

# Guía de instalación de Sun Java™ Desktop System Configuration Manager

---

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

Referencia: 817-5589-10

Abril 2004, Revision A

# Copyrights y marcas comerciales

**Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054., U.S.A. Reservados todos los derechos.**

Sun Microsystems, Inc. tiene los derechos de propiedad intelectual relacionados con la tecnología incluida en este producto. En particular, y sin limitaciones, los derechos de propiedad intelectual pueden incluir una o más de las patentes de los EE.UU. enumeradas en <http://www.sun.com/patents> y una o más patentes adicionales o solicitudes de patentes pendientes en los EE.UU. y otros países.

Este documento y el producto al que pertenece se distribuyen bajo licencias que restringen su uso, copia, distribución y descompilación. No se puede reproducir parte alguna de este producto o de este documento en ninguna forma ni por cualquier medio sin la autorización previa por escrito de Sun y sus licenciadores, si los hubiera.

El software de otras empresas, incluida la tecnología de fuentes, está protegido por copyright y posee licencia exclusiva de los proveedores de Sun.

Este producto se basa en parte del trabajo del Independent JPEG Group y el FreeType Project.

Portions Copyright 2000 SuSE, Inc. Word for Word Copyright © 1996 Inso Corp. Sistema de corrección ortográfica International CorrectSpell Copyright © 1995 de Lernout & Hauspie Speech Products N.V. Reservados todos los derechos.

Sun, Sun Microsystems, el logotipo de Sun, Java, Solaris, StarOffice, el logotipo Butterfly, el logotipo de Solaris y el de StarOffice son marcas comerciales o marcas comerciales registradas de Sun Microsystems, Inc. en EE.UU. y otros países.

UNIX es una marca registrada en los Estados Unidos y en otros países, bajo licencia exclusiva de X/Open Company, Ltd. Screen Beans y Screen Beans son marcas comerciales registradas de A Bit Better Corporation.

Adquisiciones federales: El software comercial y los usuarios del gobierno están sujetos a los términos y condiciones de licencia estándar.

ESTA DOCUMENTACIÓN SE ENTREGA "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPRESA O IMPLÍCITA, INCLUYENDO PERO NO LIMITÁNDOSE A LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO PARTICULAR, O NO INFRINGIMIENTO, SALVO QUE AMBAS RENUNCIAS SE CONSIDEREN NO VÁLIDAS LEGALMENTE.

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

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

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

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

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

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

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

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

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

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

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

# Contenido

---

<b>1</b>	<b>Introducción.....</b>	<b>5</b>
<b>2</b>	<b>Servidor LDAP.....</b>	<b>7</b>
	Conceptos.....	7
	Configuración.....	7
	Consideraciones adicionales.....	12
<b>3</b>	<b>Sun™ Web Console.....</b>	<b>13</b>
	Requisitos del sistema.....	13
	Instalación de Sun Web Console.....	14
	Ejecución de la consola.....	15
	Desinstalación de Sun Web Console.....	15
	Información sobre el puerto de Sun Web Console.....	16
<b>4</b>	<b>Sun Java™ Desktop System Configuration Manager.....</b>	<b>17</b>
	Instalación de Configuration Manager.....	17
	Ejecución de Configuration Manager.....	18
	Desinstalación de Configuration Manager.....	18
<b>5</b>	<b>Componentes del escritorio.....</b>	<b>19</b>
	Acceso a los datos/autenticación del usuario.....	19
	Configuration Agent.....	20
	Adaptador de GConf .....	22
	Adaptador de Mozilla .....	22
	Adaptador de StarOffice.....	23
<b>6</b>	<b>Apéndice A – Sun Web Console.....</b>	<b>25</b>
	Problemas conocidos.....	25
	Sintaxis de la secuencia de órdenes de configuración.....	25
	Paquetes de Sun Web Console.....	26
<b>7</b>	<b>Apéndice B – Configuration Manager.....</b>	<b>27</b>
	Paquetes de Configuration Manager.....	27
<b>8</b>	<b>Apéndice C.....</b>	<b>29</b>
	Uso de un servidor OpenLDAP con Configuration Manager.....	29
	Uso de un servidor Active Directory con Configuration Manager.....	30



## Introducción

---

Sun Java™ Desktop System Configuration Manager se ha diseñado para proporcionar una configuración central para los sistemas de escritorio que ejecuten Sun Java™ Desktop System. Los valores se pueden asignar a varios elementos de una organización, de esta manera se permite que un administrador gestione los grupos de usuarios o sistemas de un modo sencillo. Sus componentes principales son:

- Un servidor LDAP que contiene la estructura organizativa de los usuarios y sistemas que se desea gestionar; mantiene los datos de la configuración.
- Una herramienta de gestión basada en la web que permite a los administradores definir y asignar los datos de la configuración de los elementos de la estructura organizativa.
- Los componentes del escritorio instalados en el sistema del cliente, que recuperan los datos de la configuración en el nombre del usuario conectado en la actualidad y lo exponen a diversas aplicaciones, configurando Sun™ Java Desktop System.

La herramienta de gestión es una aplicación que se basa en la web y que se ejecuta en Sun Web Console. Permite al administrador navegar por la estructura organizativa del servidor LDAP y asignar normas a los elementos. Éstas se muestran y editan de acuerdo con plantillas, que definen los valores que manipulará la herramienta de gestión.

Los componentes del escritorio se organizan alrededor de Sun Java™ Desktop System Configuration Agent; éste recupera los datos de la configuración del servidor LDAP en nombre de los usuarios y los pone a disposición de varios adaptadores de configuración de sistemas, que completan la configuración local (valores predeterminados proporcionados por las aplicaciones y valores del usuario) con los valores de las normas. Los sistemas de configuración actualmente admitidos son GConf (que gestiona la configuración de las aplicaciones de Gnome, como el escritorio Gnome o Evolution), Mozilla™ Preferences y StarRegistry (sistema de configuración de StarOffice).



## Servidor LDAP

---

### Conceptos

Dentro de la estructura de Java Desktop System Configuration Manager, los datos de la configuración se asocian con las entidades, que son entradas en el depósito de LDAP y se corresponden con elementos de la estructura organizativa de la empresa.

