AIX 5L Versión 5.1

Guía de administración del Gestor del sistema basado en la Web

AIX 5L Versión 5.1

Guía de administración del Gestor del sistema basado en la Web

Segunda edición (abril de 2001)

Antes de utilizar la información de este manual, lea la información general del “Apéndice B. Avisos” en la página 55.

Esta edición se aplica a AIX 5L Versión 5.1 y a todos los releases siguientes de este producto, hasta que se indique lo contrario en nuevas ediciones.

Al final de la publicación se proporciona una hoja de comentarios para el lector. Si no aparece el formulario, dirija sus comentarios a IBM S.A., National Language Solutions Center, Avda. Diagonal 571, Edif. L’Illa, 08029 Barcelona, España. Para enviar comentarios electrónicamente, utilice esta dirección comercial de Internet: hojacom@vnet.ibm.com. Cualquier información suministrada a IBM se puede utilizar sin incurrir por ello en ninguna obligación con el remitente.

Contenido

Acerca de este manual

Este manual contiene información sobre cómo utilizar Gestor del sistema basado en la Web para administrar sistemas.

A quién va dirigido este manual

Este manual está destinado a los administradores de sistemas que deseen utilizar Gestor del sistema basado en la Web para administrar sus sistemas.

Resaltado

En este manual se utilizan los siguientes convenios de resaltado:

Negrita	Identifica mandatos, subrutinas, palabras clave, archivos, estructuras, directorios y otros elementos cuyos nombres vienen predefinidos por el sistema. También identifica objetos gráficos como botones, etiquetas e iconos que selecciona el usuario.
Cursiva	Identifica parámetros cuyos nombres o valores reales debe suministrar el usuario.
`Monoespaciado`	Identifica ejemplos de valores de datos específicos, ejemplos de texto parecido al que puede visualizar, ejemplos de partes del código del programa parecidas a las que escribiría como programador, mensajes procedentes del sistema o información que debe escribir.

ISO 9000

En el desarrollo y la fabricación de este producto se han utilizado sistemas de calidad registrados que cumplen la norma ISO 9000.

Publicaciones relacionadas

Los siguientes manuales contienen información relacionada con Gestor del sistema basado en la Web:

- *AIX 5L Version 5.1 System Management Concepts: Operating System and Devices*
- *AIX 5L Version 5.1 System Management Guide: Operating System and Devices*

Marcas registradas

Los siguientes términos son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

- AIX
- IBM

Java y todas las marcas comerciales y logotipos basados en Java son marcas registradas de Sun Microsystems, Inc. en los Estados Unidos y/o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en los Estados Unidos y/o en otros países.

Otros nombres de empresas, productos o servicios pueden ser marcas registradas o marcas de servicios de otras empresas.

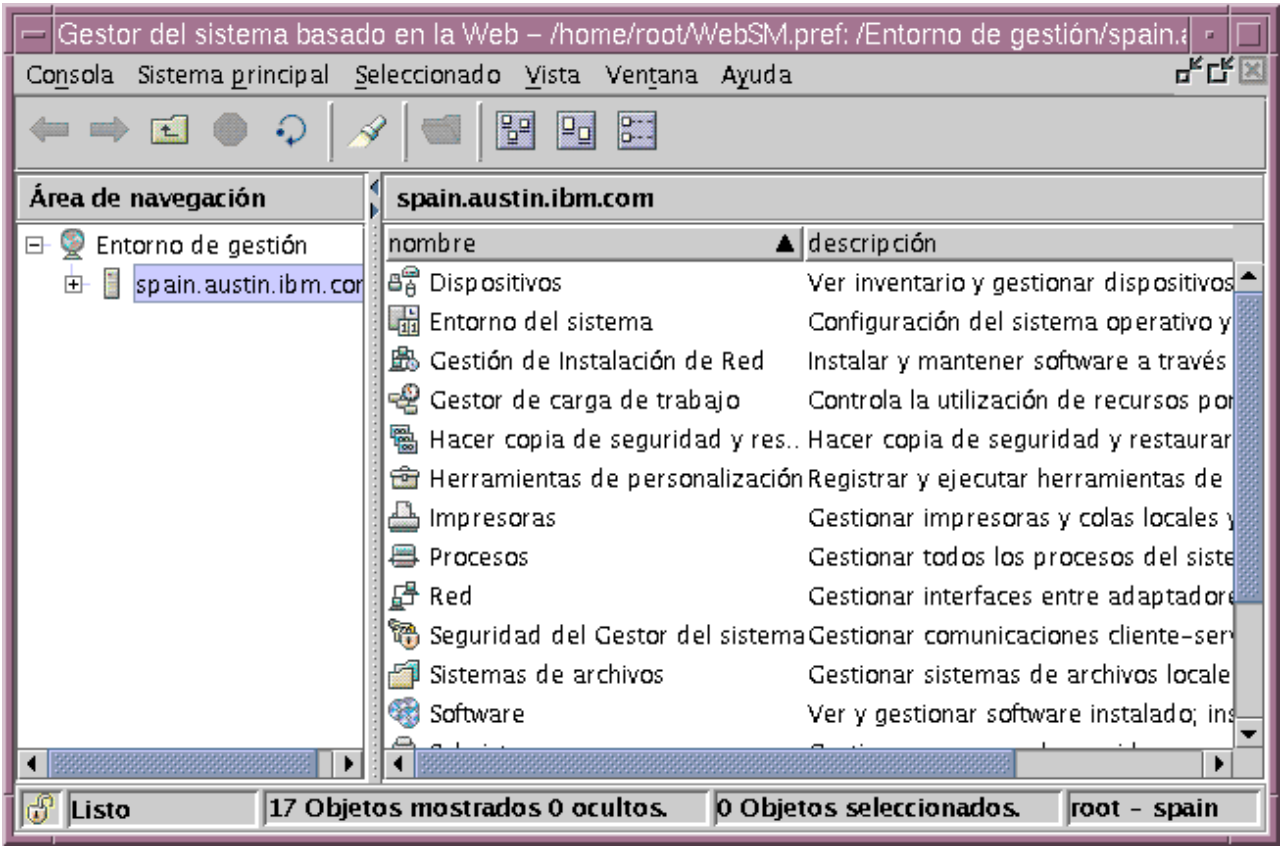
Capítulo 1. Introducción a Gestor del sistema basado en la Web

Gestor del sistema basado en la Web es una aplicación de gestión de sistemas para administrar sistemas. Se instala por omisión en sistemas gráficos y se ha revisado en profundidad para AIX 5.1.

Gestor del sistema basado en la Web ofrece una consola de gestión de sistemas para administrar varios sistemas principales. Su arquitectura modular facilita la extensión de la gama. Además, Gestor del sistema basado en la Web da soporte a la supervisión dinámica y a la notificación al administrador de sucesos del sistema.

Conceptos clave de Gestor del sistema basado en la Web

Gestor del sistema basado en la Web es una aplicación cliente-servidor que ofrece al usuario una potente interfaz para gestionar sistema UNIX. Gestor del sistema basado en la Web utiliza su interfaz gráfica para permitir al usuario acceder y gestionar varias máquinas remotas. A continuación se ofrece un ejemplo de una consola de Gestor del sistema basado en la Web:

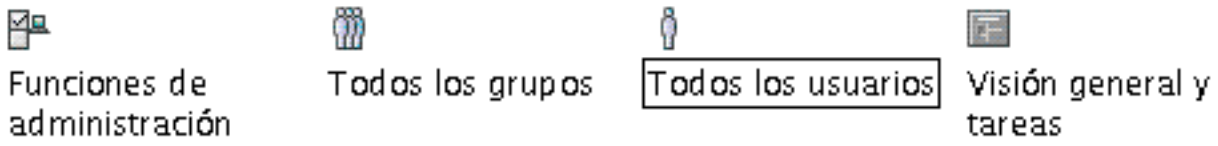


La figura muestra una *Ventana de consola* que contiene dos paneles principales. El panel de la izquierda muestra las máquinas que puede gestionar el usuario desde la Ventana de consola. Este panel recibe el nombre de *Área de navegación*. El panel de la derecha (el *Área de contenido*) muestra resultados basados en el elemento seleccionado en el *Área de navegación*. El usuario selecciona la máquina para realizar operaciones de gestión desde el Área de navegación. A medida que el usuario navega a la operación deseada en el Área de navegación, el Área de contenido se actualiza para mostrar las opciones permitidas.

La siguiente secuencia de pasos ofrece un ejemplo de cómo se puede utilizar Gestor del sistema basado en la Web para modificar las propiedades de un usuario:

1. Desde el Área de contenido, efectúe una doble pulsación en el icono **Usuario** o pulse el icono **Usuarios y grupos** en el Área de navegación.

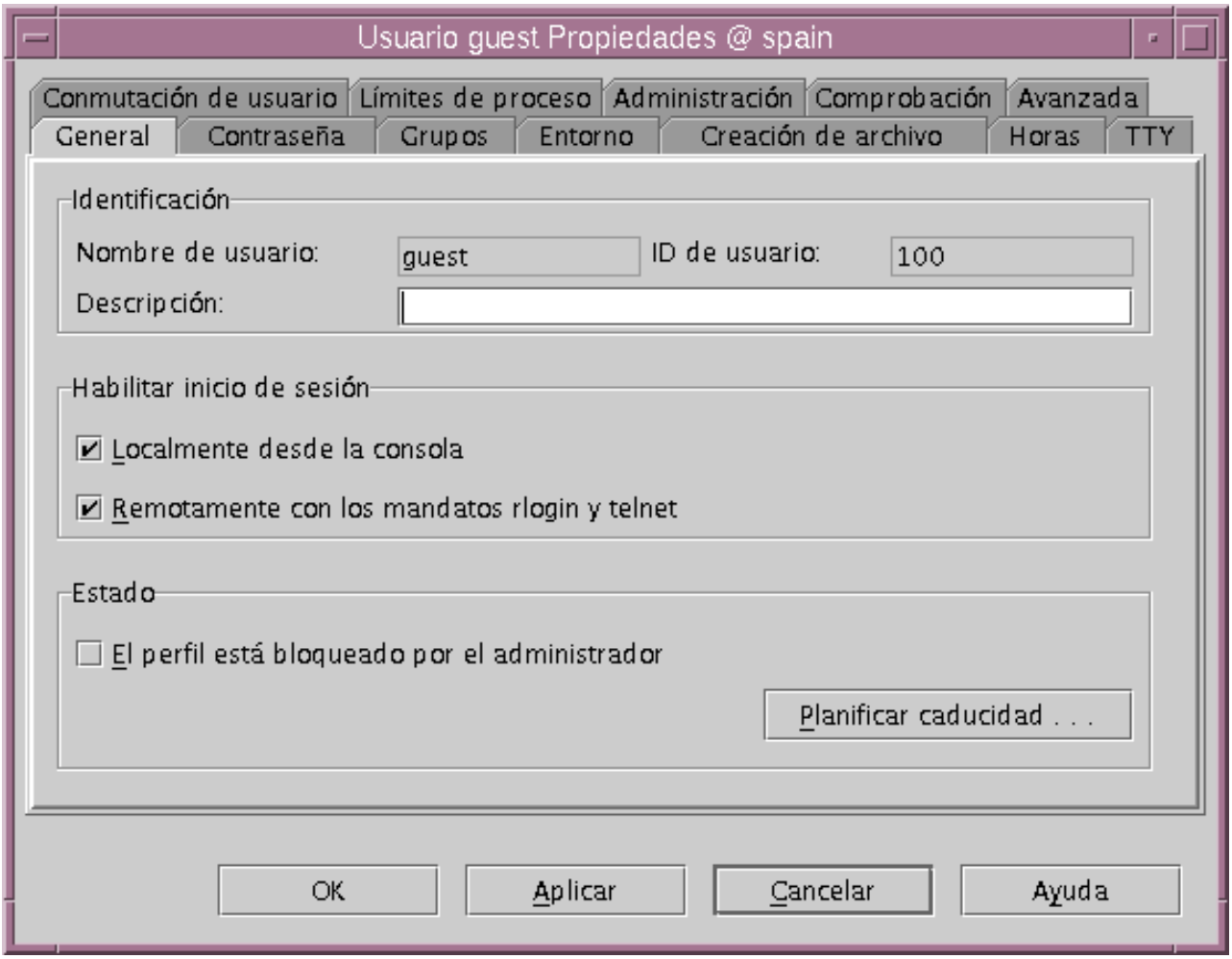
   El Área de contenido ofrecerá un aspecto parecido al siguiente:



2. Efectúe una doble pulsación en el icono **Todos los usuarios**. El Área de contenido ofrecerá un aspecto parecido al siguiente:

