Guía de instalación de Sun Desktop Manager 1.0

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

Referencia: 819–6091–10

060406@14558

Contenido

Prefacio

Este documento explica los pasos de instalación y configuración para poder utilizar Sun™ Desktop Manager 1.0.

Información general

Sun Desktop Manager se ha concebido para facilitar una configuración centralizada de sistemas de sobremesa. Los valores se pueden asignar a varios elementos de una organización o un dominio; de este modo, un administrador controla con eficiencia los grupos de usuarios o sistemas.

Organización de esta guía

El capítulo 1 proporciona una breve descripción de Sun Desktop Manager.

El capítulo 2 aborda la instalación desde el servidor de Sun Desktop Manager.

El capítulo 3 explica cómo instalar Java Desktop System Configuration Agent.

El capítulo 4 brinda información de instalación de Java Web Console.

El apéndice A contiene datos sobre los parámetros de configuración.

El apéndice B trata sobre el uso de OpenLDAP y Active Directory con Desktop Manager.

El apéndice C facilita información sobre la asignación organizativa.

Manuales relacionados

- *Sun Desktop Manager 1.0 Administration Guide*
- *Sun Desktop Manager 1.0 Developer Guide*

Documentación, asistencia y formación

Función de Sun	URL	Descripción
Documentación	`http://www.sun.com/documentation/`	Descargar documentos en PDF y HTML y solicitar documentos impresos
Asistencia y formación	`http://sunsolve.sun.com`	Obtener asistencia técnica, descargar revisiones y obtener información sobre los cursos de Sun

◆ ◆ ◆ CAPÍTULO 1

Información general y conceptos

Este documento explica los pasos necesarios de instalación y configuración para poder utilizar Sun™ Desktop Manager 1.0. Si necesita más información sobre Sun Desktop Manager, consulte el documento *Sun Desktop Manager 1.0 Administration Guide*.

Información general de Sun Desktop Manager

Sun Desktop Manager proporciona una configuración centralizada de sistemas de sobremesa. Los valores se pueden asignar a varios elementos de una organización o un dominio; de este modo, un administrador controla con eficiencia los grupos de usuarios o sistemas.

FIGURA 1–1 Arquitectura de Desktop Manager

Los componentes principales de Desktop Manager son:

- Depósitos de configuración
- Herramientas de administración
- Plantillas de Desktop Manager
- Configuration Agent
- Adaptadores de configuración

Los datos de configuración se almacenan de forma centralizada en depósitos de configuración. Los datos de configuración se controlan (creados/suprimidos/modificados/asignados/sin asignar)

mediante las herramientas de administración, que consisten en una interfaz gráfica de usuario de Desktop Manager por Internet, así como una interfaz de línea de comandos. La herramienta de administración por Internet utiliza las plantillas para generar los datos de configuración en el navegador web.

Configuration Agent recupera datos de configuración del depósito de configuración para las aplicaciones de los usuarios. El agente almacena en la memoria caché la información de configuración que ha recuperado del depósito central.

Las herramientas de administración no están asociadas al agente, lo que significa que sólo funcionan en el depósito de configuración.

Las aplicaciones de usuario, mediante los adaptadores de configuración, consultan los datos de configuración a través de Configuration Agent.

El producto permite recuperar los parámetros de configuración y aplicarlos directamente a los sistemas de configuración siguientes:

- Estructura de configuración de GConf. Gnome
- Registro de StarOffice
- Preferencias de Mozilla
- Preferencias de Java

◆ ◆ ◆ CAPÍTULO 2

Instalación de aplicaciones de administración

Este capítulo proporciona instrucciones sobre cómo instalar los componentes desde el servidor de Sun Desktop Manager.

Sun Desktop Manager

Desktop Manager brinda una herramienta de administración por Internet que se ejecuta en Java Web Console. Esta interfaz de usuario 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. Desktop Manager usa varias plantillas de configuración para mostrar valores que son específicos de distintas aplicaciones de escritorio como Gnome, Mozilla, StarOffice y Evolution.

▼ Instalación

Antes de empezar

Desktop Manager necesita tener instalado Java Web Console versión 2.2.5 o posterior. Compruebe que en el sistema haya una versión válida instalada. Para establecer si se dispone de una versión válida, proceda como superusuario (usuario root) y ejecute:

```
# smcwebserver status
```

Nota – Java Web Console 2.2.4 forma parte del sistema operativo Solaris™ 10; sin embargo, Desktop Manager necesita la versión 2.2.5 o posterior. En el directorio server/console del sistema de archivos de Desktop Manager hay una copia de la versión 2.2.5. Se puede instalar mediante la ejecución de `./setup` en dicho directorio.

Si Java Web Console no está instalado en el sistema o la versión instalada no es válida para Desktop Manager, consulte las instrucciones del Capítulo 4 para instalar por primera vez o actualizar Java Web Console. Acto seguido, vuelva a este capítulo para proseguir la instalación de Desktop Manager.

1. **Descargue el archivo comprimido de Desktop Manager y extraiga el contenido en un directorio temporal**

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

2. **Regístrese como superusuario y ejecute la secuencia de comandos de instalación con**

   ```
   # cd SunDesktopMgr-1.0/<platform>/server/manager
   # ./setup
   ```

3. **Compruebe si hay errores en la salida de la secuencia de comandos de instalación.**

   Si la instalación se ha realizado correctamente, la secuencia de comandos de instalación reinicia Java Web Console de forma automática y mediante un navegador web se puede acceder a Desktop Manager.

▼ Operación

1. **Escriba el URL siguiente en el navegador:**

   ```
   https://<nombresistema>.<nombredominio>:6789
   ```

2. **En la pantalla de inicio de sesión, escriba el nombre de usuario y la contraseña de un usuario UNIX real.**

   Se abre Java Web Console.

3. **En la página de inicio de aplicaciones de la consola, haga clic en el vínculo de Desktop Manager.**

   - **Si desea prescindir de la página de inicio de aplicaciones de la consola y pasar directamente a Desktop Manager, en el navegador especifique el URL siguiente:**

     ```
     https://<nombresistema>.<nombredominio>:6789/apoc
     ```

▼ Desinstalación de Desktop Manager

◗ **Si desea quitar Desktop Manager de Java Web Console, vaya al directorio temporal creado para la instalación, regístrese como superusuario y ejecute**

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

Problemas relacionados con la migración

Desktop Manager es compatible con versiones anteriores de Java Desktop System Configuration Manager (1.0 y 1.1). Ahora bien, es preciso tener en cuenta algunas diferencias.

En las versiones anteriores de Configuration Manager, todos los datos de perfiles se almacenaban en un determinado servidor LDAP. Dicho servidor se configuraba como parte de todo el procedimiento de instalación de Configuration Manager. El proceso también incluía la configuración de un módulo de inicio de sesión de LDAP que encapsulaba la autenticación respecto al servidor LDAP.

En cuanto a Desktop Manager, todos los pasos de la configuración se efectúan mediante un asistente, por lo que ya no es preciso efectuar ningún tipo de configuración durante la instalación. Asimismo, Desktop Manager admite varios depósitos de configuración. De esta manera, puede controlar información sobre normas en distintos servidores LDAP, depósitos basados en archivos, etcétera. Ya no hace falta configurar ningún módulo de inicio de sesión de LDAP.

No ha habido cambios en los esquemas de LDAP de las distintas versiones. Si ya había configurado un servidor LDAP para una versión anterior de Configuration Manager, cuando pase a Desktop Manager no debe realizar ningún cambio. Con ello, puede aprovechar las ventajas de Desktop Manager sin tener que actualizar el cliente (agente de Java Desktop System Configuration Manager1.1) ni el servidor LDAP.

Nota – Antes de instalar Desktop Manager, hay que quitar del sistema cualquier versión anterior de Configuration Manager o instalación de Desktop Manager. Para quitar las instalaciones anteriores, ejecute (como superusuario):

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

Tras haber instalado Desktop Manager, puede crear un depósito de configuración que apunte al servidor LDAP:

▼ Creación de un depósito de configuración

1 Escriba el URL siguiente en el navegador

```
https://<nombresistema>.<nombredominio>:6789
```

2 En la pantalla de inicio de sesión, escriba el nombre de usuario y la contraseña de un usuario UNIX real.

Se abre Java Web Console.

3 En la página de inicio de aplicaciones de la consola, haga clic en el vínculo de Sun Desktop Manager 1.0.

4 Haga clic en el botón Nuevo para iniciar el asistente de depósitos de configuración.

Dicho asistente guía los pasos sucesivos para habilitar un depósito de configuración basado en LDAP.

Precaución – De forma automática, el asistente permite migrar los datos de normas a un formato 2.0 nuevo. Se trata de una migración opcional; es útil sobre todo para mejorar el rendimiento de los agentes de Sun Desktop Manager 1.0 más recientes. Si el entorno debe seguir siendo compatible con los agentes de Java Desktop System Configuration Manager 1.1, NO efectúe esta migración.

Resolución de problemas de Desktop Manager

La instalación no es posible

Síntoma: al finalizar la instalación de Java Web Console, un mensaje indica que se no se puede iniciar porque no hay aplicaciones registradas.

Posibles causas: no se han instalado aplicaciones, incluido Desktop Manager .

Solución: instale Desktop Manager e inicie Java Web Console.

Conexión rechazada

Síntoma: intenta abrir un URL, por ejemplo `http://<` *nombresistema*`>.<`*nombredominio*`>:6789`, pero recibe un mensaje que indica que se ha rechazado la conexión.

Posibles causas: Java Web Console no se ejecuta en el servidor.

Solución: para iniciar Java Web Console, regístrese como superusuario y ejecute los comandos siguientes:

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

No se puede iniciar sesión

Síntoma: la combinación de usuario/contraseña no se acepta en la página de inicio de sesión de Java Web Console.

Posibles causas: no existe la cuenta pertinente de usuario UNIX.

Solución: compruebe que el sistema tenga un nombre de usuario UNIX con un nombre y una contraseña configurados. Si es necesario, cree una cuenta local de usuario UNIX para realizar pruebas.

No hay vínculo de Desktop Manager

Síntoma: la página de listas de aplicaciones de Java Web Console no muestra el vínculo de Sun Desktop Manager .

Posibles causas: el módulo Desktop Manager no está instalado.

Solución: para comprobar que Desktop Manager esté instalado en Java Web Console, regístrese como superusuario y ejecute el comando siguiente:

```
# smreg list -a
```

Si en la lista no aparece la aplicación `com.sun.apoc.manager_<` *versión*>, Desktop Manager se debe instalar de nuevo.

Excepción de invocación de método sobre un objeto nulo, error de Tomcat/Java o página en blanco

Síntoma: Desktop Manager se inicia, pero en pantalla sólo aparece una página en blanco o mensajes de error.

Posibles causas: si el error menciona `NoClassDefFoundError: sun/tools/javac/Main`, significa que Java Web Console utiliza una versión incorrecta de Java.

