



# Guide d'installation de Sun Desktop Manager 1.0



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

Référence : 819-6092-10

Copyright 2006 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. Aucune partie de ce produit ou document ne peut être reproduite sous quelque forme ou par quelque moyen que ce soit sans l'autorisation écrite préalable de Sun et de ses bailleurs de licence éventuels. 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.

Des parties de ce produit peuvent être dérivées des systèmes Berkeley BSD concédés sous licence par l'Université de Californie. 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 novateurs de Xerox en ce qui concerne la recherche et le développement du concept des interfaces visuelles ou graphiques dans le domaine informatique. Sun détient une licence non exclusive de Xerox sur l'interface graphique Xerox. Cette licence couvre également les détenteurs de licences Sun qui implémentent l'interface graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Droits du gouvernement américain – Logiciel commercial Les utilisateurs gouvernementaux sont soumis au contrat de licence standard de Sun Microsystems, Inc. et aux clauses applicables du FAR et de ses suppléments.

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

# Table des matières

---

<b>Préface</b> .....	5
<b>1 Présentation et concepts</b> .....	7
Présentation de Sun Desktop Manager .....	7
<b>2 Installation de l'application de gestion</b> .....	9
Sun Desktop Manager .....	9
▼ Installation .....	9
▼ Opération .....	10
▼ Suppression de Desktop Manager .....	10
Problèmes de migration .....	11
▼ Création d'un référentiel de configuration .....	11
Dépannage de Desktop Manager .....	12
<b>3 Composants client</b> .....	15
Configuration Agent .....	16
Informations d'initialisation .....	16
Paramètres de port .....	20
Intervalle de détection des changements .....	21
Paramètres de fonctionnement .....	22
Application des paramètres de l'agent .....	24
Paramètres supplémentaires de l'agent .....	25
Utilisation d'une stratégie locale .....	25
▼ Déploiement d'une stratégie locale .....	25
Redémarrage automatique de Configuration Agent .....	26
Accès aux données / Authentification des utilisateurs .....	26
Adaptateurs .....	27
Adaptateur GConf .....	27

Adaptateur Java Preferences .....	28
Adaptateur Mozilla .....	28
Adaptateur StarOffice .....	29
Adaptateur de définition du bureau .....	29
Suppression des adaptateurs .....	29
Dépannage de l'adaptateur .....	30
Dépannage de Configuration Agent .....	30
Questions et réponses .....	30
<b>4 Console Web de Java .....</b>	<b>45</b>
Installation .....	45
Configuration système requise .....	45
Installation de la Console Web de Java .....	46
Exécution de la console .....	46
Suppression de la Console Web de Java .....	47
Dépannage de la Console Web de Java .....	47
Impossible d'installer la Console Web de Java .....	47
Connexion refusée .....	47
Impossible de se connecter .....	48
Aucun lien à Desktop Manager .....	48
Exception du pointeur nul, erreur Tomcat/Java ou page blanche .....	48
Autres problèmes .....	48
<b>A Paramètres de configuration .....</b>	<b>51</b>
<b>B Utilisation d'OpenLDAP et d'Active Directory avec Desktop Manager .....</b>	<b>55</b>
Utilisation d'un serveur OpenLDAP avec Desktop Manager .....	55
Utilisation d'un serveur Active Directory avec Desktop Manager .....	56
<b>C Mappage organisationnel .....</b>	<b>57</b>
Mappage organisationnel .....	57

# Préface

---

Ce document décrit les procédures d'installation et de configuration nécessaires au déploiement de Sun™ Desktop Manager 1.0.

## Présentation

Sun Desktop Manager a pour objectif de fournir une configuration centrale pour les hôtes de bureau. Les paramètres peuvent être assignés à divers éléments de la structure d'une organisation ou d'un domaine, ce qui permet à l'administrateur de gérer efficacement les groupes d'utilisateurs ou d'hôtes.

## Organisation de ce manuel

Le [Chapitre 1](#) présente brièvement Sun Desktop Manager.

Le [Chapitre 2](#) traite de l'installation côté serveur de Sun Desktop Manager.

Le [Chapitre 3](#) fournit des informations sur l'installation de Java Desktop System Configuration Agent.

Le [Chapitre 4](#) fournit des informations sur l'installation de la Console Web de Java.

L'[Annexe A](#) inclut des informations sur les paramètres de configuration.

L'[Annexe B](#) détaille l'utilisation d'OpenLDAP et d'Active Directory avec Desktop Manager.

L'[Annexe C](#) donne des informations sur le mappage organisationnel.

## Documentation connexe

- *Guide d'administration Sun Desktop Manager 1.0*
- *Sun Desktop Manager 1.0 Developer Guide*

## Documentation, support et formation

Fonction Sun	URL	Description
Documentation	<a href="http://www.sun.com/documentation/">http://www.sun.com/documentation/</a>	Télécharger des documents PDF et HTML, et commander des documents imprimés
Support et formation	<a href="http://sunsolve.sun.com">http://sunsolve.sun.com</a>	Obtenir une assistance technique, télécharger des patches et recevoir des informations sur les cours Sun

# Présentation et concepts

Ce document décrit les procédures d'installation et de configuration nécessaires au déploiement de Sun™ Desktop Manager 1.0. Pour une présentation plus exhaustive de Sun Desktop Manager, consultez le *Guide d'administration Sun Desktop Manager 1.0*.

## Présentation de Sun Desktop Manager

Sun Desktop Manager propose une configuration centrale pour les hôtes de bureau. Les paramètres peuvent être assignés à divers éléments de la structure d'une organisation ou d'un domaine, ce qui permet à l'administrateur de gérer efficacement les groupes d'utilisateurs ou d'hôtes.

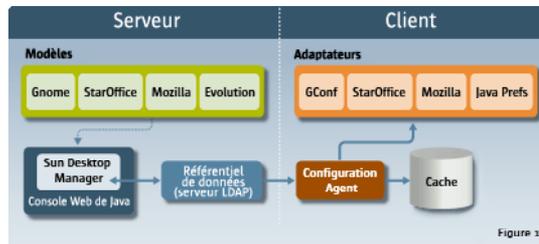


FIGURE 1-1 Architecture de Desktop Manager

Les composants principaux de Desktop Manager sont :

- Référentiels de configuration
- Outils de gestion
- Modèles de Desktop Manager
- Configuration Agent
- Adaptateurs de configuration

Les données de configuration sont centralisées dans les référentiels de configuration. Elles sont gérées (créées, supprimées, modifiées, assignées ou leur assignation est annulée) à l'aide des outils de

gestion. Ces derniers se composent d'une interface graphique utilisateur Desktop Manager Web et d'une interface de ligne de commande. L'outil de gestion Web utilise les modèles pour le rendu des données de configuration dans le navigateur Web.

Configuration Agent extrait les données de configuration du référentiel de configuration pour le compte des applications utilisateur. L'agent met en cache les informations provenant du référentiel de configuration centrale.

Les outils de gestion sont indépendants de l'agent, ce qui signifie qu'ils agissent seulement sur le référentiel de configuration.

Les applications utilisateur (faisant appel aux adaptateurs de configuration) interrogent les données de configuration via Configuration Agent.

Le produit prend directement en charge la récupération et l'application des paramètres des systèmes de configuration suivants :

- GConf : structure de configuration Gnome
- StarOffice Registry
- Mozilla Preferences
- Java Preferences

# Installation de l'application de gestion

---

Ce chapitre présente les instructions sur l'installation des composants côté serveur de Sun Desktop Manager.

## Sun Desktop Manager

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

### ▼ Installation

#### **Avant de commencer**

Desktop Manager nécessite l'installation de la Console Web de Java, version 2.2.5 ou ultérieure. Veuillez vous assurer qu'une version valide est installée sur votre système. Pour effectuer cette opération, connectez-vous en tant que superutilisateur (root) et exécutez la commande :

```
# smcwebserver status
```

---

**Remarque** – La Console Web de Java 2.2.4 fait partie du système d'exploitation Solaris™ 10, cependant Desktop Manager exige la version 2.2.5 ou ultérieure. Une copie de la version 2.2.5 est fournie dans l'archive Desktop Manager située dans le répertoire du serveur/de la console. Elle peut être installée en exécutant `./setup` dans ce répertoire.

---

Si la Console Web de Java n'est pas installée sur votre système ou si la version installée ne convient pas à Desktop Manager, consultez les instructions du [Chapitre 4](#) pour installer ou mettre à jour, au préalable, la Console Web de Java. Revenez ensuite au chapitre actuel pour poursuivre l'installation de Desktop Manager.

**1 Téléchargez l'archive zip de Desktop Manager et extrayez le contenu dans un répertoire temporaire.**

```
# unzip SunDesktopMgr-1.0.zip
```

**2 Connectez-vous en tant que superutilisateur (root) et exécutez le script d'installation via**

```
# cd SunDesktopMgr-1.0/<plate-forme>/server/manager
```

```
# ./setup
```

**3 Consultez la sortie des scripts d'installation pour détecter toute erreur éventuelle.**

Si l'installation a réussi, le script d'installation redémarre automatiquement la Console Web de Java ; vous pouvez alors accéder au Desktop Manager à l'aide d'un navigateur Web.

## ▼ Opération

**1 Saisissez l'URL suivant dans votre navigateur :**

```
https://<nomd'hôte>.<nomdedomaine>:6789
```

**2 Dans l'écran de connexion, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur Unix.**

La Console Web de Java s'ouvre.

**3 Dans la page de lancement de l'application de la console, cliquez sur le lien Desktop Manager.**

- **Si vous voulez passer outre cette page et ouvrir directement Desktop Manager, saisissez l'URL suivant dans votre navigateur :**

```
https://<nomd'hôte>.<nomdedomaine>:6789/apoc
```

## ▼ Suppression de Desktop Manager

- ▶ **Pour supprimer Desktop Manager de la Console Web de Java, passez au niveau du répertoire temporaire que vous avez créé pour l'installation, connectez-vous en tant que superutilisateur (root) et exécutez la commande :**

```
# cd server/manager
```

```
# ./setup -u
```

## Problèmes de migration

Desktop Manager est compatible avec les versions précédentes de Java Desktop System Configuration Manager (versions 1.0 et 1.1). Cependant, il convient de noter certaines différences.

Dans les versions précédentes de Configuration Manager, toutes les données de profil sont stockées dans un serveur LDAP spécifié. Ce serveur LDAP est configuré au cours de la procédure d'installation globale de Configuration Manager. Celle-ci inclut la configuration d'un module de connexion LDAP qui encapsule les données d'authentification par rapport au serveur LDAP.

Pour Desktop Manager, l'ensemble des différentes étapes de configuration est réalisé par le biais de l'assistant ; toute opération de configuration au cours de l'installation est inutile. Desktop Manager inclut désormais la prise en charge de plusieurs référentiels de configuration. Cependant, il est possible de gérer les données de stratégie stockées sur différents serveurs LDAP, référentiels fichier, etc. La configuration d'un module de connexion LDAP spécifique n'est plus nécessaire.

Le schéma LDAP n'a subi aucune modification d'une version à l'autre. Si vous avez déjà configuré un serveur LDAP pour une version précédente de Configuration Manager, aucun changement n'est nécessaire lorsque vous passez à Desktop Manager. En conséquence, vous pouvez utiliser Desktop Manager sans mettre à jour le côté client (agent de Java Desktop System Configuration Manager 1.1) ou le côté LDAP.

