer de serveur LDAP sans réinstaller Configuration Manager.

Exécution de Configuration Manager

▼ Démarrage de Configuration Manager

- Étapes**
1. Tapez l'URL suivante dans votre navigateur :
`https://<nomhôte>.<nomdomaine>:6789`

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

La Sun Web Console s'ouvre.

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

**Informations
supplémentaires**

Accès direct à Configuration Manager

Si vous souhaitez ignorer la page de lancement de la Sun Web Console 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 à partir de la Sun Web Console, accédez au répertoire Configuration Manager correspondant sur le CD-ROM Java Desktop System Management Tools, puis exécutez la commande `./setup -u`.

Remarque – Lorsque vous désinstallez Configuration Manager, le module de connexion LDAP est supprimé de la Sun Web Console.

Composants de bureau - Linux

Pour accéder aux données de configuration à partir de Configuration Manager, un client de bureau a besoin de 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. Les informations sont associées à une entité 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 du CD-ROM Java Desktop System. Vous pouvez également utiliser la commande 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_secrcp
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 polycmgr.properties figurant dans le répertoire /opt/apoc/lib. Dans YaST2, vous pouvez ajouter ces données dans la section Réseau/Options avancées .

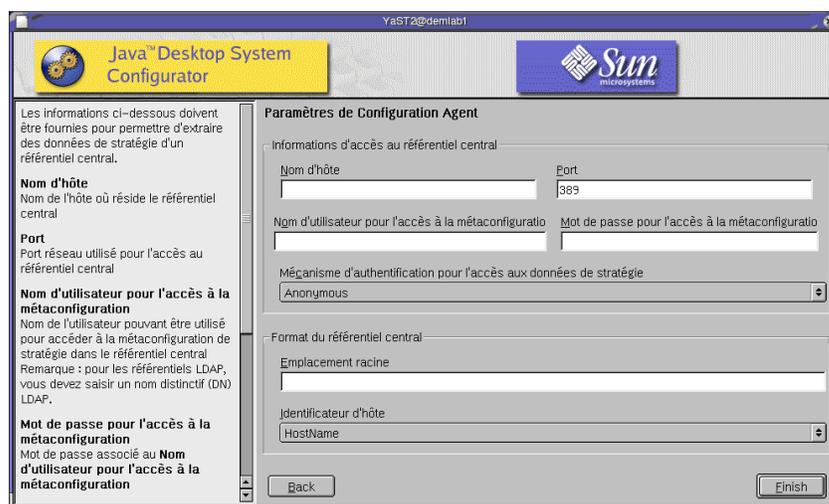


FIGURE 5-1 Java Desktop System Configuration Agent dans YaST

Les informations suivantes sont requises pour exécuter Configuration Agent :

Remarque – Les clés du fichier de propriétés associées sont indiquées entre parenthèses, le cas échéant.

- **Nom d'hôte** (Server) : nom d'hôte du serveur LDAP.
- **Port** (Port) : numéro de port du serveur LDAP.
- **Nom d'utilisateur pour l'accès à la métaconfiguration** (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 à la métaconfiguration** (Password) : mot de passe d'un utilisateur LDAP enregistré.

Remarque – Si l'accès anonyme est activé dans le répertoire, ce paramètre peut rester vide.

- **Mécanisme 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 de l'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.
- **Délai d'expiration de connexion** (Connect Timeout)\~: indique la durée en secondes au bout de laquelle les tentatives de connexion au serveur LDAP expirent. La valeur par défaut est 1 seconde.

Remarque – Lorsque vous modifiez les paramètres d'initialisation et de fonctionnement, vous devez redémarrer Configuration Agent.

Avant de redémarrer Configuration Agent sur le bureau, vérifiez qu'aucune des applications clientes associées n'est en cours d'exécution, connectez-vous en tant que racine et tapez 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 les paramètres localement, éditez le fichier `apocd.properties` dans le répertoire `/opt/apoc/lib`. Pour configurer les 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 `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](#)" à la page 32 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 relatives aux ports de Configuration Agent

Configuration Agent utilise deux ports\~:

- le port du démon (par défaut, le 38900), utilisé par le démon pour communiquer avec les applications clientes.
- Le port d'administration du démon (par défaut, le 38901) utilisé par le programme de contrôle du démon, `apocdctl`, pour communiquer avec le démon.