Nombre ▲	Descripción	Tipo
adm		Administrador
alex		Básico
bin		Administrador
daemon		Administrador
guest		Básico
imnadm		Básico
invscout		Básico
ipsec		Básico
lp		Básico
lpd		Administrador
lvtuser		Básico
nobody		Administrador

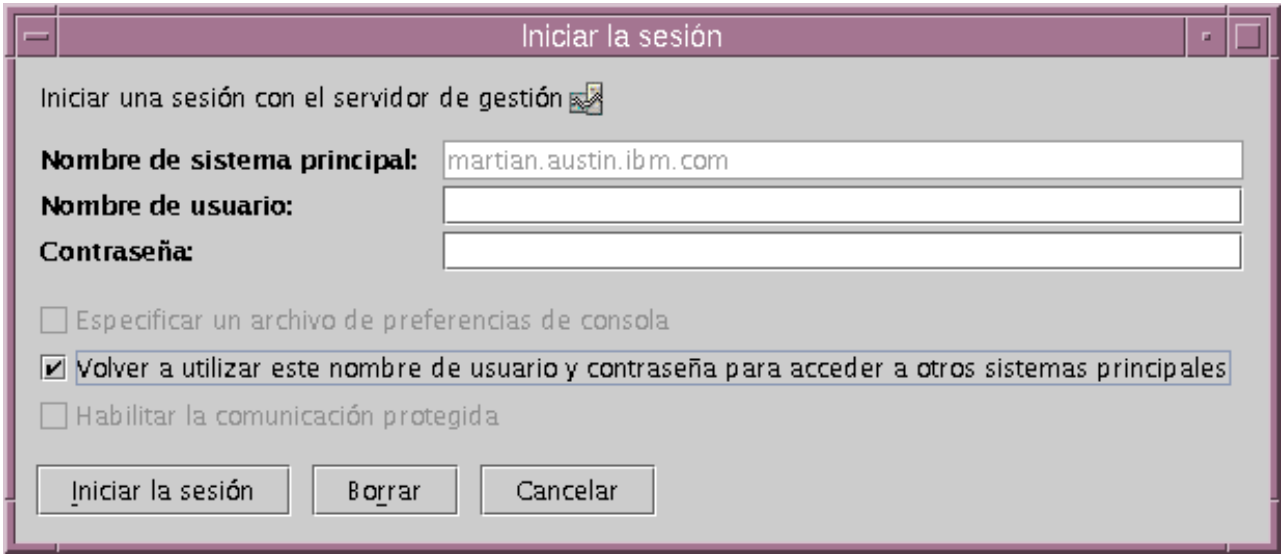
3. Efectúe una doble pulsación en el icono que representa el usuario cuyas propiedades desea modificar. Aparece un diálogo de propiedades parecido al de la siguiente ilustración:



Utilice este diálogo para modificar las propiedades del usuario seleccionado.

4. Para guardar los cambios, pulse el botón **OK**. Para cancelar los cambios, pulse el botón **Cancelar**.

La parte del cliente de la aplicación Gestor del sistema basado en la Web se ejecuta en la *máquina de gestión*. En el ejemplo anterior, no se ha indicado si el usuario modificado era un usuario de la máquina que ejecutaba Gestor del sistema basado en la Web (el cliente) o de la máquina gestionada (un servidor). Para modificar un usuario de una máquina gestionada, seleccione una máquina en el Área de navegación. Si aún no se ha accedido a esta máquina, aparece un diálogo parecido al siguiente:



Utilice este diálogo para iniciar una sesión en la máquina gestionada. Después de iniciar una sesión en una máquina, puede realizar operaciones desde la consola de Gestor del sistema basado en la Web en otra máquina gestionada y volver a la máquina (seleccionándola en el Área de navegación) sin tener que volver a iniciar la sesión.

Cada usuario de Gestor del sistema basado en la Web deseará mantener una máquina *inicial* de Gestor del sistema basado en la Web. Esta máquina *inicial* se debe utilizar como máquina de gestión, aunque el usuario inicie Gestor del sistema basado en la Web desde una máquina que no sea la máquina *inicial*. Esto se debe a que el aspecto inicial de la ventana de consola depende de un archivo de la máquina de gestión. Esto permite a un usuario de Gestor del sistema basado en la Web iniciar Gestor del sistema basado en la Web en la mesa de un colega, especificar una máquina *inicial* personal como la máquina de gestión y crear una ventana de consola con las preferencias guardadas del usuario.

La parte más importante de las preferencias guardadas del usuario puede ser el Entorno de gestión de la máquina. El Entorno de gestión es un potente mecanismo que sirve para definir un grupo de máquinas de las que es responsable un administrador y acceder a las mismas. Cuando un usuario selecciona una máquina del Entorno de gestión, inicia un *servidor de Gestor del sistema basado en la Web* en la máquina seleccionada. Este servidor ofrece al cliente (e indirectamente a la ventana de consola) *objetos remotos gestionados*. La parte del cliente de la aplicación presenta estos objetos remotos gestionados a través de ventanas y otros elementos de la interfaz gráfica de usuario (GUI). Trabajando con estos elementos de la GUI, la parte cliente de la aplicación puede mostrar información sobre objetos de la *máquina gestionada* remota y permitir al usuario actualizar esta información.

Después de que una máquina del Entorno de gestión esté *activa* (para ello hay que seleccionar una máquina en el Entorno de gestión e iniciar una sesión en la máquina), el usuario puede pasar de gestionar una máquina a gestionar otra con una pocas pulsaciones de ratón.

Como resultado, el administrador puede gestionar un gran número de máquinas a través de una potente interfaz.

Modalidades de funcionamiento

Gestor del sistema basado en la Web se puede configurar para que se ejecute en varias modalidades de funcionamiento. Los entornos operativos en los que se puede iniciar Gestor del sistema basado en la Web son *aplicación autónoma*, *cliente-servidor* y *applet*. Estas modalidades de funcionamiento se describen en las siguientes secciones:

Las modalidades de funcionamiento son las siguientes:

- “Modalidad de aplicación autónoma”
- “Modalidad cliente-servidor”
- “Modalidad de applet”
- “Modalidad PC Client” en la página 6

Modalidad de aplicación autónoma

No hace falta ninguna configuración para ejecutar Gestor del sistema basado en la Web en la modalidad de aplicación autónoma. Desde la línea de mandatos, escriba el siguiente mandato:

```
/usr/websm/bin/wsm
```

Para iniciar la Consola de Gestor del sistema basado en la Web desde Common Desktop Environment (CDE), haga lo siguiente:

1. Seleccione el icono **Gestor de aplicaciones** en el panel principal de CDE.
2. Seleccione el icono **Admin_sistema**.
3. Seleccione el icono **Consola de gestión**.

Por omisión, puede realizar tareas de gestión de sistemas en la máquina en la que ha iniciado la consola.

Modalidad cliente-servidor

Puede gestionar su máquina local desde la consola de Gestor del sistema basado en la Web. También puede gestionar máquinas que se han configurado para la gestión remota (consulte el tema “Configuración de Gestor del sistema basado en la Web en modalidad cliente-servidor” en la página 8). Para especificar las máquinas que desea gestionar, añádalas al Entorno de gestión (consulte el “Capítulo 4. Configuración del Entorno de gestión” en la página 29).

También puede seleccionar un sistema principal que no sea su máquina local como *máquina de gestión*. Para ello, utilice el siguiente mandato:

```
/usr/websm/bin/wsm -host [sistema principal máquina gestión]
```

El sistema principal que especifique como [*sistema principal máquina gestión*] se muestra bajo el Área de navegación como el primer nombre de sistema principal bajo la lista de sistemas principales que se pueden gestionar. Este sistema principal también se utiliza para cargar el archivo de preferencias de usuario de Gestor del sistema basado en la Web (**$HOME/WebSM.pref**). Si se utiliza el argumento **-host**, se muestra la consola de la máquina que está utilizando, pero se utiliza el archivo de preferencias del sistema principal remoto que especifique (consulte el tema “Archivos de preferencias” en la página 20).

> **Nota:** Cualquier sistema principal de destino que Gestor del sistema basado en la Web deba gestionar debe tener el servidor de Gestor del sistema basado en la Web instalado y configurado. Consulte el tema “Configuración de Gestor del sistema basado en la Web en modalidad cliente-servidor” en la página 8 para obtener más información.

Modalidad de applet

La modalidad de applet es parecida a utilizar Gestor del sistema basado en la Web en modalidad cliente-servidor cuando se utiliza el argumento **-host**. En modalidad cliente-servidor, se utiliza el siguiente mandato:

```
/usr/websm/bin/wsm -host [máquina de gestión]
```

mientras que en modalidad de applet, el usuario dirige el navegador a

```
http://máquina de gestión/wsm.html
```

En ambos casos, *máquina de gestión* es la máquina que contiene la aplicación Gestor del sistema basado en la Web. La *máquina gestionada* es la primera máquina que se lista en el Entorno de gestión.

Existe una diferencia significativa entre utilizar la modalidad de applet y la de cliente-servidor. En modalidad de applet, sólo se puede gestionar un grupo de máquinas que tengan instalada la misma versión de Gestor del sistema basado en la Web. El motivo es que, en general, las applets están restringidas, por razones de seguridad, a cargar sólo clases Java desde el servidor HTTP que ejecuta la applet. Mientras que las clases Java necesarias para hacer funcionar la consola de Gestor del sistema basado en la Web vienen de la *máquina de gestión*, se utiliza otro grupo de clases Java para realizar tareas en las máquinas gestionadas. Estas clases se deben cargar desde la máquina que se gestiona (que no es la misma que la máquina de gestión) para que estas clases coincidan con el sistema operativo que se gestiona. En modalidad de applet, esta situación no es posible.

Modalidad PC Client

La modalidad PC Client permite al usuario ejecutar la consola de Gestor del sistema basado en la Web en un PC Windows y gestionar sistemas AIX remotos. Este método es parecido a utilizar Gestor del sistema basado en la Web en modalidad cliente-servidor cuando se utiliza el argumento *-host*. Hay varias formas de iniciar PC Client en la plataforma Windows:

- Efectúe una doble pulsación en el icono **PC Client de Gestor del sistema basado en la Web** situado en el escritorio de Windows para abrir el panel de inicio de sesión en el que se entra el sistema principal, nombre de usuario y contraseña.
- Pulse el botón Inicio en la barra de tareas y seleccione **Programas —> Gestor del sistema basado en la Web —> PC Client de Gestor del sistema basado en la Web**.
- Desde un indicador de MS-DOS, ejecute el mandato **wsm.bat** que se encuentra en el directorio bin de PC Client.
- Mediante el Explorador de Windows o Netscape Communicator, efectúe una doble pulsación en el icono **wsm.bat** de la carpeta bin de PC Client.

Al igual que sucede con la modalidad cliente-servidor, los sistemas listados en el área Entorno de gestión son máquinas gestionadas. Sin embargo, PC Client difiere de la modalidad cliente-servidor en que el sistema Windows que ejecuta PC Client es la máquina de gestión y no se muestra en el área Entorno de gestión.

Las cuestiones sobre seguridad son idénticas a las de la modalidad cliente-servidor en lo referente a la carga de clases, en contraste con las limitaciones de la modalidad de applet, en la que sólo se puede gestionar un grupo de máquinas que tengan la misma versión de Gestor del sistema basado en la Web instalada. Para obtener más información sobre seguridad, consulte el “Capítulo 5. Seguridad de Gestor del sistema basado en la Web” en la página 33.

Para obtener más información, consulte los temas “Modalidad cliente-servidor” en la página 5 y “Modalidad de applet” en la página 5.

Aplicaciones de personalización

Puede utilizar las Herramientas de personalización para añadir mandatos y aplicaciones existentes disponibles en el sistema AIX al entorno de Gestor del sistema basado en la Web, para que luego se puedan ejecutar directamente desde la Ventana de consola.

Si desea más integración de la que ofrece la aplicación Herramientas de personalización, puede ampliar la potencia de Gestor del sistema basado en la Web escribiendo aplicaciones de personalización. Para escribir aplicaciones de personalización hay que conocer el lenguaje de programación Java. Si su organización está interesada en este tema, póngase en contacto con el representante de ventas.

Capítulo 2. Requisitos de la instalación y del sistema

Los temas siguientes ofrecen información sobre la instalación de Gestor del sistema basado en la Web:

Requisitos mínimos recomendados del sistema

Para poder utilizar Gestor del sistema basado en la Web se necesita que el sistema cliente tenga al menos las siguientes características:

- Sistema operativo base AIX 5.1 (incluido Java 1.3.0.0)
- Pantalla gráfica conectada
- 50 MB de espacio libre en disco
- 256 MB de memoria
- 300 MHz de CPU

Si utiliza un PC para ejecutar Gestor del sistema basado en la Web en modalidad de applet, debe tener una velocidad de procesador de al menos 500 MHz.