---

**Remarque** – Avant d'installer Desktop Manager, vous devez d'abord supprimer toute installation précédente de Configuration Manager ou de Desktop Manager sur votre système. Pour supprimer une installation précédente, exécutez la commande (en tant que superutilisateur) :

```
# cd server/manager  
# ./setup -u
```

---

Après avoir installé Desktop Manager, vous pouvez créer un référentiel de configuration qui désigne votre serveur LDAP existant :

### ▼ Création d'un référentiel de configuration

- 1 **Saisissez l'URL suivant dans votre navigateur :**  
`https://<nomd'hôte>.<nomdedomaine>:6789`
- 2 **Dans l'écran de connexion, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur Unix.**  
La Console Web de Java s'ouvre.
- 3 **Dans la page de lancement de l'application de la console, cliquez sur le lien Sun Desktop Manager 1.0.**

#### 4 Cliquez sur le bouton **Nouveau** pour lancer l'assistant du référentiel de configuration.

L'assistant vous guide tout au long du processus de paramétrage du référentiel de configuration LDAP.



---

**Attention** – L'assistant vous propose automatiquement de convertir les données de stratégie existantes au format 2.0, plus récent. Cette migration est facultative et vise principalement à améliorer les performances des nouveaux agents de Sun Desktop Manager 1.0. Tant que vous devez prendre en charge les agents de Java Desktop System Configuration Manager 1.1 dans votre environnement, ne procédez PAS à la migration.

---

## Dépannage de Desktop Manager

### Installation impossible

Symptôme : à la fin de l'installation de la Console Web de Java un message indique qu'elle ne peut pas être démarrée car aucune application n'est enregistrée.

Causes possibles : aucune application n'est installée, notamment Desktop Manager.

Solution : installez Desktop Manager, puis lancez la Console Web de Java.

### Connexion refusée

Symptôme : vous essayez d'ouvrir un URL adéquat, par exemple `http://<nomd'hôte>.<nomdedomaine>:6789`, mais un message vous indique que la connexion est refusée.

Causes possibles : la Console Web de Java n'est pas en cours d'exécution sur le serveur.

Solution : pour lancer la Console Web de Java, connectez-vous en tant que superutilisateur et exécutez les commandes suivantes :

```
#smcwebserver status  
#smcwebserver start
```

### Impossible de se connecter

Symptôme : la combinaison utilisateur/mot de passe est refusée à la page de connexion de la Console Web de Java.

Causes possibles : le compte d'utilisateur UNIX n'existe pas.

Solution : vérifiez si le nom d'utilisateur UNIX correspondant et le mot de passe associé sont configurés sur votre système. Si nécessaire, créez un compte d'utilisateur UNIX local de manière à effectuer des tests.

## Aucun lien à Desktop Manager

Symptôme : la page dressant la liste des applications de Console Web de Java n'affiche pas le lien à Sun Desktop Manager.

Causes possibles : le module Desktop Manager n'est pas installé.

Solution : pour vérifier si Desktop Manager est installé dans la Console Web de Java, connectez-vous en tant que superutilisateur et exécutez la commande suivante :

```
# smreg list -a
```

Si la liste ne contient pas l'application `com.sun.apoc.manager_<version>`, vous devez réinstaller Desktop Manager.

## Exception du pointeur nul, erreur Tomcat/Java ou page blanche

Symptôme : vous lancez Desktop Manager mais seule une page blanche ou des messages d'erreur apparaissent.

Causes possibles : si l'erreur mentionne `NoClassDefFoundError: sun/tools/javac/Main`, la Console Web de Java n'utilise pas la version Java qui convient.

Solution : l'environnement Java de la Console Web de Java actuelle peut être contrôlé en exécutant la commande `# smreg list -p` et en consultant la propriété `java.home`. Cette propriété doit désigner un répertoire de base Java valable et celui-ci doit contenir un kit de développement Java (JDK). Si cette valeur n'est pas correctement définie, vous devez exécuter la commande suivante :

```
# smreg add -p java.home=<RÉPERTOIRE_DE_BASE_JAVA>
```

---

**Remarque** – `<RÉPERTOIRE_DE_BASE_JAVA>` doit désigner une installation valide, par exemple où `javac` se trouve dans le sous-répertoire `bin`.

---

Vous devez ensuite redémarrer la Console Web de Java au moyen de la commande suivante :

```
# smcwebserver restart
```

## Impossible de se connecter à un serveur SSL LDAP

Symptôme : après avoir fourni les détails sur le serveur LDAP dans l'assistant de création du référentiel et avoir coché la case Utiliser SSL, appuyez sur Suivant a pour effet d'afficher un message indiquant qu'il est impossible de joindre le serveur.

Causes possibles : un numéro de port incorrect a été fourni, le serveur LDAP n'est pas configuré pour détecter les connexions utilisant le protocole SSL sur ce port ou les certificats appropriés ne figurent pas dans le keystore de la Console Web de Java.

Solution : vérifiez, en premier lieu, si le serveur LDAP est configuré pour détecter les demandes de connexions SSL sur le port spécifié dans l'assistant. Si tel est le cas, assurez-vous que l'autorité de certification ou le certificat du serveur LDAP figure dans le keystore de la Console Web de Java. Ce

dernier se trouve dans `/etc/opt/webconsole/keystore`. Le certificat peut être ajouté à l'aide de la commande `keytool -import -file <fichier de certificat> -keystore /etc/opt/webconsole/keystore`. Le mot de passe par défaut pour ce keystore est **changeit**. Pour que le changement prenne effet au niveau de Desktop Manager, la Console Web de Java doit être redémarrée au moyen de la commande `smcwebserver restart`.

### **Écriture sur le répertoire impossible.**

Symptôme : lors de la création d'un moteur de traitement fichier ou hybride, le message "Écriture sur le répertoire impossible" s'affiche.

Causes possibles : un utilisateur hors accès ne dispose pas des autorisations appropriées.

Solution : assignez les autorisation d'écriture à l'utilisateur hors accès.

## Composants client

---

Pour accéder aux données de configuration de Desktop Manager, un client de bureau a besoin du système Java Desktop System Configuration Agent. Configuration Agent communique avec le référentiel des données de configuration distantes ainsi qu'avec les adaptateurs et intègre les données dans des systèmes de configuration spécifiques. Les systèmes de configuration actuellement pris en charge sont GConf, Java Preferences, Mozilla Preferences et StarOffice Registry.

Une version de Configuration Agent est fourni avec le système d'exploitation Solaris 10. Cependant, Desktop Manager exige une version plus récente de cet outil. Cette dernière est installée lors de l'installation des composants client de Desktop Manager et de leurs patchs respectifs.

Pour installer les composants client de Desktop Manager :

1. Téléchargez l'archive zip de Desktop Manager et extrayez le contenu dans un répertoire temporaire.

```
# unzip SunDesktopMgr-1.0.zip
```

2. Installez les patchs recommandés.

Ces patchs se trouvent dans le répertoire `SunDesktopMgr-1.0/<plate-forme>/client/Patches`. Conformez-vous aux instructions d'installation fournies pour chaque patch.

3. Connectez-vous en tant que superutilisateur (root) et exécutez le script d'installation via :

```
# cd SunDesktopMgr-1.0/<plate-forme>/client  
# ./setup
```

# Configuration Agent

Configuration Agent est un élément intégré aux différents packages répertoriés dans le tableau suivant :

Nom du package Solaris	Description
SUNWapbas	Bibliothèques partagées de Configuration
SUNWapmsc	Fichiers divers de Configuration Agent
SUNWapoc	Configuration Agent
SUNWapdc	Assistant de Configuration Agent

Lorsque vous installez ces packages, les fichiers requis par cette API sont installés. Vous pouvez installer les packages manuellement ou au cours de l'installation de Java Desktop System. Une fois l'installation terminée, vous devez configurer et activer Configuration Agent sur votre système.

---

**Remarque** – Les packages Configuration Agent sont installés sous Solaris lors de l'installation de Java Desktop System ; cependant, Desktop Manager regroupe ces fichiers en patches au cours de l'installation afin d'offrir le niveau de fonctionnalité qui convient.

---

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 jeu de fichiers de propriétés tels que `policymgr.properties`, `apocd.properties` et `os.properties`. Ces fichiers sont stockés en local dans le répertoire `/etc/apoc`. Vous pouvez modifier manuellement ces fichiers de propriétés (voir [Annexe A](#)) ou utiliser l'assistant de configuration pour Configuration Agent.

L'assistant de configuration intègre une interface graphique utilisateur qui vous guide au cours de la définition des paramètres requis de Configuration Agent. Un écran d'aide est disponible pour chaque page de l'assistant. Vous pouvez lancer l'assistant en tant que superutilisateur (root) par le biais du script `/usr/bin/apoc-config`.

---

**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

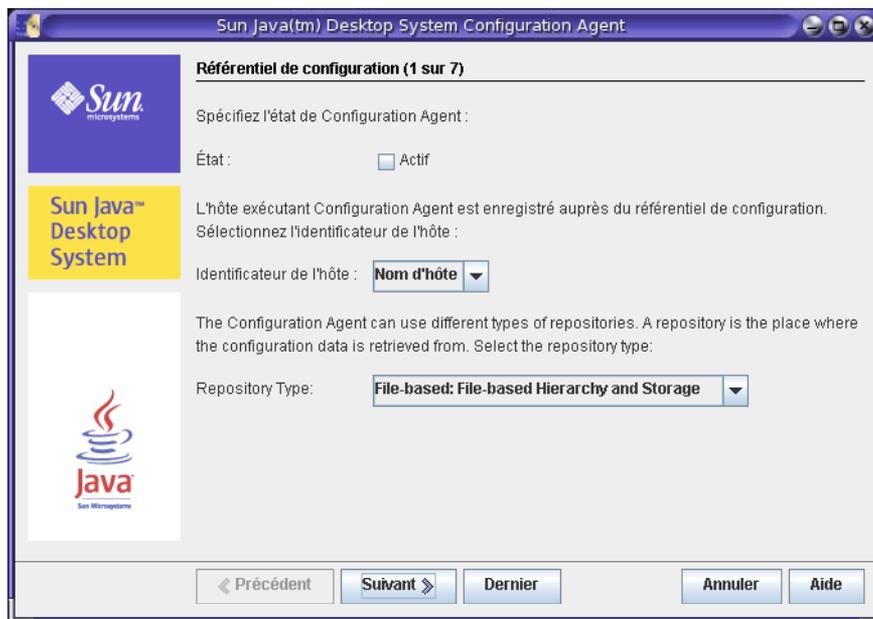


FIGURE 3-1 Configuration Agent, référentiel de configuration

---

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

---

- **État** : état de Configuration Agent. La case à cocher peut être utilisée pour activer ou désactiver Configuration Agent. Pour pouvoir utiliser le référentiel de configuration, Configuration Agent doit être actif. L'activation inclut automatiquement l'enregistrement nécessaire à la fonction de gestion de service ( smf(5) ) sous Solaris.
- **Identificateur de l'hôte (HostIdentifierType)** : peut être de type "NomHôte" : ou "AdresseIP". Lorsque vous recherchez des informations sur la stratégie d'un hôte particulier, Configuration Agent identifie l'hôte actuel par son nom ou par l'adresse IP. Choisissez la valeur correcte en fonction de la manière dont votre hôte est identifié dans le champ Type de référentiel sélectionné.
- **Type de référentiel** : servez-vous de ce paramètre pour indiquer à Configuration Agent si la hiérarchie de votre organisation et les données de configuration sont définies selon un stockage LDAP ou un stockage fichier ou encore selon une combinaison de ces deux types.