Modification du port du démon\~ :

Pour modifier le port du démon, vous devez modifier la propriété `DaemonPort` dans le fichier `apocd.properties` du démon et les entrées `apocd` dans `/etc/services` et `/etc/inetd.conf`. Ensuite, redémarrez le démon et rechargez `inetd`.

Modification du port d'administration du démon\~:

Pour modifier le port d'administration du démon, vous devez modifier la propriété `DaemonAdminPort` dans le fichier `apocd.properties` du démon. Ensuite, redémarrez 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.

Composants de bureau - Solaris™

Ce chapitre fournit des informations spécifiques relatives au système d'exploitation Solaris.

Pour accéder aux données de configuration à partir de Configuration Manager, un client de bureau a besoin de 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.

Configuration Agent

Configuration Agent fait partie des packages `SUNWapbas`, `SUNWapmsc` et `SUNWapoc`. Lorsque vous installez le package Solaris SVR4, les fichiers nécessaires à cette API sont installés. Vous pouvez installer les packages manuellement ou par le biais de l'installation Java Desktop System. Une fois l'installation terminée, vous devez configurer et activer Configuration Agent sur votre système.

Pour accéder aux données de configuration distantes, Configuration Agent a besoin de quelques informations d'initialisation, telles que le nom d'hôte et le port du serveur LDAP. Ces informations figurent dans un ensemble de fichiers de propriétés, notamment `polycmgr.properties`, `apocd.properties` et `os.properties`. Ces fichiers sont stockés localement dans le répertoire `/etc/apoc`. Vous pouvez modifier ces fichiers de propriétés manuellement ou utiliser l'assistant de configuration de Configuration Agent.

L'assistant de configuration intègre une interface graphique utilisateur qui vous guide dans les paramètres requis de Configuration Agent. Un écran d'aide est disponible pour chaque page de l'assistant. Vous pouvez démarrer l'assistant en tant que

superutilisateur (racine) à l'aide du script `/usr/bin/apoc-config`. Une entrée de menu est également disponible sur le bureau sous Préférences/Système/Paramètres réseau ou sous Matériel///Carte réseau dans le gestionnaire de fichiers Nautilus.

Remarque – Vous pouvez également démarrer l'assistant sans lancer l'interface graphique. Par exemple, exécutez `/usr/bin/apoc-config -nodisplay` pour démarrer l'assistant en mode console.

Informations d'initialisation

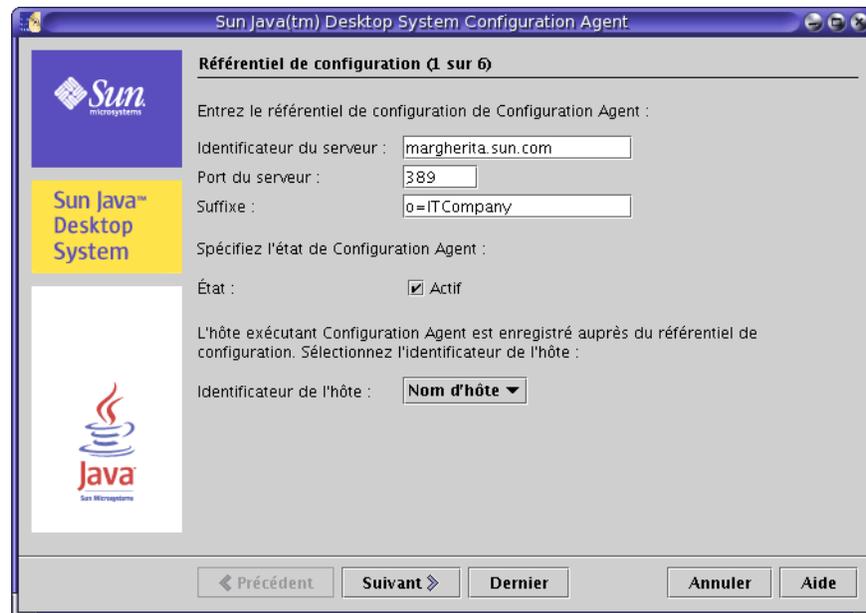


FIGURE 6-1 Configuration Agent, référentiel de configuration

Remarque – Les clés du fichier de propriétés associées sont indiquées entre parenthèses, le cas échéant.

