Sun Java™ Desktop System Configuration Manager

Installationshandbuch

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054,
U.S.A. 650-960-1300

Teilenr. 817-5588-10

April 2004, Version A

Copyright und Marken

Inhalt

KAPITEL 1

Einführung

Sun Java™ Desktop System Configuration Manager dient zur zentralisierten Konfiguration von Desktop-Systemen, auf welchen Sun Java™ Desktop System ausgeführt wird. Dank der Möglichkeit, Einstellungen für verschiedene Elemente einer Organisationsstruktur vorzunehmen, können Administratoren auf einfache, bequeme Weise Benutzer- oder Rechnergruppen verwalten. Die Hauptkomponenten sind:

- ein LDAP-Server mit der Organisationsstruktur der zu verwaltenden Benutzer und Rechner, in dem die Konfigurationsdaten abgelegt werden,
- ein webbasiertes Verwaltungstool, das es Administratoren ermöglicht, Konfigurationsdaten zu definieren und den Elementen dieser Organisationsstruktur zuzuweisen,
- auf dem Client-Rechner installierte Desktop-Komponenten zum Abrufen der Konfigurationsdaten für den jeweils angemeldeten Benutzer und die Weitergabe dieser Daten an die verschiedenen Anwendungen innerhalb von Java Desktop System.

Bei dem Verwaltungstool handelt es sich um eine webbasierte Anwendung, die mit Sun Web Console ausgeführt wird. Sie ermöglicht es dem Administrator, die Organisationsstruktur des LDAP-Servers zu durchsuchen und deren Elementen Richtlinien zuzuweisen. Die Anzeige und Bearbeitung der Richtlinien erfolgt mithilfe von Richtlinienvorlagen, aus welchen die Einstellungen hervorgehen, die mit dem Verwaltungstool beeinflusst werden können.

Die Desktop-Komponenten sind um Sun Java™ Desktop System Configuration Agent angelegt. Dieser Agent ruft die Konfigurationsdaten für den jeweiligen Benutzer vom LDAP-Server ab und stellt sie verschiedenen Konfigurationssystem-Adaptern zur Verfügung, die wiederum die lokale Konfiguration (durch Anwendungs- und Benutzereinstellungen festgelegte Standardwerte) um die Richtlinieneinstellungen ergänzen. Derzeit werden die Konfigurationssysteme GConf (für die Konfiguration von Gnome-Anwendungen wie dem Gnome-Desktop oder Evolution), Mozilla-Einstellungen und StarRegistry (das Konfigurationssystem von StarOffice) unterstützt.

KAPITEL 2

LDAP-Server

Konzepte

Im Rahmen von Java Desktop System Configuration Manager werden Konfigurationsdaten Entitäten zugeordnet. Dabei handelt es sich um Einträge in der LDAP-Datensammlung, die einzelnen Elementen in der Organisationsstruktur des Unternehmens entsprechen.

Es werden folgende Entitäten unterschieden:

- Organisation: in der Regel eine organisatorische (Abteilung, Gruppe, Team) oder ortsbezogene (Kontinent, Land, Standort) Einheit der Gesamthierarchie.
- Benutzer: ein Zweigende in der Gesamthierarchie und, wie der Name schon sagt, in der Regel ein Benutzer.
- Domäne: eine logische Gliederungseinheit für die Netzwerkorganisation.
- Rechner: ebenfalls ein Zweigende in der Gesamthierarchie, das aber einen Rechner im Netzwerk darstellt.
- Rolle: diese Entität stellt Eigenschaften dar, (normalerweise eine funktionelle Unterscheidung wie Administration oder Standortverwaltung), die einer Gruppe von Benutzern zugewiesen werden.

Die Organisations- und Benutzerentitäten bilden eine als Benutzerbaum bezeichnete Struktur, die Domänen- und Rechnerentitäten den so genannten Rechnerbaum. Diese beiden Bäume sind voneinander unabhängig, werden aber innerhalb des Frameworks auf ähnliche Weise manipuliert.

Die Beziehung zwischen Organisations- oder Domänenentitäten und anderen Einträgen definiert sich durch die Position der Einträge innerhalb der Datensammlung. Das bedeutet, dass Organisations- und Domänenentitäten beliebige, im Baum unter ihnen befindliche Einträge enthalten können. Die Beziehung zwischen Rollen und Benutzern oder Rechnern wird durch die Attribute der Benutzer- und Rechnereinträge bestimmt.

Die einer Entität zugeordneten Konfigurationsdaten werden in speziellen, durch das Framework verwalteten Einträgen gespeichert. Diese Einträge sind durch die zugehörigen Dienstnamen und Dienstbehälter bezeichnet.

Einrichtung

Folgendes ist erforderlich, wenn Sie einen bereits vorhandenen LDAP-Server für Configuration Manager einsetzen möchten:

- Erweitern des Server-Schemas zur Unterstützung der benutzerdefinierten Objektklassen und Attribute, die zum Speichern von Konfigurationsdaten durch Configuration Manager benötigt werden.
- Anpassen der Zuordnungsinformationen für die Einträge in der Datensammlung sowie der von Configuration Manager unterstützten Entitäten und Speichern dieser auf dem Server.

Bereitstellungstools

Für den Einsatz eines bereits vorhandenen LDAP-Servers mit Configuration Manager werden die folgenden auf der Installations-CD befindlichen Bereitstellungstools benötigt:

- `88apoc-registry.ldif` – Eine Schemadatei, mit der die zum Speichern von Konfigurationsdaten erforderlichen Objektklassen und Attribute eingeführt werden.
- `OrganizationMapping` – Eine Standardeigenschaftendatei, in der die Zuordnung zwischen LDAP-Einträgen und Configuration Manager-Entitäten beschrieben ist.
- `UserProfileMapping` – Eine Standardeigenschaftendatei, in der die Zuordnung zwischen den Attributen für LDAP-Benutzereinträge und Attributen für Configuration Manager-Benutzerprofile beschrieben ist.
- `createServiceTree` – Ein Skript, durch das die Zuordnungsdateien in der LDAP-Datensammlung abgelegt werden.
- `DeployApoc:` – Ein Skript zum Erweitern des Schemas des LDAP-Servers und Ablegen der Zuordnungsdateien in der LDAP-Datensammlung.

Schema-Erweiterung

Die Konfigurationsdaten werden in Eintragsbäumen abgelegt, die an die Einträge anschließen, auf welche sich die Daten beziehen. Bevor die Objektklassen und Attribute für diese Bäume auf einem LDAP-Server gespeichert werden können, müssen Sie sie in das LDAP-Serverschema einfügen. Die zum Hinzufügen der Objekte und Klassen zu Sun Java Systems Directory Server mitgelieferte Erweiterungsdatei verwendet das Format LDIF. Um diese Objekte einem anderen LDAP-Server hinzuzufügen, müssen Sie ein von diesem Server unterstütztes Format verwenden.