Solución: para verificar el entorno Java actual de Java Web Console, ejecute `# smreg list -p` y observe la propiedad `java.home`. Dicha propiedad debe apuntar a un inicio de Java correcto, que debe ser un JDK. Si el valor no se ha definido correctamente, ejecute el comando siguiente:

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

Nota – <*JAVA_HOME*> debe apuntar a una instalación válida, por ejemplo una en que `javac` se pueda encontrar en el subdirectorio `bin`.

A continuación, reinicie Java Web Console con el comando siguiente:

```
# smcwebserver restart
```

No se puede conectar a un servidor LDAP SSL

Síntoma: una vez especificada la información del servidor LDAP en el asistente para creación de depósitos, incluida la selección de la casilla Use SSL, al hacer clic en Siguiente se genera un mensaje que indica que no se ha podido contactar con el servidor.

Posibles causas: el número de servidor suministrado es incorrecto, el servidor LDAP no se ha conectado para que escuche las conexiones utilizando SSL en dicho puerto, o en el almacén de claves de Java Web Console faltan los certificados pertinentes.

Solución: en primer lugar, compruebe que el servidor LDAP esté configurado para escuchar las solicitudes de conexión SSL en el puerto especificado en el asistente. Si está correcto, compruebe que la autoridad de certificación o el certificado del servidor LDAP estén en el almacén de claves de Java Web Console, que se ubica en `/etc/opt/webconsole/keystore`. El certificado se puede agregar con el comando `keytool -import -file <certificate file> -keystore /etc/opt/webconsole/keystore`. La contraseña predeterminada del almacén de claves es **`changeit`**. Java Web Console se debe reiniciar para que ese cambio lo pueda detectar Desktop Manager mediante el comando `smcwebserver restart`.

No es posible escribir en el directorio

Síntoma: al crear un componente trasero basado en archivos o híbrido, aparece un mensaje de error “No es posible escribir en el directorio” .

Posibles causas: el usuario sin privilegios de acceso carece de los pertinentes permisos.

Solución: asigne al usuario sin privilegios de acceso los permisos adecuados.

◆ ◆ ◆ CAPÍTULO 3

Componentes del cliente

Para poder acceder a los datos de configuración desde Desktop Manager, un cliente de escritorio necesita Java Desktop System Configuration Agent. Configuration Agent se comunica con el depósito remoto de datos de configuración y con los adaptadores, además de integrar los datos en sistemas de configuración específicos. Los sistemas de configuración actualmente admitidos son Java Preferences, Mozilla Preferences y StarOffice Registry.

El sistema operativo Solaris 10 proporciona una versión de Configuration Agent. Ahora bien, Desktop Manager necesita una versión más actual de dicha herramienta. Esta versión nueva forma parte de la instalación de los componentes del cliente de Desktop Manager y las soluciones asociadas.

Para instalar los componentes del cliente de Desktop Manager:

1. Descargue el archivo comprimido de Desktop Manager y extraiga el contenido en un directorio temporal

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

2. Instale las modificaciones recomendadas.

   Las modificaciones se ubican en el directorio `SunDesktopMgr-1.0/<platform>/client/Patches`. Siga las instrucciones de instalación de cada modificación.

3. Regístrese como superusuario y ejecute la secuencia de comandos de instalación con

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

Configuration Agent

Configuration Agent forma parte de un conjunto de distintos paquetes, enumerados en la tabla siguiente:

Nombre del paquete de Solaris	Descripción
SUNWapbas	Bibliotecas de configuración compartidas
SUNWapmsc	Archivos diversos de Configuration Agent
SUNWapoc	Configuration Agent
SUNWapdc	Asistente de Configuration Agent

Al instalar estos paquetes se instalan los archivos que esta API necesita. Puede instalar los paquetes manualmente o a través de la instalación de Java Desktop System. Después de la instalación debe configurar y habilitar Configuration Agent en el sistema.

Nota – Los paquetes de Configuration Agent se instalan como parte del sistema operativo Solaris al instalar Java Desktop System; sin embargo, Desktop Manager modifica estos archivos durante la instalación para proporcionar el nivel de funcionalidad adecuado.

Para acceder a los datos remotos de la configuración, Configuration Agent requiere alguna información sobre la rutina de carga, como el nombre del sistema y el puerto del servidor LDAP. Esta información se mantiene en un conjunto de archivos de propiedades, como `policymgr.properties` , `apocd.properties` u `os.properties`. Estos archivos están almacenados localmente en el directorio `/etc/apoc`. Los archivos de propiedades se pueden editar manualmente (consulte el Apéndice A) o utilizar el asistente de configuración de Configuration Agent.

El asistente de configuración ofrece una interfaz gráfica de usuario que le guía a través de los ajustes de configuración necesarios para Configuration Agent. A cada página del asistente le corresponde una pantalla de ayuda. Puede iniciar el asistente como superusuario (root) mediante la secuencia de comandos `/usr/bin/apoc-config`.

Nota – El asistente también se puede iniciar sin arrancar la interfaz gráfica. Por ejemplo, ejecute `/usr/bin/apoc-config -nodisplay` para iniciar el asistente en modo consola.

Información sobre la rutina de carga

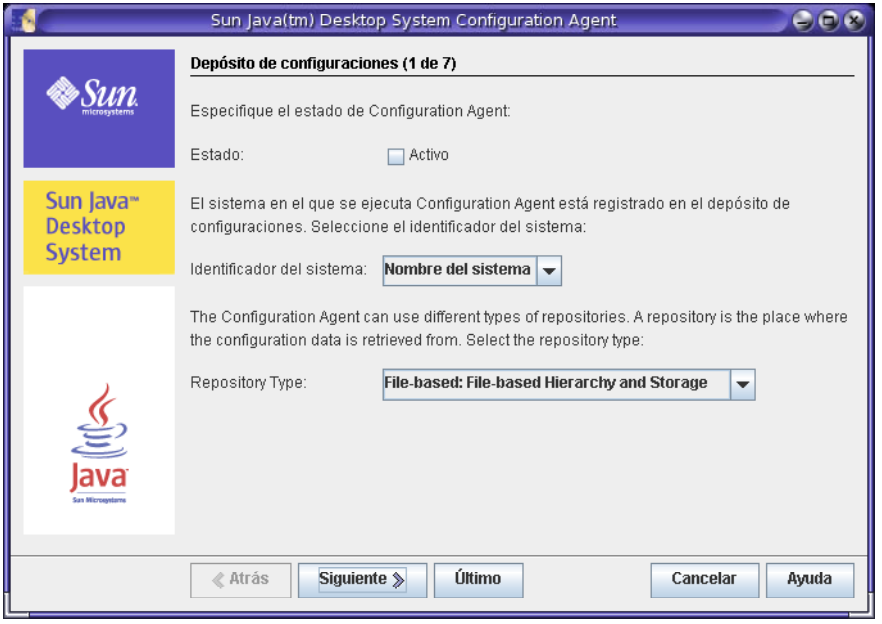

FIGURA 3–1 Depósito de configuración de Configuration Agent

Nota – Las claves asociadas del archivo de propiedad se indican entre paréntesis, cuando corresponda.

- Estado: estado de Configuration Agent. La casilla de verificación se puede utilizar para activar o desactivar Configuration Agent. Para usar el depósito de configuración, Configuration Agent debe estar activo. La activación incluye automáticamente el registro correspondiente con la función de administración de servicios (smf(5)) de Solaris.
- Identificador del sistema: puede ser “Nombre del sistema” o “Dirección”. Cuando se buscan datos relativos a normas propias del sistema, Configuration Agent identifica el sistema activo mediante el nombre del sistema o la dirección IP. Seleccione el valor correcto según cómo se haya identificado el sistema en el tipo de depósito seleccionado.
- Tipo de depósito: este valor sirve para indicar a Configuration Agent si los datos de configuración y jerarquía organizativa se definen en un almacenamiento LDAP, en uno basado en archivos o una combinación de ambos.

Nota – Para habilitar o deshabilitar manualmente Configuration Agent, inicie sesión como **`superusuario`** y escriba el comando `/usr/lib/apoc/apocd enable` o `/usr/lib/apoc/apocd disable`, respectivamente.

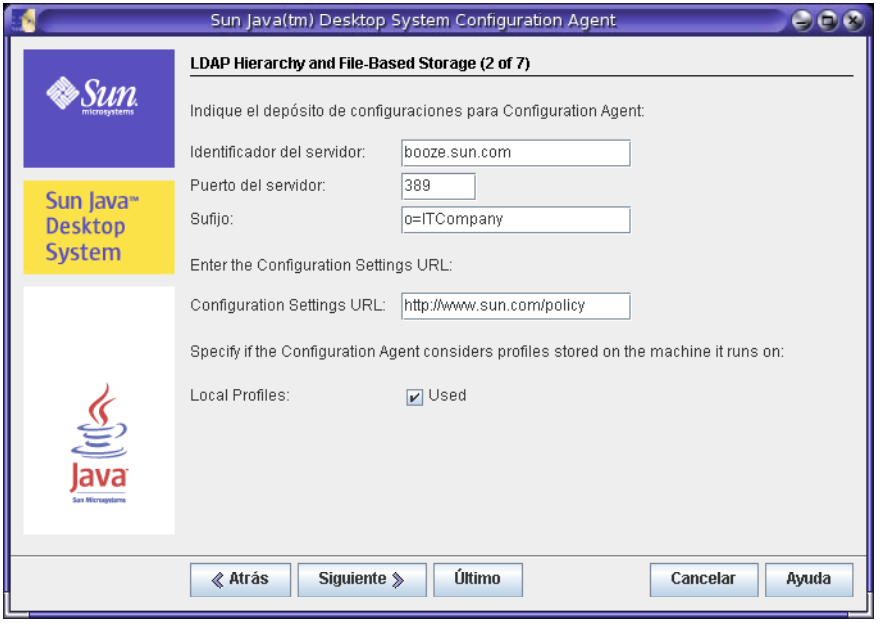

FIGURA 3–2 Configuration Agent, jerarquía LDAP y almacenamiento basado en archivos

---

Nota – La pantalla de la Figura 3–2 varía según el valor de Tipo de depósito que se haya seleccionado en la pantalla anterior. Si elige un tipo de depósito LDAP o Híbrido, debe proporcionar valores para Identificador del servidor, Puerto del servidor y Sufijo. Si para Tipo de depósito elige Basado en archivos o Híbrido, se necesita el URL de valores de configuración.

- Identificador del servidor: nombre del sistema del servidor LDAP.
- Puerto del servidor: número del puerto del servidor LDAP.
- Sufijo: DN base del depósito LDAP.
- URL de valores de configuración: URL que indica la ubicación del depósito basado en archivos.

  Se puede usar una lista de URL para especificar directorios alternativos si no funcionara la conexión con el primero. La lista puede constar de uno o más URL separados por espacios en blanco. Cada URL tiene la forma `archivo://<rutaarchivo>` , `http://<sistema>:<puerto>/<rutaarchivo>` o `https://<sistema>:<puerto>/<rutaarchivo>`. Si necesita más información, consulte el Apéndice A.