- **Identificateur du serveur** (Server) : nom d'hôte du serveur LDAP.
- **Port du serveur** (Port) : numéro de port du serveur LDAP.
- **Suffixe** (BaseDn) : DN de base du référentiel LDAP.

- **État** : état de Configuration Agent. Cette case à cocher permet d'activer ou de désactiver Configuration Agent. Pour pouvoir utiliser le référentiel de configuration, Configuration Agent doit être actif. L'activation inclut automatiquement l'enregistrement nécessaire avec inetd.

Remarque – Pour activer ou désactiver manuellement Configuration Agent, connectez-vous en tant que **racine** et tapez la commande `/usr/lib/apocd enable` ou `/usr/lib/apocd disable`.

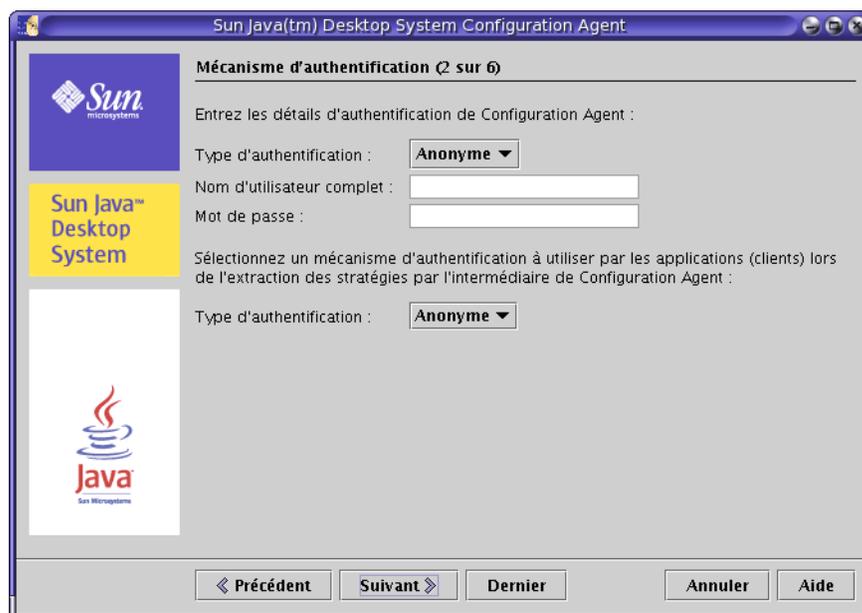


FIGURE 6-2 Configuration Agent, mécanisme d'authentification

- **Identificateur de l'hôte** (HostIdentifier) : peut être "HostName" ou "IPAddress". L'identificateur défini 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.
- **Type d'authentification** de Configuration Agent : peut être "Anonyme" ou "Simple". Si vous sélectionnez "Anonyme", les champs **Nom d'utilisateur complet** et **Mot de passe** sont automatiquement désactivés.
- **Nom d'utilisateur complet** (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 (Password) : mot de passe d'un utilisateur LDAP enregistré.

Remarque – Si l'accès anonyme est activé dans le répertoire, ce paramètre peut rester vide.

- **Type d'authentification** pour les applications (AuthType) : peut être "Anonyme" ou "GSSAPI", selon le mode d'authentification des utilisateurs employé par le serveur LDAP.

Paramètres de port

Configuration Agent :

- **Port de l'agent** (DaemonPort) : utilisé par l'agent pour communiquer avec les applications clientes (la valeur par défaut est **38900**).
- **Port d'administration** (DaemonAdminPort) : utilisé par le programme de contrôle de l'agent, `apocdctl`, pour communiquer avec l'agent (la valeur par défaut est **38901**).