Si utiliza un PC para ejecutar Gestor del sistema basado en la Web en modalidad PC Client, consulte "Requisitos mínimos recomendados para PC Client" en la página 10 para ver los requisitos adicionales.

Aunque no es absolutamente necesario disponer de un sistema que cumpla estos requisitos de memoria y velocidad de procesador, el rendimiento puede disminuir significativamente en máquinas de menor potencia. Pero los requisitos mínimos del sistema expuestos anteriormente se aplican principalmente al sistema cliente. Si el sistema cliente no cumple con los requisitos mínimos recomendados del sistema, puede disminuir el rendimiento.

Puesto que en las máquinas servidor no se muestran gráficos al usuario, no es imprescindible que cumplan con los requisitos mínimos recomendados del sistema. Para obtener detalles, consulte el tema "Modalidades de funcionamiento" en la página 4.

En las modalidades de applet y cliente-servidor, la máquina cliente no es necesariamente la máquina en la que ve la consola de Gestor del sistema basado en la Web.

No se recomienda utilizar Gestor del sistema basado en la Web con emuladores de X (como los que se utilizan en un PC). El rendimiento con estos emuladores no es satisfactorio.

Instalación de Gestor del sistema basado en la Web

Para poder utilizar Gestor del sistema basado en la Web, se debe instalar en el cliente utilizado para ejecutarlo y en las máquinas gestionadas. Si tiene AIX 5.1 o posterior instalado en la máquina, es posible que ya tenga Gestor del sistema basado en la Web instalado.

Para comprobarlo, entre lo siguiente:

```
lslpp -h sysmgt.websm.framework
```

Si Gestor del sistema basado en la Web no está instalado, verá un mensaje parecido al siguiente:

```
lslpp: Archivo sysmgt.websm.framework no instalado.
```

Si Gestor del sistema basado en la Web está instalado, verá algo parecido a lo siguiente:

```
Archivo         Nivel     Acción       Estado       Fecha        Hora
----------------------------------------------------------------------------
Vía: /usr/lib/objrepos
  sysmgt.websm.framework
                5.1.0.0     COMPROMETER  COMPLETAR    03/09/01     17:30:14

Vía: /etc/objrepos
  sysmgt.websm.framework
                5.1.0.0     COMPROMETER  COMPLETAR    03/09/01     17:35:31
```

Si no tiene el archivo **sysmgt.websm.framework** instalado, utilice las herramientas de instalación del sistema operativo. Para acceder a las herramientas de instalación, utilice el siguiente mandato (suponiendo que el CD de AIX 5.1 esté cargado en la unidad de CD):

```
/usr/lib/instl/sm_inst installp_cmd -a \
-d /dev/cd0 -f sysmgt.websm.framework  -c -N -g -X
```

Esta acción instala el grupo de imágenes necesario para ejecutar Gestor del sistema basado en la Web.

Configuración de Gestor del sistema basado en la Web en modalidad cliente-servidor

En modalidad cliente-servidor (consulte el tema “Modalidades de funcionamiento” en la página 4), el cliente de Gestor del sistema basado en la Web solicita servicios de servidor a una máquina gestionada a través del puerto de inetd 9090. La modalidad cliente-servidor tiene que estar habilitada en los servidores que se van a gestionar como máquinas remotas. Puede habilitar e inhabilitar una máquina para que actúe como Servidor de Gestor del sistema basado en la Web mediante el mandato **wsmserver** (consulte el tema “Herramientas de línea de mandatos” en la página 22) del modo siguiente:

```
/usr/websm/bin/wsmserver -enable
```

Nota: La modalidad cliente-servidor *no* está habilitada por omisión.

Para inhabilitar una máquina para que no se pueda gestionar desde un cliente de Gestor del sistema basado en la Web, ejecute el siguiente mandato:

```
/usr/websm/bin/wsmserver -disable
```

Si tiene que utilizar un número de puerto que no sea 9090, puede definir un número de puerto alternativo en el archivo **/etc/services**. Si lo hace, debe utilizar el argumento **-port** con el mandato **wsm** (consulte el tema “Herramientas de línea de mandatos” en la página 22).

Archivos opcionales disponibles con Gestor del sistema basado en la Web

Los siguientes archivos opcionales se pueden instalar para añadir funciones adicionales a Gestor del sistema basado en la Web:

sysmgt.websm.accessibility
: Añade soporte para usuarios con problemas de visión mediante tecnología de habla simulada. Se necesita el Self Voicing Kit (SVK) para utilizar la tecnología de habla simulada con Gestor del sistema basado en la Web. Si se instala el SVK en la máquina, este archivo permite que SVK

funcione con Gestor del sistema basado en la Web. Para obtener más información sobre cómo obtener, instalar y configurar el SVK, vaya a:
http://www.alphaworks.ibm.com/tech/svk

sysmgt.msg.*Idioma del entorno nacional*.websm.apps
Permite utilizar el idioma de su entorno nacional si la variable de entorno **LANG** está definida o si se utiliza el argumento *-lang* con el mandato **wsm**.

sysmgt.websm.security
Añade soporte para la comunicación Secure Socket Layer entre cliente y servidor. Da soporte al cifrado de 40 bits. Disponible en Expansion Pack.

sysmgt.websm.security-us
Añade soporte para la comunicación Secure Socket Layer entre cliente y servidor. Da soporte al cifrado de 128 bits. Disponible en Expansion Pack. Puede que las leyes de exportación e importación impidan la disponibilidad de este archivo en algunos países.

Los archivos de la tabla anterior no se instalan por omisión como parte del sistema operativo base (AIX 5.1). Sin embargo, se pueden instalar de forma similar a la descrita anteriormente para instalar las imágenes principales de Gestor del sistema basado en la Web. Los archivos **sysmgt.websm.security** y **sysmgt.websm.security-us** están disponibles en el CD de Expansion Pack. Desde el soporte que contiene el archivo, utilice el siguiente mandato:

```
/usr/lib/instl/sm_inst installp_cmd -a -d /dev/cd0 \
-f archivo_que_desea_instalar -c -N -g -X
```

Requisitos de la instalación para dar soporte a la modalidad de applet

Además de la modalidad de aplicación estándar de Gestor del sistema basado en la Web, necesita el archivo **sysmgt.websm.webaccess** para dar soporte a la modalidad de applet. Este archivo se instala automáticamente con el sistema operativo base.

La máquina que se va a utilizar como **máquina de gestión** se debe configurar como un Servidor HTTP. Esto se puede realizar instalando y configurando el Servidor HTTP que elija. El Servidor HTTP de IBM está disponible en el Expansion Pack de AIX 5.1. Utilice el mandato **/usr/websm/bin/configassist** para configurar automáticamente el Servidor HTTP.

La tabla siguiente identifica los requisitos para utilizar Gestor del sistema basado en la Web en modalidad de applet con varios navegadores:

Plataforma	Navegador	Requisitos
PC	Netscape Communicator	• Versión 4.7 ó 4.7x de Netscape Communicator. (No se da soporte a Netscape Communicator 6.0.) • El conector 1.3 Java debe estar instalado.
PC	Internet Explorer	• El sistema operativo debe ser Windows 98 (o posterior) o Windows NT 4.0 (o posterior). • Versión 5.0 (o posterior) de Internet Explorer. • El conector 1.3 Java debe estar instalado.

Nota: La modalidad de applet no recibe soporte en la plataforma basada en POWER. Consulte “Modalidades de funcionamiento” en la página 4 para ver cómo gestionar máquinas basadas en POWER.

Para configurar un servidor para la modalidad de applet, siga los pasos siguientes:

1. Instale un Servidor HTTP en la máquina en la que reside Gestor del sistema basado en la Web. El servidor Web recomendado es el Servidor HTTP de IBM. Consulte la documentación correspondiente a cada producto para ver cómo instalar y configurar el Servidor HTTP.
2. Cuando el Servidor HTTP se esté ejecutando, puede configurar Gestor del sistema basado en la Web para que se ejecute desde áquel con el siguiente mandato:

   ```
   /usr/websm/bin/configassist
   ```
3. En el Asistente para la configuración, continúe hasta llegar al panel principal.
4. Seleccione **Configurar un servidor Web para ejecutar Gestor del sistema basado en la Web en un navegador**.
5. Seleccione **Siguiente**.
6. Siga las instrucciones de los siguientes paneles para terminar las configuraciones.

Configuración del cliente (navegador)

A continuación se muestran los requisitos para el cliente:

- Netscape Communicator 4.7 ó 4.7x (no se da soporte a Netscape Communicator 6.0) o Internet Explorer 5.0.
- El conector Java 1.3

Si utiliza Internet Explorer como navegador, se le solicitará que baje el conector automáticamente. Si pulsa **sí**, el conector se baja y se ejecuta su script de instalación. Si pulsa **no**, se sale de Gestor del sistema basado en la Web.

Si utiliza Netscape Communicator como navegador, es posible que no localice el conector de Java correcto. Si esto sucede, puede bajarlo e instalarlo de forma manual.

Instalación de PC Client de Gestor del sistema basado en la Web

Los temas siguientes contienen información sobre cómo instalar PC Client de Gestor del sistema basado en la Web:

- “Requisitos mínimos recomendados para PC Client”
- “Requisitos de instalación para dar soporte a la modalidad PC Client”

Requisitos mínimos recomendados para PC Client

Si va a utilizar un PC para ejecutar Gestor del sistema basado en la Web en modalidad PC Client,

- 60 MB de espacio libre en disco en la unidad por omisión para su uso temporal durante el procedimiento de instalación
- 50 MB de espacio libre en disco en la unidad que piensa utilizar para instalar PC Client de Gestor del sistema basado en la Web
- Velocidad de procesador de PC de al menos 500 MHz
- 256 MB de memoria

Requisitos de instalación para dar soporte a la modalidad PC Client

Para instalar PC Client de Gestor del sistema basado en la Web a través de una red, debe tener el archivo **sysmgt.websm.webaccess** instalado en al menos un sistema AIX. Este archivo se instala automáticamente con el sistema operativo base.

La máquina utilizada para instalar PC Client de Gestor del sistema basado en la Web se debe configurar como un Servidor HTTP. Esto se realiza instalando y configurando el Servidor HTTP que elija. El Servidor HTTP de IBM está disponible en el Expansion Pack de AIX 5.1. Utilice el mandato **/usr/websm/bin/configassist** para configurar automáticamente el Servidor HTTP.

La tabla siguiente identifica los requisitos para instalar PC Client de Gestor del sistema basado en la Web en una plataforma PC:

Netscape Communicator	• Versión 4.7 ó 4.7x de Netscape Communicator. • No se da soporte a Netscape Communicator 6.0.
Internet Explorer	• Versión 5.0 o posterior de Internet Explorer.

Configuración de un servidor de AIX para la instalación de PC Client

Siga los pasos siguientes para configurar un servidor de AIX para la instalación de PC Client de Gestor del sistema basado en la Web:

1. Instale un Servidor HTTP en el servidor en el que reside Gestor del sistema basado en la Web. El servidor Web recomendado es el Servidor HTTP de IBM. Consulte la documentación correspondiente a cada producto para ver cómo instalar y configurar el Servidor HTTP.
2. Cuando el Servidor HTTP se esté ejecutando, ejecute el mandato siguiente para configurar Gestor del sistema basado en la Web:
   `/usr/websm/bin/configassist`
3. En el Asistente para la configuración, continúe hasta llegar al panel principal.
4. Seleccione **Configurar un servidor Web para ejecutar Gestor del sistema basado en la Web en un navegador**.
5. Seleccione **Siguiente**.
6. Siga las instrucciones de los siguientes paneles para terminar las configuraciones.

Instalación de PC Client de Gestor del sistema basado en la Web en el sistema Windows

1. Desinstale cualquier versión anterior de PC Client de Gestor del sistema basado en la Web. Para obtener más información, consulte el tema “Desinstalación de PC Client de Gestor del sistema basado en la Web de un sistema Windows”.
2. Entre la siguiente dirección Web en el navegador Web del PC:
   *nombre sistema principal***/pc_client/pc_client.html**, donde *nombre sistema principal* es el nombre del servidor de AIX configurado para la instalación de PC Client de Gestor del sistema basado en la Web.
3. Pulse **Continuar** en la ventana de aviso para instalar.
4. En Internet Explorer, aparece un aviso de seguridad que le solicita permiso para instalar temporalmente y ejecutar un archivo JVM de Java. Seleccione **SÍ** para completar la instalación. En Netscape Communicator, aparecen dos mensajes de seguridad de Java; debe seleccionar **Otorgar** para ambos para completar la instalación.
5. Cuando aparezca el panel **Programa de instalación de PC Client**, pulse **Siguiente** para continuar.
6. Para instalar utilizando la ubicación por omisión, pulse **Siguiente**; de lo contrario, entre la ubicación deseada y pulse **Siguiente**.
7. Aparecerá un panel de confirmación que le muestra la ubicación de instalación, el paquete que se va a instalar y el tamaño aproximado del paquete de instalación. Pulse **Siguiente** para comenzar la instalación.
8. Aparece un panel de estado que muestra que la instalación se ha completado satisfactoriamente o mensajes si se han producido errores durante la instalación. Pulse **Finalizar** para cerrar el panel.