---

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

---

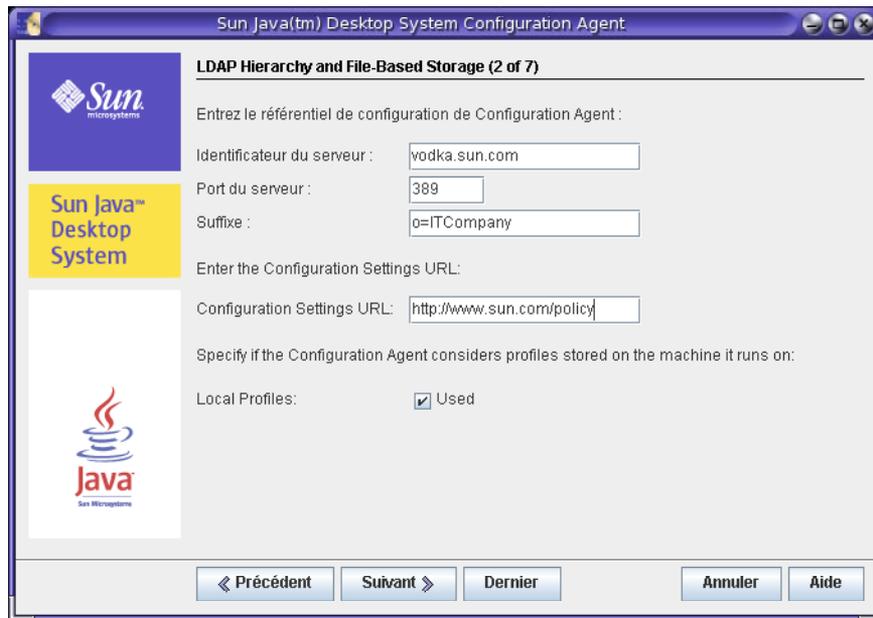


FIGURE 3-2 Configuration Agent, hiérarchie LDAP et stockage fichier

**Remarque** – L'écran tel qu'il est illustré à la [Figure 3-2](#) peut varier selon le type de référentiel choisi à l'écran précédent. Les champs Identificateur du serveur, Port du serveur et Suffixe doivent être remplis si un référentiel de type LDAP ou hybride est choisi. Vous devez remplir le champ URL des paramètres de configuration si le type est fichier ou hybride.

- Identificateur du serveur : nom d'hôte du serveur LDAP.
- Port du serveur : numéro de port du serveur LDAP.
- Suffixe : DN de base du référentiel LDAP.
- URL des paramètres de configuration : URL spécifiant l'emplacement du référentiel fichier.

Une liste des URL peut être utilisée pour spécifier les référentiels de secours au cas où la connexion au premier URL échoue. La liste se compose d'un ou plusieurs URL séparés par des espaces, au format fichier://<chemind'accès>, http://<hôte>:<port>/<chemind'accès> ou https://<hôte>:<port>/<chemind'accès>. Pour plus d'informations, voir [Annexe A](#).

**Remarque** – L'agent essaie d'abord d'accéder au serveur LDAP à l'aide d'une connexion SSL. S'il échoue, l'agent tente d'établir une connexion SSL standard.

Pour que la connexion SSL soit établie, le certificat adéquat doit figurer dans le keystore de l'environnement d'exécution Java. Ce keystore, pour un JRE standard, se trouve dans le <répertoire d'installation>/lib/security/cacerts et pour un JDK standard dans le <répertoire d'installation>/jre/lib/security/cacerts. Le certificat de l'autorité de certification ou du serveur LDAP doit être ajouté à ce magasin à l'aide de la commande `keytool -import -file <fichier de certificat> -keystore <emplacement du fichier cacerts>`. Le mot de passe par défaut pour ce keystore est **changeit**.

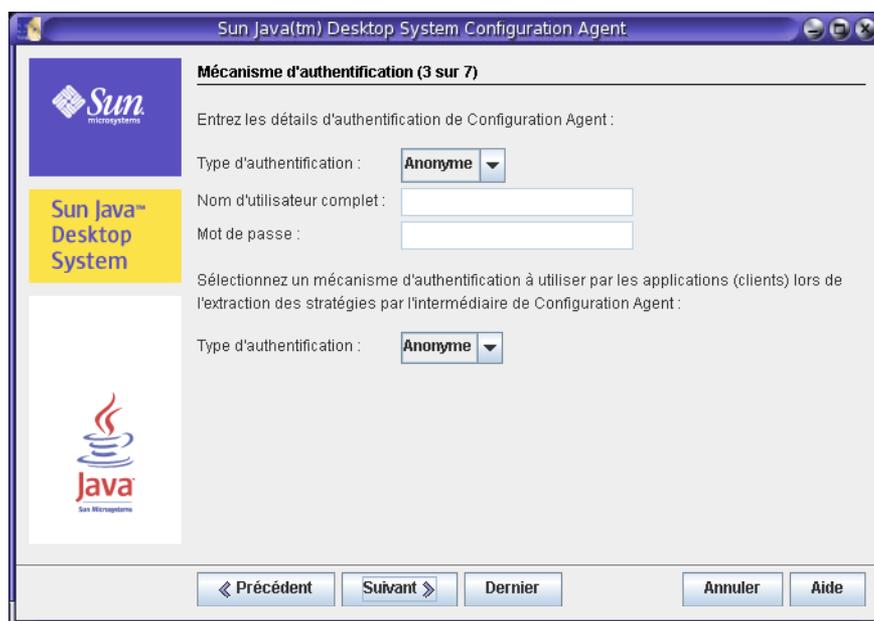


FIGURE 3-3 Configuration Agent, mécanisme d'authentification

- 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.
- Mot de passe (Password) : mot de passe d'un utilisateur LDAP enregistré.

---

**Remarque** – Si l'accès anonyme est activé dans le répertoire, les paramètres Nom d'utilisateur complet et Mot de passe peuvent rester vierges.

---

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

---

**Remarque** – Pour plus d'informations, reportez-vous aux sections "[Accès aux données / Authentification des utilisateurs](#)" à la page 26.

---

## Paramètres de port

Configuration Agent utilise deux ports :

- 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 contrôleur de l'agent, apocd, pour communiquer avec l'agent (la valeur par défaut est **38901**).

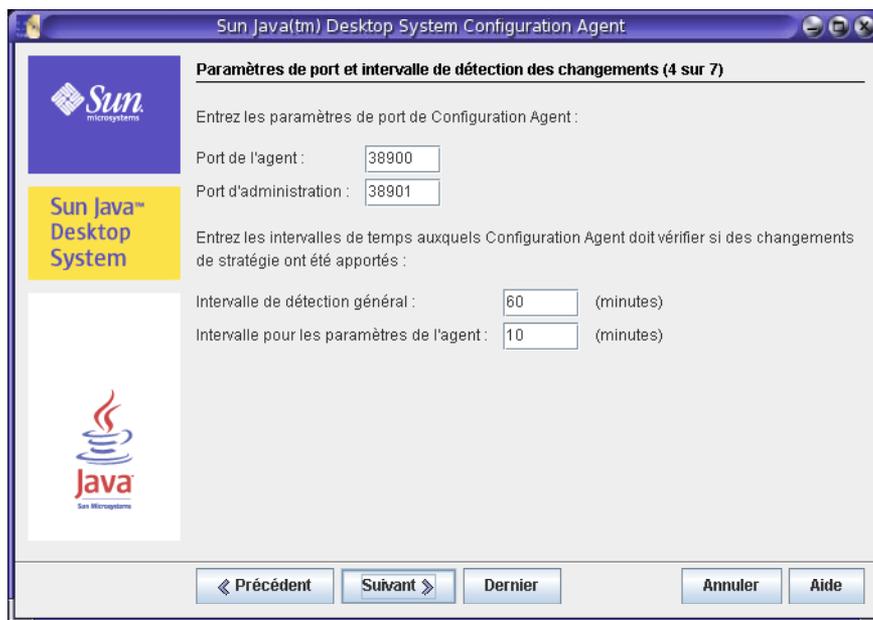


FIGURE 3-4 Configuration Agent, paramètres de port

## 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 changements 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 l'impact de la configuration distante sur les applications clientes. Une fois le test terminé, rétablissez la valeur initiale du paramètre.

## Paramètres de fonctionnement

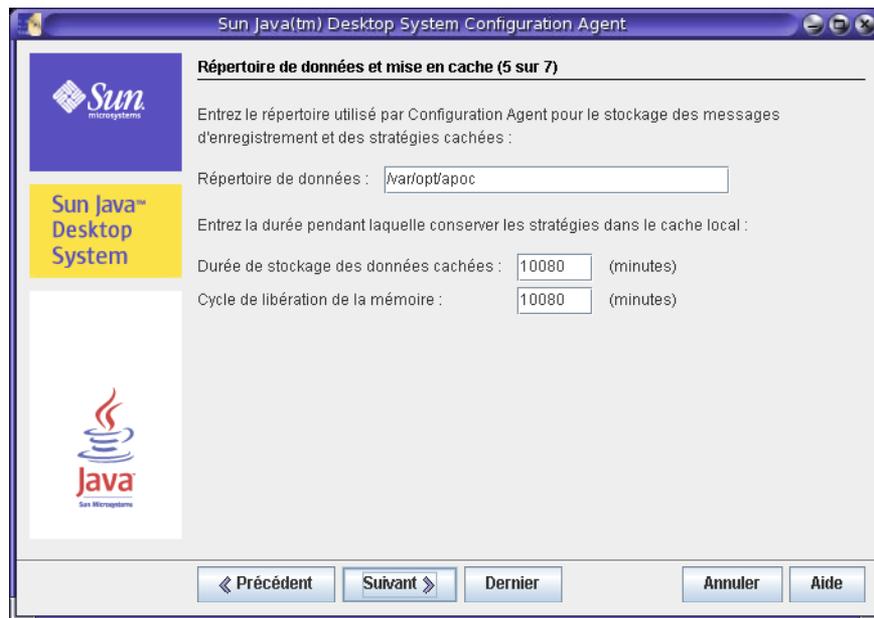


FIGURE 3-5 Configuration Agent, répertoire de données

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.

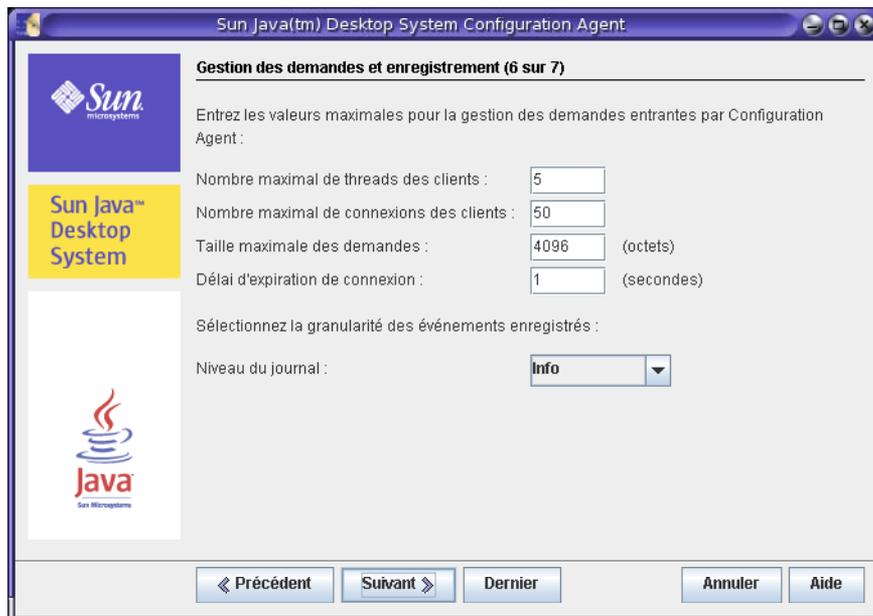


FIGURE 3-6 Configuration Agent, gestion des demandes et enregistrement

- 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 de l'agent. Le niveau de détail de la journalisation doit être une valeur cohérente avec les niveaux du journal Java. Par ordre décroissant de gravité, ces niveaux sont les suivants :
  - *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 centralisés 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 Desktop Manager pour spécifier les paramètres de fonctionnement de manière globale.