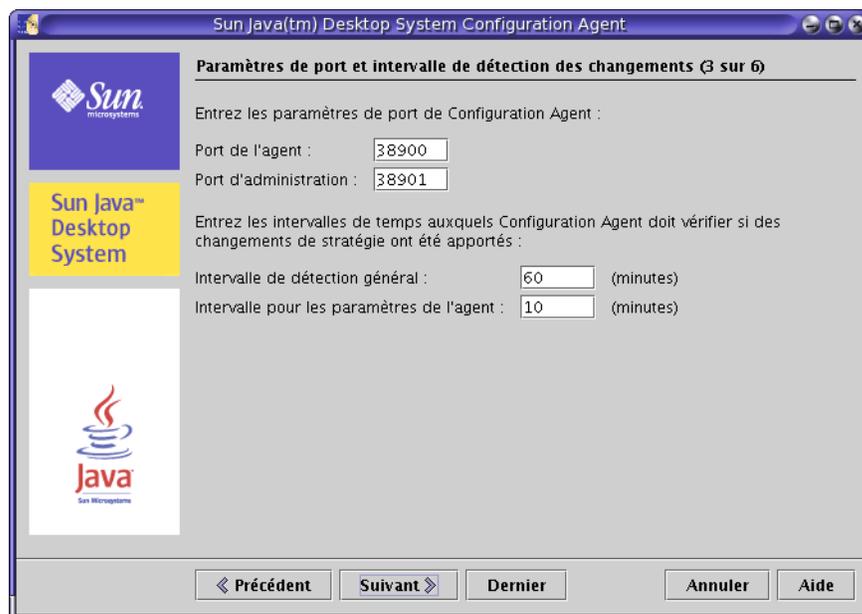


FIGURE 6-3 Configuration Agent, paramètres de port

Intervalle de détection des changements

Configuration Agent recherche régulièrement les changements apportés aux données de configuration en utilisant deux intervalles :

- **Intervalle de détection général** (ChangeDetectionInterval) : intervalle (en minutes) entre les cycles de détection des changements des données de configuration des applications (ou clients) de bureau.

Remarque – Si vous indiquez la valeur -1, la détection des changements est désactivée.

- **Intervalle pour les paramètres de l'agent** (DaemonChangeDetectionInterval) : intervalle en minutes entre les cycles de détection des changements des paramètres de configuration propres à l'agent.

Remarque – Si vous indiquez la valeur -1, la détection des modifications est désactivée.

Vous pouvez utiliser l'intervalle de détection général pour affiner la propagation des modifications des données de configuration distantes sur les applications côté client. La valeur entrée pour ce paramètre correspond à la durée maximum (en minutes) qui s'écoule avant que les modifications apportées à distance ne se reflètent dans les applications clientes.

Si vous indiquez des valeurs peu élevées, l'activité de Configuration Agent et du serveur LDAP est augmentée. Vous devez donc ajuster avec précaution la valeur de ces paramètres. 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.

Paramètres de fonctionnement

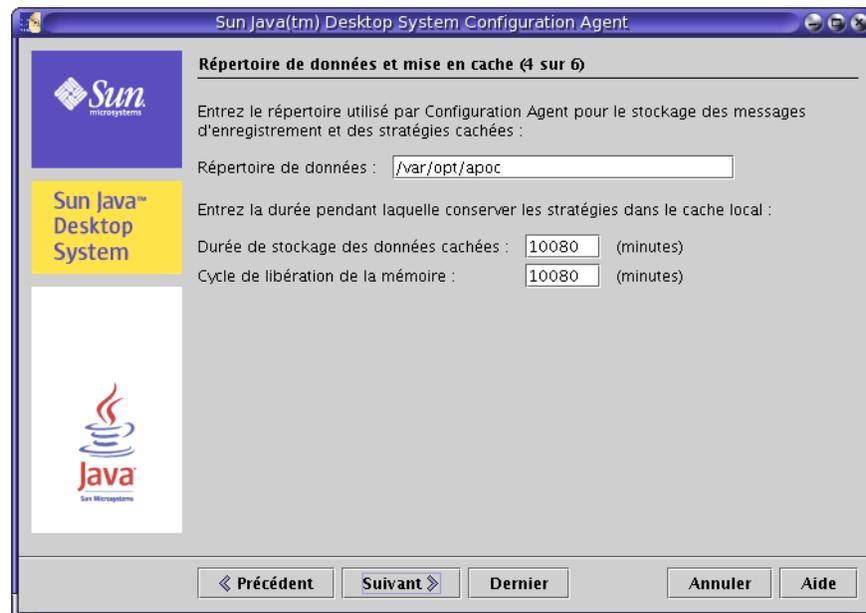


FIGURE 6-4 Configuration Agent, répertoire de données

Vous pouvez configurer les paramètres suivants :

- **Répertoire de données (DataDir)** : répertoire utilisé pour stocker les données d'exécution. Le répertoire par défaut est `/var/opt/apoc`.
- **Durée de stockage des données cachées (TimeToLive)** : intervalle en minutes pendant lequel les données de configuration qui ne sont pas hors ligne demeurent dans la base de données locale.