Desinstalación de PC Client de Gestor del sistema basado en la Web de un sistema Windows

1. En la barra de tareas, seleccione **Inicio —> Configuración —> Panel de control**.
2. En el **Panel de control**, efectúe una doble pulsación en el icono **Agregar o quitar programas**.

3. Seleccione **PC Client de Gestor del sistema basado en la Web** en la lista de programas de la pestaña **Instalar o desinstalar** y luego pulse el botón **Agregar o quitar** para iniciar el Asistente para desinstalar.
4. Pulse **Siguiente** en el panel inicial.
5. Pulse **Siguiente** en el panel de confirmación para desinstalar PC Client.
6. Aparece un panel de estado que muestra que la instalación se ha completado satisfactoriamente o mensajes si se han producido errores durante la instalación. Pulse **Finalizar** para cerrar el panel.

Requisitos de instalación para el soporte de Secure Socket Layer

Para que Gestor del sistema basado en la Web funcione en una modalidad segura (mediante zócalos SSL que cifran los datos que se transmiten por la red), se debe instalar y configurar el archivo **sysmgt.websm.security** en las máquinas cliente y servidor.

Para el cifrado de 128 bits de los datos que se envían por la red, se debe instalar el archivo **sysmgt.websm.security-us** además del archivo **sysmgt.websm.security**. Encontrará información detallada sobre la configuración en el “Capítulo 5. Seguridad de Gestor del sistema basado en la Web” en la página 33.

Integración de Gestor del sistema basado en la Web en la Consola de gestión de Tivoli Netview

Si utiliza Tivoli NetView para AIX, puede integrar Gestor del sistema basado en la Web en la consola. Esta integración permite que los sistemas servidor de AIX que aparecen en la consola de NetView se gestionen mediante Gestor del sistema basado en la Web.

Para integrar Gestor del sistema basado en la Web en Tivoli NetView, ejecute el siguiente mandato escribiendo:

```
/usr/websm/bin/install_nv6k
```

Nota: Debe tener Tivoli NetView instalado y funcionando correctamente para poder ejecutar este mandato.

Para eliminar Gestor del sistema basado en la Web de Tivoli NetView, ejecute el siguiente mandato escribiendo:

```
/usr/websm/bin/remove_nv6k
```

Capítulo 3. Utilización de Gestor del sistema basado en la Web

Puede acceder a la consola de Gestor del sistema basado en la Web desde cualquier sistema que esté conectado localmente a la consola y esté ejecutando un escritorio gráfico. Siga uno de los siguientes métodos para iniciar la consola de Gestor del sistema basado en la Web:

- Efectúe una doble pulsación en el icono **Consola de gestión** de Common Desktop Environment (CDE). Seleccione el icono **Gestor de aplicaciones** en el panel principal de CDE y luego abra la carpeta **Admin_sistema**. El icono **Consola de gestión** se encuentra en esta carpeta.
- Escriba `wsm` en una ventana de terminal.
- Si se ha configurado un sistema principal con un Servidor HTTP, se puede acceder al mismo de forma remota desde cualquier sistema que pueda ejecutar Internet Explorer de Microsoft o Netscape Communicator con el conector de Java. Para acceder a la consola desde un navegador, entre la dirección Web del sistema: (***nombre sistema principal***/wsm.html).

La consola contiene cinco elementos distintos, consistentes en:

Área de navegación

El *Área de navegación* muestra una jerarquía de iconos que representan grupos de sistemas, sistemas individuales, recursos gestionados y tareas. Cada icono del Área de navegación identifica un *conector*. En el punto superior, o raíz del árbol, se encuentra el *Entorno de gestión*. El conector Entorno de gestión contiene uno o más conectores de sistemas principales gestionados por la consola. Cada conector del sistema contiene varios conectores de aplicaciones que contienen objetos gestionados, tareas y acciones correspondientes al grupo relacionado de entidades del sistema y recursos.

Cuando pulsa en un icono de conector en el Área de navegación, se abre para mostrar su contenido en el Área de contenido. Los iconos del Área de navegación que vienen precedidos de un símbolo de expansión (signo más o '+') representan conectores que contienen otros conectores. Cuando el símbolo de expansión está en estado cerrado (signo menos o '-'), cuando se pulsa una sola vez el icono, el conector muestra sus conectores de nivel inferior en el Área de contenido, pero no amplía la rama del Área de navegación representada por el símbolo de expansión. Cuando se pulsa una sola vez el símbolo de expansión, se amplía la rama del Área de navegación, mostrando los conectores de nivel inferior, pero no se actualiza el Área de contenido. Al efectuar una doble pulsación en un icono del Área de navegación, la rama de navegación se amplía y el área de contenido se actualiza para mostrar los conectores de nivel inferior.

Puede ajustar la anchura del Área de navegación con respecto al Área de contenido pulsando y arrastrando la barra del Área de navegación hacia la derecha o hacia la izquierda. Si tiene que maximizar el espacio disponible para el Área de contenido dentro de la consola, puede cerrar por completo el área de navegación arrastrando la banda hacia la izquierda todo lo que pueda. Si pulsa una vez la banda, el Área de navegación también se cierra y si la vuelve a pulsar se abre en su posición anterior.

Área de contenido

El área de contenido muestra el contenido de un conector. Hay tres tipos de conectores principales definidos por lo que se presenta en el área de contenido:

- “Contenedores”
- “Visiones generales” en la página 16
- “Ejecutadores” en la página 16

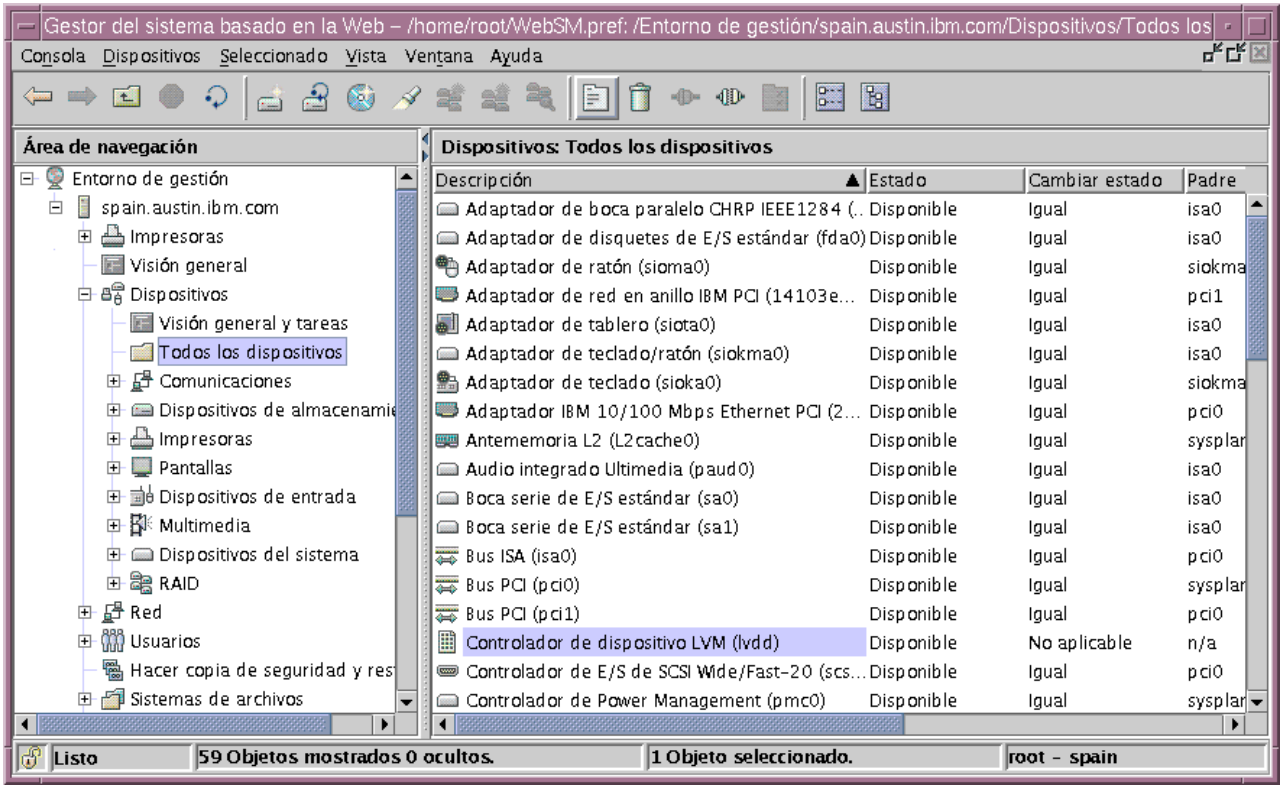
Contenedores

Los contenedores o *conectores de contenedor* albergan otros conectores, iconos que representan recursos del sistema (*objetos gestionados*) o una combinación de objetos gestionados y conectores. Los contenedores constituyen el tipo más común de conector de la interfaz de usuario de Gestor del sistema basado en la Web. Puede considerarlos como carpetas que albergan otras carpetas u objetos de información.

Los contenedores le permiten ver propiedades así como crear, suprimir o realizar otras acciones sobre recursos del sistema. Presentan objetos de recursos en una o más *vistas*. Gestor del sistema basado en la Web da soporte a las siguientes vistas:

- Icono grande
- Icono pequeño
- Detalles
- Árbol
- Detalles en árbol

La siguiente ilustración es un ejemplo de la vista Detalles de consola:



Las vistas Icono grande, Icono pequeño y Detalles le permiten decidir qué objetos desea ver en la vista *filtrando* la vista. El hecho de filtrar la vista puede resultar útil si un contenedor tiene gran cantidad de objetos y sólo desea ver determinados objetos o tipos de objetos. Por ejemplo, si está gestionando usuarios, es posible que sólo desee ver usuarios administrativos.

Las vistas Icono grande, Icono pequeño y Detalles también le permiten cambiar el orden en el que se listan los objetos en la vista clasificándolos. Puede clasificar objetos según distintos atributos (o *propiedades*) del objeto.

Puede clasificar de dos formas:

- **Vista de iconos**

  Puede clasificar los objetos seleccionando el menú **Vista** y luego **Organizar iconos**. Verá una lista de opciones de menú correspondientes a propiedades por las que puede clasificar la vista.
- **Vista de detalles**

  Puede clasificar objetos pulsando la cabecera de columna que define un atributo según el que desea clasificar. La cabecera de columna cambia entre clasificaciones ascendentes y descendentes tras cada pulsación.

  La vista de detalles también le permite cambiar el orden de las columnas y la anchura de las columnas individuales. Para cambiar la posición de una columna, arrastre la cabecera de la columna a la posición deseada (la cabecera de columna que se encuentra más a la izquierda, que suele ser el nombre de los objetos, no se puede mover). Para cambiar la anchura de una columna, arrastre la línea que divide dos cabeceras de columna hacia la derecha o hacia la izquierda.

En Gestor del sistema basado en la Web, los iconos se suelen utilizar para indicar el estado de un objeto gestionado. La tabla siguiente muestra algunos convenios que se utilizan para indicar condiciones o estados habituales:

Condición o estado	Aspecto	Iconos de ejemplo	Significado
Objeto normal, activo	Icono lleno	  	Cuenta de usuario activa Volumen lógico (en línea) Proceso activo
Objeto inactivo, no configurado, incompleto	Contorno de objeto sin relleno	  	Cuenta de usuario caducada Volumen lógico (fuera de línea) Proceso inactivo
Falta objeto	Contorno de objeto punteado		Proceso defunct (zombie)
Procesando - el objeto se está actualizando	Indicador de reloj		Actualizando
Problema con objeto	Indicador de alerta		Aviso
Problema grave con objeto - se necesita atención inmediata	Indicador de problema grave		Problema grave

Visiones generales

Los conectores de visión general, que son interfaces parecidas a una página Web que se muestran en el área de contenido, hacen lo siguiente:

- Explican la función suministrada por uno o más conectores que forman una aplicación.
- Ofrecen acceso fácil a tareas rutinarias o *de iniciación*
- Resumen el estado de los recursos clave gestionados por la aplicación

Puesto que las visiones generales no muestran objetos, pueden ofrecer un acceso más rápido y sencillo a las tareas que se realizan con frecuencia. Las visiones generales también se utilizan cuando una función de gestión se basa puramente en tareas y no necesita iconos que representen recursos del sistema (por ejemplo, copia de seguridad y restauración).