Se reconocen las siguientes entidades:

- Organización: normalmente representa una unidad organizativa (divisiones, grupo, equipos) o geográfica (continente, país, sede) de la jerarquía general.
- Usuario: representa un nodo de hoja de la estructura general y, como su nombre indica, normalmente es un usuario.
- Dominio: representa una unidad de estructuración lógica para la organización en red.
- Sistema: también representa un nodo de hoja de la jerarquía general pero apunta a una máquina de la red.
- Rol: representa las propiedades, normalmente una distinción de términos de las funciones (administrador, gestión de la sede), que se aplican a un conjunto de usuarios.

Las entidades de la organización y el usuario se utilizan para definir un árbol del usuario, mientras que las entidades del dominio y del sistema definen un árbol del sistema. Estos dos árboles son independientes pero se gestionan de manera similar en la estructura.

La relación de las entidades del dominio y la organización con otras entradas se define mediante la ubicación física de las entradas dentro del depósito. Es decir, las entidades de la organización y el dominio pueden incluir entradas situadas por debajo de ellas en el árbol. La relación de los roles con los usuarios o con los sistemas la definen los atributos del usuario y las entradas del sistema.

Los datos de configuración asociados con una entidad se almacenan en entradas especiales que se gestionan mediante la estructura y que se identifican mediante el contenedor y el nombre del servicio asociados con las entradas.

### Configuración

Si desea utilizar un servidor LDAP con Configuration Manager, necesita:

- Ampliar el esquema del servidor para que admita las clases de objetos personalizados y los atributos utilizados por Configuration Manager para almacenar datos de la configuración.
- Personalizar y almacenar en el servidor la información de la asignación de las entradas del depósito, así como las entidades admitidas por Configuration Manager.

## Herramientas de desarrollo

Se necesitan las siguientes herramientas de desarrollo del CD de instalación para utilizar un servidor LDAP con Configuration Manager:

- `88apoc-registry.ldif`: archivo de esquema que presenta las clases y los atributos de objetos necesarios para el almacenamiento de los datos de la configuración.
- `OrganizationMapping`: archivo predeterminado de propiedades que describe la asignación entre las entradas LDAP y las entidades de Configuration Manager.
- `UserProfileMapping`: archivo predeterminado de propiedades; describe la asignación entre los atributos de las entradas del usuario LDAP y los del perfil del usuario de Configuration Manager.
- `createServiceTree`: una secuencia de órdenes que almacena los archivos de asignación en el depósito LDAP.
- `deployApoc`: una secuencia de órdenes que amplía el esquema del servidor LDAP y que almacena los archivos de asignación en el depósito LDAP.

## Ampliación del esquema

Los datos de la configuración se almacenan en árboles de entradas que se adjuntan a las entradas con que se asocian los datos. Para poder almacenar las clases de los objetos y los atributos usados por estos árboles en un servidor LDAP, debe añadir los objetos y las clases al esquema del servidor LDAP. Por ejemplo, el archivo de extensión del esquema proporcionado usa el formato LDIF para añadir estos objetos y clases a Sun Java System Directory Server. Si desea añadirlos a otros servidores LDAP, necesita utilizar un formato reconocido por los servidores.

## Asignación de la organización

Si desea definir la asignación entre las entradas LDAP y las entidades de Configuration Manager, debe editar el archivo de asignación de la organización. Los valores que coincidan con la distribución del depósito LDAP se deben proporcionar para las diversas claves.

Las entidades del usuario se identifican mediante una clase de objeto que utilizan todas las entidades, así como un atributo cuyo valor debe ser exclusivo en todo el depósito. Se puede proporcionar el formato de presentación de un nombre que afectará a la forma en que los usuarios se mostrarán en la aplicación de gestión y, opcionalmente, se puede definir una entrada del contenedor si las entradas del usuario de una organización utilizan dicha entrada. Los nombres de las claves y sus valores predeterminados son:

```
# Clase de objetos que utilizan todas las entradas del usuario
User/ObjectClass=inetorgperson
# Atributo cuyo valor en las entradas del usuario es exclusivo dentro de
este depósito
User/UniqueIdAttribute=uid
# Contenedor opcional en las entradas de la organización de las entradas
del usuario; borrar la línea si no se utiliza
User/Container=ou=People
# Formato de presentación de un nombre en la aplicación de gestión
User/DisplayNameFormat=sn, givenname
```



Las entidades del rol se identifican mediante una lista de clases de objetos posibles que utilizan, junto con los atributos correspondientes de asignación de nombres. Estas listas tienen el formato <elemento1>, <elemento2>, ..., <elementoN> y se deben alinear. Es decir, las listas deben tener el mismo número de elementos y la clase de objeto nth se debe usar con el atributo de asignación de nombres nth. Dos claves definen la relación entre los roles y los usuarios, así como entre aquéllos y los sistemas. La clave VirtualMemberAttribute debe especificar un atributo cuyos valores se puedan consultar a partir de un usuario o una entrada del sistema; también debe contener todos los DN de los roles a los que pertenezca la entrada. La clave MemberAttribute debe especificar un atributo para el filtro de búsqueda a partir de un usuario o una entrada del sistema; también contiene todos los DN de los roles a los que pertenece el usuario o el sistema. La clave VirtualMemberAttribute puede ser un atributo virtual de clase de servicio, mientras que la clave MemberAttribute debe tener un atributo físico que se pueda utilizar en un filtro. Los nombres de las claves y sus valores predeterminados son:

```
# Lista de clases de objetos para los roles
Role/ObjectClass=nsRoleDefinition
# Lista alineada de atributos correspondientes de asignación de nombres
Role/NamingAttribute=cn
# Atributo físico (utilizable en un filtro) que contenga los DN de los roles
de un usuario/sistema
Role/MemberAttribute=nsRoleDN
# Atributo cuya consulta sobre un usuario o sistema devuelve los DN de los
roles a los que pertenece
Role/VirtualMemberAttribute=nsRole
```

Las entidades de la organización se identifican de forma similar a los roles, con dos listas alineadas de clases de objetos y atributos correspondientes de la asignación de nombres. Los nombres de las claves y sus valores predeterminados son:

```
# Lista de clases de objetos para las organizaciones
Organization/ObjectClass=organization
# Lista alineada de atributos correspondientes de asignación de nombres
Organization/NamingAttribute=o
```

Las entidades de dominio se identifican de manera similar a la entidad de la organización. Los nombres de las claves y sus valores predeterminados son:

```
# Lista de clases de objetos para los dominios
Domain/ObjectClass=ipNetwork
# Lista alineada de atributos correspondientes de asignación de nombres
Domain/NamingAttribute=cn
```