Organisatorische Zuordnung

Zur Definition der Zuordnung zwischen LDAP-Einträgen und Configuration Manager-Entitäten muss die Datei OrganizationMapping bearbeitet werden. Dabei sind für die verschiedenen Schlüssel Werte anzugeben, die der Struktur der LDAP-Datensammlung entsprechen.

Benutzerentitäten sind durch eine für alle Entitäten geltende Objektklasse sowie ein Attribut gekennzeichnet, dessen Wert im Bereich der gesamten Datensammlung einmalig sein muss. Sie können ein Namensanzeigeformat liefern, das sich auf die Anzeige der Benutzernamen in der Verwaltungsanwendung auswirkt, und haben die Möglichkeit, einen Behältereintrag zu defi-

nieren, für den Fall, dass für die Benutzereinträge in der Organisation solche Einträge verwendet werden. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# Objektklasse für alle Benutzereinträge
User/ObjectClass=inetorgperson
# Attribut, dessen Wert in Benutzereinträgen im Bereich der Datensammlung einmalig sein muss
User/UniqueIdAttribute=uid
# Optionaler Behälter in Organisationseinträgen der Benutzereinträge; entfernen Sie diese Zeile, sofern sie nicht erforderlich ist.
User/Container=ou=People
# Namensanzeigeformat innerhalb der Verwaltungsanwendung
User/DisplayNameFormat=sn, givenname
```

Rollenentitäten sind durch eine Liste möglicher Objektklassen und die entsprechenden Namensattribute gekennzeichnet. Diese Listen müssen im Format <Element1>,<Element2>,...,<Element*n*> vorliegen und sich decken. Das heißt, dass die Listen dieselbe Elementanzahl aufweisen müssen und die *n*-te Objektklasse mit dem *n*-ten Namensattribut verbunden ist. Zwei Schlüssel bestimmen sowohl das Verhältnis zwischen Rollen und Benutzern als auch zwischen Rollen und Rechnern. Mit dem Schlüssel VirtualMemberAttribute ist ein Attribut anzugeben, dessen Werte von einem Benutzer- oder Rechnereintrag abgefragt werden können. Außerdem muss der Schlüssel die vollständigen DNs der Rollen enthalten, zu welchen der Eintrag gehört. Mit dem Schlüssel MemberAttribute ist ein Attribut aus einem Benutzer- oder Rechnereintrag für den Suchfilter anzugeben. Außerdem muss der Schlüssel die vollständigen DNs der Rollen enthalten, zu welchen der Benutzer oder Rechner gehört. Während der Schlüssel VirtualMemberAttribute ein virtuelles Attribut vom Typ Class Of Service sein kann, muss für den Schlüssel MemberAttribut ein tatsächliches, in einem Filter verwendbares Attribut angegeben werden. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# Liste von Objektklassen für Rollen
Role/ObjectClass=nsRoleDefinition
# Sich deckende Liste mit entsprechenden Namensattributen
Role/NamingAttribute=cn
# Tatsächliches Attribut (in einem Filter verwendbar), das die DNs der Rollen eines Benutzers/Rechners enthält
Role/MemberAttribute=nsRoleDN
# Attribut, durch dessen Abfrage für einen Benutzer oder Rechner die DNs der zugehörigen Rollen geliefert werden
Role/VirtualMemberAttribute=nsRole
```

Organisationsentitäten werden ähnlich wie Rollen durch zwei bündige Listen von Objektklassen und den dazugehörigen Namensattributen definiert. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# Liste von Objektklassen für Organisationen
Organization/ObjectClass=organization
# Sich deckende Liste mit entsprechenden Namensattributen
Organization/NamingAttribute=o
```

Domänenentitäten werden ähnlich wie Organisationsentitäten definiert. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# Liste von Objektklassen für Domänen
Domain/ObjectClass=ipNetwork
# Sich deckende Liste mit entsprechenden Namensattributen
Domain/NamingAttribute=cn
```

Rechnerentitäten werden ähnlich wie Benutzerentitäten definiert. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# Objektklasse für alle Rechnereinträge
Host/ObjectClass=ipHost
# Attribut, dessen Wert in Rechnereinträgen im Bereich der Datensammlung einmalig sein muss
Host/UniqueIdAttribute=cn
# Optionaler Behälter in Domäneneinträgen der Rechnereinträge; entfernen Sie diese Zeile, sofern sie nicht erforderlich ist.
Host/Container=ou=Hosts
```

Benutzerprofil-Zuordnung

Zur Definition der Zuordnung zwischen den Attributen der LDAP-Benutzereinträge und den Attributen der Configuration Manager-Benutzerentitäten muss die Datei UserProfileMapping bearbeitet werden. Jeder Schlüssel entspricht einem Configuration Manager-Benutzerattribut. Dem Namen eines Attributs in einem Benutzereintrag kann gemäß der Definition durch die organisatorische Zuordnung ein Schlüssel als Wert zugewiesen werden. Attribute, die in der User / DisplayNameFormat-Einstellung verwendet werden, müssen in der Datei UserProfileMapping eine Zuordnung erhalten. Sehen Sie hier die Schlüsselnamen und ihre Standardwerte:

```
# inetOrgPerson.givenName
org.openoffice.UserProfile/Data/givenname = givenname
# person.sn
org.openoffice.UserProfile/Data/sn = sn
# inetOrgPerson.initials
org.openoffice.UserProfile/Data/initials = initials
# organizationalPerson.street
org.openoffice.UserProfile/Data/street = street,postalAddress,
streetAddress
# organizationalPerson.l (Stadt)
org.openoffice.UserProfile/Data/l = l
# organizationalPerson.st (Bundesland/Kreis)
org.openoffice.UserProfile/Data/st = st
# organizationalPerson.postalCode
org.openoffice.UserProfile/Data/postalcode = postalcode
# country.c (Land)
org.openoffice.UserProfile/Data/c =
# organizationalPerson.o (Firma)
org.openoffice.UserProfile/Data/o = o,organizationName
# veraltet -- keine logische Folge für LDAP
org.openoffice.UserProfile/Data/position =
```

```
# organizationalPerson.title
org.openoffice.UserProfile/Data/title = title
# inetOrgPerson.homePhone
org.openoffice.UserProfile/Data/homephone = homephone
# organizationalPerson.telephoneNumber
org.openoffice.UserProfile/Data/telephonenumber = telephonenumber
# organizationalPerson.facsimileTelephoneNumber
org.openoffice.UserProfile/Data/facsimiletelephonenumber =
facsimiletelephonenumber,officeFax
# inetOrgPerson.mail
org.openoffice.UserProfile/Data/mail = mail
```

Bereitstellung

Nachdem Sie die Zuordnungsdateien an die Gegebenheiten der LDAP-Datensammlung angepasst haben, können sie bereitgestellt werden. Wenn das Schema des LDAP-Servers die erforderlichen Objektklassen und Attribute bereits umfasst, kann das Skript `createServiceTree` direkt ausgeführt werden. Anderenfalls ist zunächst das Skript `deployApoc` auszuführen.

Das Skript `deployApoc` ist auf Sun Java System Directory Server zugeschnitten. Es kopiert die mitgelieferte Schema-Erweiterungsdatei in das richtige Verzeichnis, beendet den LDAP-Server und startet ihn neu und ruft anschließend das Skript `createServiceTree` auf. Für die Ausführung des Skripts müssen Sie über die Berechtigung zum Kopieren von Dateien in die Schema-Datensammlung, zum Beenden und zum Starten des Servers verfügen. Es wird mit folgendem Befehl aufgerufen:

```
./deployApoc <Directory_Server-Verzeichnis>
```

Dabei ist der Parameter `<Directory_Server-Verzeichnis>` der Pfad zu dem Unterverzeichnis `slapd-<Servername>` einer Directory Server-Installation. Angenommen, bei der Installation wurden die Standardverzeichnisse übernommen und der Servername lautet `meinServer.meineDomäne`, so heißt das Verzeichnis `/var/Sun/mps/slapd-meinServer.meineDomäne`.

Unabhängig davon, ob es direkt oder durch das Skript `deployApoc` aufgerufen wird, fordert das Skript `createServiceTree` den Benutzer zur Eingabe der Adresse des LDAP-Servers (Host-Name, Port-Nummer und Basis-DN) und der Definition eines Benutzers mit Administrationsrechten (vollständiger DN und Passwort) auf. Anschließend erstellt es im LDAP-Server einen Startdienst-Baum und legt die Zuordnungsdateien darin ab. Das Skript kann mit beliebigen Berechtigungen ausgeführt werden.
Der Aufrufbefehl lautet:

```
./createServiceTree
```

Daraufhin wird der Benutzer zur Eingabe von Folgendem aufgefordert:

- Rechnername (Standardwert: localhost): Rechnername des LDAP-Servers,
- Port-Nummer (Standardwert: 389): Port-Nummer des LDAP-Servers,
- Base-DN: Base-DN der LDAP-Datensammlung,
- Benutzer-DN (Standardwert: cn=Directory Manager): vollständiger DN eines Benutzers mit ausreichenden Berechtigungen zum Erstellen neuer Einträge unter dem Base-DN,
- Passwort: Passwort dieses Benutzers,

Es wird ein Eintrag mit dem DN:

```
ou=ApocRegistry,ou=default,ou=OrganizationConfig,ou=1.0,ou=ApocService,
ou=services,<Base-DN>
```

erzeugt und mit dem Inhalt der zwei Zuordnungsdateien angefüllt.

Wie bereits angemerkt, wird für die durch das Skript `deployApoc` durchgeführten Operationen ein LDAP-Server vorausgesetzt, der sich in Bezug auf die Installationsverzeichnisse, seine Struktur und die Schema-Erweiterungsprozedur so gut wie nicht von Sun Java System Directory Server unterscheidet. Bei anderen Verzeichnissen ist das Schema manuell zu erweitern, bevor das Skript `createServiceTree` ausgeführt werden kann. Weitere Informationen zur Verwendung von OpenLDAP und ActiveDirectory entnehmen Sie bitte Anhang C.

Der erzeugte Baum, der mit dem Baum zum Ablegen der Konfigurationsdaten für die Entitäten übereinstimmt, deckt sich mit der Struktur der Bäume, die in Sun Java System Identity Server für die Dienstverwaltung zum Einsatz kommen.

Weitere Überlegungen

Eine Voraussetzung für den Betrieb des Configuration Manager-Frameworks ist, dass eine Verbindung mit Lese- und Suchberechtigung zum LDAP-Server hergestellt werden kann. Nur so ist es möglich, den vollständigen DN zu ermitteln, der einem vom Desktop stammenden Benutzer- oder Rechner-Bezeichner zugeordnet ist. Deshalb muss die Datensammlung entweder so konfiguriert sein, dass anonyme Verbindungen erlaubt sind, oder es muss ein spezieller Benutzer mit Lese- und Suchberechtigung für diesen Zweck erstellt werden.

Die Verwaltungsanwendung erzeugt Dienstbäume unter Einträgen in Entitäten, die zum Ablegen der Konfigurationsdaten für diese Entitäten dienen. Folglich müssen zu Verwaltungszwecken verwendete Benutzereinträge die Berechtigung zum Erzeugen von Untereinträgen unter den von ihnen verwalteten Einträgen aufweisen.

Die Authentifizierung der Framework-Benutzer seitens der Desktop-Clients kann über die Methoden Anonymous (anonym) und GSSAPI erfolgen. Für die anonyme Methode muss in der gesamten Datensammlung der anonyme Lese- und Suchzugriff aktiviert sein, da die Desktop-Clients bei ihren Versuchen, Daten vom LDAP-Server abzurufen, keine Berechtigungsnachweise vorlegen. Für die Methode GSSAPI (mit Authentifizierung per Kerberos) muss der LDAP-Server gemäß den Angaben im Kapitel „Implementing Security“ im Dokument „Sun Java System Directory Server Administration Guide“ konfiguriert werden.

KAPITEL 3

Sun™ Web Console

Sun Web Console ist darauf ausgerichtet, eine gemeinsame, webbasierte Systemverwaltungslösung für Sun Microsystems zu schaffen. Sie dient als der eine, zentrale Einstiegspunkt, von dem aus Benutzer auf Systemverwaltungsanwendungen mit einer einheitlichen Benutzeroberfläche zugreifen können.

Die Konsole basiert auf einem Webmodell. Dafür sprechen zahlreiche gute Gründe. Der Hauptgrund ist, dass Systemadministratoren ihre Verwaltungsanwendungen über einen Webbrowser erreichen können sollen.

Sun Web Console bietet:

- eine gemeinsame Authentifizierung und Autorisierung
- eine gemeinsame Anmeldung
- einen einzelnen Einstiegspunkt für den Zugriff auf sämtliche Verwaltungsanwendungen über denselben HTTPS-Port
- ein einheitliches Aussehen

Die Konsole bietet den Vorteil, dass Sie sich als Administrator nur einmal anmelden müssen, um dann alle beliebigen Anwendungen innerhalb der Konsole verwenden zu können.

Systemvoraussetzungen

Sun Web Console unterstützt mehrere Client- und Server-Betriebssysteme sowie verschiedene Browser.

Client

- Netscape 4.7x, 6.2x und 7.x unter Solaris 8 oder höher
- Netscape 4.7x, 6.2x und 7.x unter Windows 98, 98 SE, ME, 2000 und XP
- Internet Explorer 5.x und 6.x unter Windows 98, 98 SE, ME, 2000 und XP
- Mozilla unter Linux und Solaris

Server

- Solaris 8 oder höher
- Redhat 8 oder höher, Redhat Enterprise Linux 2.1
- SuSE Linux 2.1 oder höher
- J2SE Version 1.4.1_03 oder höher
- Wenn J2SE 1.4.1 oder eine niedrigere Version auf dem Server erkannt wird, fordert Sie das Einrichtungsprogramm dazu auf, die Installation mit der J2SE-Version der Java Desktop System Management Tools-CD zu aktualisieren.
- Tomcat: 4.0.3 oder höher

  Tomcat ist auf der Java Desktop System Management Tools-CD enthalten.

Installation von Sun Web Console

Lesen Sie vor der Installation von Sun Web Console bitte die Zusammenfassung der Packages und die Hinweise zu bekannten Problemen in Anhang A dieses Dokuments.

Die Sun Web Console-Installationsdateien für die Betriebssysteme Solaris SPARC (Version 8 oder höher) und Linux sind auf der Java Desktop System Management Tools-CD enthalten.

1. Wechseln Sie auf der Java Desktop System Management Tools-CD in das Sun Web Console-Verzeichnis für das Betriebssystem, auf dem Sie die Konsole installieren möchten.

   Auf Linux-Systemen wechseln Sie in das Verzeichnis `/linux/swc` und auf Solaris SPARC-Systemen in das Verzeichnis `/solsparc/swc`.

2. Geben Sie `./setup` ein.

   Sun Web Console erstellt standardmäßig keine Installationsprotokolldatei. Geben Sie Folgendes ein, um ein Installationsprotokoll mit dem Namen „Protokolldatei“ anzulegen: `./setup | tee Protokolldatei`

   Hinweis: Ein Großteil der Installation und Konfiguration der Konsole erfolgt automatisch, sobald Sie `setup` ausführen. Genaueres zur `setup`-Anwendung für Sun Web Console entnehmen Sie bitte Anhang A.

3. Falls Sie Sun Web Console in einer anderen Sprache verwenden möchten, müssen Sie für jede Sprache zwei zusätzliche Packages installieren. Die Namen der verschiedenen Sprachen-Packages finden Sie in nachstehender Tabelle. Führen Sie in diesem Fall einen der folgenden Schritte durch:

   - Unter Solaris: Geben Sie `pkgadd -d path/pkgname.pkg pkgname` ein, wobei *pkgname* durch den Namen des Sprachen-Packages zu ersetzen ist, das hinzugefügt werden soll.
   - Unter Linux: Geben Sie `rpm -i path/pkgname<...>.rpm` ein, wobei *pkgname* durch den Namen des Packages zu ersetzen ist, das hinzugefügt werden soll.

Package-Name	Beschreibung
SUNWcmcon, SUNWcmctg	Sun™ Web Console 2.0 in vereinfachtem Chinesisch
SUNWdmcon, SUNWdmctg	Sun™ Web Console 2.0 in Deutsch
SUNWemcon, SUNWemctg	Sun™ Web Console 2.0 in Spanisch
SUNWfmcon, SUNWfmctg	Sun™ Web Console 2.0 in Französisch
SUNWhmcon, SUNWhmctg	Sun™ Web Console 2.0 in traditionellem Chinesisch
SUNWimcon, SUNWimctg	Sun™ Web Console 2.0 in Italienisch
SUNWjmcon, SUNWjmctg	Sun™ Web Console 2.0 in Japanisch
SUNWkmcon, SUNWkmctg	Sun™ Web Console 2.0 in Koreanisch
SUNWsmcon, SUNWsmctg	Sun™ Web Console 2.0 in Schwedisch

Ausführen der Konsole

Normalerweise muss der Sun Web Console-Server nur beendet und neu gestartet werden, um eine neue Anwendung zu registrieren.

Bevor Sie Sun Web Console zum ersten Mal starten, vergewissern Sie sich bitte, dass die Installation von Configuration Manager abgeschlossen ist.

- Zum Starten von Sun Web Console geben Sie `smcwebserver start` ein.
- Zum Beenden von Sun Web Console geben Sie `smcwebserver stop` ein.
- Um auf Sun Web Console zuzugreifen, geben Sie folgende URL in Ihren Browser ein: `https://<Rechnername>.<Domänenname>:6789`