Nota – Configuration Agent intenta acceder al servidor LDAP primero mediante una conexión SSL. Si no lo consigue, intenta una conexión SSL normal.

Para que la conexión SSL sea válida, en el almacén de claves de JRE (Java Runtime Environment) debe estar el certificado correspondiente. El almacén de claves se ubica en un JRE estándar en `<installation directory>/lib/security/cacerts`; en el caso de un JDK (Java Development Kit), se encuentra en`<installation directory>/jre/lib/security/cacerts`. La autoridad de certificación o el certificado del servidor LDAP se deben agregar al almacén con el comando `keytool -import -file <certificate file> -keystore <cacerts file location>`. La contraseña predeterminada del almacén de claves es **`changeit`**.

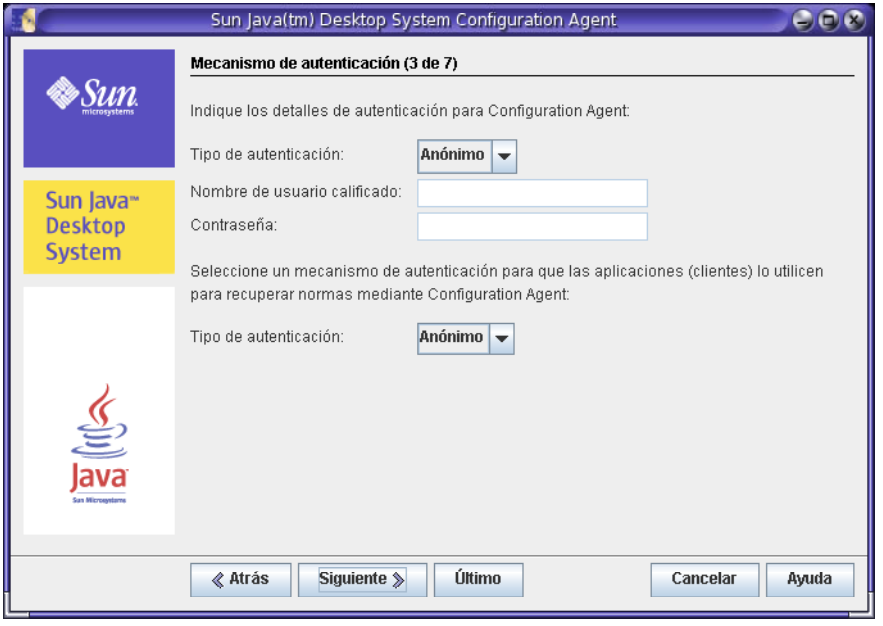

FIGURA 3–3 Mecanismo de autenticación de Configuration Agent

- Tipo de autenticación para Configuration Agent: puede ser "Anónimo" o "Simple". Si se selecciona "Anónimo", los campos Nombre de usuario calificado y Contraseña quedan deshabilitados automáticamente.
- Nombre de usuario calificado: DN completo de un usuario con derechos de acceso de búsqueda y lectura en el depósito.
- Contraseña: contraseña de un usuario LDAP registrado.

Nota – Si el acceso anónimo está habilitado en el directorio, los parámetros Nombre de usuario calificado y Contraseña se pueden dejar en blanco.

- Tipo de autenticación para aplicaciones: puede ser “Anónimo” o “GSSAPI”, según cómo autentique el servidor LDAP a los usuarios.

Nota – Para obtener más información, consulte “Acceso a los datos/autentificación del usuario” en la página 26.

Valores de puertos

Configuration Agent usa dos puertos:

- Puerto del agente: lo usa el agente para comunicarse con las aplicaciones cliente (el predeterminado es **`38900`**).
- Puerto de administración: lo utiliza el programa de control del agente, `apocd`, para comunicarse con el agente (el valor predeterminado es **`38901`**).

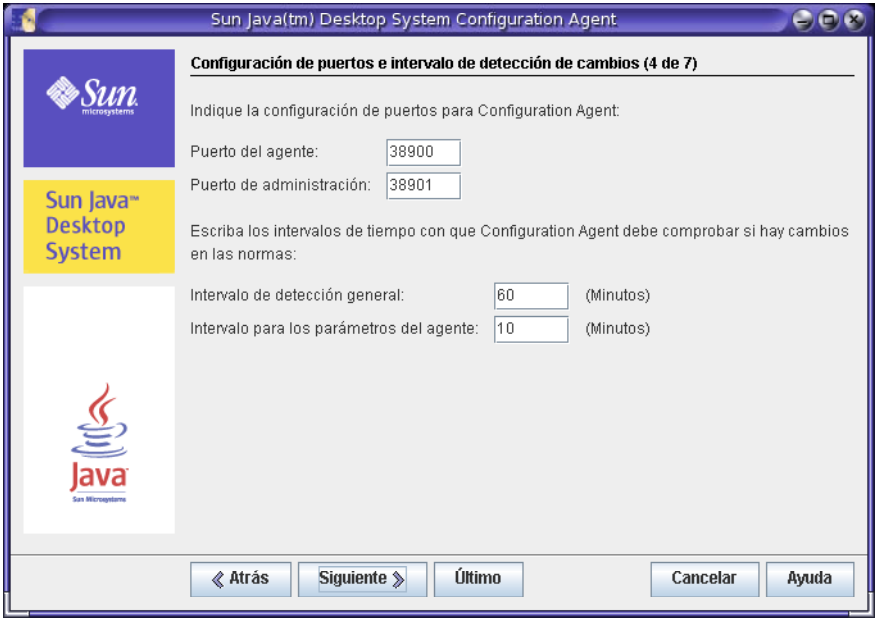

FIGURA 3–4 Valores de puertos de Configuration Agent

Intervalo de detección de cambios

Configuration Agent comprueba periódicamente los posibles cambios en los datos de configuración utilizando dos intervalos:

- Intervalo de detección general: intervalo en minutos entre los ciclos de detección de cambios para los datos de configuración de aplicaciones del escritorio (clientes).

  Nota – Si se especifica **-1** se desactiva la detección de cambios.

- Intervalo para los parámetros del agente: intervalo en minutos entre los ciclos de detección de cambios para los valores de configuración específicos del agente.

  Nota – Si se especifica **-1** se desactiva la detección de cambios.

El intervalo de detección general se puede utilizar para ajustar la propagación remota de cambios en los datos de configuración a aplicaciones del lado del cliente. El valor que proporcione a 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 inferiores producen una mayor actividad en Configuration Agent y en 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, y así comprobar los efectos de la configuración remota en las aplicaciones del cliente. Tras completar la comprobación, devuelva a esta configuración el valor inicial.

Valores de funcionamiento

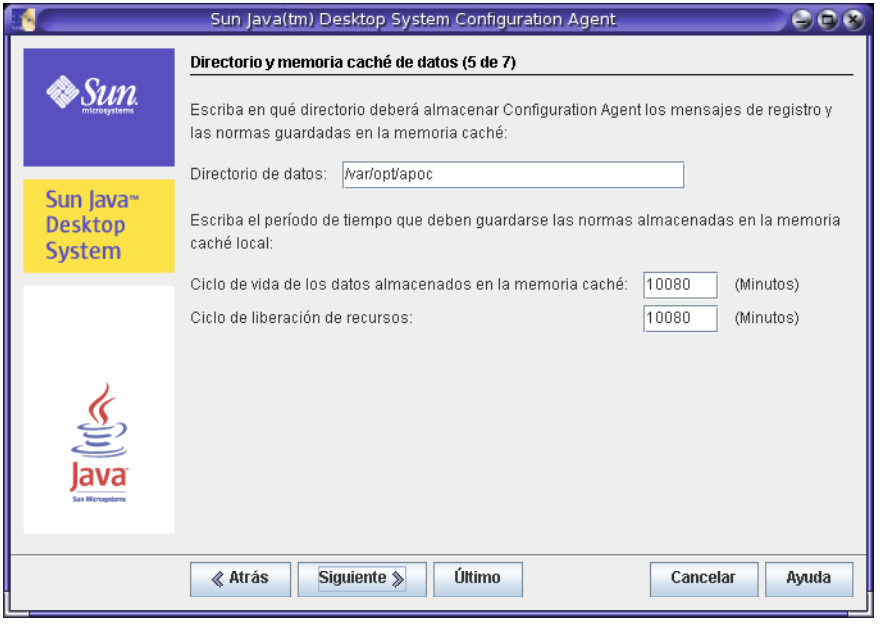

FIGURA 3–5 Directorio de datos de Configuration Agent

Pueden configurarse los valores siguientes:

- Directorio de datos: directorio utilizado para almacenar datos del tiempo de ejecución. El valor predeterminado es **`/var/opt/apoc`**.
- Ciclo de vida de los datos almacenados en la memoria caché: minutos que permanecen en la base de datos local los datos de configuración que no están fuera de línea.

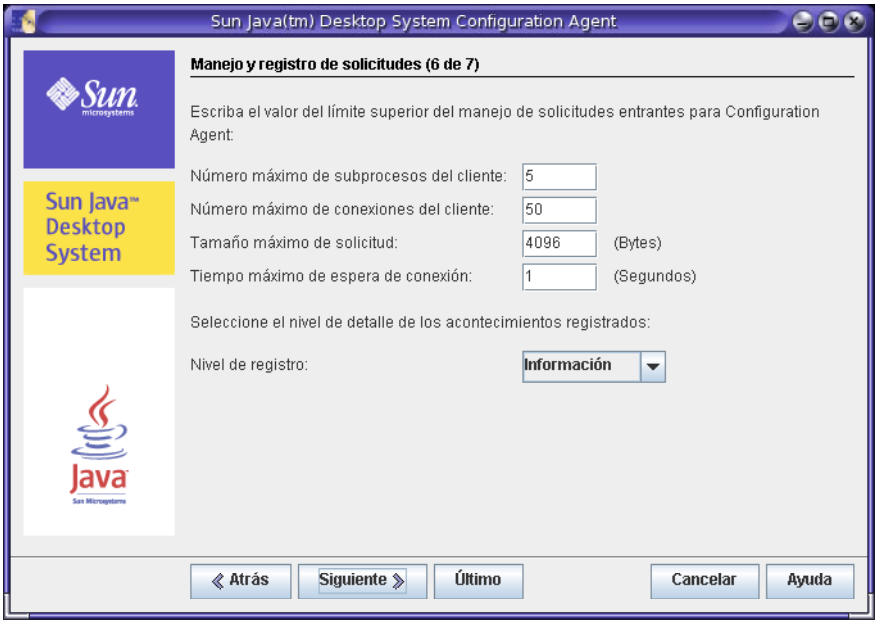

FIGURA 3–6 Manejo de solicitudes y registro cronológico de Configuration Agent

- Ciclo de liberación de recursos: minutos entre los ciclos de liberación de recursos en la base de datos local de la configuración.
- Número máximo de subprocesos del cliente: número máximo de solicitudes de los clientes que pueden procesarse simultáneamente.
- Número máximo de conexiones del cliente: número máximo de conexiones de los clientes.
- Tamaño máximo de solicitud: tamaño máximo de las solicitudes de los clientes.
- Tiempo máximo de espera de conexión: indica el intervalo permitido para que el servidor LDAP responda a una solicitud de conexión. El valor predeterminado es un segundo.
- Nivel de registro: nivel de detalles en los archivos de registro del agente. Los niveles de registro se corresponden con los de Java Logger. En orden de gravedad decreciente, estos niveles son:
  - *GRAVE*
  - *ADVERTENCIA*
  - *INFORMACIÓN*
  - *CONFIGURACIÓN*
  - *DETALLADO*
  - *MUY DETALLADO*
  - *MÁXIMO DETALLE*

Nota – Casi todos los valores de configuración de funcionamiento, excepto Directorio de datos y Tiempo máximo de espera de conexión, también pueden mantenerse centralmente mediante las normas pertinentes almacenadas en el servidor LDAP. Para utilizar esta función, no adapte los valores de configuración correspondientes mediante el asistente. En lugar de ello, use las normativas del Configuration Agent que hay en Desktop Manager para especificar valores de funcionamiento centralmente.