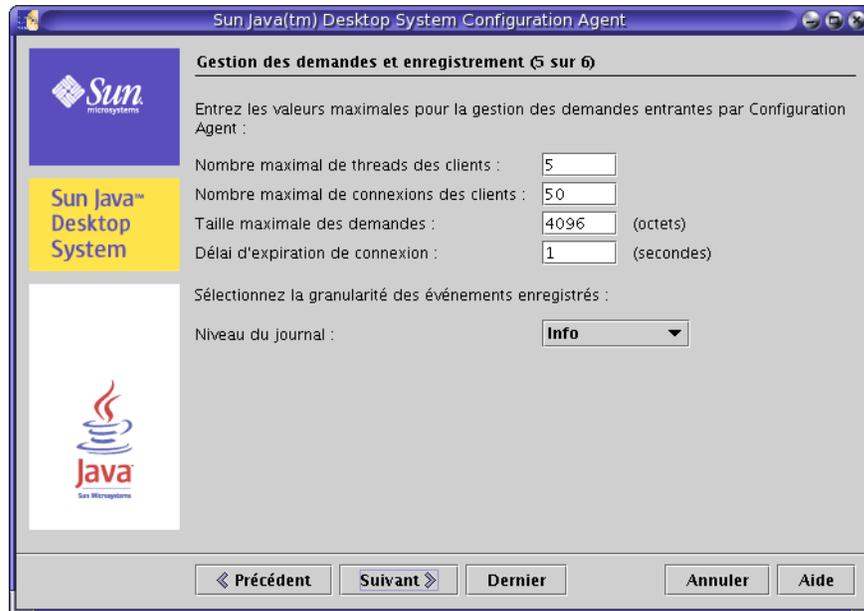


FIGURE 6-5 Configuration Agent, gestion des demandes et enregistrement

- **Cycle de libération de la mémoire** (GarbageCollectionInterval) : intervalle en minutes entre les cycles de libération de la mémoire dans la base de données de configuration locale.
- **Nombre maximal de threads des clients** (MaxClientThreads) : nombre maximal de demandes des clients pouvant être traitées simultanément.
- **Nombre maximal de connexions des clients** (MaxClientConnections) : nombre maximal de connexions des clients.
- **Taille maximale des demandes** (MaxRequestSize) : taille maximale des demandes des clients.
- **Délai d'expiration de connexion** (ConnectTimeout) : indique l'intervalle accordé au serveur LDAP pour répondre à une demande de connexion. La valeur par défaut est une seconde.
- **Niveau du journal** (LogLevel) : niveau de détail dans les fichiers journaux des agents. Le niveau de détail d'enregistrement 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*
- *LE PLUS FIN*

Remarque – La plupart des paramètres de fonctionnement, à l’exception des paramètres **Répertoire de données** et **Délai d’expiration de connexion**, peuvent être gérés centralement à l’aide des stratégies correspondantes stockées sur le serveur LDAP. Si vous souhaitez utiliser cette fonction, n’adaptez pas les paramètres correspondants à l’aide de l’assistant. Utilisez plutôt les stratégies de Configuration Agent disponibles dans Configuration Manager pour spécifier centralement les paramètres de fonctionnement.

Application des paramètres de l’agent

À l’exception des paramètres “Répertoire de données” et “Délai d’expiration de connexion”, les paramètres de fonctionnement stockés sur le serveur LDAP par le biais de Configuration Manager prennent automatiquement effet lors du prochain cycle de détection des changements de la configuration de l’agent (voir `DaemonChangeDetectionInterval`).