Ejecutadores

Los conectores de ejecución se parecen a las visiones generales. Son paneles parecidos a una página Web que describen y ofrecen un punto de ejecución para aplicaciones que ejecutan su propia ventana fuera de la consola de Gestor del sistema basado en la Web.

Acciones de menús y de la barra de herramientas

La barra de menús de la consola ofrece todas las operaciones que se realizan en la consola y en objetos gestionados. Los menús están organizados del siguiente modo:

Menú Consola

El Menú Consola contiene opciones que controlan la consola. Le permite añadir y eliminar sistemas del entorno de gestión, guardar preferencias de consola, especificar si se debe intentar automáticamente iniciar una sesión en un sistema principal con una contraseña guardada, ver el registro de la sesión de consola y salir de la consola (consulte el tema “Archivos de preferencias” en la página 20).

Menú *Objeto*

El título del Menú *Objeto* cambia para indicar el tipo de recurso gestionado por el conector actual. Por ejemplo, cuando se selecciona el conector que gestiona dispositivos de hardware, el título del Menú Objeto pasa a ser *Dispositivos*. El Menú Objeto contiene opciones generales y acciones para un conector que no requieren la selección de objetos específicos sobre los que actuar. Normalmente, las acciones para crear nuevos objetos de recursos están en el Menú Objeto. La función **buscar** también se encuentra en el Menú Objeto. El contenido del Menú Objeto se actualiza cuando se selecciona un nuevo conector.

Menú Seleccionado

El Menú Seleccionado contiene las acciones correspondientes a un conector que necesitan que el usuario seleccione los objetos gestionados sobre los que se aplicará la acción, como por ejemplo *Abrir*, *Propiedades*, *Copiar*, *Suprimir* o *Iniciar*. El contenido del Menú Seleccionado se actualiza cuando se selecciona un nuevo conector. Se inhabilita cuando se cargan los conectores Visión general y Ejecutar.

Menú Ver

El Menú Ver contiene opciones para navegar, como por ejemplo *Retroceder*, *Avanzar* y *Subir un nivel*. También incluye opciones para personalizar la consola en el submenú *Mostrar*. Por ejemplo, puede seleccionar entre mostrar u ocultar la barra de herramientas y la barra de estado. Cuando se cargan conectores de contenedor, el Menú Ver incluye opciones que controlan el modo en que se presentan los objetos. Por ejemplo, si el conector ofrece distintas opciones de vistas, como *Icono grande*, *Icono pequeño*, *Detalles* y *Árbol*, estas opciones se listan aquí. Si el conector sólo da soporte a una vista, no se lista ninguna opción de vista. Cuando un conector muestra un icono o vista de *Detalles*, el Menú Ver incluye opciones para clasificar y filtrar el contenedor.

Menú Ventana

El Menú Ventana contiene acciones para gestionar subventanas en el espacio de trabajo de la

consola. *Ventana nueva* crea una nueva subventana de consola en el espacio de trabajo. Otras opciones controlan el modo en que se presentan todas las subventanas de consola. Por ejemplo, puede elegir entre hacer que las ventanas cubran por completo el espacio de trabajo como mosaicos o tenerlas organizadas en cascada.

Menú Ayuda
El Menú Ayuda contiene opciones de ayuda al usuario. Cuando el sistema que está actuando como servidor de gestión de sistemas está correctamente configurado con un Servidor HTTP para que actúe como *Servidor de documentación*, se puede acceder a gran cantidad de información en línea mediante un navegador Web. Las distintas opciones le permiten ver el contenido de la ayuda, buscar ayuda sobre un tema determinado y ver información de ayuda sobre teclas de atajo.

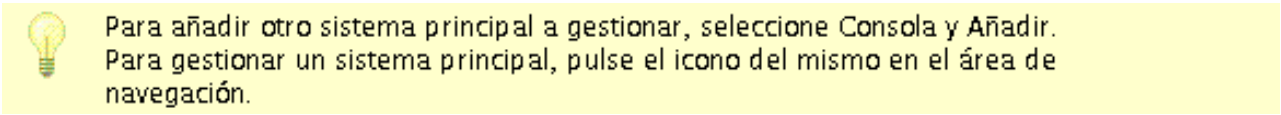
Menús emergentes
Los menús emergentes (a veces denominados *menús de contexto*) ofrecen un modo rápido de acceder a opciones de menús. Para utilizar menús emergentes con un ratón, apunte a un objeto y pulse el botón derecho de un ratón de dos o de tres botones. El menú emergente contiene las acciones halladas en los menús Seleccionado y Objeto correspondientes al objeto u objetos actuales.

Barra de herramientas
La barra de herramientas contiene acciones que se utilizan con frecuencia y que están disponibles cuando el conector actual está cargado. Incluye controles de navegación y las opciones Buscar y Ver (si están disponibles). La barra de herramientas también ofrece una ayuda de sugerencias de la herramienta cuando el puntero del ratón permanece sobre un icono de la barra de herramientas durante unos segundos.

Área de sugerencias

El Área de sugerencias ofrece respuestas rápidas a preguntas frecuentes. Una *sugerencia* puede ser una simple instrucción de una línea, como por ejemplo ″Para añadir otro sistema principal a gestionar, seleccione Consola y luego Añadir″. Pero normalmente las sugerencias están en formato de enlaces de hipertexto. Si la ayuda basada en el navegador está correctamente configurada, al pulsar una sugerencia de hipertexto se abre el navegador Web por omisión en el tema descrito en el enlace. Puede elegir entre visualizar u ocultar la Barra de sugerencias marcando o eliminando la marca de la opción Área de sugerencias del submenú Mostrar bajo *Ver*.

La siguiente ilustración es un ejemplo de una sugerencia.



Barra de estado

La *barra de estado* se muestra en el borde inferior de una ventana de consola. Tiene cinco campos para mostrar información de estado, del modo siguiente:

- Un icono de **candado** indica si la consola se está ejecutando en modalidad *segura*. En modalidad segura, las comunicaciones entre la plataforma cliente que está ejecutando la consola y el sistema gestionado se cifran mediante SSL. El icono de **candado** está cerrado en modalidad segura y abierto cuando no está activa la modalidad de comunicaciones seguras.
- Estado de carga de conector. Cuando un conector está cargado, se muestra el texto `Listo`. Cuando se está cargando un conector, aparece una barra de progreso.
- Número de objetos visibles en el área de contenido. Los objetos pueden estar presentes en el sistema principal gestionado pero ocultos de la vista debido a un filtro de la vista.

- Número de objetos seleccionados en el área de contenido.
- Contexto de seguridad (nombre de usuario y nombre de sistema principal) en el que está el administrador para el conector actualmente activo.

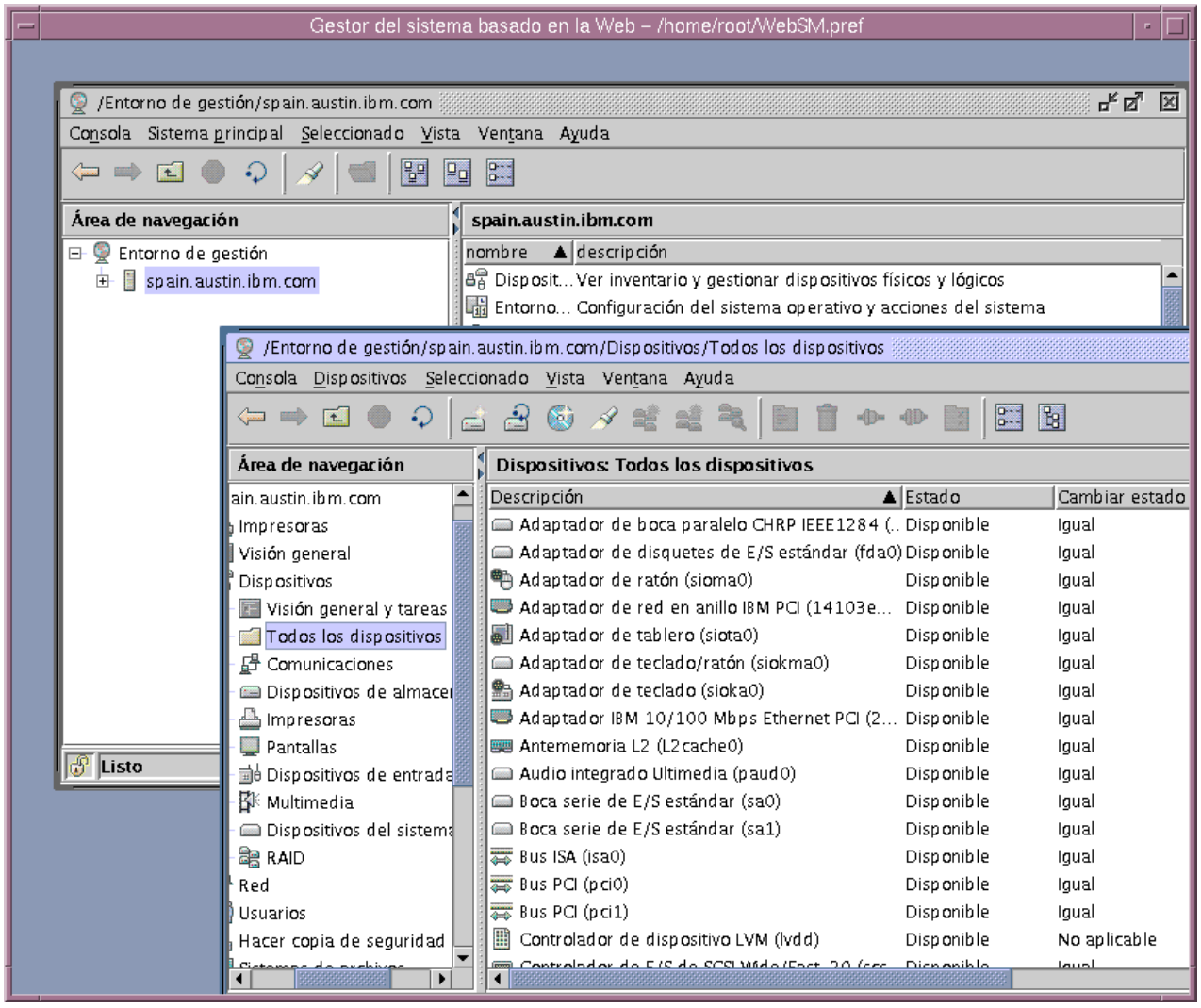
La barra de estado se puede ocultar o mostrar seleccionando o deseleccinando la opción **Barra de estado** en el submenú Mostrar bajo Ver.

Espacio de trabajo de consola

La consola de Gestor del sistema basado en la Web tiene una Interfaz de múltiples documentos (MDI) que permite al usuario presentar diferentes perspectivas en el Entorno de gestión. Una MDI se puede definir para que muestre varias subventanas, denominadas *documentos*, dentro del marco externo de la ventana, denominado *espacio de trabajo*. Por omisión, cuando se abre la consola se muestra una sola ventana de documento en estado maximizado. Para crear varias vistas del Entorno de gestión, primero tiene que reducir el tamaño de la ventana de documento utilizando los controles de gestión de ventanas de la parte derecha de la barra de herramientas.

El símbolo del centro reduce el tamaño de la ventana de documento. El símbolo situado más a la izquierda minimiza la ventana dentro de la consola externa. Puede crear una segunda ventana de documento seleccionando la opción **Ventana nueva** en el Menú Ventana.

Puede navegar de forma independiente a distintas ubicaciones dentro de cada ventana de documento. De este modo, puede comparar fácilmente valores de configuración de distintos recursos en distintos sistemas principales. El siguiente diagrama ilustra este proceso.



El Menú Ventana de cada ventana interna ofrece opciones de menú para gestionar varias ventanas del espacio de trabajo. La tabla siguiente resume estas opciones.

Opción de menú	Función
Ventana nueva	Crea una nueva replica de la ventana interna del espacio de trabajo.
Cascada	Organiza las ventanas internas en una pila.
Mosaico horizontal	Organiza las ventanas internas de forma que llenen por completo el espacio de trabajo de izquierda a derecha.
Mosaico vertical	Organiza las ventanas internas de forma que llenen por completo el espacio de trabajo de arriba a abajo.
Minimizar otras ventanas	Minimiza todas las ventanas internas excepto la ventana que tiene actualmente el foco (la ventana desde la que se ha elegido esta opción de menú).
Restaurar todo	Restaura todas las ventanas minimizadas a su tamaño y posición anteriores.
1. /Entorno de gestión/	Lista de las ventanas internas actuales. Al seleccionar una ventana de esta lista, se abre (si estaba minimizada), se coloca la primera y adquiere el foco.