Sun Web Console unterstützt standardmäßig die Unix-basierte Authentifizierung und RBAC (rollenbasierte Zugriffskontrolle). Es können jedoch auch andere Authentifizierungsmechanismen wie beispielsweise die LDAP-Authentifizierung konfiguriert werden.

> **Hinweis:** Die Standardzeitüberschreitung für Sitzungen beträgt 15 Minuten. Der Zeitüberschreitungswert kann mit dem Befehl `smreg` modifiziert werden. Möchten Sie die Zeitüberschreitung beispielsweise auf 5 Minuten einstellen, geben Sie `smreg add -p -c session.timeout.value=5` ein.

Weitere Informationen zu Befehlen für Sun Web Console finden Sie in den Manpages smcwebserver und smreg.

Deinstallation von Sun Web Console

Zum Deinstallieren von Sun Web Console führen Sie `/usr/lib/webconsole/setup -u` aus.

Hinweis: Führen Sie diesen Befehl nicht im Verzeichnis `/usr/lib/webconsole` oder einem der entsprechenden Unterverzeichnisse aus, sonst schlägt `pkgrm` fehl.

Port-Informationen für Sun Web Console

Configuration Manager verwendet die Ports von Sun Web Console:

- 8005 zum Beenden des Dienstes und
- 6789 für HTTPS-Zugriffe.

In der Datei `/etc/opt/webconsole/server.xml` können diese beiden Ports geändert werden. Starten Sie Sun Web Console nach der Änderung mit `/usr/sbin/smcwebserver neu`.

KAPITEL 4

Sun Java™ Desktop System Configuration Manager

Configuration Manager ist ein Verwaltungstool, das unter Sun Web Console ausgeführt wird. Diese webbasierte Benutzeroberfläche erlaubt es Administratoren, die Hierarchie einer Organisation zu durchlaufen und darin Richtlinien für Desktop-Anwendungen festzulegen. Es können Richtlinien für jedes Element in der Hierarchie definiert werden, beispielsweise für Organisationen, Rollen, Benutzer, Domänen und Rechner. In Configuration Manager werden die für die einzelnen Desktop-Anwendungen Gnome, Mozilla, StarOffice und Evolution spezifischen Einstellungen in verschiedenen Konfigurationsvorlagen präsentiert.

Installation von Configuration Manager

Bevor Configuration Manager installiert werden kann, muss eine funktionierende Installation von Sun Web Console vorhanden sein.

1. Wechseln Sie in das entsprechende Configuration Manager-Verzeichnis auf der Java Desktop System Management Tools-CD.

   Auf Linux-Systemen wechseln Sie in das Verzeichnis `/linux/apoc`. Auf Solaris SPARC-Systemen wechseln Sie in das Verzeichnis `/solsparc/apoc.`

2. Geben Sie `./setup` ein.

3. Geben Sie den Rechnernamen des LDAP-Servers ein.

   Der Standardname lautet localhost.

4. Geben Sie die Port-Nummer des LDAP-Servers ein (Standardwert: 389).

5. Geben Sie den Base-DN der LDAP-Datensammlung ein.

6. Geben Sie den Namen der Objektklasse zur Identifizierung von Benutzerentitäten ein. Die Standardobjektklasse ist inetorgperson.

   Weitere Einzelheiten entnehmen Sie bitte dem Abschnitt „Organisatorische Zuordnung“ im Kapitel „LDAP-Server“.

7. Geben Sie einen innerhalb der gesamten LDAP-Datensammlung einmaligen Attributnamen ein. Das Standardattribut ist uid.

   Weitere Einzelheiten entnehmen Sie bitte dem Abschnitt „Organisatorische Zuordnung“ im Kapitel „LDAP-Server“.

8. Geben Sie den vollständigen DN eines Benutzers ein, der über die erforderlichen Zugriffsrechte für Abfragen auf dem LDAP-Server verfügt.

   Dabei kann es sich um einen beliebigen vollständigen DN mit Lese- und Suchzugriff handeln. Wenn der Zugriff anonym erfolgen soll, lassen Sie dieses Feld leer.

9. Geben Sie ein Passwort für den Benutzer ein, dem Sie die LDAP-Zugriffsrechte zugewiesen haben.

   Für den anonymen Zugriff auf den LDAP-Server ignorieren Sie diesen Schritt.

Bei der Installation wird Sun Web Console ein zusätzliches Anmeldemodul hinzugefügt, das die Authentifizierung von Benutzern über LDAP erlaubt.

Am Ende der Installation startet Sun Web Console automatisch neu, und es kann auf Configuration Manager zugegriffen werden.

Hinweis: Die Einstellungen für Configuration Manager lassen sich mithilfe des Skripts `/usr/share/webconsole/apoc/configure` jederzeit ändern. Sie können mithilfe des Skripts beispielsweise den LDAP-Server wechseln, ohne Configuration Manager neu installieren zu müssen.

Ausführen von Configuration Manager

1. Um auf Configuration Manager zuzugreifen, geben Sie folgende URL in Ihren Browser ein:

   `https://<Rechnername>.<Domänenname>:6789`

2. An der Eingabeaufforderung geben Sie den Benutzernamen (UID) und das Passwort eines vorhandenen LDAP-Benutzers ein.

   Sun Web Console wird geöffnet.

3. Im Konsolenfenster klicken Sie auf **Sun Java™ Desktop System Configuration Manager.**

Hinweis: Wenn Sie die Startseite von Sun Web Console überspringen und direkt auf Configuration Manager zugreifen möchten, geben Sie folgende URL in Ihren Browser ein:

`https://<Rechnername>.<Domänenname>:6789/apoc`

Deinstallation von Configuration Manager

Zum Deinstallieren von Configuration Manager über Sun Web Console wechseln Sie in das entsprechende Configuration Manager-Verzeichnis auf der Java Desktop System Management Tools-CD und führen dann `./setup -u` aus.

Hinweis: Wenn Sie Configuration Manager deinstallieren, wird das LDAP-Anmeldemodul aus Sun Web Console entfernt.

KAPITEL 5

Desktop-Komponenten

Für den Zugriff auf die Konfigurationsdaten über Configuration Manager benötigen Desktop-Clients Sun Java™ Desktop System Configuration Agent. Configuration Agent kommuniziert mit der entfernten Konfigurationsdatensammlung und den Adaptern und fügt Daten in spezifische Konfigurationssysteme ein. Derzeit werden die Konfigurationssysteme GConf, Mozilla-Einstellungen und StarOffice Registry unterstützt.

All diese Komponenten werden mit Java Desktop System geliefert und installiert.

Zugriff auf Daten / Benutzerauthentifizierung

Configuration Agent ruft in Abhängigkeit von der Anmelde-ID des jeweiligen Desktop-Benutzers Informationen vom LDAP-Server ab. Durch die User / UniqueIdAttribute-Einstellung der organisatorischen Zuordnungsdatei wird die Anmelde-ID einer Benutzerentität auf dem LDAP-Server zugeordnet. Außerdem ruft Configuration Agent Informationen über den Rechner ab, wie zum Beispiel dessen Namen oder IP-Adresse. Diese Informationen werden durch die Host / UniqueId-Attribute-Einstellung der organisatorischen Zuordnungsdatei einer Rechnerentität auf dem LDAP-Server zugeordnet.

Es kann anonym oder mit der GSSAPI-Methode auf den LDAP-Server zugegriffen werden. Der anonyme Zugriff erfordert keinen Eingriff seitens des Desktops. Für die GSSAPI-Methode müssen auf dem Desktop Kerberos-Berechtigungsnachweise erworben werden. Damit der Kerberos-Berechtigungsnachweiserwerb in die Benutzeranmeldung integriert werden kann, muss das Modul `pam_krb5` auf dem Java Desktop System-Rechner installiert und konfiguriert sein. Im Verzeichnis `/usr/share/doc/packages/pam_krb5/README.SuSE` auf der Java Desktop System-CD finden Sie Beispielkonfigurationen für das pam-Modul. Auch mithilfe von gdm lässt sich Kerberos in die Benutzeranmeldung integrieren. Verwenden Sie hierzu beispielsweise die folgende Datei /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
```