## 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 Desktop Manager prennent automatiquement effet lors du prochain cycle de détection des changements de la configuration de l’agent (voir `DaemonChangeDetectionInterval`).

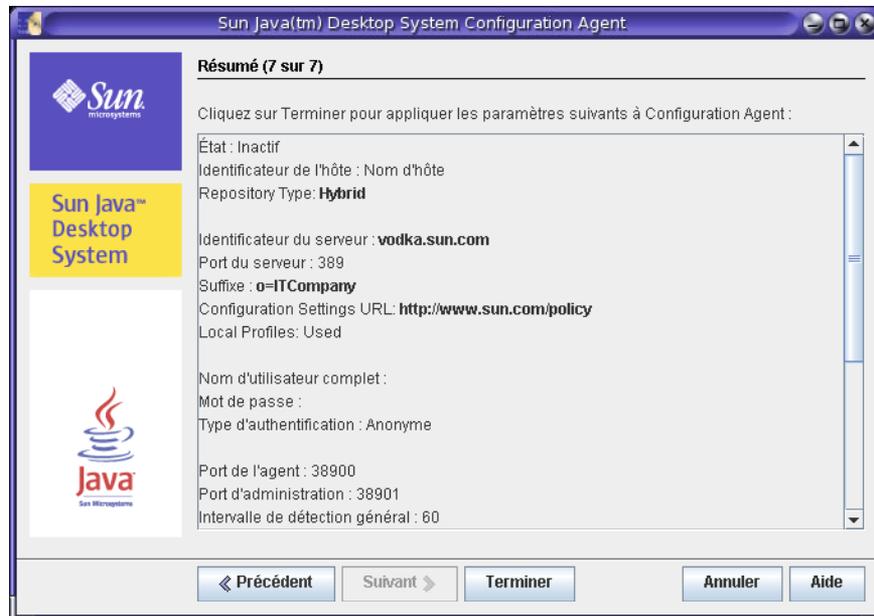


FIGURE 3-7 Configuration Agent, résumé

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 cliente n’est en cours d’exécution, connectez-vous en tant que root, puis tapez la commande `/usr/lib/apoc/apocd restart`.

---

## Paramètres supplémentaires de l’agent

---

**Remarque** – Les paramètres ne sont pas disponibles dans l’assistant de configuration.

---

- Application de la stratégie locale (ApplyLocalPolicy) : utilisez ce paramètre pour indiquer si oui ou non les données liées à la stratégie disponibles sur l’hôte local doivent être mises à la disposition des applications clientes. La valeur “true” : (vrai) indique que les données de stratégie locale doivent être disponibles. La valeur “false” : (faux) indique que les données de stratégie locale ne doivent pas être disponibles. Pour plus de détails, voir [“Utilisation d’une stratégie locale” à la page 25](#).

## Utilisation d’une stratégie locale

Vous pouvez configurer Configuration Agent pour appliquer les paramètres de configuration de la stratégie déployée localement en plus ou à la place d’une stratégie globalement disponible. Procédez de la manière suivante pour déployer une telle stratégie locale :

### ▼ Déploiement d’une stratégie locale

- 1 L’utilisation de Desktop Manager permet de créer un profil avec les paramètres de stratégie requis.
- 2 L’utilisation de Desktop Manager permet d’exporter le profil vers un fichier zip.
- 3 Sur votre hôte client, créez le répertoire  
`${DataDir}/Policies/profiles/PROFILE_REPOSITORY_default` , s’il n’existe pas déjà.  
`${DataDir}` correspond à la valeur du répertoire de données Configuration Agent qui est par défaut `/var/opt/apoc`.
- 4 Copiez le fichier zip précédemment exporté vers  
`${DataDir}/Policies/profiles/PROFILE_REPOSITORY_default`.
- 5 Assurez-vous que Configuration Agent est configuré de manière à appliquer les stratégies locales disponibles (pour plus de détails, voir [“Paramètres supplémentaires de l’agent ” à la page 25](#)).

**Remarque** – Si vous modifiez le paramètre Profils locaux (ApplyLocalPolicy) de Configuration Agent, vous devez recharger Configuration Agent en vous connectant en tant que root et en tapant la commande `/usr/lib/apoc/apocd reload`.

Toute stratégie locale ainsi déployée sera mise à la disposition des clients au cours du prochain cycle de détection des changements de Configuration Agent.

---

## Redémarrage automatique de Configuration Agent

En cas d'échec, Configuration Agent sera automatiquement réinitialisé. Le fonction de gestion de service ( smf(5) ) est responsable de cette décision. Si cette fonction considère qu'un redémarrage n'est pas approprié (lorsque, par exemple, un grand nombre d'échecs se sont déjà produits), Configuration Agent passe en mode de maintenance.

Lorsque Configuration Agent n'est pas relancé, vous devez désactiver temporairement l'agent en vous connectant en tant qu'utilisateur root et en exécutant la commande `/usr/lib/apoc/apocd disable`. Vous devez ensuite résoudre les problèmes à l'origine de l'échec de l'agent et le réactivez en exécutant la commande `/usr/lib/apoc/apocd enable`.

## Accès aux données / Authentification des utilisateurs

Configuration Agent récupère des informations auprès 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 un élément d'utilisateur sur le serveur LDAP. Configuration Agent récupère également des informations relatives à l'hôte, par exemple son nom ou son adresse IP. Les informations sont associées à un élément d'hôte sur le serveur LDAP par le biais du paramètre `Host/UniqueIdAttribute` du fichier de mappage organisationnel. Pour plus d'informations sur le mappage organisationnel, voir [Annexe C](#).

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 de Kerberos à la connexion de l'utilisateur, le module `pam_krb5` doit être installé et configuré sur l'hôte Java Desktop System.

Vous pouvez utiliser `gdm` pour intégrer Kerberos à la connexion de l'utilisateur, par exemple, en utilisant le fichier `/etc/pam.d/gdm` :

```
##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

```

Si vous intégrez Kerberos à la connexion de l'utilisateur de cette manière, vous devez activer la prise en charge de Kerberos par l'économiseur d'écran. Par exemple, vous pouvez utiliser le fichier `/etc/pam.d/xscreensaver` suivant :

```

auth required pamkrb5.so use_first_pass missing_keytab_ok
ccache=SAFE putenv_direct

```

## Adaptateurs

Les adaptateurs d'applications sont des extensions des systèmes de configuration prises en charge par Desktop Manager. Les adaptateurs permettent à différentes applications de prendre en compte les données de configuration centrales, en fonction des systèmes de configuration. Les systèmes de configuration pris en charge sont :

- GConf : système de configuration Gnome, utilisé par les applications de bureau et la plupart des applications Gnome, comme Evolution
- StarOfficeRegistry : système de configuration utilisé par StarOffice et OpenOffice.org
- Mozilla Preferences : système de configuration utilisé par Mozilla
- Java Preferences : API de configuration offertes aux applications Java

Un adaptateur de définition du bureau est également fourni. Il permet d'intégrer des lanceurs de bureau, des options de menu et des programmes de démarrage au bureau de l'utilisateur.

## Adaptateur GConf

L'adaptateur GConf fait partie du package `SUNWapoc-adapter-gconf` pour Solaris. Lorsque vous installez l'adaptateur à partir du package correspondant, le chemin d'accès aux sources de données GConf dans `/etc/gconf/2/path` est mis à jour afin d'inclure les sources Desktop 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.

## Configuration de l'adaptateur GConf

L'adaptateur GConf est configuré au cours de son installation, cependant son fonctionnement dépend de la présence du fichier de chemin GConf (`/etc/GConf/2/path`) de deux sources de données représentant les paramètres centraux obligatoires et les paramètres par défaut. Bien que le

fichier du chemin d'accès contient les informations GConf correctes pour la prise en compte des paramètres centralisés comme requis après l'installation du système, les administrateurs doivent s'assurer que les sources de données munies du préfixe "apoc" sont encore présentes dans le fichier. En effet, ils pourraient être amenés à modifier ce chemin afin d'inclure des sources de données personnalisées supplémentaires. Vous devez également contrôler que les sources de données se trouvent entre les paramètres locaux obligatoires et les paramètres d'utilisateur pour ce qui est de la source de données représentant les paramètres centraux obligatoires et entre les paramètres d'utilisateur et les paramètres locaux par défaut pour ce qui est de la source de données représentant les paramètres centraux par défaut.

## Adaptateur Java Preferences

L'adaptateur Java Preferences fait partie du package `SUNWapc j` pour Solaris.

### Configuration de l'adaptateur Java Preferences

L'adaptateur Java Preferences est fourni comme implémentation de l'API des préférences qui doit être utilisée en tant que wrapper d'une autre implémentation existante (telle que le système fichier par défaut fourni avec JRE). Pour activer l'utilisation de la configuration centrale dans une application Java utilisant l'API des préférences, un script de démarrage doit être écrit pour cette application, à l'aide du script `/usr/lib/apoc/apoc j launchJava`. Ce script doit définir quelques variables d'environnement, puis inclure le script `apoc j launch` à la fin (ce qui démarre l'application Java dans l'environnement qui convient). Les variables d'environnement à définir sont les suivantes :

- `JAVA` : contient le chemin d'accès à l'exécutable d'exécution Java
- `APPLICATION` : contient la partie finale de l'appel d'exécution de Java standard pour ces applications. Par exemple, `nomdelaclass [arguments]` pour le démarrage d'une seule classe ou `- jar nomjar [arguments]` pour le démarrage d'une archive jar.

Les variables d'environnement facultatives supplémentaires pouvant être définies sont :

- `CLASSPATH` : fichiers de classe ou fichiers jar sous forme d'une liste séparée par deux-points devant faire partie du chemin de classe de l'application
- `DEFINES` : chaîne contenant les instructions de définition devant faire partie du démarrage de l'application
- `PREFFACTORY` : nom de classe usine dans l'implémentation sous-jacente de l'API des préférences que l'application doit utiliser

## Adaptateur Mozilla

L'adaptateur Mozilla fait partie du package `SUNWmozapoc - adapter` pour Solaris.

### Configuration de l'adaptateur Mozilla

L'adaptateur Mozilla est configuré au cours de l'installation de ce produit et n'exige aucune configuration supplémentaire.

## Adaptateur StarOffice

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

### Configuration de l'adaptateur StarOffice

L'adaptateur StarOffice est configuré au cours de l'installation de ce produit et n'exige aucune configuration supplémentaire.

## Adaptateur de définition du bureau

L'adaptateur de définition du bureau se compose des packages suivants :

Nom du package	Description
SUNWapleg	binaires d'accès à la configuration
SUNWardsa	adaptateur de définition du bureau
SUNWardsa-misc	intégration système pour adaptateur

Ces packages sont installés si les composants client Desktop Manager sont installés et ne demandent aucune configuration supplémentaire.

### Configuration de l'adaptateur de définition du bureau

L'adaptateur de définition du bureau est configuré par le processus d'installation à utiliser à la connexion d'un utilisateur et ne demande aucune configuration supplémentaire.

## Suppression des adaptateurs

Les adaptateurs Mozilla et StarOffice sont supprimés à la désinstallation de ces produits. Il est possible de supprimer les adaptateurs GConf, Java Preferences et l'adaptateur de définition du bureau à l'aide des outils système de gestion de package adéquats en retirant les packages mentionnés dans la section Installation.