Archivos de preferencias

El archivo de **preferencias** sirve para controlar las siguientes funciones de Gestor del sistema basado en la Web:

- Formatear una ventana hija en la ventana de consola de modo que sólo se muestren los componentes especificados por el usuario
- Configurar preferencias de vista, filtro y clasificación especificadas por el usuario
- Ofrecer un mecanismo para gestionar distintos dominios de máquinas

Cuando se inicia Gestor del sistema basado en la Web, el archivo de preferencias que se elige muestra la sesión utilizando las preferencias almacenadas cuando se guardó por última vez. Esto incluye preferencias como el formato de la ventana de consola y las máquinas que se gestionan. Por omisión, el archivo de preferencias se guarda en:

```
$HOME/WebSM.pref
```

donde $HOME es el directorio inicial del usuario en la máquina de gestión.

Para guardar el estado de la consola, utilice la opción de menú **Consola -> Guardar**.

El estado de la consola también se puede guardar en otros archivos de preferencias. Para guardar el estado de la consola en un archivo que no sea el archivo por omisión, utilice la opción de menú **Consola -> Guardar como...** para visualizar un diálogo en el que puede especificar un nombre de vía de acceso alternativo.

Para utilizar un archivo de preferencias que no sea el archivo por omisión, consulte el tema “Modalidades de funcionamiento” en la página 4.

Una ventana hija dentro de la ventana de consola correspondiente a Gestor del sistema basado en la Web tiene varios componentes que se pueden visualizar u ocultar, en función de la preferencia del usuario. Estas preferencias de formato de ventanas hijas se guardan en el archivo de preferencias y se utilizan cuando se inicia una sesión con el archivo de preferencias especificado. Los componentes de la ventana hija se pueden visualizar u ocultar utilizando la opción de menú de cascada **Ver -> Mostrar**. Los componentes reales de la ventana hija que se pueden visualizar u ocultar, y si se guardan o no en el archivo de preferencias, son los siguientes:

Componente	¿Estado guardado en el archivo de preferencias?
Área de navegación	No
Barra de herramientas	Sí
Barra de sugerencias	Sí
Barra de descripción	Sí
Barra de estado	Sí

Durante una sesión de Gestor del sistema basado en la Web, un usuario puede abrir varias ventanas hijas. Las preferencias de formato de las ventanas hijas que se guardan cuando finaliza una sesión (siempre y cuando el usuario indique que las preferencias se tienen que guardar al salir) son las de la ventana hija que tenía el foco cuando el usuario finalizó la sesión. Cuando se utiliza este archivo de preferencias para iniciar otra sesión, la ventana hija de la ventana de consola (sólo se crea una ventana hija cuando se inicia una sesión) utiliza las preferencias guardadas de formato de ventanas hijas.

Para cada aplicación cargada, un usuario puede definir los objetos que se muestran y cómo se muestran mediante las opciones ver, clasificar y filtrar que están definidas por la aplicación. Las opciones que selecciona un usuario para cada aplicación se guardan en el archivo de preferencias. Luego estas

opciones se utilizan cuando se inicia una sesión con el archivo de preferencias en el que se han guardado. Un usuario puede definir estas opciones de las siguientes maneras:

- Elegir una vista de aplicación seleccionando la opción de menú y recuadro de selección **Ver -> Opción Ver**.
- Elegir un orden de clasificación para objetos seleccionando la opción del menú en cascada **Ver -> Organizar iconos**
- Elegir filtrar objetos visualizados seleccionando la opción de menú **Ver -> Filtrar iconos**

Los sistemas principales gestionados durante una sesión de Gestor del sistema basado en la Web se guardan en el archivo de preferencias. Esto permite a un usuario gestionar diferentes dominios de máquinas, iniciando sesiones con distintos archivos de preferencias. De este modo un usuario puede tener un archivo de preferencias que represente un grupo de máquinas que sean Servidores HTTP y un archivo de preferencias que represente un grupo de máquinas que sean servidores de transacciones.

Para que se guarde un grupo de máquinas en un archivo de preferencias, se deben añadir al Entorno de gestión de Gestor del sistema basado en la Web durante una sesión. Para añadir máquinas al Entorno de gestión durante una sesión, seleccione la opción de menú **Consola -> Añadir -> Sistemas principales...**. Esta opción de menú muestra un diálogo en el que un usuario puede entrar sistemas principales individuales, una lista de sistemas principales de un archivo o máquinas de sistema principal de un dominio especificado.

Manejo de errores para cargar y guardar archivos de preferencias

Las siguientes situaciones pueden ocasionar errores:

- Si el usuario no especifica ningún archivo de preferencias, se utiliza el archivo **$HOME/WebSM.pref** por omisión. Este usuario no tiene acceso de lectura a este archivo o este archivo contiene datos erróneos. Se muestra un diálogo de aviso y se utilizan valores por omisión. El usuario puede seleccionar otro archivo con la opción de menú **Consola -> Guardar como...** o puede seleccionar la opción **Guardar el estado de la consola para la siguiente sesión** en el diálogo Confirmación de salida cuando sale de una sesión de Gestor del sistema basado en la Web.
- Un usuario especifica un archivo de preferencias, pero no tiene acceso de lectura a este archivo o el archivo contiene datos erróneos. Se aplican los mismos procedimientos que en el punto anterior a estas situaciones. El usuario no tiene acceso de escritura al archivo que se está guardando. Aparece un diálogo de aviso y el usuario puede seleccionar otro archivo con la opción de menú **Consola -> Guardar como...** o puede salir sin guardar el archivo de preferencias.
- Si el proceso de carga de preferencias falla, se utilizarán valores por omisión. Durante una sesión de salida de Gestor del sistema basado en la Web, la opción **Guardar el estado...** estará deseleccionada para evitar que el usuario sobreescriba datos sin querer. El usuario puede seleccionar **Guardar el estado...** para sobreescribir el archivo seleccionado.

Herramientas de línea de mandatos

La tabla siguiente identifica los mandatos de línea de mandatos que se utilizan con frecuencia para mantener Gestor del sistema basado en la Web:

Mandato	Se utiliza para:
/usr/websm/bin/configassist	El Asistente para la configuración se muestra automáticamente después de que se instala el sistema operativo y sirve para ayudar en las tareas de configuración. También se puede ejecutar en cualquier momento para realizar tareas adicionales de configuración. Utilice el Asistente para la configuración para configurar un sistema que tenga instalado un Servidor HTTP para ejecutar Gestor del sistema basado en la Web en un navegador. Consulte el tema “Modalidad de applet” en la página 5 para obtener más información. **Argumentos:** Ninguno.
/usr/websm/bin/wsm	Iniciar una sesión de cliente de Gestor del sistema basado en la Web. **Argumentos:** • **-host *sistema principal de gestión*** Fuerza Gestor del sistema basado en la Web a que se conecte inicialmente al sistema principal especificado. Aunque puede gestionar fácilmente otros sistemas principales mientras ejecuta Gestor del sistema basado en la Web, esta opción le permite iniciar Gestor del sistema basado en la Web con las preferencias definidas en la máquina del sistema principal especificado. • **-lang *Idioma*** Especifica en qué idioma se mostrarán los mensajes. Si el archivo **sysmgt.msg.***Idioma***.websm.apps** no está instalado, los mensajes se visualizarán en inglés. • **-port *número puerto*** Hace que Gestor del sistema basado en la Web se conecte a cualquier otro sistema principal a través del puerto especificado. Este número de puerto utilizado debe coincidir con el número de puerto de las máquinas gestionadas correspondientes al servicio **wsmserver** especificado en el archivo **/etc/services**. • **-profile *vía acceso archivo preferencias*** Especifica un archivo de preferencias *alternativo*. El archivo de preferencias por omisión será un archivo denominado **WebSM.pref** situado en el directorio inicial del usuario. Esta opción permite al usuario utilizar otro archivo de preferencias. Esto puede resultar útil si el usuario gestiona distintos grupos de máquinas para distintos clientes. **Nota:** El archivo de preferencias se lee desde la máquina local o desde la máquina especificada en el argumento **-host**.

Mandato	Se utiliza para:
	• **-user *nombreusuario*** Hace que Gestor del sistema basado en la Web se ejecute como el nombre de usuario especificado. Se le solicitará la contraseña del usuario. • **DdefaultTurners=***valor* Cuando el *valor* es true, se utilizan los ajustadores de aspecto de Java en lugar de los ajustadores de Windows para nodos de árbol padre en el Área de navegación y en el Área de contenido. No se dibujan líneas de ángulo entre los objetos del árbol. • **-DdrawTreeLine=*valor*** Cuando *valor* es **true** y **-DdefaultTurners=true**, se dibujan líneas de ángulo entre los objetos del árbol en el Área de navegación y en el Área de contenido. • **-Ddatadir=*vía acceso*** Especifica un directorio alternativo en el que buscar archivos de configuración que normalmente se encuentran en **/var/websm/config/user_settings**.
/usr/websm/bin/wsmaccess	Acomodador del mandato **wsm** para habilitar las características de accesibilidad. **Argumentos:** Los mismos que **/usr/websm/bin/wsm**.
/usr/websm/bin/wsmserver	Habilita o inhabilita una máquina como servidor de Gestor del sistema basado en la Web, es decir, una máquina que se puede gestionar a través de un cliente de Gestor del sistema basado en la Web. **Argumentos:** • **-enable** Actualiza el servicio TCP/IP para que el daemon **inetd** escuche peticiones de clientes de Gestor del sistema basado en la Web en el puerto 9090. Por omisión, Gestor del sistema basado en la Web se configura durante la instalación de modo que no acepte peticiones de clientes. • **-disable** Elimina el puerto 9090 de los puertos a los que se responde mediante el daemon **inetd**. Esto hace que la máquina no responda a nuevas peticiones de clientes de Gestor del sistema basado en la Web. No termina los procesos existentes del servidor de Gestor del sistema basado en la Web. • **-start** Inicia un servidor de Gestor del sistema basado en la Web. Este servidor espera una petición de un cliente de Gestor del sistema basado en la Web. Esta opción no se necesita en operaciones normales. • **-ssloptional** Permite, según desee el usuario, que el servidor se gestione en SSL o con un zócalo estándar. • **-sslalways** Permite que un cliente gestione únicamente el servidor si se puede crear una conexión SSL entre el cliente y el servidor.

Archivos que puede editar el usuario

Es posible que el usuario o el administrador tengan que modificar algunos archivos de Gestor del sistema basado en la Web. En general, el estado de una sesión se guarda para cada usuario en el archivo de preferencias (consulte el tema “Archivos de preferencias” en la página 20). Los únicos archivos que se pueden modificar para cambiar el comportamiento global de Gestor del sistema basado en la Web son los siguientes:

- **/var/websm/config/user_settings/websm.cfg**

  Este archivo contiene valores que controlan el comportamiento global de la aplicación Gestor del sistema basado en la Web. La tabla siguiente identifica el contenido del archivo:

Nombre de variable	Descripción	Valores posibles
forcessl	Si tiene el valor **true**, indica que la máquina que contiene el archivo **websm.cfg** sólo se puede gestionar si el cliente que la intenta gestionar puede hacerlo estableciendo una conexión SSL con la máquina de gestión. Consulte el “Capítulo 5. Seguridad de Gestor del sistema basado en la Web” en la página 33. **Nota:** Gestor del sistema basado en la Web en sistemas anteriores a AIX 5.1 utilizaba una interpretación diferente para el distintivo *forcessl*. En aquel momento, la interpretación era que se necesitaba una comunicación SSL si el distintivo *forcessl* tenía el valor true *y* SSL estaba configurado en el servidor. En AIX 5.1, si el distintivo *forcessl* tiene el valor true y el servidor no tiene SSL configurado, el servidor no se puede gestionar mediante un cliente remoto.	**true** o **false**
remote_timeout	El periodo de tiempo (en milisegundos) que un cliente esperará una conexión con una máquina gestionada. Si no se puede establecer la conexión durante este periodo de tiempo, el cliente abandona el servidor. Si el cliente no abandonara el servidor, continuaría esperando de forma indefinida si se intentara gestionar una máquina no existente.	**Valores enteros** Un valor adecuado puede depender del rendimiento de la red. El valor por omisión es 30000 (30 segundos). Si el rendimiento de la red es lento (es frecuente que no se pueda acceder a una máquina remota, aunque se sepa que la máquina existe y está disponible), se debe aumentar el valor.