Aplicación de valores de configuración de agentes

Con la excepción de "Directorio de datos" y "Tiempo máximo de espera de conexión", los valores de funcionamiento que se han almacenado en el servidor LDAP con Desktop Manager entran en vigor automáticamente en el siguiente ciclo de detección de cambios de la configuración del agente (véase DaemonChangeDetectionInterval).

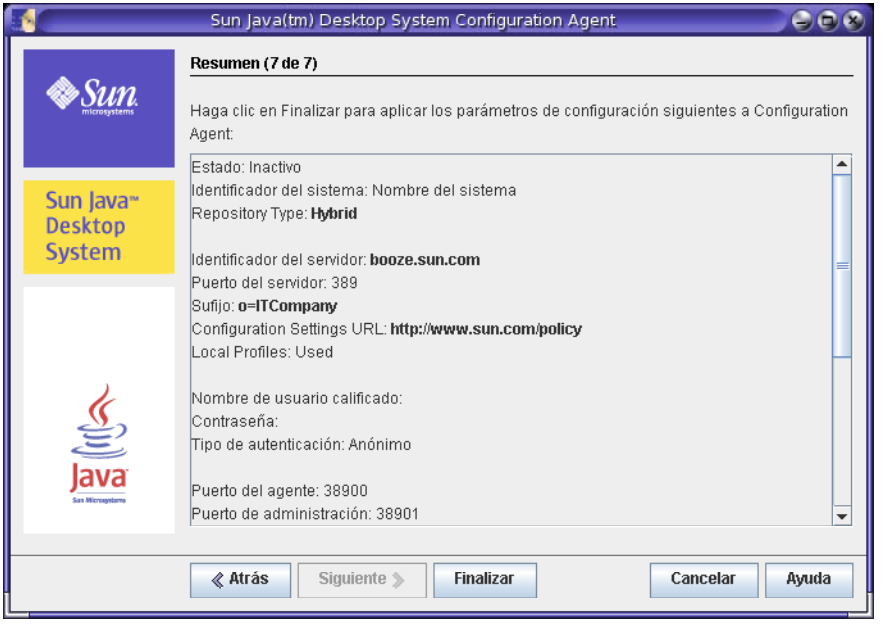

FIGURA 3–7 Página de resumen de Configuration Agent

Todos los demás valores de configuración cambiados localmente requieren que Configuration Agent vuelva a cargarse o reiniciarse. Si se utiliza el asistente de configuración, esta recarga o reinicio se lleva a cabo automáticamente.

Nota – Para reiniciar Configuration Agent manualmente, compruebe que no haya en ejecución aplicaciones cliente relacionadas, inicie sesión como superusuario y escriba el comando `/usr/lib/apoc/apocd restart`.

Parámetros adicionales de Configuration Agent

Nota – Los parámetros siguientes no figuran en el asistente de configuración.

- Aplicación de normas locales (ApplyLocalPolicy): este parámetro sirve para indicar si las aplicaciones cliente deben poder acceder o no a los datos de las normas del sistema local. El valor "true" especifica que se puede acceder a los datos de las normas locales. El valor "false" establece que no se puede acceder a dichos datos. Si desea más información, consulte "Uso de las normas locales" en la página 25.

Uso de las normas locales

Configuration Agent se puede configurar para que aplique parámetros de configuración de normas desarrolladas localmente, además de o como alternativa a cualquier norma de carácter global. Utilice los pasos siguientes para aplicar cualquier norma local:

▼ Desarrollo de una norma local

1. **Con Desktop Manager, cree un perfil con los pertinentes parámetros de norma.**
2. **Mediante Desktop Manager, exporte el perfil a un archivo comprimido (zip).**
3. **En el sistema cliente, si no lo hay, cree el directorio**
   `${DataDir}/Policies/profiles/PROFILE_REPOSITORY_default`.
   `${DataDir}` corresponde al valor del directorio de datos de Configuration Agent, que de forma predeterminada es `/var/opt/apoc`.
4. **Copie el archivo comprimido exportado en**
   `${DataDir}/Policies/profiles/PROFILE_REPOSITORY_default`.
5. **Compruebe que Configuration Agent esté configurado para aplicar normas locales (consulte "Parámetros adicionales de Configuration Agent" en la página 25 para obtener más información).**

Nota – Si modifica el parámetro "ApplyLocalPolicy" de Configuration Agent, se puede volver a cargar Configuration Agent iniciando sesión como `superusuario` y escribiendo el comando `/usr/lib/apoc/apocd reload`.

Los clientes tendrán acceso a las normas locales desarrolladas de esta forma en el próximo ciclo de detección de cambios de Configuration Agent.

Reinicio automático de Configuration Agent

Si se da un fallo, Configuration Agent se reinicia automáticamente. La función de administración de servicios (smf(5)) se encarga de decidirlo. Si esta función establece que no es apropiado reiniciarlo (por ejemplo, porque ya ha habido demasiados fallos), Configuration Agent pasa a modo de mantenimiento.

Si no se reinicia Configuration Agent, es aconsejable deshabilitarlo temporalmente; para ello, inicie sesión como superusuario y escriba el comando `/usr/lib/apoc/apocd disable`, solucione los problemas que afectan al agente y vuélvalo a habilitar mediante el comando `/usr/lib/apoc/apocd enable`.

Acceso a los datos/autentificación del usuario

Configuration Agent recupera información del servidor LDAP basándose en el ID de inicio de sesión de un usuario del escritorio. El valor `User/UniqueIdAttribute` del archivo de organización asigna el identificador del inicio de sesión a un elemento de usuario del servidor LDAP. Configuration Agent también recupera información sobre el sistema, como su nombre o dirección IP. Esta información se asigna a un elemento del sistema en el servidor LDAP a través del valor `Host/UniqueIdAttribute` del archivo de asignación de la organización. Si necesita más información sobre las asignaciones organizativas, consulte el Apéndice C.

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. Para integrar la adquisición de credenciales de Kerberos con el inicio de sesión del usuario, el módulo `pam_krb5` debe estar instalado y configurado en el sistema Java Desktop System.

Puede utilizar `gdm` para integrar Kerberos con el inicio de sesión de usuario, por ejemplo, mediante el siguiente archivo `/etc/pam.d/gdm`:

```
#%PAM-1.0
auth   required    pam_unix2.so  nullok #set_secrpc
auth   optional  pam_krb5.so use_first_pass missing_keytab_ok ccache=SAFE putenv_direct
account required    pam_unix2.so
password required    pam_unix2.so  #strict=false
```

```
session required    pam_unix2.so  # trace or none
session required    pam_devperm.so
session optional    pam_console.so
```

Si integra de este modo Kerberos con el inicio de sesión, es conveniente que habilite la compatibilidad del protector de pantalla con Kerberos. Puede utilizar, por ejemplo, el siguiente archivo `/etc/pam.d/xscreensaver` :

```
auth required pamkrb5.so use_first_pass missing_keytab_ok
ccache=SAFE putenv_direct
```

Adaptadores

Los adaptadores de aplicaciones son ampliaciones de los sistemas de configuración que admite Desktop Manager. Mediante los adaptadores, las aplicaciones tienen en cuenta los datos de la configuración central, según los sistemas de configuración. Los sistemas de configuración admitidos son:

- GConf: sistema de configuración de Gnome; lo utilizan el escritorio y casi todas las aplicaciones de Gnome, como Evolution.
- StarOfficeRegistry: sistema de configuración que utilizan StarOffice y OpenOffice.org.
- Mozilla Preferences: sistema de configuración que utiliza Mozilla.
- Java Preferences: API de configuración que se proporciona a las aplicaciones Java.

También se ofrece un adaptador de definiciones de escritorio (Desktop Definition), el cual agrega al escritorio del usuario elementos de menú, programas de inicio y lanzadores de escritorio.

Adaptador de GConf

Forma parte del paquete `SUNWapoc-adapter-gconf` de Solaris. Al instalar el adaptador desde el paquete correspondiente, la ruta de acceso a los orígenes de datos de GConf en `/etc/gconf/2/path` se actualiza para incluir los orígenes de Desktop Manager. Los dos orígenes de datos proporcionados por el adaptador son:

- “apoc:readonly:”: proporciona acceso a los valores no protegidos de las normas. Inserte este origen 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 este origen de datos después de los valores obligatorios locales y antes de los valores del usuario.

Configuración del adaptador de GConf

Este adaptador está configurado como parte de la instalación. Ahora bien, su funcionamiento depende de si en el archivo de ruta de acceso de GConf (`/etc/GConf/2/path`) hay dos orígenes de datos que representan los parámetros centrales y los predeterminados. Aunque este archivo de ruta

de acceso contenga la información para que GConf tenga en cuenta los parámetros centrales según lo previsto tras instalar el sistema, si los administradores deben modificar la ruta de acceso para incluir orígenes de datos personalizados, deben asegurarse de que en el archivo sigan estando los orígenes de datos con el prefijo "apoc". Los orígenes de datos deben ubicarse, por lo que respecta al origen de datos que representa los parámetros centrales obligatorios, entre los parámetros locales obligatorios y los de usuario; por su parte, el origen de datos que representa los parámetros centrales predeterminados debe estar entre los parámetros de usuario y los predeterminados locales.

Adaptador de Java Preferences

El adaptador de Java Preferences forma parte del paquete `SUNWapcj` de Solaris.