Après la suppression de l'adaptateur Java Preferences, les scripts de démarrage écrits en vue de lancer les applications Java au moyen de l'API des préférences ne doivent plus être utilisés. L'appel de Java qu'ils contiennent échoue, puisque certains d'entre eux exigent des classes qui ne sont plus disponibles.

## Dépannage de l'adaptateur

La plupart des problèmes aboutissant à l'absence de données de configuration centrales au sein des applications correspondantes provient probablement de Configuration Agent. En effet, il s'agit du système couramment utilisé par les adaptateurs afin de récupérer des données.

Si un changement de configuration centralisée ne semble pas être répercuté au niveau d'un paramètre donné (ou d'un groupe de paramètres), il est possible que l'utilisateur ait défini explicitement une valeur pour ce paramètre dans l'application (généralement, en utilisant la boîte de dialogue Options ou Préférences du produit). Dans ce cas, la préférence utilisateur prime sur les valeurs définies via Desktop Manager, sauf si les paramètres centralisés sont protégés, ce qui signifie que la valeur est imposée par l'administrateur et que l'utilisateur n'a pas l'autorisation de modifier celle-ci.

## Dépannage de Configuration Agent

Cette section répond à certaines des interrogations que vous pouvez vous poser vis à vis de la nature et du fonctionnement de Configuration Agent ; elle présente également des conseils qui vous permettront de résoudre les problèmes liés à l'Agent.

### Questions et réponses

#### Qu'est-ce que Configuration Agent et comment fonctionne-t-il ?

Configuration Agent est une application de mise en cache et de livraison de stratégie. Il a été conçu de manière à garantir la centralisation de la configuration des applications clientes de bureau sans que cela nuise aux performances de ces applications et des hôtes sur lesquelles elles fonctionnent. Pour réaliser cet objectif, les points suivants sont mis en œuvre :

- Mise en cache de toute stratégie téléchargée dans une mémoire cache accessible localement pour utilisation ultérieure par le client
- Partage de toute ressource onéreuse (comme les connexions au serveur LDAP où est hébergée la stratégie) qui peut et doit être partagée

Le scénario type selon lequel une interaction se produit entre les applications clientes et Configuration Agent est extrêmement simple et peut être décrit de la manière suivante :

1. Un utilisateur lance une des applications clientes de bureau (gconfd, Mozilla ou StarOffice).
2. L'application cliente se connecte à Configuration Agent.
3. L'application cliente demande les données de stratégie dont elle a besoin auprès de Configuration Agent.
4. Configuration Agent recherche dans la mémoire cache les données de stratégie demandées.
5. Si ces données ne s'y trouvent pas, Configuration Agent télécharge les données en question depuis un référentiel de stratégie préconfiguré et les place dans le cache.

6. Les données de stratégie sont envoyées à l'application cliente à l'origine de la demande.
7. Configuration Agent vérifie dans le référentiel de stratégie toute modification apportée aux données de stratégie.
8. Si une modification est détectée, Configuration Agent actualise son cache de manière à le mettre à jour et en informe l'application cliente.

## Comment obtenir et installer Configuration Agent ?

Configuration Agent est disponible et installé par défaut avec Solaris 10.

## Je viens d'installer Solaris 10. Que dois-je faire ensuite ?

Par défaut, Configuration Agent est désactivé et n'est pas configuré. Pour utiliser Configuration Agent, vous devez lui appliquer, au moins, la configuration minimale et l'activer. À la suite de ces opérations, vos applications clientes de bureau utiliseront automatiquement la stratégie indiquée dès que vous les relancez.

## Je veux configurer Configuration Agent. Comment faire ?

Pour configurer correctement Configuration Agent, servez-vous de son assistant. Vous pouvez lancer l'assistant en exécutant (en tant qu'utilisateur root) la commande `/usr/bin/apoc-config`. L'assistant vous guide tout au long de la procédure de configuration de l'agent. Dans la plupart des cas, la seule information à indiquer obligatoirement concerne l'emplacement de votre référentiel de stratégie.

Il est possible également de configurer Configuration Agent en modifiant manuellement les fichiers de configuration. Notez que cette solution n'est pas recommandée car il est très facile de configurer l'agent de manière non appropriée. De plus, l'assistant de Configuration Agent propose une option supplémentaire qui permet de déterminer si une modification de configuration donnée requiert le redémarrage ou le rechargement de l'agent.

## Je veux activer Configuration Agent. Comment faire ?

Vous disposez de trois moyens différents pour activer l'agent :

1. Dans l'assistant de Configuration Agent ( `/usr/bin/apoc-config` ), définissez l'état de l'agent sur Actif.
2. Dans le programme contrôleur de Configuration Agent ( `/usr/lib/apoc/apocd` ), exécutez la commande suivante en tant qu'utilisateur root :

```
/usr/lib/apoc/apocd enable
```

3. À l'aide de `smf(5)`, exécutez la commande suivante en tant que superutilisateur :

```
/usr/sbin/svcadm enable svc:/network/apocd/udp
```

## J'ai configuré et activé Configuration Agent. Comment savoir s'il fonctionne ?

La manière la plus simple pour contrôler que Configuration Agent est configuré et qu'il fonctionne consiste à créer une stratégie à l'aide de Desktop Manager et de l'assigner à un utilisateur. Connectez-vous ensuite à l'ordinateur de bureau sous l'identité de cet utilisateur et vérifiez si les paramètres de stratégie utilisés correspondent à ceux que vous avez définis. De nombreux paramètres de stratégie sont facilement détectables au cours d'une session de bureau, comme l'arrière-plan ou le thème.

## Que signifie activer Configuration Agent ?

Configuration Agent est un service conforme à smf(5) et, à ce titre, la notion d'activation de l'agent provient de l'utilitaire smf(5). Lorsque l'agent est activé, il est prêt à fournir le service pour lequel il est conçu. Les actions suivantes se produisent lorsque vous activez l'agent :

- L'agent démarre.
- Toute application cliente de bureau lancée après l'activation de l'agent peut récupérer les données de stratégie.
- L'agent redémarre automatiquement pendant la réinitialisation système.

## Comment savoir si Configuration Agent est activé ?

Servez-vous de l'une des méthodes suivantes pour déterminer si Configuration Agent est activé :

- Utilisez le programme contrôleur pour Configuration Agent. Connectez-vous en tant que superutilisateur et tapez la commande suivante :

```
/usr/lib/apoc/apocd is-enabled
```

Si l'agent est activé, le programme contrôleur renvoie un message similaire au suivant :

```
Vérification de l'état activé de Configuration Agent... Activé
```

Sinon, le programme contrôleur renvoie un message similaire au suivant :

```
Vérification de l'état activé de Configuration Agent... Désactivé
```

- Utilisez smf(5) pour exécuter la commande suivante :

```
/usr/bin/svcs svc:/network/apocd/udp:default
```

Si l'agent est activé, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
online      8:36:04    svc:/network/apocd/udp:default
```

Si l'agent est désactivé, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
disabled    15:58:34   svc:/network/apocd/udp:default
```

Si l'agent est en mode de maintenance, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
maintenance 8:38:42  svc:/network/apocd/udp:default
```

## Comment savoir si Configuration Agent fonctionne actuellement ?

Servez-vous de l'une des méthodes suivantes pour déterminer si Configuration Agent fonctionne :

- Connectez-vous en tant que superutilisateur et exécutez le programme contrôleur de Configuration Agent :

```
/usr/lib/apoc/apocd status
```

Si l'agent est activé, le programme contrôleur renvoie un message similaire au suivant :

```
Vérification de l'état de Configuration Agent... En cours
```

Sinon, le programme contrôleur renvoie un message similaire au suivant :

```
Vérification de l'état de Configuration Agent... Pas en cours
```

- Exécutez la commande suivante :

```
/usr/bin/svcs svc:/network/apocd/udp:default
```

Si l'agent est en cours d'exécution, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
online      8:36:04  svc:/network/apocd/udp:default
```

Si l'agent n'est pas en cours d'exécution, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
disabled    15:58:34  svc:/network/apocd/udp:default
```

Si l'agent est en mode de maintenance, svcs renvoie le message suivant :

```
STATE      STIME      FMRI
maintenance 8:38:42  svc:/network/apocd/udp:default
```

- Exécutez la commande suivante :

```
ps -ef | grep apoc
```

Si l'agent est en cours d'exécution, vous devez voir le processus Java associé dans la sortie de ps :