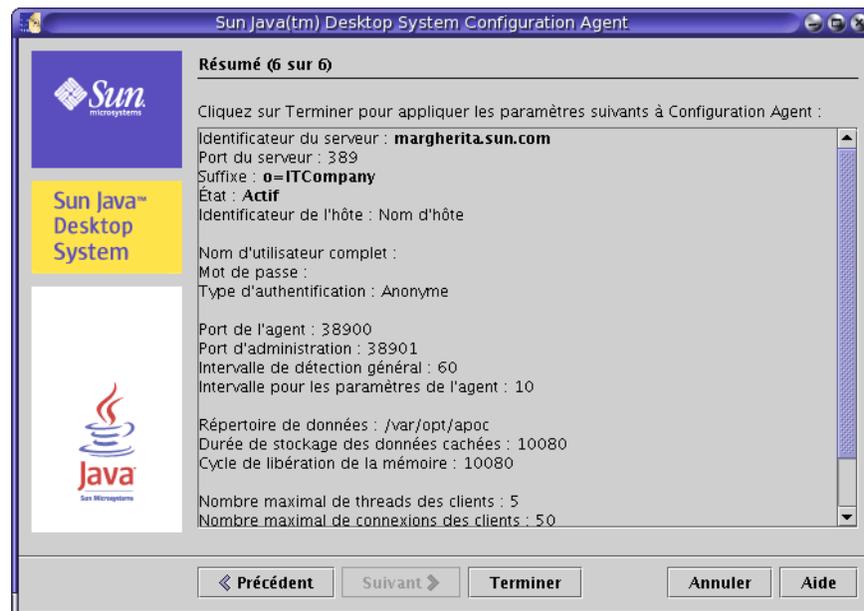


FIGURE 6-6 Configuration Agent, résumé

Tous les paramètres modifiés en local nécessitent le rechargement ou le redémarrage de Configuration Agent. Cette opération s’effectue automatiquement si vous utilisez l’assistant de configuration.

Remarque – Pour redémarrer manuellement Configuration Agent, assurez-vous qu’aucune application client n’est en cours d’exécution, connectez-vous en tant que racine, puis tapez la commande `/usr/lib/apoc/apocd restart`.

Adaptateur GConf

L’adaptateur GConf fait partie du package `SUNWapoc-adapter-gconf`. Lorsque vous installez l’adaptateur à partir du package 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. 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 `SUNWmozapoc-adapter`. 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.

Packages de la Sun Web Console

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 Sun Web Console. L'utilisateur doit explicitement se déconnecter d'une session dans la Sun Web Console avant de fermer une fenêtre d'application.

Utilisation du script d'installation

Synopsis : `setup [-h] | [-n] | [-d
<var>, <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 Sun Web Console

-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 Sun Web Console, exécutez la commande
`/usr/lib/webconsole/setup -u`.

Remarque – N'exécutez pas cette commande si vous vous trouvez dans le répertoire `/usr/lib/webconsole` ou l'un de ses sous-répertoires, sans quoi `pkgrm` échouera.

Packages de la Sun Web Console

Packages Solaris

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

RPM Linux

Nom	Description
SUNWmctag	Bibliothèque de balises de l'interface utilisateur de la Sun Web Console
SUNWmcon	Sun Web Console

Nom	Description
SUNWmcos	Services Linux communs pour la Sun Web Console
SUNWmcosx	Services spécifiques à la version Linux pour la Sun Web Console
SUNWmconr	Racine de la Sun Web Console
SUNWjato	Exécution de Sun One Application Framework
tomcat4	Tomcat

Packages de Configuration Manager

Packages de Configuration Manager

Packages Solaris

Nom	Description
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

Nom	Description
apoc-manager	Configuration Manager
apoc-agent-templates	Modèles de Configuration Agent

Nom	Description
apoc-evolution-templates	Modèles d'Evolution
apoc-gnome-templates	Modèles de Gnome
apoc-mozilla-templates	Modèles de Mozilla
apoc-staroffice-templates	Modèles de StarOffice

Utilisation d'OpenLDAP et d'Active Directory avec Configuration Manager

Utilisation d'un serveur OpenLDAP avec Configuration Manager

Pour utiliser un serveur OpenLDAP en tant que référentiel pour les données de Configuration Manager, vous devez étendre le schéma du serveur afin de prendre en charge les classes d'objet et les attributs utilisés pour stocker les données de configuration. Un fichier de schéma personnalisé nommé `apoc.schema` est disponible dans le sous-répertoire `openldap` de l'outil de déploiement de Configuration Manager fourni sur le CD-ROM Java Desktop System Management Tools.