Configuración del adaptador de Java Preferences

El adaptador de Java Preferences viene integrado en la API de preferencias (Preferences API) que se debe usar como contenedor en otra implementación que ya existe (por ejemplo, el sistema predeterminado basado en archivos de JRE). Para habilitar el uso de una configuración central en una aplicación Java que utilice Preferences API, debe escribirse una secuencia de comandos de inicio para dicha aplicación, utilizando como ayuda la secuencia `/usr/lib/apoc/apocjlaunch`. Esta secuencia de comandos debe definir algunas variables de entorno y después incluir la secuencia `apocjlaunch` al final (ello inicia la aplicación Java con el entorno adecuado). Se deben definir las variables de entorno siguientes:

- `JAVA`: contiene la ruta de acceso al ejecutable de Java Runtime.
- `APPLICATION`: contiene la parte final de la invocación de Java Runtime para esa aplicación. Por ejemplo, *classname [arguments]* para el inicio de una sola clase, o `-jar` *jarname [arguments]* para el inicio de un archivo jar.

Las variables de entorno opcionales que se pueden definir son:

- `CLASSPATH`: lista de archivos jar o de clases separados por dos puntos que deben incluirse en la ruta de acceso de clase de la aplicación.
- `DEFINES`: cadena que contiene las instrucciones de definición que deben formar parte del inicio de la aplicación.
- `PREFFACTORY`: nombre de clase del generador de clases en la implementación de Preferences API subyacente que la aplicación necesita utilizar.

Adaptador de Mozilla

El adaptador de Mozilla forma parte del paquete `SUNWmozapoc-adapter` de Solaris.

Configuración del adaptador de Mozilla

Este adaptador se configura formando parte de la instalación del producto, no precisa configuración.

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 los perfiles sin tener que hacer modificaciones especiales.

Configuración del adaptador de StarOffice

Este adaptador se configura formando parte de la instalación del producto, no precisa configuración.

Adaptador de Desktop Definition

Este adaptador se compone de los paquetes siguientes:

Nombre del paquete	Descripción
SUNWapleg	binarios de acceso (configuración)
SUNWardsa	adaptador de Desktop Definition
SUNWardsa-misc	integración de sistemas para adaptador

Estos paquetes se instalan durante la instalación de los componentes del cliente de Desktop Manager, no precisan configuración.

Configuración del adaptador de Desktop Definition

Este adaptador lo configura el proceso de instalación para que se utilice siempre que un usuario inicia sesión; no precisa configuración.

Desinstalación de los adaptadores

Los adaptadores de Mozilla y StarOffice se quitan al desinstalarse dichos productos. Los adaptadores de GConf, Java Preferences y Desktop Definition se pueden desinstalar mediante las pertinentes herramientas del sistema para administración de paquetes, quitando los mencionados paquetes de la sección de instalación.

Al quitar el adaptador de Java Preferences, las secuencias de comandos de inicio escritas para iniciar las aplicaciones Java mediante Preferences API no se deben utilizar. La invocación de Java en ellos no funciona, puesto que ya no están disponibles algunas de las clases necesarias.

Resolución de problemas de los adaptadores

Gran parte de los problemas resultantes de no ver los datos de la configuración central en las aplicaciones correspondientes es probable que se deba a Configuration Agent, puesto que es el mecanismo común que todos los adaptadores emplean para recuperar los datos.

Si una configuración central no parece surtir efecto en un parámetro determinado (o un grupo), un posible motivo es que el usuario haya definido de forma expresa un valor para ese parámetro en la aplicación (normalmente, en los cuadros de diálogo de las opciones o preferencias del producto). En tal caso, a menos que los parámetros centrales se definan como protegidos (el administrador establece el valor y el usuario no lo puede modificar), la preferencia del usuario prevalece sobre los valores establecidos con Desktop Manager.

Resolución de problemas de Configuration Agent

En esta sección se facilitan respuestas a cuestiones que puedan surgir debido a la naturaleza y el uso de Configuration Agent. Asimismo, se brindan consejos para la resolución de problemas del agente.

Preguntas y respuestas

¿En qué consiste Configuration Agent y cómo funciona?

Configuration Agent es una aplicación de distribución y puesta en memoria caché de normas. Se ha concebido y realizado para garantizar que las aplicaciones cliente del escritorio se configuren de manera centralizada sin que ello repercuta negativamente en su rendimiento y ni en los sistemas que las ejecutan. Tal cosa se consigue mediante:

- La colocación en memoria caché de las normas que se descargan en una memoria caché local a la que puedan acceder los clientes.
- Compartiendo los recursos costosos (por ejemplo, las conexiones al servidor LDAP en que se alojan las normas) que se pueden y deben compartir.

Las circunstancias habituales en que interactúan las aplicaciones cliente y Configuration Agent son muy sencillas y se resumen a continuación:

1. Un usuario inicia una de las aplicaciones cliente del escritorio (Gconf, Mozilla o StarOffice).
2. La aplicación cliente se conecta con Configuration Agent.
3. Dicha aplicación solicita los datos de normas que necesita de Configuration Agent.
4. Configuration Agent busca en su memoria caché los datos solicitados.
5. Si los datos de normas no están en la memoria caché, Configuration Agent los descarga de un depósito de normas preconfigurado y los almacena en la memoria caché.
6. Los datos de normas se envían a la aplicación cliente que los había solicitado.
7. Configuration Agent supervisa el depósito de normas para detectar los cambios que pudiera haber en los datos.
8. Si hay modificaciones, Configuration Agent actualiza la memoria caché para ponerla al día e informa a la aplicación cliente.

¿Cómo se obtiene e instala Configuration Agent?

Configuration Agent se suministra e instala de forma predeterminada con el sistema operativo Solaris 10.

Una vez instalado Solaris 10, ¿cuál es el paso siguiente?

Configuration Agent se suministra sin habilitar ni configurar. Para poder utilizarlo se debe habilitar y efectuar una configuración mínima. Una vez realizados estos pasos, las aplicaciones cliente del escritorio usan de forma automática cualquier norma que se proporcione la próxima vez que se inicien.

¿Cómo se configura Configuration Agent?

Para configurar correctamente Configuration Agent, utilicel el Asistente de Configuration Agent. El asistente se inicia (como superusuario) mediante el comando `/usr/bin/apoc-config` . El asistente guía al usuario por los pasos necesarios para la correcta configuración del agente. En muchos casos, el único dato que debe proporcionarse para que el asistente finalice el proceso es la ubicación del depósito de normas.

Configuration Agent también puede configurarse editando manualmente sus archivos de configuración. No es algo recomendable, ya que de esta forma Configuration Agent se suele configurar incorrectamente con facilidad. Asimismo, el Asistente de Configuration Agent tiene lógica adicional que establece si un cambio determinado implica o no reiniciar o volver a cargar Configuration Agent.

¿Cómo se habilita Configuration Agent?

Hay tres maneras de habilitarlo:

1. Mediante el Asistente de Configuration Agent (`/usr/bin/apoc-config`), el estado se cambia a activo.
2. Con el programa del controlador de Configuration Agent (`/usr/lib/apoc/apocd`), ejecute lo siguiente como superusuario:

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

3. Mediante smf(5), ejecute lo siguiente como superusuario:

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

Tras configurar y habilitar Configuration Agent, ¿cómo se comprueba si funciona?

La manera más fácil de cerciorarse de que Configuration Agent esté bien configurado y que funcione correctamente es crear una norma con Desktop Manager, asignarla a un usuario, iniciar sesión en el escritorio como dicho usuario y comprobar los valores de las normas establecidas para que se utilicen. En una sesión de escritorio pueden detectarse fácilmente muchos valores de normas, por ejemplo fondo y tema.

¿Qué sentido tiene habilitar Configuration Agent?

Configuration Agent es un servicio que se ajusta a la función de administración de servicios smf(5); el concepto de habilitarlo procede de esa función. Una vez habilitado, Configuration Agent ya puede funcionar. El proceso de habilitación del agente se compone de las fases siguientes:

- Se inicia Configuration Agent.
- Las aplicaciones cliente del escritorio que se hayan iniciado tras la habilitación del agente pueden recuperar datos de normas.
- Configuration Agent se reinicia automáticamente durante el arranque del sistema.

¿Cómo se comprueba si está habilitado Configuration Agent?

Se puede saber si está o no habilitado aplicando uno de los procedimientos siguientes:

- Mediante el programa del controlador de Configuration Agent. Ejecute el comando siguiente como superusuario:

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

  Si está habilitado el agente, el programa del controlador genera el mensaje siguiente:

  ```
  Checking Configuration Agent enabled status ... Enabled
  ```

  Si no lo está, el programa del controlador genera el mensaje siguiente:

  ```
  Checking Configuration Agent enabled status ... Not enabled
  ```

- Utilice smf(5) para ejecutar el comando siguiente:

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

  Si está habilitado el agente, svcs genera el mensaje siguiente:

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

  Si no lo está, svcs genera el mensaje siguiente:

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

  Si Configuration Agent está en modo de mantenimiento, svcs genera el mensaje siguiente:

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

¿Cómo se comprueba si Configuration Agent está ejecutándose?

Para verificar si Configuration Agent está funcionando, aplique uno de los métodos siguientes:

- Inicie sesión como superusuario y ejecute el programa del controlador de Configuration Agent:

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

Si está habilitado el agente, el programa del controlador genera el mensaje siguiente:

```
Checking Configuration Agent status ... Running
```

Si no lo está, el programa del controlador genera el mensaje siguiente:

```
Checking Configuration Agent status ... Not running
```

- Ejecute el comando siguiente:

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

Si Configuracion Agent está ejecutándose, svcs genera el mensaje siguiente:

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

Si no lo está, svcs genera el mensaje siguiente:

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

Si Configuration Agent está en modo de mantenimiento, svcs genera el mensaje siguiente:

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

- Ejecute el comando siguiente:

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

Si Configuration Agent está ejecutándose, en la salida de `ps` debe haber el siguiente proceso de Java asociado:

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

¿Dónde se ubican los archivos de registro?

Cuando deba resolver un problema de Configuration Agent, consulte los archivos de registro siguientes:

- Archivos de registro de smf(5):
  - El archivo de registro `/var/svc/log/network-apocd-udp:default.log` recopila eventos relativos a casos concretos de intento de inicio y parada de Configuration Agent. Asimismo, el archivo contiene los mensajes que el programa del controlador de Configuration Agent, `/usr/lib/apoc/apocd`, genera en su salida estándar para JVM o Configuration Agent.
  - El archivo de registro `/var/svc/log/svc.startd.log` almacena un registro de cinco eventos de smf(5) de nivel superior. Por ejemplo, si en un lapso temporal muy breve se suceden varios intentos no válidos de inicio de Configuration Agent, smf(5) puede decidir que no se puede

iniciar. En tal caso, smf(5) coloca Configuration Agent en modo de mantenimiento y escribe una entrada en el registro para dejar constancia de ello.

Estos dos archivos de registro se usan habitualmente si el inicio de Configuration Agent da problemas.