```
daemon 29295 29294  0 13:05:22?  0:03 java -Djava.library.path=/usr/lib/apoc
-cp /usr/share/lib/apoc/apocd.jar:/usr/s
daemon 29294  1  0 13:05:22?  0:00 sh -c java
-Djava.library.path=/usr/lib/apoc -cp /usr/share/lib/apoc/apocd.jar:
root 29345 28134  0 13:08:59 pts/1  0:00 grep apoc
```

## Où se trouvent les fichiers journaux ?

Vous pouvez consulter les fichiers journaux suivants lorsque vous avez besoin de résoudre un problème concernant Configuration Agent :

- Fichiers journaux smf(5) :
  - Le fichier `/var/svc/log/network-apocd-udp:default.log` enregistre les événements relatifs aux tentatives de démarrage ou d'arrêt spécifiques de Configuration Agent. Le fichier contient également les messages que le programme contrôleur de Configuration Agent, `/usr/lib/apoc/apocd` écrit dans la sortie standard ainsi que les messages de sortie pour JVM ou Configuration Agent.
  - Le fichier journal `/var/svc/log/svc.startd.log` conserve la trace des événements smf(5) de niveau supérieur. Si, par exemple, plusieurs tentatives de démarrage de Configuration Agent ont échoué dans un laps de temps relativement court, smf(5) peut décider de ne pas lancer Configuration Agent. En pareil cas, smf(5) place Configuration Agent en mode de maintenance et consigne une entrée de journal à cet effet.

Ces deux fichiers journaux s'avèrent utiles si vous rencontrez des difficultés à démarrer Configuration Agent.

- Fichiers journaux de Configuration Agent :

Configuration Agent place les messages dans les fichiers journaux situés dans le répertoire par défaut `/var/opt/apoc/Logs`. Le répertoire de données de Configuration Agent est `/var/opt/apoc`. Vous pouvez modifier l'emplacement de ce répertoire à l'aide de l'assistant de Configuration Agent (`/usr/bin/apoc-config`). Il est également possible de changer la granularité des messages consignés en modifiant la valeur du champ Niveau du journal dans l'assistant de Configuration Agent. Si vous pensez ne pas avoir configuré correctement Configuration Agent ou si vous êtes confronté à des échecs de l'agent, utilisez l'assistant de Configuration Agent pour choisir le niveau de journalisation le plus fin avant de consulter les fichiers journaux de l'agent. Cette opération garantit que vous aurez accès aux informations de journalisation les plus complètes.
- Fichiers journaux système :

Vous pouvez également consulter le fichier journal `/var/adm/messages` ou le fichier journal `/var/opt/SUNWut/log/messages` sur une machine SunRay afin de diagnostiquer les problèmes liés à Configuration Agent.

## Comment augmenter la granularité du système de journalisation de l'agent ?

Voir "Où se trouvent les fichiers journaux ?" à la page 33

## Qu'est-ce que le mode de maintenance ?

Dès qu'il détecte des problèmes de démarrage ou de redémarrage de l'agent, smf(5) place Configuration Agent en mode de maintenance. Si smf(5) ne parvient pas à exécuter l'agent, il essaie de le redémarrer à plusieurs reprises jusqu'à ce que l'agent démarre ou qu'il décide que ce dernier ne peut pas être lancé. Dans le dernier cas, smf(5) place l'agent en mode de maintenance pour vous indiquer qu'il est nécessaire de remédier aux problèmes rencontrés. Lorsque les problèmes sont résolus, vous pouvez effacer l'état de smf(5) de l'agent pour revenir en mode normal.

## Comment sortir du mode de maintenance en effaçant l'état de smf(5) ?

Connectez-vous en tant que superutilisateur et exécutez la commande `/usr/sbin/svcdm clear svc:/network/apocd/udp`.

## Que se passe-t-il si Configuration Agent s'arrête de fonctionner de manière inattendue ?

En pareille situation, smf(5) détecte que l'agent s'est interrompu et tente de le redémarrer. Si, pour une raison quelconque, plusieurs tentatives successives échouent, smf(5) bascule l'agent en mode de maintenance. Si l'agent redémarre, cela n'a pas d'impact sur les applications clientes de bureau en cours d'exécution. Toute application cliente se reconnecte automatiquement à l'agent dès qu'il redémarre.

## Dois-je redémarrer les applications clientes de bureau si j'active/je démarre l'agent ?

Tout dépend, en réalité, si l'agent était activé ou en cours d'exécution au moment du démarrage de l'application cliente de bureau considérée. Si l'agent était activé ou en cours d'exécution, l'application cliente avait établi une connexion avec celui-ci et tente de rétablir la connexion perdue. Ainsi, chaque fois que vous démarrez, activez ou désactivez l'agent, les applications clientes tentent de se reconnecter à l'agent. En revanche, si l'agent n'est pas activé/en cours d'exécution lorsque l'application cliente est lancée, celle-ci n'utilise pas Configuration Agent et ne tente alors pas de s'y connecter lorsque ce programme démarre. En résumé, il convient de noter les points suivants :

- Les applications clientes de bureau que vous avez démarrées alors que l'agent était activé/en cours d'exécution n'ont pas besoin d'être redémarrées.
- Les applications clientes de bureau que vous avez démarrées alors que l'agent n'était pas activé/en cours d'exécution doivent être redémarrées.

## Les applications clientes de bureau ne semblent pas utiliser les stratégies configurées. Que dois-je faire ?

Le problème le plus courant lié à Configuration Agent représente l'impossibilité de détecter les effets d'une stratégie configurée sur des applications clientes de bureau. Une configuration incorrecte de l'agent, du référentiel de stratégie ou encore la non-disponibilité du référentiel de stratégie sont, le plus souvent, à l'origine de ce problème. Les consignes suivantes peuvent contribuer à localiser et éliminer ce genre de problème :

- Assurez-vous que l'agent est configuré.
- Assurez-vous que l'agent est activé/en cours d'exécution. Si vous devez relancer l'agent, vous devez également redémarrer les applications clientes de bureau actuellement ouvertes.
- Si les problèmes persistent, augmentez temporairement la granularité du système de journalisation de l'agent et, si possible, redémarrez l'agent, de manière à consulter les messages complets et très détaillés au démarrage de l'agent.

- Si l'agent ne parvient pas à démarrer normalement, consultez la section “[Problèmes de démarrage de Configuration Agent](#)” à la page 36.
- Si l'agent démarre correctement, mais que vos applications clientes de bureau n'utilisent pas une stratégie disponible, consultez la section “Problèmes d'obtention d'une stratégie de Configuration Agent en cours d'exécution”.
- Si vous n'êtes toujours pas en mesure de résoudre un problème, veuillez contacter le support technique.

## Problèmes de démarrage de Configuration Agent

Si Configuration Agent ne peut pas être démarré et que vous êtes certain d'avoir configuré et activé Configuration Agent, pensez à consulter les fichiers journaux. Les sections suivantes décrivent les erreurs les plus courantes liées à ce problème.

### Répertoire de données de Configuration Agent erroné ou inaccessible

Le répertoire de données de Configuration Agent est créé ou utilisé par l'agent en vue de stocker les fichiers journaux, les caches de stratégies, etc. L'emplacement par défaut de ce répertoire est `/var/opt/apoc`.

Configuration Agent génère le message d'erreur suivant dans les fichiers journaux `smf(5)` lorsque le répertoire de données se trouve à un emplacement inaccessible, c'est-à-dire qui correspond à `/dev/null/cant/write/here`. Pour résoudre ce problème, utilisez l'assistant de Configuration Agent (`/usr/bin/apoc-config`) pour désigner un emplacement accessible pour le répertoire de données.

```
[ Nov 17 14:35:38 Executing start method ("/usr/lib/apoc/apocd svcStart") ]
Starting Configuration Agent ... Warning: Cannot create Log directory
'/dev/null/cant/write/here/Logs'
Warning:Failed to create log file handler
Nov 17, 2005 2:35:39 PM com.sun.apoc.daemon.misc.APOCLogger config
CONFIG: Daemon configuration:
MaxRequestSize = 4096
DaemonAdminPort = 38901
ThreadTimeToLive = 5
DaemonChangeDetectionInterval = 10
IdleThreadDetectionInterval = 15
PROVIDER_URL =
DataDir = /dev/null/cant/write/here
ApplyLocalPolicy = true
ChangeDetectionInterval = 60
MaxClientConnections = 50
GarbageCollectionInterval = 10080
InitialChangeDetectionDelay = 10
TimeToLive = 10080
ConnectionReadTimeout = 5000
DaemonPort = 38900
```

```
LogLevel = FINEST
MaxClientThreads = 5
```

```
Nov 17, 2005 2:35:39 PM Daemon main
FINER: THROW
com.sun.apoc.daemon.misc.APOCException
    at com.sun.apoc.daemon.apocd.Daemon.initAuthDir(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.init(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.main(Unknown Source)
[ Nov 17 14:36:08 Method or service exit timed out. Killing contract 980 ]
[ Nov 17 14:36:08 Method "start" failed due to signal KILL ]
```

## Utilisation d'une demande client relative à un port déjà occupé

Configuration Agent utilise des sockets de connexion TCP/IP pour communiquer avec les applications clientes de bureau. Par défaut, ces connexions transitent par le port 38900.

Le message d'erreur suivant est généré lorsque Configuration Agent est configuré pour utiliser le port 1234 qui est déjà utilisé par un autre service. Le message d'erreur est enregistré dans les fichiers journaux de Configuration Agent. Pour résoudre ce problème, utilisez l'assistant de Configuration Agent (`/usr/bin/apoc-config`) pour remplacer la valeur du paramètre Port de l'agent par un numéro de port non utilisé.

```
Nov 17, 2005 2:50:59 PM com.sun.apoc.daemon.misc.APOCLogger config
CONFIG: Daemon configuration:
MaxRequestSize = 4096
DaemonAdminPort = 38901
ThreadTimeToLive = 5
DaemonChangeDetectionInterval = 10
IdleThreadDetectionInterval = 15
PROVIDER_URL =
DataDir = /var/opt/apoc
ApplyLocalPolicy = true
ChangeDetectionInterval = 60
MaxClientConnections = 50
GarbageCollectionInterval = 10080
InitialChangeDetectionDelay = 10
TimeToLive = 10080
ConnectionReadTimeout = 5000
DaemonPort = 1234
LogLevel = FINEST
MaxClientThreads = 5
```

```
Nov 17, 2005 2:50:59 PM com.sun.apoc.daemon.misc.APOCLogger info
INFO: Daemon starting
```

```
Nov 17, 2005 2:50:59 PM com.sun.apoc.daemon.misc.APOCLogger fine
FINE: Garbage collection scheduled ( interval = 10080 minutes )
Nov 17, 2005 2:50:59 PM Daemon main
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: java.net.BindException: Address already in use
    at com.sun.apoc.daemon.transport.ChannelManager.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.run(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.main(Unknown Source)
Caused by: java.net.BindException: Address already in use
    at sun.nio.ch.Net.bind(Native Method)
    at sun.nio.ch.ServerSocketChannelImpl.bind(ServerSocketChannelImpl.java:119)
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:59)
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:52)
```

## Utilisation d'un port d'administration déjà occupé

Configuration Agent utilise les sockets de connexion TCP/IP pour communiquer avec le programme contrôleur de Configuration Agent (`/usr/lib/apoc/apocd`). Par défaut, ces connexions transitent par le port 38901.

Le message d'erreur suivant apparaît dans les journaux de Configuration Agent lorsque ce dernier est configuré pour utiliser le port 1234 qui est déjà utilisé par un autre service. Pour résoudre ce problème, utilisez l'assistant de Configuration Agent (`/usr/bin/apoc-config`) pour remplacer la valeur du paramètre Port d'administration par un numéro de port non utilisé.

```
ONFIG: Daemon configuration:
MaxRequestSize = 4096
DaemonAdminPort = 1234
ThreadTimeToLive = 5
DaemonChangeDetectionInterval = 10
IdleThreadDetectionInterval = 15
PROVIDER_URL =
DataDir = /var/opt/apoc
ApplyLocalPolicy = true
ChangeDetectionInterval = 60
MaxClientConnections = 50
GarbageCollectionInterval = 10080
InitialChangeDetectionDelay = 10
TimeToLive = 10080
ConnectionReadTimeout = 5000
DaemonPort = 38900
LogLevel = FINEST
MaxClientThreads = 5
```

```
Nov 17, 2005 2:55:11 PM com.sun.apoc.daemon.misc.APOCLogger info
INFO: Daemon starting
Nov 17, 2005 2:55:11 PM com.sun.apoc.daemon.misc.APOCLogger fine
```

```

FINE: Garbage collection scheduled ( interval = 10080 minutes )
Nov 17, 2005 2:55:11 PM com.sun.apoc.daemon.misc.APOCLogger fine
FINE: Client manager started
Nov 17, 2005 2:55:11 PM com.sun.apoc.daemon.misc.APOCLogger fine
FINE: Channel manager started
Nov 17, 2005 2:55:11 PM Daemon main
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: java.net.BindException: Address already in use
    at com.sun.apoc.daemon.admin.AdminManager.initChannel(Unknown Source)
    at com.sun.apoc.daemon.admin.AdminManager.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.run(Unknown Source)
    at com.sun.apoc.daemon.apocd.Daemon.main(Unknown Source)
Caused by: java.net.BindException: Address already in use
    at sun.nio.ch.Net.bind(Native Method)
    at sun.nio.ch.ServerSocketChannelImpl.bind(ServerSocketChannelImpl.java:119)
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:59)
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:52)
    ... 4 more

```

## Problèmes d'obtention d'une stratégie de Configuration Agent en cours d'exécution

### Spécification d'un référentiel de configuration incorrect ou absent

Configuration Agent doit se connecter à un référentiel de configuration valide pour être en mesure de télécharger et de mettre en cache les informations de stratégie. Si vous n'avez pas correctement identifié le référentiel de configuration dans la configuration de l'agent (vous avez utilisé un format erroné ou omis de spécifier un référentiel, par exemple), des erreurs similaires à l'erreur suivante sont enregistrées dans les fichiers journaux de Configuration Agent au moment du démarrage des applications clientes de bureau. Pour résoudre ce problème, servez-vous de l'assistant de Configuration Agent (/usr/bin/apoc-config) pour identifier le référentiel de configuration à utiliser.