Vous devez copier ce fichier dans le sous-répertoire `schema` du répertoire de configuration d'OpenLDAP (`/etc/openldap`) et l'ajouter au schéma OpenLDAP en l'intégrant au fichier `slapd.conf` situé dans ce répertoire. Pour ce faire, insérez la ligne `include /etc/openldap/schema/apoc.schema` à la fin de la séquence du schéma présente dans ce fichier. Pour plus d'informations sur l'extension du schéma d'un serveur OpenLDAP, reportez-vous à son manuel.

Pour préparer la base de données OpenLDAP au stockage des données de configuration, vous devez utiliser l'outil de déploiement fourni avec Configuration Manager. Le schéma ayant déjà été étendu lors de l'étape d'installation précédente, il vous suffit d'exécuter le script `createServiceTree()`. 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 les attributs typiques d'OpenLDAP est fourni dans le sous-répertoire `openldap` de l'outil de déploiement. Vous pouvez déployer ce fichier nommé `OrganizationalMapping` en écrasant le fichier du même nom dans le répertoire principal de l'outil de déploiement avant de lancer `createServiceTree()`.

Remarque – L'agent de Configuration Manager tentera de se connecter anonymement au serveur OpenLDAP en fournissant le DN de l'utilisateur pour lequel il requiert des données sans préciser de mot de passe. Ce type d'authentification anonyme peut être désactivé par défaut sur certaines versions de serveurs OpenLDAP. Dans ce cas, procédez à l'activation en ajoutant la ligne `allow bind_anon_cred` aux paramètres communs du serveur définis dans le fichier `slapd.conf` dans le répertoire de configuration d'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 en tant que référentiel pour les données de Configuration Manager, vous devez étendre le schéma du serveur afin de prendre en charge les classes d'objet et les attributs utilisés pour stocker les données de configuration. Un fichier d'extension de schéma nommé `apoc-ad.ldf` est disponible dans le sous-répertoire `ad` de l'outil de déploiement de Configuration Manager fourni sur le CD-ROM Management Tools. Pour plus d'informations, reportez-vous à la section concernant l'outil de déploiement.

Pour importer le fichier `apoc-ad.ldf` dans le schéma Active Directory, procédez comme suit :

1. Activez les extensions de schéma. Reportez-vous à la documentation d'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" <BaseDN> -f apoc-ad-registry.ldf`.

Remarque – Remplacez `<BaseDN>` par le DN de base d'Active Directory.

Utilisez l'outil de déploiement pour préparer le serveur Active Directory au stockage des données de configuration. Le schéma ayant déjà été étendu lors l'étape d'installation précédente, il vous suffit d'exécuter le script `createServiceTree`. 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 les attributs typiques d'Active Directory est fourni dans le sous-répertoire `ad` du répertoire de l'outil de déploiement. Vous pouvez déployer ce fichier nommé `OrganisationalMapping` en écrasant le fichier du même nom dans le répertoire principal de l'outil de déploiement avant de lancer `createServiceTree`.

À partir de ce moment, vous pouvez utiliser le serveur Active Directory avec Configuration Manager. Lors de l'installation de Configuration Manager, saisissez le DN complet et le mot de passe d'un utilisateur disposant de droits d'accès en 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, l'ordinateur qui exécute Configuration Manager doit connaître le nom de domaine d'Active Directory. Pour ce faire, ajoutez une ligne mappant l'adresse IP du serveur Active Directory avec son nom de domaine dans le fichier `/etc/hosts` de cet ordinateur.

Pour pouvoir extraire les données de configuration d'un hôte Java Desktop System, cet hôte doit également connaître le nom de domaine d'Active Directory. L'authentification de l'utilisateur de Java Desktop System peut s'effectuer de deux manières différentes : 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 tous les utilisateurs. Reportez-vous à la documentation Active Directory pour plus d'informations sur l'exécution de cette opération.
- Pour procéder à l'authentification à l'aide de GSSAPI, vous devez modifier le fichier `/etc/krb5.conf`, qui spécifie les paramètres Kerberos, afin de définir le domaine Active Directory et de désigner le serveur Active Directory en tant que centre de distribution de clés (Key Distribution Center ou KDC). Ce fichier 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, vous devez obtenir des informations d'identification valides pour l'utilisateur connecté à Java Desktop System. Vous pouvez extraire ces informations manuellement en exécutant la commande `kinit` et en saisissant 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. Reportez-vous à la documentation de Java Desktop System pour plus d'informations.