Las entidades de los sistemas se identifican de manera similar a las entidades del usuario. Los nombres de las claves y sus valores predeterminados son:

```
# Clase de objetos que utilizan todas las entradas del sistema
Host/ObjectClass=ipHost
# Atributo cuyo valor en las entradas del sistema es exclusivo dentro de este
depósito
Host/UniqueIdAttribute=cn
# Contenedor opcional en las entradas del dominio de las entradas del
sistema; borrar la línea si no se utiliza
Host/Container=ou=Hosts
```

## Asignación de los perfiles del usuario

Si desea definir la asignación entre los atributos de las entradas del usuario LDAP y los atributos de las entidades del usuario de Configuration Manager, debe editar el archivo de asignación del Perfil del usuario. Cada clave se corresponde con un atributo del usuario de Configuration Manager. Se puede asignar una clave como valor al nombre de un atributo en una entrada del usuario, como la identifica la asignación de la organización. Los atributos que se utilizan en la configuración de User/DisplayNameFormat se deben proporcionar en la asignación del Perfil del usuario. Los nombres de las claves y sus valores predeterminados son:

```
# inetOrgPerson.givenName
org.openoffice.UserProfile/Data/givenname = givenname
# person.sn
org.openoffice.UserProfile/Data/sn = sn
# inetOrgPerson.initials
org.openoffice.UserProfile/Data/initials = initials
# organizationalPerson.street
org.openoffice.UserProfile/Data/street =
street,postalAddress,streetAddress
# organizationalPerson.l (city)
org.openoffice.UserProfile/Data/l = l
# organizationalPerson.st (state)
org.openoffice.UserProfile/Data/st = st
# organizationalPerson.postalCode
org.openoffice.UserProfile/Data/postalcode = postalcode
# country.c (country)
org.openoffice.UserProfile/Data/c =
# organizationalPerson.o (company)
org.openoffice.UserProfile/Data/o = o,organizationName
# deprecated -- no LDAP corollary
org.openoffice.UserProfile/Data/position =
# organizationalPerson.title
org.openoffice.UserProfile/Data/title = title
# inetOrgPerson.homePhone
org.openoffice.UserProfile/Data/homephone = homephone
# organizationalPerson.telephoneNumber
org.openoffice.UserProfile/Data/telephonenumber = telephonenumber
# organizationalPerson.facsimileTelephoneNumber
org.openoffice.UserProfile/Data/facsimiletelephonenumber =
facsimiletelephonenumber,officeFax
# inetOrgPerson.mail
org.openoffice.UserProfile/Data/mail = mail
```

## Desarrollo

Después de haber personalizado los archivos de asignación para reflejar el estado del depósito LDAP, se puede proceder al desarrollo. Si el esquema del servidor LDAP ya contiene las clases de objetos y los atributos solicitados, la secuencia de órdenes `createServiceTree` se puede ejecutar directamente; de lo contrario se debe ejecutar la secuencia `deployApoc`.

La secuencia `deployApoc` está destinada a los servidores Sun Java System Directory Servers. Copia el archivo de ampliación del esquema proporcionado en el directorio adecuado y pasa al servidor LDAP; se debe invocar, a continuación, la secuencia de órdenes `createServiceTree`. Se debe ejecutar como usuario con los permisos para copiar archivos en el depósito del esquema y reiniciar el servidor; se invoca mediante:

```
./deployApoc <directorio servidor directorio>
```

El parámetro `<directorio servidor directorio>` debe ser la ruta al subdirectorio `slapd-<nombre servidor>` en una instalación del servidor de directorios. Suponiendo que la instalación utilice los directorios predeterminados y que el servidor se denomine `miservidor.midominio`, ese directorio sería `/var/Sun/mps/slapd-miservidor.midominio`.

La secuencia de órdenes `createServiceTree`, si se invoca directamente o a partir de la secuencia `deployApoc`, indicará al usuario la ubicación del servidor LDAP (nombre del sistema, número de puerto y DN básico) y la definición de un usuario con derechos administrativos (DN completo y contraseña). La secuencia crea, después, un árbol de servicio de la rutina de carga en el servidor LDAP y almacena los archivos de asignación en él. Se puede ejecutar como cualquier usuario y se invoca mediante:

```
./createServiceTree
```

Después, al usuario se le solicita:

- Nombre del sistema (predeterminado: localhost): nombre del sistema del servidor LDAP
- Número del puerto (predeterminado: 389): número del puerto del servidor LDAP
- DN: básico: DN básico del depósito LDAP
- DN del usuario (predeterminado: cn=Directory Manager): DN completo de un usuario con suficientes permisos para crear nuevas entradas bajo el DN básico
- Contraseña: contraseña de ese usuario

Una entrada cuyo DN sea:

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

se crea y se llena con el contenido de los dos archivos de asignación.

Como se ha mencionado anteriormente, las operaciones llevadas a cabo por la secuencia de órdenes `deployApoc` presuponen un servidor LDAP cuyo procedimiento de ampliación del esquema, distribución y directorios de instalación coincida en gran medida con el de Sun Java System Directory Server. Otros directorios necesitan una ampliación manual del esquema antes de poder ejecutar la secuencia `createServiceTree`. Si desea más información respecto del uso de OpenLDAP y ActiveDirectory, consulte el apéndice Apéndice C.

El árbol creado, que coincide con el que mantendrá los datos de configuración asociados con las entidades, se alinea con la estructura de los árboles utilizados para la gestión del servicio en Sun Java System Identity Server.

## Consideraciones adicionales

La estructura de Configuration Manager exige la creación de una conexión con un servidor LDAP, con permisos de lectura y de búsqueda, con el fin de identificar qué DN completo se asocia con un usuario concreto o identificador del sistema que provenga del escritorio. En consecuencia, el depósito se debe configurar para permitir conexiones anónimas o se debe crear para tal fin un usuario especial con acceso de lectura y búsqueda.

La aplicación de gestión crea árboles de servicio bajo las entradas asignadas en las entidades, para mantener los datos de la configuración de estas entidades. Por lo tanto, las entradas del usuario utilizadas para la gestión deben tener derechos para crear subentradas bajo las entradas que están gestionando.