  La única opción que Gestor del sistema basado en la Web utiliza actualmente en este archivo es el distintivo *forcessl*. Este distintivo se utiliza cuando un cliente se conecta con una máquina gestionada. Si el valor del distintivo *forcessl* es **true**, el servidor sólo se conectará a un cliente a través de conexiones seguras (zócalos SSL). Si este distintivo tiene el valor **false**, el servidor intentará comunicarse con un cliente a través de conexiones de zócalo seguras si SSL está configurado tanto en el cliente como en el servidor. Pero si hay un problema en la conexión a través de zócalos SSL, el servidor permitirá al cliente conectarse a través de zócalos no seguros (consulte el “Capítulo 5. Seguridad de Gestor del sistema basado en la Web” en la página 33).

Ayuda

Gestor del sistema basado en la Web ofrece varias formas de obtener ayuda e información adicional.

Ayuda flotante

Ofrece ayuda para iconos de la barra de herramientas. Coloque el puntero del ratón sobre un icono de la barra de herramientas y espere un par de segundos. Aparece una etiqueta de texto que identifica el significado del icono.

Sugerencias

Ofrece ayuda en tareas habituales que se realizan con el conector actualmente activo. Las sugerencias se muestran entre el menú y las barras de herramientas. Las sugerencias se ofrecen en formato de instrucciones de texto sencillas o enlaces de hipertexto con la ayuda basada en el navegador. El usuario puede ocultar o mostrar el área de sugerencias según desee utilizando el submenú Mostrar del menú Ver. (Consulte el tema “Área de sugerencias” en la página 17 para obtener más información.)

Ayuda de contexto

Ofrece ayuda sobre el uso de las ventanas de diálogo. Puede acceder a la ayuda de contexto pulsando el botón **Ayuda** de la esquina inferior derecha del diálogo. Aparece una pequeña ventana de ayuda de contexto. Cuando pulsa un control individual del diálogo, se muestra ayuda sobre el uso de dicho control en la ventana de ayuda de contexto. Cuando se está ejecutando la ayuda de contexto, sólo puede acceder a los controles del diálogo para ver ayuda. Para utilizar los controles, primero debe cerrar la ventana de ayuda de contexto pulsando el botón **Cerrar** en la ventana de ayuda de contexto o pulsando el botón **Ayuda** del diálogo desde el que visualizó la ayuda.

Ayuda basada en el navegador

Ofrece amplia información sobre tareas en el sistema de ayuda basada en el navegador. Para utilizar el sistema de ayuda basada en el navegador, primero debe tener configurado un servidor de documentos. Una vez identificado el servidor de ayuda ante el sistema principal gestionado, puede acceder a la ayuda basada en navegador realizando una selección en el menú Ayuda de la barra de menús o pulsando un enlace en un Área de sugerencias.

Filtrado y clasificación de vistas

Cuando un conector da soporte a las vistas Iconos grandes, Iconos pequeños o Detalles, puede facilitar la localización de objetos filtrando o clasificando la vista. El filtrado reduce el número de objetos que se visualizan en el área de contenido. Puede filtrar una vista especificando los nombres de objetos o definiendo una o más reglas para excluir objetos de la vista:

- Para filtrar objetos, seleccione el menú Ver y luego el icono **Filtrar**. La pestaña **Filtrar** le permite definir una lista de objetos que se deben excluir de la vista. Para especificar un objeto a ocultar, escriba su nombre en el campo que hay a la derecha del botón **Añadir**. Luego pulse el botón **Añadir**. Repita esta tarea para cada objeto que desee ocultar. También puede pulsar el botón **Examinar** para visualizar una lista de objetos que se pueden ocultar. Seleccione los objetos que desee ocultar y pulse **OK**. Estos objetos se mostrarán en la lista **Objetos ocultos**. Para eliminar los objetos listados del área de contenido, pulse **OK** o **Aplicar**.
- La pestaña **Avanzado** le permite definir entre una y tres reglas para ocultar objetos según atributos específicos de dichos objetos. Por ejemplo, para ocultar todos los usuarios administrativos del conector Todos los usuarios, abra el diálogo de filtro y seleccione la pestaña **Avanzado**. Asegúrese de que el recuadro de selección **Ocultar los objetos** esté marcado. Luego seleccione la propiedad **Tipo** y la relación **=**. Entre el valor **Administrador** coincidente y pulse **OK** o **Aplicar**. Todos los usuarios administrativos se eliminan de la vista. Puede suministrar reglas adicionales pulsando el botón **Añadir regla**. Se muestra una fila de definición de regla adicional. Se pueden combinar varias reglas mediante una operación AND. Para eliminar una regla, pulse el botón **Eliminar** que hay a la derecha de la regla. Para eliminar la última regla, borre el valor coincidente de la regla.

La pestaña **Filtrar** y la pestaña **Avanzado** se pueden utilizar juntas si el recuadro de selección **Ocultar** está marcado en ambas pestañas.

Diálogo Trabajando

El diálogo Trabajando se muestra cuando se realizan acciones de larga ejecución en un sistema gestionado. En función de la aplicación, se puede mostrar como un diálogo sencillo con una animación que indica que la acción se está procesando.

La siguiente ilustración es un ejemplo del diálogo Trabajando.

Cuando se ejecuta en modalidad sencilla, el diálogo se puede ampliar para mostrar detalles de la acción que se está ejecutando. Para ver detalles, pulse el botón **Detalles** situado en la parte inferior del diálogo. Puede ver dos tipos de detalles:

Mandatos
: El script del shell que se está ejecutando actualmente.

Mensajes
: Información que se visualiza en salida estándar (stdout).

Paralelamente, cuando se visualizan detalles puede reducir el tamaño del diálogo pulsando el mismo botón para ocultar detalles.

En función de la naturaleza de la aplicación, el diálogo Trabajando puede desaparecer automáticamente cuando la acción finaliza satisfactoriamente. Si la acción falla, el diálogo permanece abierto y se amplía para mostrar detalles de mensajes para ayudarle a diagnosticar el problema. Para tareas en las que es importante que el usuario revise los resultados de una acción que ha finalizado satisfactoriamente, el diálogo Trabajando puede permanecer abierto tras la finalización para que el usuario pueda revisar los mensajes antes de cerrar el diálogo.

Control del teclado de Gestor del sistema basado en la Web

Gestor del sistema basado en la Web se puede utilizar con o sin dispositivo de puntero, como un ratón. Si decide no utilizar un dispositivo de puntero, puede moverse entre los controles y los menús utilizando únicamente el teclado.

Utilización de mnemotécnicos y atajos

Puede acceder a funciones de menús utilizando los siguientes métodos de teclado:

- **Mnemotécnicos:** Los mnemotécnicos son letras subrayadas en opciones de menú y texto de control. Para acceder a un control u opción de menú visible, pulse la tecla Alt seguida del mnemotécnico. Cuando se utilizan mnemotécnicos, no es necesario utilizar la barra espaciadora ni la tecla Intro para seleccionar un elemento.
- **Atajos:** Los atajos (también denominados *aceleradores*) son combinaciones de teclado que acceden directamente a controles que se utilizan con frecuencia. Los atajos también utilizan una combinación de teclas para acceder a funciones, en este caso la tecla Control seguida de un carácter. A diferencia de los mnemotécnicos, los atajos de menú no necesitan que una opción de menú esté visible para poder acceder directamente a la misma.

Navegación por la consola con el teclado

Utilice las siguientes teclas o combinaciones de teclas para navegar por la consola de Gestor del sistema basado en la Web:

Pulsación de teclas	Acciones
Teclas de flecha	Mueve el foco entre: • Objetos del Área de navegación. Las flechas hacia la derecha y hacia la izquierda amplían y contraen nodos; las flechas hacia arriba y hacia abajo permiten moverse verticalmente por los elementos. • Objetos del Área de contenido • Iconos de la barra de herramientas • Elementos de menús
Control + tecla flecha	Mueve el foco de localización a otro objeto del área de contenido sin seleccionarlo. Utilizando Control+teclas flecha y la barra espaciadora puede seleccionar varios objetos que no sean contiguos.
Escape	Cierra un menú abierto sin activar una opción
F1	Abre una ayuda basada en navegador en la sección de contenido
F8	Mueve el foco a la barra divisoria entre el Área de navegación y el Área de contenido de la consola. Mueve la barra divisoria utilizando Inicio, Fin y las teclas de flecha.
F10	Mueve el foco a la barra de menú o lo aparta de la misma
Despl + tecla flecha	Amplía una selección contigua
Barra espaciadora, Intro	Selecciona el objeto que tiene el foco
Tabulador, Despl + Tabulador	Mueve el foco entre áreas de la consola

Navegación por recuadros de diálogo con el teclado

Utilice las siguientes teclas o combinaciones de teclas para navegar por recuadros de diálogo de Gestor del sistema basado en la Web:

Pulsaciones de teclas	Acciones
Alt+F6	Mueve el foco al recuadro de diálogo o fuera del mismo
Teclas de flecha	• Abre listas desplegables • Mueve entre opciones de listas • Mueve entre pestañas en diálogos con pestañas cuando una pestaña tiene el foco
Control + Tabulador, Control + Despl + Tabulador	Mueve el foco entre controles
Intro	Activa el botón de mandato que tiene el foco
Escape	Cancela el recuadro de diálogo
F1	Abre la ventana de ayuda de contexto
Barra espaciadora	• Selecciona la opción que tiene el foco • Activa el botón del mandato sobre el que está el cursor de localización.

Acceso a la ayuda con el teclado

Utilice las siguientes teclas o combinaciones de teclas para navegar por el sistema de ayuda de Gestor del sistema basado en la Web:

Nota: El sistema de ayuda tiene que estar configurado para que estas funciones de teclado funcionen correctamente.

F1	• Abre ayuda basada en navegador en el Área de contenido • En recuadros de diálogo, abre la ventana de ayuda de contexto
F9	Muestra ayuda sobre teclas.
Alt + F6	En modalidad de ayuda de contexto, mueve el foco entre la ventana de ayuda de contexto y el diálogo padre.

Registro de sesión

El Registro de sesión es un recurso de consola que efectúa un seguimiento de los cambios realizados en sistemas principales gestionados durante una sesión de Gestor del sistema basado en la Web. Cada vez que un administrador utiliza Gestor del sistema basado en la Web para realizar un cambio en un sistema principal, se crea una entrada en el registro. Las entradas también pueden generarlas las aplicaciones para notificar resultados intermedios, avisos o condiciones de error. Cada entrada incluye la hora y fecha del cambio, el usuario que realizó el cambio, el sistema principal en el que se realizó el cambio y un mensaje corto. El usuario puede efectuar una doble pulsación en un mensaje para ver el texto completo del mensaje. Pulse las columnas visualizadas en la ventana de registro para cambiar el orden de clasificación de las entradas; por ejemplo, las entradas se pueden clasificar por hora y fecha (orden por omisión), nombre de sistema principal, nombre de usuario y mensaje. La ventana de registro incluye una función *Buscar* para buscar entradas que incluyan una determinada serie de texto. El administrador también puede gestionar el registro borrando su contenido mediante el botón **Borrar** y guardándolo en un archivo.

Para ver el registro de sesión, seleccione **Consola -> Registro de sesión.**

Capítulo 4. Configuración del Entorno de gestión

El Entorno de gestión es un grupo de máquinas que un usuario puede gestionar desde dentro de la aplicación Gestor del sistema basado en la Web. El usuario puede añadir o suprimir miembros de este grupo. El Área de navegación y el Área de contenido de la ventana de la aplicación Gestor del sistema basado en la Web ofrecen una interfaz para acceder a estas máquinas. El usuario realiza tareas de administración de sistemas en este grupo de máquinas. La aplicación Gestor del sistema basado en la Web ofrece al usuario dos métodos para añadir o suprimir una máquina. El primer método es a través del menú Consola. El segundo método es a través del conector Entorno de gestión de Gestor del sistema basado en la Web. Los dos métodos guían al usuario para añadir o suprimir una máquina del Entorno de gestión.

Además, la aplicación Gestor del sistema basado en la Web ofrece al usuario métodos para guardar un grupo de máquinas en una determinada sesión. Cuando Gestor del sistema basado en la Web se ejecuta por primera vez, la única máquina presente en el Área de navegación y en el Área de contenido es la máquina de gestión. Después de que se añada una máquina, dicha máquina se puede guardar para un uso futuro si el usuario selecciona guardar preferencias a través del menú Consola o al salir de la aplicación Gestor del sistema basado en la Web.

Adición de una máquina a Gestor del sistema basado en la Web

Gestor del sistema basado en la Web identifica máquinas del Entorno de gestión por el nombre exacto que especifica el usuario cuando la máquina se añade al entorno. Esto significa que una máquina que se añade con un nombre de sistema principal calificado al completo y con una abreviatura para dicho nombre aparecerá listada dos veces en el Entorno de gestión, como si se tratara de dos máquinas distintas.