Configuration Agent

Configuration Agent ist Bestandteil des `apoc-`Packages. Wenn Sie den entsprechenden RPM-Build installieren, werden die für diese API benötigten Dateien mit inetd installiert und registriert. Sie können den RPM-Build entweder manuell oder gemeinsam mit Java Desktop System installieren.

Startinformationen

Für den Zugriff auf die entfernten Konfigurationsdaten benötigt Configuration Agent die Adresse des LDAP-Servers. Diese Adresse können Sie mit dem Konfigurationstool YaST2, mit autoYaST oder manuell hinzufügen, indem Sie die Eigenschaftendatei `policymgr.properties` im Verzeichnis `/opt/apoc/lib` bearbeiten. In YaST2 fügen Sie diese Angaben im Bereich Netzwerk/Erweitert ein.

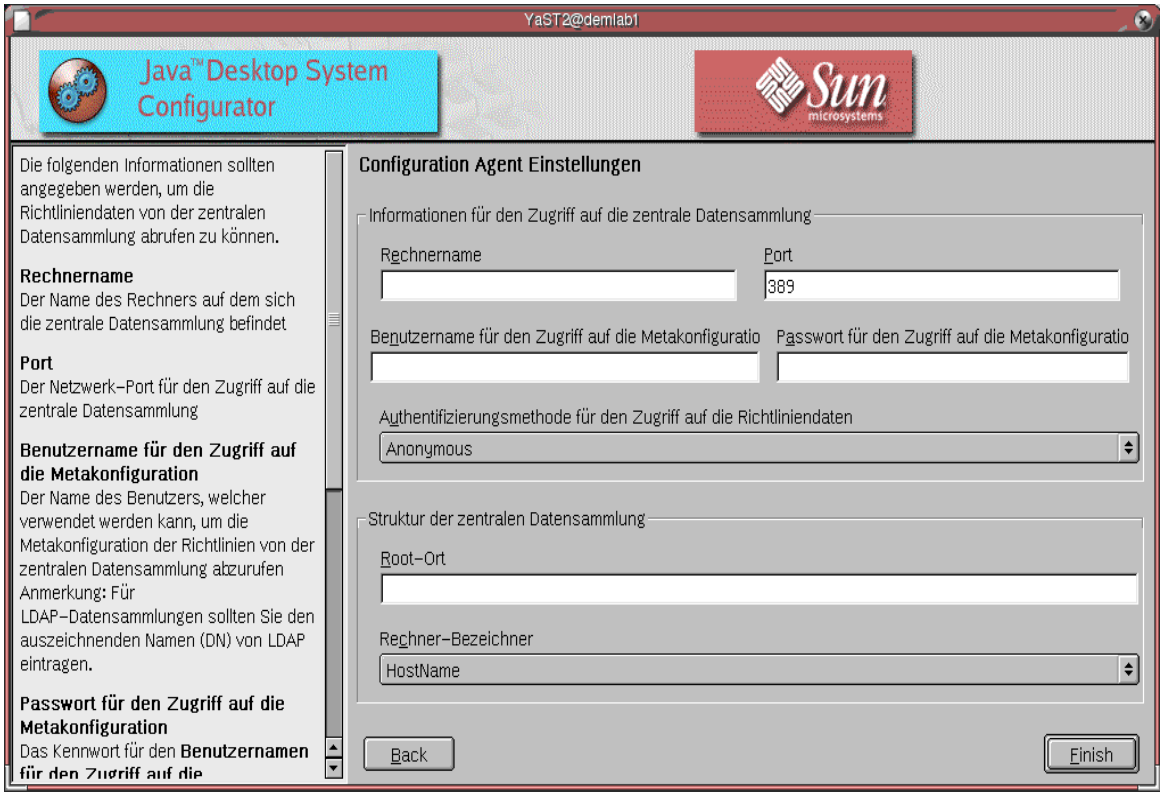

Abbildung 1 Java Desktop System Configuration Agent in YaST

Für die Ausführung von Configuration Agent werden die folgenden Informationen benötigt:

- Rechnername (Server): Rechnername des LDAP-Servers
- Port (Port): Port-Nummer des LDAP-Servers
- Benutzername für den Zugriff auf die Metakonfiguration (AuthDn): vollständiger DN eines Benutzers mit Lese- und Suchberechtigung für die Datensammlung

  Hinweis: Wurde für das Verzeichnis der anonyme Zugriff aktiviert, kann diese Einstellung leer bleiben.

- Passwort für den Zugriff auf die Metakonfiguration (Passwort): Passwort eines registrierten LDAP-Benutzers

Hinweis: Wurde für das Verzeichnis der anonyme Zugriff aktiviert, kann diese Einstellung leer bleiben.

- Authentifizierungsmethode für den Zugriff auf die Richtliniendaten (AuthType): Anonymous oder GSSAPI, je nach der Methode zur Benutzerauthentifizierung auf dem LDAP-Server
- Root-Ort (BaseDn): Base-DN der LDAP-Datensammlung
- Rechner-Bezeichner (HostIdentifier): HostName oder IP-Adresse. Diese Angabe muss mit dem Inhalt des LDAP-Attributs übereinstimmen, das zur Identifikation von Rechnern eingesetzt wird. Dieses Attribut ist in den Zuordnungsdateien als Host / UniqueIDAttribute definiert.
- Verbindungszeitüberschreitung (Connect Timeout): Dauer in Sekunden, nach deren Ablauf der Versuch, eine Verbindung zum LDAP-Server herzustellen, abgebrochen wird. Der Standardwert ist 1 Sekunde.

Hinweis: Nach jeder Änderung dieser Einstellungen muss Configuration Agent neu gestartet werden.

Um Configuration Agent auf dem Desktop neu zu starten, vergewissern Sie sich, dass keine der dazugehörigen Client-Anwendungen ausgeführt wird. Melden Sie sich als Root an, und geben Sie den Befehl `/opt/apoc/bin/apocd restart` ein.

Betriebseinstellungen

Die Betriebseinstellungen für Configuration Agent lassen sich sowohl lokal als auch entfernt konfigurieren. Für eine lokale Konfiguration bearbeiten Sie die Datei `apocd.properties` im Verzeichnis `/opt/apoc/lib`. Um die Einstellungen entfernt zu konfigurieren, greifen Sie auf die Configuration Agent-Richtlinie in Configuration Manager zurück. In der Eigenschaftendatei können die folgenden Einstellungen konfiguriert werden:

- DaemonPort: Port, den Configuration Agent auf Anfragen der dazugehörigen Clients auf dem Desktop abhört
- MaxClientThreads: Höchstanzahl für Client-Threads, die gleichzeitig abgearbeitet werden können
- MaxClientConnections: Höchstanzahl für Client-Verbindungen
- MaxRequestSize: maximale Größe für Client-Anforderungen
- DaemonChangeDetectionInterval: Intervall in Minuten zwischen Zyklen zur Erkennung von Änderungen an dieser Liste von Konfigurationseinstellungen
- ChangeDetectionInterval: Intervall in Minuten zwischen Zyklen zur Erkennung von Änderungen an Client-Konfigurationsdaten
- GarbageCollectionInterval: Intervall in Minuten zwischen Zyklen zur Bereinigung (garbage collection) der lokalen Konfigurationsdatenbank
- TimeToLive: Aufbewahrungsdauer in Minuten für Nicht-Offline-Konfigurationsdaten in der lokalen Datenbank
- LogLevel: Genauigkeit der Agent-Protokolldateien

Die Einstellung DaemonPort kann ausschließlich lokal geändert werden und wird erst nach einem Agent-Neustart wirksam. Alle übrigen Einstellungen werden mit dem nächsten Zyklus zur Erkennung von Änderungen an der Agent-Konfiguration wirksam. Bei der mit LogLevel festgelegten Genauigkeit muss es sich um einen der Java Logger-Levelwerte handeln. Diese lauten, nach abnehmender Wichtigkeit geordnet: ERNST, WARNUNG, INFO, KONFIGURATION, DETAILS, MEHR DETAILS und MAX. DETAILS.

Weitergabe von Konfigurationsdatenänderungen

Mit der unter „Betriebseinstellungen“ beschriebenen Einstellung ChangeDetectionInterval lässt sich die Weitergabe von entfernten Konfigurationsdatenänderungen an clientseitige Anwendungen einstellen. Der Wert, den Sie für diese Einstellung festlegen, bestimmt, wie viele Minuten maximal verstreichen, bevor entfernt vorgenommene Änderungen auf die Client-Anwendungen übertragen werden. Je niedriger der Wert von ChangeDetectionInterval ist, desto höher fällt die Configuration Agent- und LDAP-Server-Aktivität aus. Bedenken Sie dies bitte, wenn Sie einen Wert für diese Einstellung wählen. Günstig wäre es zum Beispiel, den Wert für die anfängliche Bereitstellungsphase auf eine Minute einzustellen, damit sich die Auswirkung der entfernten Konfiguration auf die Client-Anwendungen leicht testen lässt, und die Einstellung nach Abschluss dieser Tests auf den Ausgangswert zurückzusetzen.