La autenticación de los usuarios de la estructura de los clientes del escritorio se puede efectuar con dos métodos denominados Anonymous y GSSAPI. El primero necesita que se habilite el acceso anónimo para lectura y búsqueda en todo el depósito, puesto que los clientes del escritorio no proporcionarán credenciales cuando intenten recuperar datos del servidor LDAP. Si desea utilizar el método GSSAPI (con el uso de Kerberos para la autenticación), el servidor LDAP se debe configurar como se describe en el capítulo "Implementing Security" de la guía "Sun Java System Directory Server Administration Guide".

## Sun™ Web Console

---

Sun Web Console se ha diseñado para producir una solución de gestión del sistema basada en la web para Sun Microsystems. Se utiliza como ubicación donde los usuarios pueden acceder a las aplicaciones de la gestión del sistema, las cuales proporcionan una interfaz coherente para el usuario.

La consola se basa en un modelo de web por muchos motivos. No obstante, el principal es facilitar a los administradores del sistema el uso de un navegador de web para el acceso a las aplicaciones de gestión del sistema.

Sun Web Console proporciona:

- Autorización y autenticación habituales
- Registro común
- Un único punto de entrada para todas las aplicaciones de gestión del sistema a través del mismo puerto, basado en HTTPS.
- Un aspecto familiar

Una de las ventajas principales de la consola es que el administrador puede iniciar la sesión una vez y utilizar cualquier aplicación dentro de la consola.

## Requisitos del sistema

Sun Web Console admite varios sistemas operativos del cliente y del servidor, así como diferentes navegadores.

### Cliente

- Netscape™ 4.7x, 6.2x y 7.x en Solaris 8 o una versión superior
- Netscape 4.7x, 6.2x y 7.x en Windows 98, 98 SE, ME, 2000 y XP
- Internet Explorer 5.x y 6.x en Windows 98, 98 SE, ME, 2000 y XP
- Mozilla en Linux y Solaris

## Servidor

- Solaris 8 o superior
- Redhat 8 o superior, Redhat Enterprise Linux 2.1
- SuSE Linux 2.1 o superior
- J2SE™ Version 1.4.1\_03 o superior
- Si se detecta J2SE 1.4.1 o una versión anterior en el servidor, el programa de configuración indica la necesidad de modernizar la instalación mediante la versión J2SE del CD de Java Desktop System Management Tools.
- Tomcat: 4.0.3 o superior

Tomcat se incluye en el CD de Java Desktop System Management Tools.

## Instalación de Sun Web Console

Antes de instalar Sun Web Console, lea las secciones de resumen del paquete y problemas conocidos en el apéndice A de esta guía.

Los binarios de instalación de Sun Web Console para los sistemas operativos Solaris SPARC® (versión 8 o superior) y Linux están disponibles en el CD de Java Desktop System Management Tools.

Para instalar Sun Web Console:

1. En el CD de Java Desktop System Management Tools, sitúese en el directorio de Sun Web Console que corresponda al sistema operativo donde desee instalar la consola.

En los sistemas Linux, sitúese en `/linux/swc` y en Solaris SPARC cambie a `/solsparc/swc`.

2. Escriba `./setup`

De manera predeterminada, Sun Web Console no crea un archivo de registro de la instalación. Si desea crear un registro de la instalación con el nombre "logfile", escriba `./setup | tee logfile`

**Nota:** la mayor parte de la instalación y configuración de la consola web se efectúa automáticamente al ejecutar la configuración. Si desea información más detallada sobre la aplicación de configuración de Sun Web Console, consulte el apéndice A.

3. Si desea adaptar el entorno nacional de Sun Web Console, necesita instalar dos paquetes adicionales para cada idioma. Use la tabla siguiente para determinar el nombre del paquete del idioma y siga uno de estos procedimientos:

- En Solaris, escriba `pkgadd -d path/pkgname.pkg pkgname`, donde `pkgname` es el nombre del paquete del idioma que desea añadir.
- En Linux, escriba `rpm -i path/pkgname<...>.rpm`, donde `pkgname` es el nombre del paquete que desea añadir.

Nombre del paquete	Descripción
SUNWcmcon, SUNWcmctg	Sun™ Web Console 2.0 para el idioma chino simplificado
SUNWdmcon, SUNWdmctg	Sun™ Web Console 2.0 para el idioma alemán
SUNWemcon, SUNWemctg	Sun™ Web Console 2.0 para el idioma español
SUNWfmcon, SUNWfmctg	Sun™ Web Console 2.0 para el idioma francés
SUNWhmcon, SUNWhmctg	Sun™ Web Console 2.0 para el idioma chino tradicional
SUNWimcon, SUNWimctg	Sun™ Web Console 2.0 para el idioma italiano
SUNWjmcon, SUNWjmctg	Sun™ Web Console 2.0 para el idioma japonés
SUNWkmcon, SUNWkmctg	Sun™ Web Console 2.0 para el idioma coreano
SUNWsmcon, SUNWsmctg	Sun™ Web Console 2.0 para el idioma sueco

## Ejecución de la consola

Normalmente sólo es necesario detener y reiniciar el servidor de Sun Web Console cuando se desee registrar una nueva aplicación.

Antes de iniciar Sun Web Console por primera vez, asegúrese de que se haya completado la instalación de Configuration Manager.

- Si desea iniciar Sun Web Console, escriba `smcwebserver start`.
- Si desea detener Sun Web Console, escriba `smcwebserver stop`.
- Si desea acceder a Sun Web Console, escriba el URL siguiente en el navegador:  
`https://<nombre_sistema>.<nombre_dominio>:6789`

Desde el primer momento, Sun Web Console admite la autenticación basada en Unix y el Control de acceso basado en rol (RBAC). No obstante, también puede configurar otros mecanismos de autenticación como LDAP.

**Nota:** el tiempo de espera predeterminado para la sesión es de 15 minutos. Puede configurar la duración del tiempo de espera con la orden `smreg`. Por ejemplo, para configurar la duración del tiempo de espera en 5 minutos, escriba `smreg add -p -c session.timeout.value=5`.

Si desea más información sobre las órdenes para Sun Web Console, consulte las páginas de comando `man smcwebserver` y `smreg`.

## Desinstalación de Sun Web Console

Si desea desinstalar Sun Web Console, ejecute `/usr/lib/webconsole/setup -u`.

**Nota:** no ejecute esta orden si se encuentra en el directorio `/usr/lib/webconsole` o en cualquiera de los subdirectorios relacionados; de lo contrario `pkgrm` fallará.