```

FINER: New client added
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authenticating user geoffh
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authentication successful
Nov 18, 2005 1:59:23 PM PolicyBackend openPolicyBackend
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.environment.InvalidParameterException: The parameter organisation
PROVIDER_URL#protocol (null) is not valid, the value must be comprised in

```

```

{ldaps,ldap,https,http,file}.
  at com.sun.apoc.daemon.apocd.PolicyBackend.<init>(Unknown Source)
  at com.sun.apoc.daemon.apocd.HostPolicyBackend.<init>(Unknown Source)
  at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyBackend(Unknown Source)
  at com.sun.apoc.daemon.apocd.Cache$DataSource.openPolicyBackend(Unknown Source)
  at com.sun.apoc.daemon.apocd.Cache$DataSource.open(Unknown Source)
  at com.sun.apoc.daemon.apocd.Cache.createDataSources(Unknown Source)
  at com.sun.apoc.daemon.apocd.Cache.<init>(Unknown Source)
  at com.sun.apoc.daemon.apocd.CacheFactory.createNewCache(Unknown Source)
  at com.sun.apoc.daemon.apocd.CacheFactory.openCache(Unknown Source)
  at com.sun.apoc.daemon.apocd.Session.<init>(Unknown Source)
  at com.sun.apoc.daemon.transaction.CreateSessionTransaction.executeTransaction
(Unknown Source)
  at com.sun.apoc.daemon.transaction.Transaction.execute(Unknown Source)
  at com.sun.apoc.daemon.apocd.ClientEventHandler.handleEvent(Unknown Source)
  at com.sun.apoc.daemon.apocd.EventWorkerThread.run(Unknown Source)
Caused by: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.environment.InvalidParameterException:
The parameter organisation PROVIDER_URL#protocol (null) is not valid,
the value must be comprised in {ldaps,ldap,https,http,file}.
  at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyMgr(Unknown Source)
  ... 14 more
Caused by: com.sun.apoc.spi.environment.InvalidParameterException: The parameter
organisation PROVIDER_URL#protocol (null) is not valid, the value must be comprised in
{ldaps,ldap,https,http,file}.
  at com.sun.apoc.spi.PolicyMgrFactoryImpl.createPolicyMgr(Unknown Source)
  ... 15 more
Nov 18, 2005 1:59:23 PM PolicyBackend openPolicyBackend

```

## Impossible de se connecter à un référentiel de stratégie

Configuration Agent doit se connecter à un référentiel de configuration valide pour être en mesure de télécharger et de mettre en cache les informations de stratégie. Si la connexion ne peut pas être établie, des erreurs similaires à la suivante sont enregistrées dans les fichiers journaux de Configuration Agent au démarrage des applications clientes de bureau. Dans le cas suivant, l'hôte `sobuild` n'existe pas, ne peut pas être contacté, ni ne peut accéder à un serveur LDAP via le port 389. Pour résoudre ce problème, servez-vous de l'assistant de Configuration Agent (`/usr/bin/apoc-config`) pour vous assurer que vous avez convenablement identifié le référentiel de stratégie et, dans ce cas-là, que l'accès au référentiel est possible. Par exemple, pour un référentiel LDAP, vous devez vérifier le fonctionnement d'un serveur LDAP, la disponibilité sur le réseau de l'ordinateur hébergeant le serveur LDAP et le fait que le port spécifié est celui qui est utilisé par le serveur LDAP.

Si vous essayez d'accéder à un serveur LDAP par une connexion SSL, assurez-vous que le certificat approprié est disponible dans le keystore correspondant de l'environnement d'exécution Java utilisé pour exécuter Configuration Agent. Reportez-vous à la section [“Configuration Agent” à la page 16](#) pour plus d'informations sur la commande `apoc-config`.

```

FINER: New client added
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authenticating user geoffh
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authentication successful
Nov 18, 2005 2:17:43 PM PolicyBackend openPolicyBackend
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.OpenConnectionException: An error occured while connecting to
ldap://sobuild:389.
    at com.sun.apoc.daemon.apocd.PolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.HostPolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.open(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.createDataSources(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.createNewCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.openCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.Session.<init>(Unknown Source)
    at com.sun.apoc.daemon.transaction.CreateSessionTransaction.executeTransaction
(Unknown Source)
    at com.sun.apoc.daemon.transaction.Transaction.execute(Unknown Source)
    at com.sun.apoc.daemon.apocd.ClientEventHandler.handleEvent(Unknown Source)
    at com.sun.apoc.daemon.apocd.EventWorkerThread.run(Unknown Source)
Caused by: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.OpenConnectionException: An error occured while
connecting to ldap://sobuild:389. at
com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyMgr(Unknown Source)
    ... 14 more
Caused by: com.sun.apoc.spi.OpenConnectionException: An error occured while
connecting to ldap://noSuchHost:389.
    at com.sun.apoc.spi.ldap.LdapClientContext.prepareConnection(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapClientContext.connect(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapConnectionHandler.openAuthorizedContext(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapConnectionHandler.connect(Unknown Source)
    at com.sun.apoc.spi.ldap.entities.LdapOrganizationProvider.open(Unknown Source)
    at com.sun.apoc.spi.PolicyMgrFactoryImpl.createPolicyMgr(Unknown Source)
    ... 15 more
Caused by: netscape.ldap.LDAPException: failed to connect to server sobuild:389 (91);
Cannot connect to the LDAP server
    at netscape.ldap.LDAPConnSetupMgr.connectServer(LDAPConnSetupMgr.java:422)
    at netscape.ldap.LDAPConnSetupMgr.openSerial(LDAPConnSetupMgr.java:350)
    at netscape.ldap.LDAPConnSetupMgr.connect(LDAPConnSetupMgr.java:244)

```

```
at netscape.ldap.LDAPConnSetupMgr.access$0(LDAPConnSetupMgr.java:241)
at netscape.ldap.LDAPConnSetupMgr$1.run(LDAPConnSetupMgr.java:179)
at java.lang.Thread.run(Thread.java:595)
Nov 18, 2005 2:17:44 PM PolicyBackend openPolicyBackend
```

## Connexion à un référentiel de stratégie non configuré

Avant que Configuration Agent puisse localiser les données de stratégie dans un référentiel de stratégie, il convient de configurer celui-ci correctement. Si vous spécifiez un référentiel de stratégie non configuré ou incorrectement configuré, des erreurs similaires à celle indiquée par la suite sont enregistrées dans les fichiers journaux de Configuration Agent au démarrage des applications clientes de bureau. Pour résoudre ce problème, veuillez consulter la section

```
FINER: New client added
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authenticating user geoffh
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authentication successful
Nov 18, 2005 2:36:55 PM PolicyBackend openPolicyBackend
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.environment.RemoteEnvironmentException: Error on reading the
configuration data on LDAP server ldap://sobuild:389.
    at com.sun.apoc.daemon.apocd.PolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.HostPolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.open(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.createDataSources(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.createNewCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.openCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.Session.<init>(Unknown Source)
    at com.sun.apoc.daemon.transaction.CreateSessionTransaction.executeTransaction
(Unknown Source)
    at com.sun.apoc.daemon.transaction.Transaction.execute(Unknown Source)
    at com.sun.apoc.daemon.apocd.ClientEventHandler.handleEvent(Unknown Source)
    at com.sun.apoc.daemon.apocd.EventWorkerThread.run(Unknown Source)
```

## **J'ai remarqué, dans les fichiers journaux de Configuration Agent, un message relatif à un "nombre maximal de connexions des clients". Que signifie-t-il ?**

Chaque application cliente de bureau (gconfd, Mozilla, StarOffice) activée par Configuration Agent établit une connexion avec Configuration Agent lorsqu'il fonctionne. La limite de telles connexions est spécifiée dans la configuration de l'agent. Par défaut, elle est fixée à 50. Si un ordinateur est utilisé par plusieurs utilisateurs, il est possible d'augmenter cette limite en changeant le paramètre "Nombre maximal de connexions des clients" dans l'assistant de Configuration Agent (/usr/bin/apoc-config). Lorsque Configuration Agent atteint le nombre maximal de connexions, un message d'erreur similaire au message suivant est reporté dans les fichiers journaux de Configuration Agent :

```
Nov 18, 2005 3:20:55 PM com.sun.apoc.daemon.misc.APOCLogger warning
AVERTISSEMENT : le nombre maximal de connexions de clients ( 50 ) a été atteint.
Aucune nouvelle connexion client ne peut être établie à ce stade.
```

## **J'ai modifié certaines stratégies à l'aide de Desktop Manager mais les modifications ne sont pas visibles sur mes ordinateurs client.**

Lors de la conception de Configuration Agent, le principe selon lequel les données de stratégies créées par Desktop Manager sont relativement statiques a été établi. En d'autres termes, elles ne sont pas susceptibles d'être modifiées régulièrement. Ce principe est le résultat de l'approche selon laquelle Configuration Agent consulte, par intermittence, le référentiel de stratégie pour prendre connaissance d'éventuels changements. Par défaut, l'agent vérifie le référentiel une fois par heure pour toutes les applications de bureau en cours. En conséquence, lorsque vous apportez une modification à l'aide de Desktop Manager, les applications de bureau en cours n'en sont informées qu'au bout d'une heure. Si vous le voulez, vous pouvez utiliser l'assistant de Configuration Agent (/usr/bin/apoc-config) pour modifier la valeur de l'"Intervalle de détection générale" afin d'augmenter la fréquence des vérifications du référentiel. Une autre solution consiste à obliger Configuration Agent à actualiser les données de stratégie pour l'ensemble des applications connectées. Pour cela, vous vous connectez en tant que superutilisateur et exécutez la commande /usr/lib/apoc/apocd change-detect.



# Console Web de Java

---

La Console Web de Java 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 Java 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.

L'un des avantages de la console est qu'un administrateur peut se connecter une fois et utiliser ensuite n'importe quelle application de la console.

## Installation

### Configuration système requise

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

## Client

- Netscape™ 6.2x et 7.x pour Solaris 10
- Netscape 6.2x et 7.x pour Windows 98, 98 SE, ME, 2000 et XP
- Internet Explorer 5.5x et 6.x pour Windows 98, 98 SE, ME, 2000 et XP
- Mozilla 1.4x pour Solaris
- Firefox 1.0 pour Solaris

## Serveur

- Solaris10
- Red Hat Application Server 2.1, 3.0
- SuSE Linux 8.0 ou 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 Console Web de Java

La Console Web de Java 2.2.4 fait partie du système d'exploitation Solaris 10, cependant Desktop Manager exige la version 2.2.5. Une copie de la version 2.2.5 est fournie dans l'archive Desktop Manager située dans le répertoire `server/console`. Elle peut être installée en exécutant `./setup` dans ce répertoire.

Si vous avez installé la Console Web de Java 3.0, vous devez désinstaller la version 3.0, puis installez la Console Web de Java 2.2.5 à partir du répertoire `server/console` indiqué ci-dessus.

## Exécution de la console

En général, il suffit d'arrêter et de redémarrer le serveur de la Console Web de Java lorsque vous voulez enregistrer une nouvelle application.



---

**Attention** – Avant de démarrer la Console Web de Java pour la première fois, assurez-vous que l'installation de Desktop Manager est terminée. La Console Web de Java ne s'exécute *pas* correctement tant que vous n'avez pas déployé au moins une application dans la console.

---

- Pour démarrer la Console Web de Java, tapez `smcwebserver start`.
- Pour arrêter la Console Web de Java, tapez `smcwebserver stop`.

- Pour redémarrer la Console Web de Java, tapez `smcwebserver restart`.
- Pour accéder à la Console Web de Java, saisissez l'URL suivant dans votre navigateur :  
`https://<nomd'hôte>.<nomdedomaine>:6789`

La Console Web de Java prend en charge, sans configuration supplémentaire, l'authentification Unix et le contrôle d'accès basé sur les rôles (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 Console Web de Java, consultez les pages de manuel relatives à `smcwebserver` et à `smreg`.

## Suppression de la Console Web de Java



---

**Attention** – Si vous travaillez sous Solaris, vous ne pouvez pas supprimer la Console Web de Java, car elle fait partie intégrante du système d'exploitation.

---

## Dépannage de la Console Web de Java

### Impossible d'installer la Console Web de Java

Symptôme : à la fin de l'installation, un message indique que la Console Web de Java ne peut pas démarrer car aucune application n'est enregistrée.

Causes possibles : dès qu'un module Desktop Manager est installé, il lance la Console Web de Java.

### Connexion refusée

Symptôme : vous essayez d'ouvrir l'URL qui convient, par exemple, `https://<votre.serveur>:6789`, mais la connexion est refusée.

Causes possibles : la Console Web de Java n'est pas en cours d'exécution sur le serveur.

## Impossible de se connecter

---

**Remarque** – Par défaut, le module de connexion LDAP n'est pas installé. En conséquence, les informations d'identification de connexion ne sont pas comparées à celles qui sont enregistrées dans le serveur LDAP ; seules les informations d'identification système ordinaires sont requises. Cette section relative au dépannage s'applique uniquement si vous avez installé manuellement le module de connexion LDAP.

---

Symptôme : vous avez accédé à la page de connexion de la console Web, mais la combinaison utilisateur/mot de passe est refusée.

Causes possibles :

- Le serveur LDAP ne fonctionne pas.
- Le module d'authentification de la console Web LDAP n'est pas correctement configurée.
- L'utilisateur n'existe pas sur le serveur LDAP.
- L'utilisateur a un mot de passe différent sur le serveur LDAP.

## Aucun lien à Desktop Manager

Symptôme : vous êtes connecté à la console Web, mais la page dressant la liste des applications ne contient pas Desktop Manager.

Causes possibles :

- Le module Desktop Manager n'est pas installé.

## Exception du pointeur nul, erreur Tomcat/Java ou page blanche

Symptôme : vous ouvrez Desktop Manager mais aucune valeur ne s'affiche, seule une page blanche ou des messages d'erreur apparaissent.

Causes possibles : si l'erreur mentionne `NoClassDefFoundError: sun/tools/javac/Main`, la Console Web de Java utilise une installation Java erronée.

## Autres problèmes

Si le serveur Web ne fonctionne pas correctement, les fichiers journaux peuvent vous aider à trouver des informations relatives à ce problème. Ils se trouvent dans `/var/log/webconsole/`. Vous pouvez augmenter le niveau de détail de la journalisation à l'aide de `smreg` :