Port-Informationen für Configuration Agent

Configuration Agent verwendet zwei Ports:

1. Daemon-Port (Standardeinstellung ist 38900), über den der Daemon mit den Client-Anwendungen kommuniziert.
2. Daemon-Administrationsport (Standardeinstellung ist 38901), über den das Daemon-Controller-Programm `apocdct1` mit dem Daemon kommuniziert.

Ändern des Daemon-Ports:

Wenn Sie einen anderen Daemon-Port angeben möchten, müssen Sie die Eigenschaft `DaemonPort` in der Datei `apocd.properties` für den Daemon sowie die `apocd`-Einträge in `/etc/services` und `/etc/inetd.conf` ändern. Anschließend müssen Sie den Daemon neu starten und `inetd` neu laden.

Ändern des Daemon-Administrationsports:

Wenn Sie einen anderen Daemon-Administrationsport angeben möchten, müssen Sie die Eigenschaft `DaemonAdminPort` in der Datei `apocd.properties` für den Daemon ändern. Starten Sie den Daemon anschließend neu.

GConf-Adapter

Der GConf-Adapter ist Bestandteil des Packages `apoc-adapter-gconf`. Wenn Sie den Adapter aus dem entsprechenden RPM-Build installieren, wird der Pfad der GConf-Datenquellen in `/etc/gconf/2/path` aktualisiert, d. h., die Configuration Manager-Quellen werden aufgenommen. Unter `/etc/gconf/2/path.apocBackup` wird eine Sicherungskopie des alten Pfads abgelegt. Bezieht sich der alte Pfad auf benutzerdefinierte Datenquellen, müssen Sie den Pfad aktualisieren, indem Sie die Abweichungen vom Standardpfad in den neu installierten Manager-Pfad übertragen. Der Adapter stellt die folgenden beiden Datenquellen zur Verfügung:

- „apoc:readonly:“: ermöglicht den Zugriff auf ungeschützte Einstellungen über die Richtlinien. Fügen Sie diese Datenquelle nach den Benutzereinstellungen und vor den lokalen Standardwerten ein.
- „apoc:readonly:mandatory@“: ermöglicht den Zugriff auf geschützte Einstellungen über die Richtlinien. Fügen Sie diese Datenquelle nach den obligatorischen lokalen Einstellungen und vor den Benutzereinstellungen ein.

Mozilla-Adapter

Der Mozilla-Adapter ist Bestandteil des Packages mozilla-`apoc-integration`. Wenn Sie den Adapter aus dem entsprechenden RPM-Build installieren, werden die erforderlichen Dateien einer vorhandenen Mozilla-Installation hinzugefügt und automatisch registriert.

StarOffice-Adapter

Der StarOffice-Adapter ist in Standardinstallationen von StarOffice enthalten und ermöglicht den Zugriff auf Richtlinienkonfigurationsdaten, ohne dass Sie spezielle Änderungen vornehmen müssen.

KAPITEL 6

Anhang A – Sun Web Console

Bekannte Probleme

Sicherheit

Bei bestimmten Benutzeraktionen bleiben Sitzungen unter Umständen weiterhin aktiv, ohne dass dies dem Benutzer ersichtlich ist. Beispielsweise wird der Benutzer durch das Schließen eines Browserfensters nicht automatisch von Sun Web Console abgemeldet. Vor dem Schließen von Anwendungsfenstern muss sich der Benutzer also explizit von der Sitzung in Sun Web Console abmelden.

Syntax für Einrichtungsskripten

Zusammenfassung: `setup [-h] | [-n] | [-d <Ver>,<Arch>[,Client1,Client2, ...]] [-u [-f]]`

-h = Erklärung zur Syntax ausgeben

-n = Server am Ende der Installation nicht starten

-u = Sun Web Console deinstallieren

-f = Tomcat und Java 1.4 deinstallieren (vorausgesetzt, diese Packages wurden mit der Einrichtungsanwendung setup installiert). Dieser Parameter kann nur in Verbindung mit dem Parameter -u eingesetzt werden.

Wenn Sie eine vollständige Beschreibung der verfügbaren Einrichtungsparameter wünschen, geben Sie den Befehl `setup -h` ein.

Zum Deinstallieren von Sun Web Console führen Sie `/usr/lib/webconsole/setup -u` aus.

Hinweis: Führen Sie diesen Befehl nicht im Verzeichnis `/usr/lib/webconsole` oder einem der entsprechenden Unterverzeichnisse aus, sonst schlägt `pkgrm` fehl.

Sun Web Console-Packages

Solaris-Packages

Package-Name	Beschreibung
SUNWmctag	Sun Web Console UI Tag-Bibliothek
SUNWmcon	Sun Web Console
SUNWmcos	Gemeinsame Solaris-Dienste für Sun Web Console
SUNWmcosx	Versionsspezifische Solaris-Dienste für Sun Web Console
SUNWmconr	Sun Web Console-Root
SUNWjato	Sun One Application Framework-Laufzeit
SUNWtcatu	Tomcat

Linux-RPMs

Package-Name	Beschreibung
SUNWmctag	Sun Web Console UI Tag-Bibliothek
SUNWmcon	Sun Web Console
SUNWmcos	Gemeinsame Linux-Dienste für Sun Web Console
SUNWmcosx	Versionsspezifische Linux-Dienste für Sun Web Console
SUNWmconr	Sun Web Console-Root
SUNWjato	Sun One Application Framework-Laufzeit
tomcat4	Tomcat

Anhang B – Configuration Manager

Configuration Manager-Packages

Solaris-Packages

Package-Name	Beschreibung
SUNWapm	Configuration Manager
SUNWapmca	Configuration Agent-Vorlagen
SUNWapmev	Evolution-Vorlagen
SUNWapmgo	Gnome-Vorlagen
SUNWapmmo	Mozilla-Vorlagen
SUNWapmso	StarOffice-Vorlagen

Linux-RPMs

Package-Name	Beschreibung
apoc-manager	Configuration Manager
apoc-agent-templates	Configuration Agent-Vorlagen
apoc-evolution-templates	Evolution-Vorlagen
apoc-gnome-templates	Gnome-Vorlagen
apoc-mozilla-templates	Mozilla-Vorlagen
apoc-staroffice-templates	StarOffice-Vorlagen

KAPITEL 8

Anhang C

Verwenden eines OpenLDAP-Servers mit Configuration Manager

Wenn Sie einen OpenLDAP-Server als Datensammlung für die Configuration Manager-Daten einsetzen möchten, muss das Schema des Servers auf die Objektklassen und Attribute ausgeweitet werden, die zum Speichern von Konfigurationsdaten verwendet werden. Das Unterverzeichnis `openldap` des Bereitstellungstools von Configuration Manager, das Sie auf der Java Desktop System Management Tools-CD finden, enthält die Datei `apoc.schema` für benutzerdefinierte Schemata.