# Información sobre el puerto de Sun Web Console

Configuration Manager usa los puertos de Sun Web Console:

- 8005 para cerrar el servicio
- 6789 para conseguir acceso a documentos http.

Ambos puertos se pueden cambiar en `/etc/opt/webconsole/server.xml`. Después de cambiarlos, reinicie Sun Web Console con `/usr/sbin/smcwebserver restart`.



# Sun Java™ Desktop System Configuration Manager

---

Configuration Manager proporciona una herramienta de administración que se ejecuta en Sun Web Console. Esta interfaz del usuario basada en la web permite que un administrador recorra la jerarquía de una organización con el fin de definir normas para las aplicaciones del escritorio. Estas normas se pueden definir para cada elemento de la jerarquía, por ejemplo para organizaciones, roles, usuarios, dominios y sistemas. Configuration Manager usa varias plantillas de configuración para mostrar los valores específicos de diversas aplicaciones del escritorio como Gnome, Mozilla, StarOffice y Evolution.

## Instalación de Configuration Manager

Antes de instalar Configuration Manager, necesita una instalación de trabajo de Sun Web Console.

1. Sitúese en el directorio correspondiente de Configuration Manager en el CD de Java Desktop System Management Tools.

En los sistemas Linux, sitúese en `/linux/apoc`. En Solaris SPARC, sitúese en `/solsparc/apoc`.

2. Escriba `./setup`.
3. Escriba el nombre del sistema del servidor LDAP.  
El nombre predeterminado es `localhost`.
4. Escriba el número del puerto del servidor LDAP (predeterminado: 389).
5. Escriba el DN básico del depósito LDAP.
6. Escriba el nombre de la clase de objetos que se utiliza para identificar las entidades del usuario. La clase de objetos predeterminada es `inetorgperson`.

Si desea más información, consulte la sección Asignación de la organización en el capítulo Servidor LDAP.

7. Escriba el nombre de un atributo que sea exclusivo en todo el depósito LDAP. El atributo predeterminado es `uid`.

Si desea más información, consulte la sección Asignación de la organización en el capítulo Servidor LDAP.

8. Escriba el DN completo de un usuario que tenga derechos de acceso necesarios para efectuar consultas en el servidor LDAP.

Utilice cualquier DN que tenga acceso de lectura y búsqueda. Si desea un acceso anónimo, deje este campo en blanco.

9. Escriba una contraseña para el usuario a quien asignó los derechos de acceso LDAP.

Si configura un acceso anónimo al servidor LDAP, obvie este paso.

Durante la instalación se añade un módulo adicional de inicio de sesión a Sun Web Console que permite autenticar los usuarios a través de LDAP.

Al final de la instalación Sun Web Console se reinicia automáticamente; de esta manera se puede acceder a Configuration Manager.

**Nota:** puede modificar la configuración anterior de Configuration Manager en cualquier momento mediante la secuencia de órdenes `/usr/share/webconsole/apoc/configure`. Por ejemplo, puede utilizar ésta para situarse en un servidor LDAP diferente sin reinstalar Configuration Manager.

## Ejecución de Configuration Manager

1. Si desea acceder a Configuration Manager, escriba el URL siguiente en el navegador:

```
https://<nombre:sistema>.<nombre_dominio>:6789
```

2. Escriba en el indicador el nombre del usuario (uid) y la contraseña de un usuario LDAP.

Se abre Sun Web Console.

3. En la ventana de la consola, haga clic en **Sun Java™ Desktop System Configuration Manager**.

**Nota:** si no desea ver la página de inicio de Sun Web Console y prefiere ir directamente a Configuration Manager, escriba el URL siguiente en el navegador:

```
https://<nombre_sistema>.<nombre_dominio>:6789/apoc
```

## Desinstalación de Configuration Manager

Si desea desinstalar Configuration Manager de Sun Web Console, sitúese en el directorio correspondiente de Configuration Manager en el CD de Java Desktop System Management Tools y después ejecute `./setup -u`.

**Nota:** si desinstala Configuration Manager, el módulo de inicio de sesión LDAP se borra de Sun Web Console.

## Componentes del escritorio

---

Si desea acceder a los datos de configuración desde Configuration Manager, un cliente del escritorio necesita Sun Java™ Desktop System Configuration Agent. Configuration Agent se comunica con el depósito remoto de datos de configuración y los adaptadores e integra los datos en sistemas específicos de configuración; en la actualidad se admiten GConf, Mozilla Preferences y StarOffice Registry.

Todos estos componentes se incluyen e instalan como parte de Java Desktop System.

## Acceso a los datos/autenticación del usuario

Configuration Agent recupera información del servidor LDAP basada en el ID del inicio de sesión de un usuario del escritorio. El valor User/UniqueIdAttribute del archivo de asignación de la organización asigna el identificador del inicio de sesión a una entidad del usuario en el servidor LDAP. Configuration Agent también recupera la información sobre el sistema, como el nombre o la dirección IP del sistema. Esta información se asigna a una entidad de sistemas en el servidor LDAP a través del valor Host/UniqueIdAttribute del archivo de asignación de la organización.