```
smreg add -p debug.trace.level=3  
smreg add -p debug.trace.options=tmp
```

Les paramètres initiaux peuvent être rétablis en exécutant :

```
smreg add -p debug.trace.level=0  
smreg add -p debug.trace.options=m
```

Le vidage complet de la base de données de configuration est déclenché en exécutant :

```
smreg list
```

Il est possible que le serveur Web hébergeant Desktop Manager ne soit pas correctement éteint, c'est pourquoi ses ports sont occupés. Cela empêche le redémarrage de tout nouveau serveur Web. Si la commande `smcwebserver start/restart` émet des messages d'erreur ou si Desktop Manager est toujours accessible même après une commande `smcwebserver stop`, ou encore si un serveur qui vient d'être démarré se comporte comme le serveur précédent, vérifiez si le port 6789 est en cours d'utilisation (`netstat -a | grep 6789`) ou si le serveur Web fonctionne toujours (`ps -ef | grep java`). Dans l'un ou l'autre des cas, le processus correspondant doit être arrêté et le port 6789 ne doit plus être utilisé.



# Paramètres de configuration

---

Ces paramètres peuvent être définis pour les composants Desktop Manager suivants :

- Desktop Manager, dans les fichiers définissant les référentiels de configuration (situés dans `/etc/opt/SUNWapcmg/`).
- Configuration Agent, dans le fichier `/etc/apoc/policymgr.properties`.
- Interface de la ligne de commande Desktop Manager, dans le fichier `$HOME/pgtool.properties`, avec la restriction que l'interface de la ligne de commande prenne uniquement en charge les référentiels LDAP purs.

Un préfixe peut être apposé aux paramètres pour indiquer le fournisseur du référentiel auxquels ils s'appliquent. Pour chaque fournisseur, le paramètre doté du préfixe est traité en premier. Si un tel paramètre n'est pas défini, le paramètre sans préfixe est utilisé.

TABLEAU A-1 Préfixes

Valeur du préfixe	Fournisseur du référentiel
ORGANIZATION_	Arborescence de l'organisation
DOMAIN_	Arborescence du domaine
PROFILE_	Profils
ASSIGNMENT_	Assignations
LDAP_META_CONF_	Mappage des données pour des référentiels LDAP

TABLEAU A-2 Paramètres

Nom	Description	Valeurs disponibles	Valeur par défaut
PROVIDER_URL	URL spécifiant la connexion au référentiel. Une liste des URL peut être utilisée pour spécifier les référentiels de secours au cas où la connexion au premier URL échoue.	Liste d'un ou de plusieurs URL séparés par des espaces aux formats suivants : ldap://<hôte>:<port>/<DNdebase> ldaps://<hôte>:<port>/<DNdebase> file://<chemindufichier> http://<host>:<port>/<chemindufichier> https://<hôte>:<port>/<chemindufichier>	Aucune, paramètre obligatoire
SECURITY_PRINCIPAL	Nom d'utilisateur pour la connexion au référentiel.	Nom d'utilisateur d'un utilisateur doté de droits d'accès en lecture et en recherche pour le référentiel ou aucune valeur pour les connexions anonymes.	Aucune, connexion anonyme
SECURITY_CREDENTIALS	Mot de passe pour l'utilisateur défini dans SECURITY_PRINCIPAL.	Texte brouillé ou non du mot de passe.	Aucune
SECURITY_CREDENTIALS_ENCODING	Indique si le mot de passe défini dans SECURITY_PRINCIPAL est brouillé. Avertissement : le brouillage du mot de passe ne constitue qu'un masque placé au-dessus du mot de passe, il ne peut, en aucune façon, être considéré comme un type de chiffrement sécurisé.	“brouillé” : (scramble) si le mot de passe est brouillé (automatiquement effectué par les assistants au cours de la génération des données de configuration). “aucun” : (none) si le mot de passe s'affiche sous forme d'un texte lisible ; utilisez cette valeur si vous voulez modifier le mot de passe.	“aucun” : (none)
MAX_SEARCH_RESULT	Le nombre maximal de résultats à l'issue d'une recherche dans un référentiel. Remarque : le schéma des préfixes ne s'applique pas à ce paramètre.	Nombre positif, 0 équivaut à aucune limite.	100

Les paramètres suivants concernent exclusivement les référentiels LDAP.

TABLEAU A-3 Paramètres spécifiques à LDAP

Nom	Description	Valeurs disponibles	Valeur par défaut
Nom d'utilisateur complet (AuthDn)	DN complet d'un utilisateur à signaler la première fois que l'utilisateur accède au référentiel LDAP, de manière à récupérer l'utilisateur défini dans SECURITY_PRINCIPAL.	Nom d'utilisateur d'un utilisateur doté de droits d'accès en lecture et en recherche pour le référentiel ou aucune valeur pour les connexions anonymes.	Aucune, accès anonyme
Mot de passe (Password)	Mot de passe associé à AuthDN.	Texte brouillé ou non du mot de passe.	Aucun
Chiffrement du mot de passe (Password_ENCODING)	Indique si le mot de passe défini est brouillé. Avertissement : le brouillage du mot de passe ne constitue qu'un masque placé au-dessus du mot de passe, il ne peut, en aucune façon, être considéré comme un type de chiffrement sécurisé.	“brouillé” : (scramble) si le mot de passe est brouillé (automatiquement effectué par les assistants au cours de la génération des données de configuration). “aucun” : (none) si le mot de passe s'affiche sous forme d'un texte lisible ; utilisez cette valeur si vous voulez modifier le mot de passe.	“aucun” :
Délai d'expiration de connexion (ConnectTimeout)	Délai d'établissement de la connexion en secondes.	Nombre positif, 0 pour un délai illimité.	1

## EXEMPLE A-1 Exemple d'un moteur de traitement hybride

Exemple d'un moteur de traitement hybride dans lequel les informations sur les hôtes et les utilisateurs sont extraites d'un référentiel LDAP tandis que les profils et leurs assignations sont enregistrés dans le système de fichiers.

```
#Organization, Domain, MetaConf
PROVIDER_URL = ldap://server1.sun.com:389/o=apoc ldap://server2.sun.com:389/o=apoc
SECURITY_PRINCIPAL = jmonroe
SECURITY_CREDENTIALS = JmonroE
SECURITY_CREDENTIALS_ENCODING = none
AuthDn = cn=reader,ou=special users,o=apoc
Password = lakjflajf
Password_ENCODING = scramble
ConnectTimeout = 5
```

```
#Profile
```

EXEMPLE A-1 Exemple d'un moteur de traitement hybride (Suite)

```
PROFILE_PROVIDER_URL = file:///path/to/repository
```

```
#Assignment
```

```
ASSIGNMENT_PROVIDER_URL = file:///path/to/repository
```

# Utilisation d'OpenLDAP et d'Active Directory avec Desktop Manager

---

## Utilisation d'un serveur OpenLDAP avec Desktop Manager

Pour utiliser un serveur OpenLDAP en tant que référentiel pour les données de Desktop 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 appelé `apoc.schema` se trouve dans le répertoire `/usr/share/webconsole/apoc/deploy`.

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.

Après l'extension du schéma des serveurs OpenLDAP, l'assistant d'ajout de référentiel de configuration permet de terminer la fin de la procédure de configuration dans Desktop Manager.

---

**Remarque** – L'agent de Desktop 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 Desktop Manager

Pour utiliser un serveur Active Directory en tant que référentiel pour les données de Desktop 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 du schéma nommé `apoc-ad.ldf` se trouve dans le répertoire `/usr/share/webconsole/apoc/deplo`.

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 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" <DNbase> -f apoc-ad-registry.ldf` .

---

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

---

Après l'extension du schéma des serveurs Active Directory, l'assistant d'ajout de référentiel de configuration permet de terminer le reste de la procédure de configuration dans Desktop Manager.

Lorsque vous êtes invité à indiquer les informations d'identification LDAP dans l'assistant d'ajout de référentiel de configuration, spécifiez le DN complet et le mot de passe d'un utilisateur ayant des droits de lecture de 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 Desktop 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 récupérer les données de configuration d'un hôte de bureau, cet hôte doit également connaître le nom de domaine d'Active Directory. L'authentification de l'utilisateur du bureau 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 tous les utilisateurs. 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, l'utilisateur doit être authentifié sur le serveur Active Directory et les informations d'identification de l'utilisateur doivent figurer sur le système. Pour cela, il est nécessaire de configurer l'authentification Kerberos sur votre système, ce qui permet de générer des informations d'identification au moment de la connexion. Pour plus d'informations à ce sujet, veuillez consulter les guides d'administration de votre système.

# Mappage organisationnel

---

## Mappage organisationnel

Pour définir le mappage entre les entrées LDAP et les éléments de Desktop 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 éléments d'utilisateur sont identifiés par une classe d'objet que tous les éléments 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 éléments de rôle sont identifiés 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'*n*ème classe d'objet doit être utilisée avec l'*n*ème 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 :

```
# 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 éléments d'organisation sont identifiés 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 :

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

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

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

Les éléments d'hôte sont identifiés d'une manière similaire aux éléments d'utilisateur. Le nom des clés et leurs valeurs par défaut sont :

```
# 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
```