- Registros de Configuration Agent:

  Configuration Agent escribe mensajes de registro en los archivos de registro del directorio predeterminado `/var/opt/apoc/Logs`. El "directorio de datos" de Configuration Agent es `/var/opt/apoc` . La ubicación de este directorio se puede cambiar con el Asistente de Configuration Agent (`/usr/bin/apoc-config`). El nivel de detalle de los mensajes de registro se puede modificar cambiando el "nivel de registro" con el Asistente de Configuration Agent. Si sospecha que no ha configurado correctamente Configuration Agent, o el agente falla en algún otro caso, use el Asistente de Configuration Agent y establezca el nivel de registro en "Máximo detalle" antes de consultar los archivos de registro del agente. De esta forma, dispondrá de la información de registro más exhaustiva posible.

- Registros del sistema:

  Para realizar un diagnóstico de los problemas de Configuration Agent, también puede consultar los archivos de registro `/var/adm/messages` o `/var/opt/SUNWut/log/messages` de una máquina SunRay.

¿Cómo se incrementa el nivel de detalle del mecanismo de registro del agente?

Consulte "¿Dónde se ubican los archivos de registro?" en la página 33

¿En qué consiste el modo de mantenimiento?

smf(5) coloca Configuration Agent en modo de mantenimiento al detectar problemas en los inicios o reinicios. Si smf(5) no consigue iniciarlo, lo intenta varias veces más hasta lograrlo o termina determinando que Configuration Agent no se puede iniciar. Si sucede eso, smf(5) coloca el agente en modo de mantenimiento para indicar al usuario que se debe solucionar el problema detectado. Una vez resuelta la situación, se puede anular el estado establecido por smf(5) para que Configuration Agent reanude el funcionamiento normal.

¿Cómo se sale del modo de mantenimiento o se anula el estado de smf(5)?

Inicie sesión como superusuario y ejecute el comando `/usr/sbin/svcadm clear svc:/network/apocd/udp`.

¿Qué sucede si de repente Configuration Agent deja de funcionar?

smf(5) detecta que se ha parado e intenta reiniciarlo. Si por algún motivo los intentos de reinicio sucesivos no son válidos, smf(5) coloca Configuration Agent en modo de mantenimiento. Si se logra reiniciar el agente, las aplicaciones cliente del escritorio que están en ejecución no resultan afectadas. Las aplicaciones cliente se vuelven a conectar automáticamente con el agente en cuanto se reinicia.

Si se inicia o habilita Configuration Agent, ¿hay que reiniciar las aplicaciones cliente del escritorio?

Depende de si el agente estaba habilitado o en ejecución al iniciarse una determinada aplicación cliente. Si Configuration Agent estaba habilitado o ejecutándose, la aplicación cliente había establecido una conexión con él; si la conexión se pierde, intenta restablecerla. Es decir, cada vez que Configuration Agent se inicia, habilita o deshabilita, las aplicaciones cliente siempre intentan restablecer la conexión en cuanto el agente vuelve a ejecutarse. Si el agente no estaba habilitado ni ejecutándose al iniciarse la aplicación cliente, ésta no usa Configuration Agent ni intenta conectarse con él en cuanto se inicia. Teniendo en cuenta todo lo dicho, puede afirmarse lo siguiente:

- Las aplicaciones cliente del escritorio iniciadas cuando Configuration Agent estaba habilitado o ejecutándose no se deben reiniciar.
- Las aplicaciones cliente del escritorio iniciadas cuando Configuration Agent no estaba habilitado o en ejecución se deben reiniciar.

¿Qué debe hacerse si parece que las aplicaciones cliente del escritorio no utilizan las normas configuradas?

El problema más habitual relacionado con Configuration Agent es la imposibilidad de observar los efectos de una norma configurada en las aplicaciones cliente del escritorio. Los motivos más comunes son un agente configurado incorrectamente, un depósito de normas de configuración mal configurado o no disponible. Las indicaciones siguientes pueden ayudar a diagnosticar y solucionar estos problemas:

- Compruebe que Configuration Agent esté configurado.
- Compruebe que esté habilitado o ejecutándose. Si debe iniciar el agente, reinicie también las aplicaciones cliente del escritorio que estén abiertas.
- Si los problemas siguen sin solucionarse, de forma temporal aumente el nivel de detalle del mecanismo de registro de Configuration Agent y, si es posible, reinícielo a fin de que, desde que se inicie el agente, en los mensajes de registro disponga de información lo más detallada posible.
- Si Configuration Agent no se inicia, consulte la sección "Problemas al iniciar Configuration Agent" en la página 35.
- Si se inicia pero las aplicaciones cliente del escritorio no emplean una norma, consulte la sección "Problemas en la obtención de normas cuando Configuration Agent está en ejecución".
- Si no ha podido solucionar los problemas, consulte a los responsables de asistencia técnica.

Problemas al iniciar Configuration Agent

Si no se puede iniciar Configuration Agent y considera que lo ha configurado y habilitado correctamente, consulte los archivos de registro. En las secciones siguientes se explican los errores más habituales relativos a este problema.

No se puede acceder al directorio de datos de Configuration Agent o no es válido

El agente crea y utiliza el directorio de datos para almacenar archivos de registro, memorias caché de normas, etcétera. La ubicación predeterminada de este directorio es `/var/opt/apoc`.

Configuration Agent genera el mensaje de error siguiente en los registros de smf(5) si el directorio de datos se establece en una ubicación inaccesible, es decir, `/dev/null/cant/write/here`. Para resolver este problema, use el asistente de Configuration Agent (`/usr/bin/apoc-config`) para que el directorio de datos apunte a una ubicación a la que se pueda acceder.

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


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

Uso de un puerto de solicitudes de cliente que ya está ocupado

Configuration Agent utiliza conexiones de zócalo TCP/IP para comunicarse con las aplicaciones cliente del escritorio. De forma predeterminada, estas conexiones se efectúan a través del puerto 38900.

Si Configuration Agent se ajusta para utilizar el puerto 1234, que ya lo ocupa otro servicio, se genera el mensaje de error siguiente. Este mensaje aparece en los registros de Configuration Agent. Para solucionar este problema, use el Asistente de Configuration Agent (`/usr/bin/apoc-config`) para asignar al agente un número de puerto disponible.

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


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

Uso de un puerto de administración que ya está ocupado

Configuration Agent utiliza conexiones de zócalo TCP/IP para comunicarse con su programa del controlador (`/usr/lib/apoc/apocd`). De forma predeterminada, estas conexiones se efectúan a través del puerto 38901.

En los registros de Configuration Agent aparece el mensaje de error siguiente si el agente se ha ajustado para utilizar el puerto 1234, que ya lo ocupa otro servicio. Para solucionar este problema, use el Asistente de Configuration Agent (`/usr/bin/apoc-config`) para asignar al agente otro puerto de administración que esté disponible.

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


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

```
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:59)
    at sun.nio.ch.ServerSocketAdaptor.bind(ServerSocketAdaptor.java:52)
    ... 4 more
```

Problemas en la obtención de normas cuando Configuration Agent está en ejecución

La especificación del depósito de configuración no es válida o falta

Para descargar y poner en memoria caché la información de normas, Configuration Agent debe conectarse con un depósito de configuración válido. Si identifica incorrectamente dicho depósito en la configuración del agente, por ejemplo mediante un comando no válido o porque no especifica un depósito, en los registros de Configuration Agent aparecen errores parecidos al siguiente cuando se inician las aplicaciones cliente del escritorio. Para solucionar este problema, use el Asistente de Configuration Agent (`/usr/bin/apoc-config`) para identificar el depósito de configuración que va a utilizar.

```
FINER: New client added
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authenticating user geoffh
Nov 18, 2005 1:59:22 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authentication successful
Nov 18, 2005 1:59:23 PM PolicyBackend openPolicyBackend
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.environment.InvalidParameterException: The parameter organisation
PROVIDER_URL#protocol (null) is not valid, the value must be comprised in
{ldaps,ldap,https,http,file}.
    at com.sun.apoc.daemon.apocd.PolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.HostPolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.open(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.createDataSources(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.createNewCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.openCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.Session.<init>(Unknown Source)
    at com.sun.apoc.daemon.transaction.CreateSessionTransaction.executeTransaction
(Unknown Source)
    at com.sun.apoc.daemon.transaction.Transaction.execute(Unknown Source)
    at com.sun.apoc.daemon.apocd.ClientEventHandler.handleEvent(Unknown Source)
    at com.sun.apoc.daemon.apocd.EventWorkerThread.run(Unknown Source)
```

```
Caused by: com.sun.apoc.daemon.misc.APOCException:
 com.sun.apoc.spi.environment.InvalidParameterException:
 The parameter organisation PROVIDER_URL#protocol (null) is not valid,
 the value must be comprised in {ldaps,ldap,https,http,file}.
    at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyMgr(Unknown Source)
    ... 14 more
Caused by: com.sun.apoc.spi.environment.InvalidParameterException: The parameter
organisation PROVIDER_URL#protocol (null) is not valid, the value must be comprised in
{ldaps,ldap,https,http,file}.
    at com.sun.apoc.spi.PolicyMgrFactoryImpl.createPolicyMgr(Unknown Source)
    ... 15 more
Nov 18, 2005 1:59:23 PM PolicyBackend openPolicyBackend
```

No es posible conectar con el depósito de normas

Para descargar y poner en memoria caché información de normas, Configuration Agent debe conectarse con un depósito de configuración válido. Si no puede establecerse la conexión, en los registros de Configuration Agent aparecen errores similares al siguiente cuando se inician las aplicaciones cliente del escritorio. En el caso siguiente, no existe la variable sobuild del sistema, no se puede contactar o no se puede acceder a un servidor LDAP a través del puerto 389. Para solucionar este problema, mediante el Asistente de Configuration Agent (`/usr/bin/apoc-config`) compruebe que haya identificado correctamente el depósito de normas y, en tal caso, asegúrese de que tenga acceso a dicho depósito. Por ejemplo, en un depósito LDAP, debe comprobar que haya en ejecución un servidor LDAP, que la máquina en que se aloja esté disponible en la red y que dicho servidor utilice el puerto especificado.