Diese Datei muss in das Unterverzeichnis `schema` des OpenLDAP-Konfigurationsverzeichnisses (`/etc/openldap`) kopiert und in das OpenLDAP-Schema importiert werden. Hierzu fügen Sie an das Ende der Schema-Include-Sequenz in der Datei `slapd.conf`, die sich in demselben Verzeichnis befindet, die Zeile include `/etc/openldap/schema/apoc.schema` ein. Weitere Informationen zur Erweiterung des Schemas eines OpenLDAP-Servers entnehmen Sie bitte der Dokumentation des jeweiligen Servers.

Die OpenLDAP -Datenbank muss mit dem Bereitstellungstool von Configuration Manager auf die Speicherung von Konfigurationsdaten vorbereitet werden. Nachdem im vorigen Installationsschritt das Schema bereits erweitert wurde, bleibt nur noch das Skript `createServiceTree` auszuführen. Das Skript muss aus dem Verzeichnis des Bereitstellungstools mit den Rechten eines beliebigen Benutzers und dem folgenden Befehl gestartet werden: `./createServiceTree`. Wie bereits im Abschnitt über das Bereitstellungstool in diesem Dokument dargestellt, fordert das Skript den Benutzer zur Eingabe von Informationen über die OpenLDAP-Datenbank auf. Das Unterverzeichnis `openldap` des Bereitstellungstools enthält eine Standard-Zuordnungsdatei mit typischen OpenLDAP-Objektklassen und -Attributen. Diese Datei heißt `OrganisationalMapping`. Um sie bereitzustellen, kopieren Sie die Datei vor dem Aufrufen von `createServiceTree` über die gleichnamige Datei im Hauptverzeichnis des Bereitstellungstools.

Beachten Sie bitte, dass Configuration Manager Agent versucht, eine anonyme Verbindung zum OpenLDAP-Server herzustellen und dazu zwar den DN des Benutzers, für den Daten angefordert werden, aber kein Passwort angibt. Eine derartige anonyme Authentifizierung kann bei einigen Versionen von OpenLDAP-Servern unter Umständen standardmäßig deaktiviert sein. In diesem Fall muss die Zeile allow `bind_anon_cred` in die gemeinsamen Serverparameter eingefügt werden, die in der Datei file `slapd.conf` im OpenLDAP-Konfigurationsverzeichnis (`/etc/openldap`) definiert sind. Weitere Informationen zu diesem Parameter entnehmen Sie bitte der Dokumentation des jeweiligen Servers.

Verwenden eines Active Directory-Servers mit Configuration Manager

Wenn Sie einesnActive Directory-Server als Datensammlung für die Configuration Manager-Daten einsetzen möchten, muss das Schema des Servers auf die Objektklassen und Attribute ausgeweitet werden, die zum Speichern von Konfigurationsdaten verwendet werden. Das Unterverzeichnis `ad` des Configuration Manager-Bereitstellungstools auf der Management Tools-CD enthält eine Schema-Erweiterungsdatei namens `apoc-ad.ldf`. Weitere Informationen entnehmen Sie bitte dem Abschnitt über das Bereitstellungstool.

Importieren Sie die Datei `apoc-ad.ldf` wie folgt in das Active Directory-Schema:

1. Aktivieren Sie die Schema-Erweiterung. Siehe hierzu die Active Directory-Dokumentation.
2. Geben Sie Folgendes in die Befehlszeile ein: `ldifde -i -c "DC=Sun,DC=COM"` *<Basis-DN>* `-f apoc-ad-registry.ldf.`

   Hinweis: Ersetzen Sie dabei *<Basis-DN>* durch den Basis-DN für Active Directory.

Der Active Directory-Server muss mit dem Bereitstellungstool auf die Speicherung von Konfigurationsdaten vorbereitet werden. Nachdem im vorigen Installationsschritt das Schema bereits erweitert wurde, bleibt nur noch das Skript `createServiceTree` auszuführen. Das Skript muss aus dem Verzeichnis des Bereitstellungstools mit den Rechten eines beliebigen Benutzers und dem folgenden Befehl gestartet werden: `./createServiceTree`. Es fordert den Benutzer zur Eingabe von Informationen über die Active Directory-Datenbank auf. Das Unterverzeichnis `ad` des Bereitstellungstools enthält eine Standard-Zuordnungsdatei mit typischen Active Directory-Objektklassen und -Attributen. Diese Datei heißt `OrganisationalMapping`. Um sie bereitzustellen, kopieren Sie die Datei vor dem Aufrufen von `createServiceTree` über die gleichnamige Datei im Hauptverzeichnis des Bereitstellungstools.

Damit ist die Vorbereitung des Active Directory-Servers für die Verwendung mit Configuration Manager abgeschlossen. Geben Sie bei der Installation von Configuration Manager den vollständigen DN und das Passwort eines Benutzers mit Leseberechtigung für den Baum an. Dabei kann es sich um einen Benutzer ohne weitere Berechtigungen für Active Directory handeln. Genaueres zur Einrichtung eines solchen Benutzers entnehmen Sie bitte der Active Directory-Dokumentation. Außerdem müssen Sie dem System, auf dem Configuration Manager ausgeführt wird, den Domänennamen von Active Directory mitteilen. Hierzu können Sie in die Datei `/etc/hosts` dieses Systems eine Zeile mit der Zuordnung zwischen der IP-Adresse des Active Directory-Servers und dessen Domänennamen einfügen.

Zum Abrufen der Konfigurationsdaten von einem Java Desktop System-Host muss der Domänenname von Active Directory auch diesem Host mitgeteilt werden. Die Authentifizierung von Java Desktop System-Benutzern kann entweder anonym oder per GSSAPI erfolgen.

- Für die Authentifizierung über anonyme Verbindungen muss der Active Directory-Server so konfiguriert sein, dass alle Benutzer leseberechtigt sind. Näheres hierzu entnehmen Sie bitte der Active Directory-Dokumentation.

- Für die Authentifizierung per GSSAPI müssen Sie die Datei `/etc/krb5.conf`, in der die Kerberos-Parameter angegeben sind, bearbeiten. Sie muss den Active Directory-Bereich definieren und auf den Active Directory-Server als KDC (Key Distribution Center) verweisen. Auch müssen die von Active Directory unterstützten DES-Typen, nämlich `des-cbc-crc` und `des-cbc-md5`, als Standardverschlüsselungstypen in der Datei angegeben werden. Genaue Anweisungen hierzu finden Sie in der Kerberos-Dokumentation. Vor dem Zugriff auf die Konfigurationsdaten müssen gültige Berechtigungsnachweise für den bei Java Desktop System angemel-

deten Benutzer vorgelegt werden. Dies kann manuell durch Ausführung des Befehls `kinit` und Eingabe des in Active Directory definierten Benutzerpassworts manuell vorgenommen werden. Andere Schemata generieren diese Berechtigungsnachweise bei der Anmeldung möglicherweise automatisch. Weitere Informationen entnehmen Sie bitte der Dokumentation zu Java Desktop System.