Hay dos métodos para acceder al servidor LDAP, Anonymous o GSSAPI. Si desea un acceso anónimo no es necesaria ninguna acción en el escritorio. Con respecto al método GSSAPI, las credenciales de Kerberos se deben conseguir en el escritorio. Si desea integrar la adquisición de credenciales de Kerberos en el inicio de sesión del usuario, se debe instalar y configurar el módulo pam\_krb5 en la máquina de Java Desktop System. Puede encontrar configuraciones de ejemplo para el módulo pam en el directorio /usr/share/doc/packages/pam\_krb5/README. SuSE del CD de Java Desktop System. También puede utilizar gdm para integrar Kerberos en el inicio de sesión del usuario, por ejemplo, mediante el uso del archivo de /etc/pam.d/gdm siguiente:

```
##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 forma parte del paquete apoc. Cuando instale el RPM correspondiente, los archivos necesarios para esta API se instalan y registran con inetd. Puede instalar manualmente el RPM o mediante la instalación de Java Desktop System.

## Información sobre la rutina de carga

Si desea acceder a los datos para la configuración remota, se debe proporcionar Configuration Agent con la ubicación del servidor LDAP. Puede añadir esta ubicación mediante la herramienta de configuración YaST2, autoYaST o editando manualmente el archivo de propiedades `policymgr.properties` en el directorio `/opt/apoc/lib`. En YaST2 puede añadir estos datos en la sección Red/Avanzado.

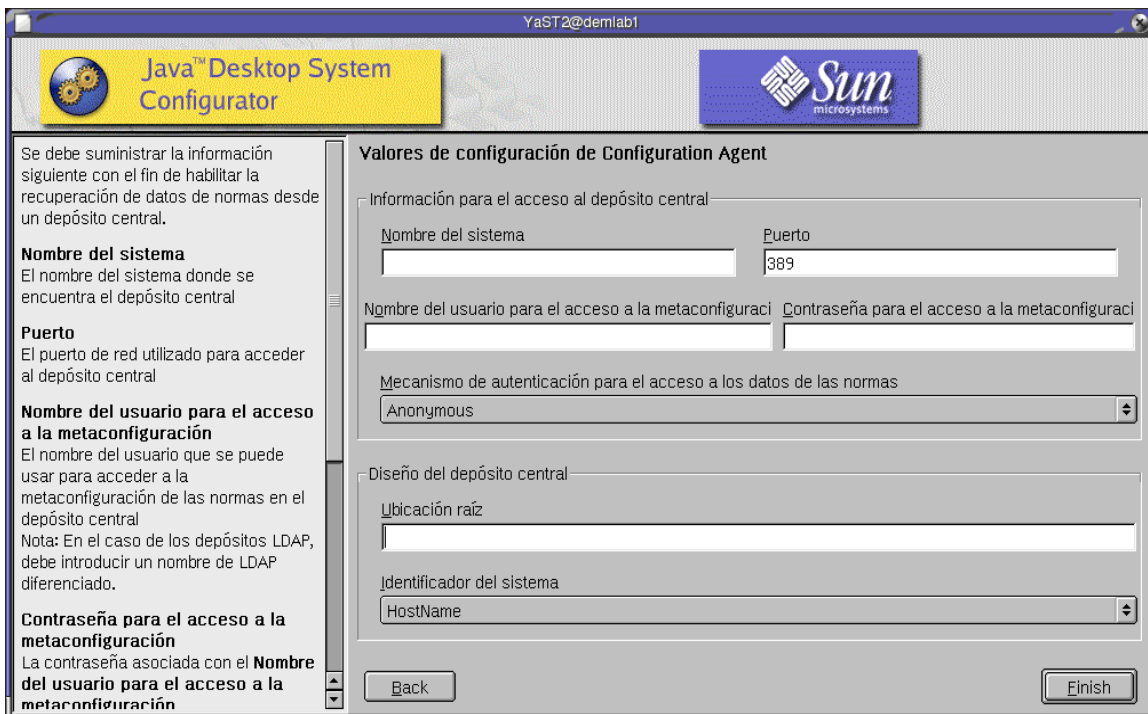


Figura 1 Java Desktop System Configurator en YaST

Se necesita la información siguiente para ejecutar Configuration Agent:

- Nombre del sistema (Server): nombre del sistema del puerto del servidor
- Puerto (Port): número del puerto del servidor LDAP
- Nombre del usuario para el acceso a los metadatos (AuthDn): DN completo de un usuario con derechos de acceso de búsqueda y lectura en el depósito

**Nota:** si se habilita un acceso anónimo al directorio, esta configuración se puede dejar en blanco

- Contraseña de acceso a los metadatos (Password): contraseña de un usuario LDAP registrado

**Nota:** si se habilita un acceso anónimo al directorio, esta configuración se puede dejar en blanco.

- Mecanismo de autenticación para el acceso a los datos de las normas (AuthType): puede ser anónimo o GSSAPI, según cómo autentique el servidor LDAP a los usuarios

- Ubicación de la raíz (BaseDn): DN básico del depósito LDAP
- Identificador del sistema (HostIdentifier): puede ser HostName o IPAddress y se debe configurar para que coincida con el contenido del atributo LDAP que se utiliza para identificar sistemas. Este atributo se define en los archivos de asignación como Host/UniqueIdAttribute
- Tiempo de espera de la conexión (Connect Timeout): indica los segundos tras los que expirarán los intentos de conexión con el servidor LDAP. El valor predeterminado es 1 segundo.

**Nota:** siempre que cambie estos valores, debe reiniciar Configuration Agent.

Si desea reiniciar Configuration Agent en el escritorio, asegúrese de que no se esté ejecutando ninguna de las aplicaciones relacionadas con el cliente; inicie la sesión como usuario root y escriba la orden /opt/apoc/bin/apocd restart.

## Valores de funcionamiento

Puede configurar los valores de funcionamiento de Configuration Agent de forma local o remota. En el primer caso, edite el archivo `apocd.properties` en el directorio `/opt/apoc/lib`; en el segundo, utilice la norma de Configuration Agent en Configuration Manager. Los valores siguientes se pueden configurar en el archivo de propiedades:

- `DaemonPort`: puerto donde Configuration Agent recibe comunicación de los clientes en el escritorio
- `MaxClientThreads`: número máximo de solicitudes de los clientes que se pueden procesar simultáneamente
- `MaxClientConnections`: número máximo de conexiones de los clientes
- `MaxRequestSize`: tamaño máximo de las solicitudes de los clientes
- `DaemonChangeDetectionInterval`: minutos entre los ciclos de detección de cambios en esta lista de valores de configuración
- `ChangeDetectionInterval`: minutos entre los ciclos de detección de cambios en los datos de configuración del cliente
- `GarbageCollectionInterval`: minutos entre los ciclos de liberación de recursos en la base de datos local de la configuración
- `TimeToLive`: minutos que permanecen en la base de datos local los datos de configuración que no están fuera de línea
- `LogLevel`: nivel de detalles en los archivos de registro del agente

El valor `DaemonPort` sólo se puede modificar localmente y necesita un reinicio del agente para que los cambios surtan efecto. Todos los demás valores entran en vigor en el próximo ciclo de detección de cambios en la configuración del agente. El nivel de registro especificado en `LogLevel` debe ser un valor coherente con los niveles de Java Logger. En orden de gravedad decreciente, estos niveles son: GRAVE, ADVERTENCIA, INFORMACIÓN, CONFIGURACIÓN, BUENO, MEJOR y EL MEJOR.

## Difusión de los cambios en los datos de la configuración

Puede utilizar el valor `ChangeDetectionInterval` que se describe en la sección Valores de funcionamiento para ajustar la difusión de los cambios en los datos de la configuración remota en las aplicaciones de los clientes. El valor que proporcione para esta configuración es la duración máxima en minutos que transcurre antes de que los cambios efectuados de manera remota se reflejen en las aplicaciones del cliente. Los valores menores de `ChangeDetectionInterval` provocan una mayor actividad en Configuration Agent y el servidor LDAP. Por ello debe tener cuidado cuando ajuste el valor de la configuración. Por ejemplo,

en una fase inicial del desarrollo puede ajustar este valor en un minuto, de manera que sea posible comprobar fácilmente el impacto de la configuración remota en las aplicaciones del cliente. Tras completar la comprobación, devuelva a esta configuración el valor inicial.