Si intenta acceder a un servidor LDAP mediante una conexión SSL, compruebe que el certificado pertinente esté disponible en el almacén de claves asociado con el Java Runtime Environment que se emplea para ejecutar Configuration Agent. Consulte la sección "Configuration Agent" en la página 16 para obtener más información sobre `apoc-config`.

```
FINER: New client added
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authenticating user geoffh
Nov 18, 2005 2:17:43 PM com.sun.apoc.daemon.misc.APOCLogger finest
FINEST: Authentication successful
Nov 18, 2005 2:17:43 PM PolicyBackend openPolicyBackend
FINER: THROW
com.sun.apoc.daemon.misc.APOCException: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.OpenConnectionException: An error occured while connecting to
ldap://sobuild:389.
    at com.sun.apoc.daemon.apocd.PolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.HostPolicyBackend.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyBackend(Unknown Source)
```

```
    at com.sun.apoc.daemon.apocd.Cache$DataSource.openPolicyBackend(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache$DataSource.open(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.createDataSources(Unknown Source)
    at com.sun.apoc.daemon.apocd.Cache.<init>(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.createNewCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.CacheFactory.openCache(Unknown Source)
    at com.sun.apoc.daemon.apocd.Session.<init>(Unknown Source)
    at com.sun.apoc.daemon.transaction.CreateSessionTransaction.executeTransaction
(Unknown Source)
    at com.sun.apoc.daemon.transaction.Transaction.execute(Unknown Source)
    at com.sun.apoc.daemon.apocd.ClientEventHandler.handleEvent(Unknown Source)
    at com.sun.apoc.daemon.apocd.EventWorkerThread.run(Unknown Source)
Caused by: com.sun.apoc.daemon.misc.APOCException:
com.sun.apoc.spi.OpenConnectionException: An error occured while
connecting to ldap://sobuild:389. at
com.sun.apoc.daemon.apocd.PolicyBackendFactory.openPolicyMgr(Unknown Source)
    ... 14 more
Caused by: com.sun.apoc.spi.OpenConnectionException: An error occured while
connecting to ldap://noSuchHost:389.
    at com.sun.apoc.spi.ldap.LdapClientContext.prepareConnection(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapClientContext.connect(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapConnectionHandler.openAuthorizedContext(Unknown Source)
    at com.sun.apoc.spi.ldap.LdapConnectionHandler.connect(Unknown Source)
    at com.sun.apoc.spi.ldap.entities.LdapOrganizationProvider.open(Unknown Source)
    at com.sun.apoc.spi.PolicyMgrFactoryImpl.createPolicyMgr(Unknown Source)
    ... 15 more
Caused by: netscape.ldap.LDAPException: failed to connect to server sobuild:389 (91);
Cannot connect to the LDAP server
    at netscape.ldap.LDAPConnSetupMgr.connectServer(LDAPConnSetupMgr.java:422)
    at netscape.ldap.LDAPConnSetupMgr.openSerial(LDAPConnSetupMgr.java:350)
    at netscape.ldap.LDAPConnSetupMgr.connect(LDAPConnSetupMgr.java:244)
    at netscape.ldap.LDAPConnSetupMgr.access$0(LDAPConnSetupMgr.java:241)
    at netscape.ldap.LDAPConnSetupMgr$1.run(LDAPConnSetupMgr.java:179)
    at java.lang.Thread.run(Thread.java:595)
Nov 18, 2005 2:17:44 PM PolicyBackend openPolicyBackend
```

Conexión con un depósito de normas no configurado

Para que Configuration Agent pueda encontrar datos de normas en un depósito de normas, dicho depósito debe estar bien configurado. Si especifica un depósito que está mal configurado o que no lo está, en los registros de Configuration Agent aparecen errores similares al siguiente cuando se inician las aplicaciones cliente del escritorio. Para resolver este problema, consulte la sección .

```
FINER: New client added
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: CreateSession transaction started
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finer
FINER: Creating new client session
Nov 18, 2005 2:36:55 PM com.sun.apoc.daemon.misc.APOCLogger finest
```

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

En los registros de Configuration Agent figura un mensaje relativo al "número máximo de conexiones del cliente". ¿Qué significa?

Cada aplicación cliente del escritorio (Gconf, Mozilla, StarOffice) activada por Configuration Agent abre una conexión con el agente cuando se ejecuta. En los parámetros de Configuration Agent se establece el límite de las conexiones que se pueden realizar. El valor máximo predeterminado de conexiones es 50. En una máquina con varios usuarios, quizá deba aumentar el "límite de las conexiones del cliente" mediante el asistente de Configuration Agent (`/usr/bin/apoc-config`). Si Configuration Agent llega al máximo de conexiones permitidas, en los registros de Configuration Agent aparecen mensajes de error similares al siguiente:

```
Nov 18, 2005 3:20:55 PM com.sun.apoc.daemon.misc.APOCLogger warning
WARNING: The maximum number of client connections ( 50 ) has been reached.
No new client connections can be established at this time.
```

La modificación de algunas normas mediante Desktop Manager no se refleja en las máquinas cliente

Una de las premisas al diseñar Configuration Agent es que los datos de normas creados por Desktop Manager son relativamente estáticos, es decir, no son susceptibles de cambiarse con frecuencia. Esta premisa se refleja en el hecho de que el agente consulta de vez en cuando el depósito de normas para detectar posibles modificaciones. De forma predeterminada, Configuration Agent comprueba el depósito una vez cada hora para todas las aplicaciones que se ejecutan en el escritorio. Así, tras

realizar un cambio con Desktop Manager, debe esperarse a que transcurra una hora para notificar el cambio a las aplicaciones que se ejecutan. Si lo desea, con el Asistente de Configuration Agent (`/usr/bin/apoc-config`) puede cambiar el "intervalo de detección general" para incrementar la frecuencia de las comprobaciones en el depósito. Asimismo, puede establecer que Configuration Agent actualice los datos de normas de todas las aplicaciones conectadas iniciando sesión como superusuario y ejecutando el comando `/usr/lib/apoc/apocd change-detect`.

◆ ◆ ◆ CAPÍTULO 4

Java Web Console

Java Web Console está diseñado para ser una solución de gestión del sistema común y basada en la web de 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 acceder a las aplicaciones de gestión del sistema.

Java Web Console se caracteriza por:

- 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 de la consola es que el administrador puede iniciar la sesión una vez y utilizar cualquier aplicación dentro de la consola.

Instalación

Requisitos de sistema

Java Web Console admite varios sistemas operativos cliente y servidor así como varios navegadores.

Cliente

- Netscape™ 6.2x y 7.x en Solaris 10
- Netscape 6.2x y 7.x en Windows 98, 98 SE, ME, 2000 y XP
- Internet Explorer 5.5x y 6.x en Windows 98, 98 SE, ME, 2000 y XP

- Mozilla 1.4x en Solaris
- Firefox 1.0 en Solaris

Servidor

- Solaris 10
- Red Hat Application Server 2.1, 3.0
- SuSE Linux 8.0 o superior
- J2SE Versión 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 con la versión J2SE del Java Desktop System Management Tools CD.
- Tomcat: 4.0.3 o superior

  Tomcat se incluye en el Java Desktop System Management Tools CD

Instalación de Java Web Console

Java Web Console 2.2.4 forma parte del sistema operativo Solaris 10; sin embargo, Desktop Manager necesita la versión 2.2.5. Hay una copia de la versión 2.2.5 en el sistema de archivos de Desktop Manager, en el directorio `server/console` . Se puede instalar mediante la ejecución de `./setup` en dicho directorio.

Si tiene instalado Java Web Console 3.0, debe desinstalar la versión 3.0 e instalar la versión 2.2.5 de Java Web Console que está en el directorio `server/console`, como se ha indicado antes.

Ejecución de la consola

En general, para registrar una aplicación nueva sólo se debe detener y reiniciar el servidor de Java Web Console.

Precaución – Antes de iniciar por primera vez Java Web Console, compruebe que haya concluido el proceso de instalación de Desktop Manager. Java Web Console *no* se ejecuta correctamente hasta que no haya en marcha como mínimo una aplicación de la consola.

- Para iniciar Java Web Console, escriba `smcwebserver start`.
- Para detener Java Web Console, escriba `smcwebserver stop`.
- Para reiniciar Java Web Console, escriba `smcwebserver restart`.
- Para acceder a Java Web Console, indique el URL siguiente en el navegador: `https://`*<nombresistema>*`.`*<nombredominio>*`:6789`

Java Web Console permite la autenticación basada en UNIX y RBAC (Role-Based Access Control, Control de acceso basado en roles) sin tener que configurarla. No obstante, también puede configurar otros mecanismos de autentificación como LDAP.

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

Para obtener más información sobre los comandos de Java Web Console, consulte las páginas smcwebserver y smreg man.

Desinstalación de Java Web Console

Precaución – Si utiliza el sistema operativo Solaris, Java Web Console no se puede quitar porque es parte de él.

Resolución de problemas de Java Web Console

No se puede instalar Java Web Console

Síntoma: al final de la instalación, un mensaje indica que Java Web Console no se puede iniciar porque no hay aplicaciones registradas.

Posibles causas: tras instalarse el módulo Desktop Manager, se inicia Java Web Console.

Conexión rechazada

Síntoma: intenta abrir un URL determinado, por ejemplo `https://`*<su.servidor>*`:6789`, pero se rechaza la conexión.

Posibles causas: Java Web Console no se ejecuta en el servidor.

No se puede iniciar sesión

Nota – De forma predeterminada, no se instala el módulo de inicio de sesión LDAP. Como consecuencia, las credenciales de inicio de sesión no se comparan con las que están almacenadas en el servidor LDAP y únicamente hacen falta las credenciales normales de inicio de sesión del sistema. Esta sección de resolución de problemas sólo es válida si ha instalado manualmente el módulo de inicio de sesión de LDAP.

Síntoma: se puede acceder a la página de inicio de sesión de Web Console, pero se rechaza la combinación de nombre de usuario y contraseña.

Posibles causas:

- El servidor LDAP no está en ejecución.
- Se ha configurado incorrectamente el módulo de autenticación LDAP de Web Console.
- El usuario no existe en el servidor LDAP.
- El usuario tiene una contraseña distinta en el servidor LDAP.

No hay vínculo de Desktop Manager

Síntoma: se puede iniciar sesión en Web Console, pero Desktop Manager no figura en la página de listas de aplicaciones.

Posibles causas:

- El módulo Desktop Manager no está instalado.

Excepción de invocación de método sobre un objeto nulo, error de Tomcat/Java o página en blanco

Síntoma: se abre Desktop Manager pero en pantalla no aparecen valores, sino sólo una página en blanco o mensajes de error.

Posibles causas: si el error menciona `NoClassDefFoundError: sun/tools/javac/Main` , significa que Java Web Console utiliza una instalación incorrecta de Java.

Otros problemas

Si el servidor web no funciona correctamente, puede haber información al respecto en los archivos de registro. Se ubican en `/var/log/webconsole/`. El nivel de detalle de la información del registro se puede aumentar mediante el comando `smreg`:

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

La configuración original se puede restaurar mediante:

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

El volcado completo de la base de datos de configuración se activa mediante:

```
smreg list
```

Es posible que el servidor web que aloja Desktop Manager no se cierre correctamente y deje en uso los puertos. Esta situación imposibilita el inicio de un nuevo servidor web. Si el comando `smcwebserver start/restart` emite mensajes de error, o si todavía puede accederse a Desktop Manager incluso después de un comando `smcwebserver stop`, o si el servidor iniciado sigue comportándose como el anterior, compruebe si el puerto 6789 sigue en uso (`netstat -a | grep 6789`) o si el servidor web continúa en ejecución (`ps -ef | grep java`). Sea cual sea la situación, se debe cancelar el proceso correspondiente y dejar de utilizar el puerto 6789.

◆ ◆ ◆ APÉNDICE A

Parámetros de configuración

Estos parámetros se pueden definir para los siguientes componentes de Desktop Manager:

- Desktop Manager, en los archivos que definen los depósitos de configuración (en `/etc/opt/SUNWapcmg/`).
- Configuration Agent, en el archivo `/etc/apoc/policymgr.properties`.
- Desktop Manager CLI, en el archivo `$HOME/pgtool.properties`, con la restricción de que CLI sólo es compatible con depósitos LDAP puros.