## Información sobre el puerto de Configuration Agent

El Configuration Agent utiliza dos puertos:

1. El puerto del daemon (el predeterminado es 38900), utilizado por el daemon para comunicarse con aplicaciones clientes.
2. El puerto de administración del daemon (el predeterminado es 38901), utilizado por el controlador del daemon, `apocdctl`, al comunicarse con el daemon.

Cambio del puerto del daemon:

Si desea cambiar el puerto del daemon debe modificar la propiedad, `DaemonPort`, en el archivo `apocd.properties` del daemon y las entradas `/etc/services` y `/etc/inetd.conf`. Después, reinicie el daemon y vuelva a cargar `inetd`.

Cambio del puerto de administración del daemon:

Si desea cambiar el puerto de administración del daemon, debe modificar la propiedad `DaemonAdminPort` en el archivo de propiedades `apocd.properties` del daemon. Después, reinicie el daemon.

## Adaptador de GConf

El adaptador de GConf es parte del paquete `apoc-adapter-gconf`. Cuando se instala el adaptador desde el RPM correspondiente, la ruta de las fuentes de datos de GConf en `/etc/gconf/2/` se actualiza para incluir las fuentes de Configuration Manager. Se almacena una copia de seguridad de la vieja ruta en `/etc/gconf/2/path.apocBackup`. Si ésta se refiere a fuentes de datos personalizadas, es necesario actualizarla fusionando los cambios de la ruta predeterminada con la ruta del gestor recién instalado. Las dos fuentes de datos proporcionadas por el adaptador son:

- “`apoc:readonly:`”: proporciona acceso a los valores no protegidos de las normas. Inserte esta fuente de datos después de los valores del usuario y antes de los valores predeterminados locales.
- “`apoc:readonly:mandatory@:`”: proporciona acceso a los valores protegidos de las normas. Inserte esta fuente de datos después de los valores obligatorios locales y antes de los valores del usuario.

## Adaptador de Mozilla

El adaptador de Mozilla es parte del paquete `mozilla-apoc-integration`. Cuando se instala el adaptador desde el RPM correspondiente, los archivos necesarios se añaden a una instalación existente de Mozilla y se registran automáticamente.

# Adaptador de StarOffice

El adaptador de StarOffice se incluye en una instalación estándar de StarOffice y permite el acceso a los datos de configuración de las normas sin modificaciones especiales.





## Apéndice A – Sun Web Console

---

### Problemas conocidos

#### Seguridad

Es posible que una sesión quede activa debido a ciertas acciones del usuario, sin que éste se aperciba de ello. Por ejemplo, si un usuario cierra una ventana del navegador no se termina la sesión de Sun Web Console automáticamente. Es decir, un usuario debe terminar explícitamente la sesión en Sun Web Console antes de cerrar las ventanas de una aplicación.

### Sintaxis de la secuencia de órdenes de configuración

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

-h = imprime la instrucción de la sintaxis

-n = no inicia el servidor al final de la instalación

-u = desinstala Sun Web Console

-f = desinstala Tomcat y Java 1.4 si estos paquetes se instalaron con alguna aplicación de configuración. Sólo puede utilizar este parámetro junto con el parámetro -u.

Si desea una descripción completa de los parámetros de configuración disponibles, ejecute `setup -h`.

Si desea desinstalar Sun Web Console, ejecute `/usr/lib/webconsole/setup -u`

**Nota:** no ejecute esta orden si se encuentra en el directorio `/usr/lib/webconsole` o en cualquiera de los subdirectorios relacionados; de lo contrario `pkgrm` falla.

# Paquetes de Sun Web Console

## Paquetes de Solaris

Nombre del paquete	Descripción
SUNWmctag	Biblioteca de etiquetas de la interfaz de Sun Web Console
SUNWmcon	Sun Web Console
SUNWmcos	Servicios habituales de Solaris para Sun Web Console
SUNWmcosx	Servicios específicos de la versión de Solaris para Sun Web Console
SUNWmconr	Raíz de Sun Web Console
SUNWjato	Tiempo de ejecución de Sun One Application Framework
SUNWtcatu	Tomcat

## RPM de Linux

Nombre del paquete	Descripción
SUNWmctag	Biblioteca de etiquetas de la interfaz de Sun Web Console
SUNWmcon	Sun Web Console
SUNWmcos	Servicios habituales de Linux para Sun Web Console
SUNWmcosx	Servicios específicos de la versión de Linux para Sun Web Console
SUNWmconr	Raíz de Sun Web Console
SUNWjato	Tiempo de ejecución de Sun One Application Framework
tomcat4	Tomcat

## Apéndice B – Configuration Manager

---

### Paquetes de Configuration Manager

#### Paquetes de Solaris

Nombre del paquete	Descripción
SUNWapm	Configuration Manager
SUNWapmca	Plantillas de Configuration Agent
SUNWapmev	Plantillas de Evolution
SUNWapmgo	Plantillas de Gnome
SUNWapmmo	Plantillas de Mozilla
SUNWapmso	Plantillas de StarOffice

#### PM de Linux

Nombre del paquete	Descripción
apoc-manager	Configuration Manager
apoc-agent-templates	Plantillas de Configuration Agent
apoc-evolution-templates	Plantillas de Evolution
apoc-gnome-templates	Plantillas de Gnome
apoc-mozilla-templates	Plantillas de Mozilla
apoc-staroffice-templates	Plantillas de StarOffice



## Apéndice C

---

### Uso de un servidor OpenLDAP con Configuration Manager

Si desea usar un servidor OpenLDAP como depósito de los datos de Configuration Manager, el esquema de los datos se debe ampliar para abarcar las clases de objetos y los atributos utilizados para almacenar los datos de configuración. Se puede encontrar un archivo de esquema personalizado llamado `apoc.schema` en el subdirectorio `openldap` de la herramienta de desarrollo Configuration Manager proporcionada en el CD de Java Desktop System Management Tools.

Este archivo se debe copiar en el subdirectorio `schema` del directorio de configuración de OpenLDAP (`/etc/openldap`) y añadir al esquema OpenLDAP incluyéndolo en el archivo `slapd.conf` ubicado en ese directorio. Para conseguirlo se debe insertar la línea `/etc/openldap/schema/apoc.schema` al final de la secuencia del esquema del archivo. Si desea más información sobre la ampliación del esquema de un servidor OpenLDAP, consulte el manual del servidor.