Estos parámetros se pueden definir con prefijo para establecer a qué proveedor de depósitos se aplican. En cada proveedor tiene preferencia el parámetro con prefijo. Si no se define dicho parámetro, se emplea el parámetro sin el prefijo.

TABLA A–1 Prefijos

Valor del prefijo	Proveedor de depósitos
ORGANIZATION_	Árbol de la organización
DOMAIN_	Árbol del dominio
PROFILE_	Perfiles
ASSIGNMENT_	Asignaciones
LDAP_META_CONF_	Asignación de datos en el caso de depósitos LDAP

TABLA A–2 Parámetros

Nombre	Descripción	Valores posibles	Valor predeterminado

PROVIDER_URL	URL que indica la conexión con el depósito. Se puede usar una lista de URL para especificar depósitos de reserva en caso de que no funcione la conexión con el primero.	Proporcione una lista con uno o más URL separados por espacios en blanco; cada URL debe tener una de las formas siguientes:
		`ldap://<sistema>:<puerto>/<DN base>`
		`ldaps://<sistema>:<puerto>/archivo <DN base> ://<ruta de archivo>`
		`http://<sistema>:<puerto>/<ruta de archivo>`
		`https://<sistema>:<puerto>/<ruta de archivo>`
			Ninguno, parámetro obligatorio

SECURITY_PRINCIPAL	Nombre del usuario para conectarse con el depósito.	Nombre de usuario con derechos de lectura y acceso de búsqueda en el depósito o sin especificar valor en el caso de conexión de acceso anónimo.	Ninguno, conexión de acceso anónimo
SECURITY_CREDENTIALS	Contraseña de usuario definida en SECURITY_PRINCIPAL.	Contraseña codificada o de texto normal.	Ninguna
SECURITY_CREDENTIALS_ENCODING	Indica si está codificada la contraseña definida en SECURITY_PRINCIPAL. Advertencia: la codificación de la contraseña es sólo una máscara, no consiste en ninguna clase de cifrado de seguridad.	“scrambled” (codificada) si la contraseña lo está (los asistentes lo efectúan automáticamente al generar los datos de configuración). “none” (ninguna) si la contraseña aparece en texto normal; para poder editar la contraseña, seleccione este parámetro.	“none” (ninguna)
MAX_SEARCH_RESULT	Cantidad máxima de resultados que proporciona un proceso de búsqueda en cualquier depósito. >Nota: el esquema de prefijos parece no aplicarse a este parámetro.	Número positivo; 0 significa sin límite.	100

Los parámetros siguientes corresponden sólo a depósitos LDAP.

TABLA A–3 Parámetros exclusivos de LDAP

Nombre	Descripción	Valores posibles	Valor predeterminado
Nombre de usuario calificado	DN totalmente cualificado de un usuario que se utiliza para el primer acceso al depósito LDAP, a fin de recuperar el usuario definido en SECURITY_PRINCIPAL.	Nombre de un usuario con derechos de lectura y acceso de búsqueda en el depósito, o sin valor en caso de conexiones anónimas.	Ninguno, acceso anónimo
Contraseña	Contraseña para Nombre de usuario cualificado.	Contraseña codificada o de texto normal.	Ninguna
Password_ENCODING	Indica si la contraseña especifiada en Contraseña está codificada. Advertencia: la codificación de la contraseña es sólo una máscara, no consiste en ninguna clase de cifrado de seguridad.	"scrambled" (codificada) si la contraseña lo está (los asistentes lo efectúan automáticamente al generar los datos de configuración). "none" (ninguna) si la contraseña aparece en texto normal; para poder editar la contraseña, seleccione este parámetro.	"none" (ninguna)
Tiempo máximo de espera de conexión	Tiempo máximo de espera de establecimiento de conexión en segundos.	Número positivo; 0 significa sin límite.	1

EJEMPLO A–1 Ejemplo de componente trasero híbrido

A continuación se muestra un ejemplo de componente trasero híbrido; la información relativa a los usuarios y sistemas de componentes traseros se obtiene de un depósito LDAP, mientras que los perfiles y sus asignaciones se almacenan en el sistema de archivos.

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

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

EJEMPLO A–1 Ejemplo de componente trasero híbrido *(Continuación)*

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

◆ ◆ ◆ APÉNDICE B

Utilización de OpenLDAP y Active Directory con Desktop Manager

Utilización de un servidor OpenLDAP con Desktop Manager

Para usar un servidor OpenLDAP como depósito para los datos de Desktop Manager, el esquema del servidor debe ampliarse para incluir las clases y atributos de objetos que se utilizan para almacenar los datos de configuración. Un archivo de esquemas personalizados denominado `apoc.schema` se encuentra en el directorio `/usr/share/webconsole/apoc/deploy`.

Este archivo debe copiarse en el subdirectorio `schema` del directorio de configuración de OpenLDAP (`/etc/openldap`) y agregarse al esquema de OpenLDAP incluyéndolo en el archivo `slapd.conf` que se encuentra en ese directorio. Esto se consigue insertando la línea `include /etc/openldap/schema/apoc.schema` al final de la secuencia de inclusiones de esquemas que haya en el archivo. Para más información sobre la ampliación de los esquemas de los servidores OpenLDAP, consulte el manual del servidor.

Al haber ampliado el esquema de los servidores OpenLDAP, el resto de la configuración puede realizarse con el Asistente para nuevo depósito de configuración de Desktop Manager.

Nota – Desktop Manager Agent intentará conectar con el servidor OpenLDAP anónimamente proporcionando el DN del usuario para el que necesita datos, pero sin contraseña. Este modo de autenticación anónima puede estar inhabilitado de forma predeterminada en algunas versiones de servidores OpenLDAP, en cuyo caso deberá habilitarse agregando una línea que diga `allow bind_anon_cred` en los parámetros del servidor común definidos en el archivo `slapd.conf` que hay en el directorio de configuración de OpenLDAP (`/etc/openldap`). Para obtener más información sobre el parámetro, consulte el manual del servidor.

Utilización de un servidor Active Directory con Desktop Manager

Para usar un servidor Active Directory como depósito para los datos de Desktop Manager, el esquema del servidor debe ampliarse para incluir las clases y atributos de objetos utilizados para almacenar datos de configuración. Un archivo de ampliación de esquemas denominado `apoc-ad.ldf` se encuentra en el directorio `/usr/share/webconsole/apoc/deploy`.

El archivo `apoc-ad.ldf` debe importarse en el esquema de Active Directory siguiendo estos pasos:

1. Habilite las extensiones del esquema. Consulte la documentación de Active Directory para más información sobre cómo realizar esta operación.
2. Ejecute lo siguiente desde la línea de comandos: **`ldifde -i -c "DC=Sun,DC=COM" <`***`BaseDN`***`> -f apoc-ad-registry.ldf`**.

Nota – Sustituya <*BaseDN*> por el DN base de Active Directory.

Al haber ampliado el esquema de los servidores Active Directory, el resto de la configuración puede realizarse con el Asistente para nuevo depósito de configuración de Desktop Manager.

Cuando el Asistente para nuevo depósito de configuración solicite credenciales de LDAP, facilite todo el DN y la contraseña de un usuario con derechos de lectura en el árbol. Puede ser un usuario que no pueda usar Active Directory con ningún otro propósito. Consulte la documentación de Active Directory si desea más información sobre cómo configurar dicho usuario. El nombre de dominio de Active Directory también debe conocerlo la máquina que está ejecutando Desktop Manager. Esto puede conseguirse agregando una línea que correlacione la dirección IP del servidor Active Directory con su nombre de dominio en el archivo `/etc/hosts` de esa máquina.

Para recuperar los datos de configuración de un sistema de escritorio, el nombre de dominio de Active Directory también debe ser conocido para ese sistema. La autenticación del usuario del escritorio puede realizarse de dos maneras: anónimamente y mediante GSSAPI.

- Para autenticar usando conexiones anónimas, el servidor de Active Directory debe estar configurado para conceder permisos de lectura a todo el mundo. Consulte la documentación de Active Directory para más información sobre cómo realizar esta operación.
- Para autenticar mediante GSSAPI, el usuario se debe haber autenticado respecto a Active Directory y las credenciales de usuario deben estar disponibles en el sistema. Esto es factible mediante la autenticación Kerberos en el sistema, lo cual genera estas credenciales al iniciar sesión. Para obtener más información al respecto, consulte las pertinentes guías de administración del sistema.

◆ ◆ ◆ APÉNDICE C

Asignación organizativa

Asignación organizativa

Para definir la asignación entre las entradas de LDAP y los elementos de Desktop Manager, debe editarse el archivo `Organization`. Los valores que coincidan con la distribución del depósito LDAP se deben proporcionar a las diversas claves.

Los elementos 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 muestran 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 objeto que usan todas las entradas del usuario
User/ObjectClass=inetorgperson
# Atributo cuyo valor en entradas del usuario es exclusivo dentro del depósito
User/UniqueIdAttribute=uid
# Contenedor opcional en entradas de organización de las entradas del usuario,
# eliminar línea si no se utiliza
User/Container=ou=People
# Formato de nombre de visualización dentro de la aplicación de gestión
User/DisplayNameFormat=sn, givenname
```

Los elementos 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 utilizan el formato `<item1>,<item2>,...,<itemN>` y se deben alinear. Es decir, las listas deben tener el mismo número de elementos y la clase de objeto nth se debe utilizar 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 entrada del sistema; también debe contener todos los DN de los roles a los que pertenece la entrada. La clave *MemberAttribute* debe especificar un atributo para el filtro de búsqueda a partir de un usuario o 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 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 objeto para roles
Role/ObjectClass=nsRoleDefinition
# Lista alineada de atributos de nombre correspondientes
Role/NamingAttribute=cn
# Atributo físico (usable en filtro) que contiene los DN
# de los roles de un usuario/sistema
Role/MemberAttribute=nsRoleDN
# Atributo cuya consulta en un usuario o sistema devuelve los DN de
# los roles a los que pertenece
Role/VirtualMemberAttribute=nsRole
```

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

```
# Lista de clases de objeto para organizaciones
Organization/ObjectClass=organization
# Lista alineada de atributos de nombre correspondientes
Organization/NamingAttribute=o
```

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

```
# Lista de clases de objeto para dominios
Domain/ObjectClass=ipNetwork
# Lista alineada de atributos de nombre correspondientes
Domain/NamingAttribute=cn
```

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

```
# Clase de objeto que usan todas las entradas de sistema
Host/ObjectClass=ipHost
# Atributo cuyo valor en las entradas de sistema es exclusivo dentro del depósito
Host/UniqueIdAttribute=cn
# Contenedor opcional en entradas de dominio de las entradas de sistema,
# eliminar línea si no se utiliza
Host/Container=ou=Hosts
```