Con el fin de preparar la base de datos de OpenLDAP para almacenar los datos de la configuración, se debe usar la herramienta de desarrollo Configuration Manager. Una vez ampliado el esquema en el paso previo de la instalación, sólo es necesario ejecutar la secuencia `createServiceTree` que se debe iniciar desde el directorio de la herramienta de desarrollo como cualquier usuario, mediante la orden siguiente: `./createServiceTree`. La secuencia indica al usuario la información sobre la base de datos OpenLDAP como se explica en la sección de la herramienta de desarrollo de este documento. Se proporciona un archivo de asignación predeterminado que utiliza atributos y clases de objetos habituales presentes en OpenLDAP en el subdirectorio `openldap` de la herramienta de desarrollo. El archivo recibe el nombre de `OrganisationalMapping` y se puede implementar copiándolo sobre el archivo con el mismo nombre del directorio principal de la herramienta de desarrollo antes de lanzar `createServiceTree`.

Tenga en cuenta que el agente de Configuration Manager intentará la conexión con el servidor OpenLDAP de manera anónima, proporcionando el DN del usuario para el que solicita los datos, pero no la contraseña. Este método de autenticación anónima puede que esté inhabilitado de manera predeterminada en algunas versiones de servidores de OpenLDAP, en cuyo caso se debe habilitar; para ello añada la línea `bind_anon_cred` en los parámetros comunes del servidor en el archivo `slapd.conf` situado en el directorio de configuración de OpenLDAP (`/etc/openldap`). Si desea más información sobre este parámetro, consulte el manual del servidor.

# Uso de un servidor Active Directory con Configuration Manager

Si desea usar un servidor Active Directory como depósito de los datos de Configuration Manager, el esquema de los datos se debe ampliar para abarcar las clases de objetos y los atributos utilizados para almacenar los datos de configuración. Se puede encontrar un archivo de ampliación de esquema llamado `apoc-ad.ldf` en el subdirectorio `ad` de la herramienta de desarrollo Configuration Manager proporcionada en el CD de Management Tools. Para obtener más información, consulte la sección de la herramienta de desarrollo.

El archivo `apoc-ad.ldf` se debe importar al esquema de Active Directory mediante los pasos siguientes:

1. Habilite las extensiones del esquema. Consulte la documentación de Active Directory si desea más información sobre cómo llevar a cabo esta operación.
2. Ejecute la orden siguiente desde el indicador de órdenes: `ldifde -i -c "DC=Sun,DC=COM" <Base DN> -f apoc-ad-registry.ldf.`

**Nota:** sustituya `<Base DN>` por el DN básico de Active Directory.

Se debe usar la herramienta de desarrollo con el fin de preparar el servidor Active Directory para que almacene los datos de la configuración. Una vez ampliado el esquema en el paso previo de la instalación, sólo es necesario ejecutar la secuencia `createServiceTree` que se debe iniciar desde el directorio de la herramienta de desarrollo como cualquier usuario, mediante la orden siguiente: `./createServiceTree`. La secuencia indica al usuario la información sobre la base de datos de Active Directory. Se proporciona un archivo de asignación predeterminado que utiliza atributos y clases de objetos habituales presentes en Active Directory en el subdirectorio `ad` del directorio de la herramienta de desarrollo. Este archivo recibe el nombre de `OrganizationalMapping` y se puede implementar copiándolo sobre el archivo con el mismo nombre del directorio principal de la herramienta de desarrollo antes de lanzar `createServiceTree`.

A partir de este momento, el servidor Active Directory se podrá usar con Configuration Manager. A la hora de instalar Configuration Manager, proporcione el DN completo y la contraseña de un usuario con derechos de lectura respecto del árbol. Puede ser un usuario que no tenga acceso para usar Active Directory con cualquier otro propósito. Consulte la documentación de Active Directory si desea obtener más información sobre cómo configurar dicho usuario. Además, la máquina que ejecute Configuration Manager debe conocer el nombre del dominio de Active Directory. Para ello añada una línea para asignar la dirección IP del servidor Active Directory con su nombre de dominio en el archivo `/etc/hosts` de esa máquina.

Para poder recuperar los datos de la configuración desde un sistema Java Desktop System, éste debe conocer el nombre del dominio de Active Directory. La autenticación del usuario de Java Desktop System se puede hacer de dos modos: de manera anónima y mediante GSSAPI.

- Si desea autenticar las conexiones anónimas, el servidor Active Directory se debe configurar para garantizar los derechos de lectura a todos los usuarios. Consulte la documentación de Active Directory si desea más información sobre cómo llevar a cabo esa operación.
- Si desea autenticar mediante GSSAPI, el archivo `/etc/krb5.conf`, que especifica los parámetros de Kerberos, se debe modificar para definir el ámbito de Active Directory y apuntar al servidor de Active Directory como Centro de distribución de claves (KDC). También se debe especificar, al igual que los tipos de cifrado, los tipos DES compatibles con Active Directory, es

decir, `des-cbc-crc` y `des-cbc-md5`. Consulte la documentación de Kerberos si desea obtener más información sobre cómo llevar a cabo esta operación. Antes de acceder a los datos de configuración, es preciso obtener las credenciales válidas para el usuario que haya iniciado la sesión en Java Desktop System. Lo puede efectuar manualmente ejecutando la orden `kinit` y proporcionando al usuario la contraseña definida en Active Directory. Es posible que otros esquemas generen estas credenciales de manera automática al iniciar la sesión. Consulte la documentación de Java Desktop System si desea obtener más información.