Por ejemplo, si el nombre del dominio es *micorp.com*, podrá crear una máquina gestionada en el Entorno de gestión denominada *nombre_máquina*, así como *nombre_máquina.micorp*.com. Para Gestor del sistema basado en la Web, se trata de dos máquinas distintas. Aparece un diálogo de aviso que le informa de que hay otra máquina con el mismo primer elemento del nombre de sistema principal y le alerta de que se añadirán ambas, *nombre_máquina* y *nombre_máquina.micorp*.com. Si no desea tener ambos nombres de máquina en el Entorno de gestión, puede evitarlo.

Puede utilizar cualquiera de los dos métodos siguientes para añadir una máquina a Gestor del sistema basado en la Web:

Menú Consola:

1. Seleccione **Consola** en el menú de la aplicación Gestor del sistema basado en la Web.
2. Seleccione **Añadir**.
3. Seleccione **Sistemas principales**.

Conector Entorno de gestión de Gestor del sistema basado en la Web:

1. Seleccione **Entorno de gestión** en el Área de navegación.
2. Seleccione **Entorno de gestión** en el menú de la aplicación Gestor del sistema basado en la Web.
3. Seleccione **Nuevo**.
4. Seleccione **Sistemas principales**.

Después de que el usuario haya iniciado el diálogo para añadir, puede añadir la máquina de una de las tres maneras siguientes:

- Añada un solo sistema principal con opción para verificar su existencia en la red.
- Añada una lista de sistemas de un archivo.

- Añada sistemas de un dominio.

Ejemplos

Para añadir una sola máquina denominada `chocolate.austin.ibm.com`:

1. Seleccione **Añadir el sistema principal con este nombre:**
2. Entre `chocolate.austin.ibm.com` en el campo de texto.
3. Pulse el botón **Añadir**.

El nombre del sistema asignado aparece en el Área de navegación y en el Panel de navegación. Un mensaje que aparece bajo la barra de proceso indica `Se ha añadido satisfactoriamente... chocolate.austin.ibm.com`.

Para añadir una sola máquina y verificar su existencia en la red:

1. Seleccione **Añadir el sistema principal con este nombre:**
2. Entre `coconut.austin.ibm.com` en el campo de texto.
3. Seleccione **Verificar que el sistema principal está en la red**.
4. Pulse el botón **Añadir**.

El nombre del sistema asignado aparece en el Área de navegación y en el Panel de navegación. Si el sistema principal no existe en la red, aparece un diálogo de error de Gestor del sistema basado en la Web que indica que no se puede establecer contacto con el siguiente sistema principal.

Para añadir una lista de máquinas de un archivo:

1. Seleccione **Añadir los sistemas principales listados en este archivo.**
2. Entre la vía de acceso completa al archivo en el campo de texto o seleccione **Examinar** y seleccione **archivo**.
3. Seleccione **sí** en el diálogo de confirmación para añadir la lista de máquinas.

Un mensaje bajo la barra de proceso indica que la máquina se está añadiendo actualmente. Una vez completado el proceso, aparece un mensaje que indica `Finalizado satisfactoriamente`. Los sistemas añadidos aparecen en el Área de navegación y en el Panel de navegación.

Para añadir máquinas de un dominio:

1. Seleccione **Añadir los sistemas de este dominio**.
2. Entre el nombre del dominio.
3. Seleccione **sí** en el diálogo de confirmación para añadir la lista de máquinas.

Un mensaje bajo la barra de proceso indica que la máquina se está añadiendo actualmente. Una vez completado el proceso, aparece un mensaje que indica `Finalizado satisfactoriamente`. Los sistemas añadidos aparecen en el Área de navegación y en el Panel de navegación.

Eliminación de una máquina

La aplicación Gestor del sistema basado en la Web ofrece dos métodos para eliminar o suprimir máquinas del Área de navegación:

Menú Consola:

1. Seleccione **Consola** en el menú de la aplicación Gestor del sistema basado en la Web.
2. Seleccione **Eliminar**.
3. Seleccione **Sistemas principales**.
4. Seleccione las máquinas que desea eliminar.

5. Pulse el botón **Eliminar**.
6. Seleccione **sí** en el diálogo de confirmación para eliminar las máquinas seleccionadas.

Conector Entorno de gestión:

1. Seleccione **Entorno de gestión** en el Área de navegación.
2. Seleccione las máquinas que desea suprimir del Panel de navegación.
3. Seleccione **Seleccionado** en el menú de la aplicación Gestor del sistema basado en la Web.
4. Seleccione **sí** en el diálogo de confirmación para eliminar las máquinas seleccionadas.

Capítulo 5. Seguridad de Gestor del sistema basado en la Web

Seguridad de Gestor del sistema basado en la Web permite un funcionamiento seguro de Gestor del sistema basado en la Web en modalidad cliente-servidor. En la modalidad de funcionamiento seguro de Gestor del sistema basado en la Web, las máquinas gestionadas son servidores y los usuarios de gestión son los clientes. La comunicación entre los servidores y los clientes se realiza sobre el protocolo SSL, que ofrece autentificación de servidores, cifrado de datos e integridad de datos. El usuario gestiona la máquina de Gestor del sistema basado en la Web utilizando una cuenta en dicha máquina y se autentifica ante el servidor de Gestor del sistema basado en la Web enviando el ID de usuario y la contraseña sobre el protocolo SSL protegido.

Cada servidor de Gestor del sistema basado en la Web tiene su clave privada y un certificado de su clave pública firmado por una Autoridad de certificados (CA) en la que confíen los clientes de Gestor del sistema basado en la Web. La clave privada y el certificado del servidor se guardan en el archivo de anillo de claves privadas del servidor. El cliente de Gestor del sistema basado en la Web tiene un archivo de anillo de claves públicas que contiene los certificados de las CA en las que confía.

En modalidad de applet (trabajando desde el navegador), se debe asegurar al cliente que la applet (archivos **.class**) que llega al navegador procede del servidor que el cliente espera. Además, en esta modalidad, el archivo de anillo de claves públicas reside en el servidor y se transfiere al cliente con el resto de los archivos **.class** de la applet, porque el navegador no permite que las applets lean archivos locales. Para la autentificación del emisor y la integridad de estos archivos, el cliente debe utilizar las funciones SSL del navegador y ponerse en contacto con el servidor únicamente con el protocolo **HTTPS** (HTTPS://...). Para ello, puede utilizar la función SSL del Servidor HTTP en cada máquina gestionada o puede utilizar el daemon **SMGate** que se instala con Seguridad de Gestor del sistema basado en la Web. El daemon **SMGate** sirve como pasarela SSL entre el navegador del cliente y el servidor Web.

Esta sección explica los siguientes procedimientos y procesos relacionados con Seguridad:

Instalación de Seguridad de Gestor del sistema basado en la Web

El archivo de Seguridad de Gestor del sistema basado en la Web, **sysmgt.websm.security**, si está disponible, se encuentra en el Expansion Pack de AIX 5.1.

Dispone también de un archivo adicional, **sysmgt.websm.security-us**, con mayor capacidad de cifrado, en el Expansion Pack de AIX 5.1 que se suministra en algunos países. Para poder utilizar este archivo debe tener instalado **sysmgt.websm.security**.

Configuración de Seguridad de Gestor del sistema basado en la Web

Seguridad de Gestor del sistema basado en la Web ofrece una interfaz gráfica y una interfaz de línea de mandatos para realizar la configuración para una administración segura. Para acceder a la interfaz gráfica, seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Visión general y estado**. Estas tareas sólo están visibles en modalidad local. En los distintos escenarios que se muestran a continuación, reciben el nombre de Visión general de Autoridad de certificados y Visión general de seguridad del servidor. En estos escenarios se utiliza la interfaz gráfica. Para cada paso se muestra el mandato correspondiente.

Escenarios de seguridad

A continuación se explican los siguientes escenarios o posibilidades de configuración:

- “Utilización de archivos de anillo de claves Ready-to-Go”
- “Administración de varios sitios” en la página 36
- “Cómo evitar la transferencia de claves privadas” en la página 39
- “Utilización de otra Autoridad de certificados” en la página 41.

Utilización de archivos de anillo de claves Ready-to-Go

La utilización de archivos de anillo de claves Ready-to-Go suele ser el modo más rápido de conseguir un estado operativo de seguridad. En este escenario, utilice una sola máquina para definir una CA (Autoridad de certificados) interna y generar archivos de anillo de claves ready-to-go para todos sus servidores y clientes de Gestor del sistema basado en la Web. Esto genera un archivo de anillo de claves públicas que debe copiar en todos los servidores y clientes, así como un archivo exclusivo de anillo de claves privadas para cada servidor.

Los siguientes pasos describen cómo utilizar archivos de anillo de claves ready-to-go:

1. **Defina una Autoridad de certificados interna de Gestor del sistema basado en la Web.** .

   Debe utilizar un sistema seguro para la CA porque su clave privada constituye los datos más sensibles de la configuración de seguridad de Gestor del sistema basado en la Web.

   > **Nota:** No utilice estaciones de trabajo sin disco o sin datos como Autoridades de certificados, porque la clave privada se transferiría por la red.

   Una vez elegida la máquina CA, inicie una sesión localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado una sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o applet.

   Seleccione **Entorno de gestión—>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Autoridad de certificados**.

   En la lista de tareas correspondiente a **Autoridad de certificados**, seleccione **Configurar este sistema como una Autoridad de certificados de Gestor del sistema basado en la Web**. Cuando se abra el asistente, especifique la siguiente información:

   - **Nombre distintivo de la Autoridad de certificados**
     Entre un nombre descriptivo que le ayude a identificar la máquina CA y la instancia de la CA; por ejemplo, el nombre del sistema principal de la máquina más un número de secuencia. Se permiten blancos en el nombre. Si vuelve a definir la CA, utilice un número de secuencia diferente y así podrá determinar qué instancia de la CA ha firmado el certificado. El nombre no debe ser exacto al nombre de TCP/IP completo, ya que esto no funcionará con el daemon **SMGate**.
   - **Nombre de organización**
     Entre un nombre descriptivo que identifique su empresa u organización.
   - **Código de país ISO**
     Entre su código de país ISO de dos caracteres o selecciónelo en la lista.
   - **Fecha de caducidad**
     Una vez caducado el certificado, vuelva a configurar la seguridad de Gestor del sistema basado en la Web volviendo a definir la CA y generando nuevos archivos de anillo de claves privadas para todos los servidores. Puede cambiar esta fecha o aceptar el valor por omisión.
   - **Directorio de anillo de claves públicas**
     El anillo de claves públicas que contiene el certificado de la CA se graba en este directorio. Copie este archivo en el directorio **/usr/websm/codebase** de todos los servidores y clientes de Gestor del sistema basado en la Web.

- **Contraseña**
  El archivo de anillo de claves privadas de la CA se cifra con esta contraseña. Tiene que entrar esta contraseña cada vez que realice una tarea en esta CA.

También puede definir una CA interna desde la línea de mandatos con el mandato **/usr/websm/bin/smdefca**.

2. **Genere archivos de anillo de claves privadas para sus servidores de Gestor del sistema basado en la Web.**

   Especifique nombres de TCP/IP completos para todos los servidores de Gestor del sistema basado en la Web.

   En la lista de tareas correspondiente a **Autoridad de certificados**, seleccione **Generar archivos de anillo de claves privadas del servidor**. En el diálogo Contraseña de CA, entre la contraseña que especificó cuando definió la CA. Luego especifique la siguiente información:

   - **Lista de servidores**
     Añada los nombres de los servidores de Gestor del sistema basado en la Web a la lista. Puede entrarlos en el diálogo de uno en uno o puede suministrar un archivo que contenga una lista de servidores, uno por línea. Para obtener nombres de servidores del archivo, entre el nombre del archivo en el campo de entrada **Archivo que contiene lista de servidores** y pulse el botón **Examinar archivo**. Utilice el diálogo **Examinar archivo de lista de servidores** para seleccionar algunos o todos los servidores de la lista.
   - **Nombre de organización**
     Entre un nombre descriptivo que identifique su empresa u organización.
   - **Código de país ISO**
     Entre su código de país ISO de dos caracteres o selecciónelo en la lista.
   - **Ubicación de archivos de anillo de claves privadas**
     Entre el directorio en el que desea que se escriban los archivos de anillo de claves privadas del servidor. Luego tiene que distribuirlos a los servidores e instalarlos.
   - **Longitud en bits de claves del servidor**
     Seleccione una **longitud** de clave (este campo sólo aparece si tiene el archivo **sysmgt.websm.security-us** instalado).
   - **Fecha de caducidad**
     Una vez caducado el certificado, tiene que generar nuevos archivos de anillo de claves privadas para sus servidores. Puede cambiar esta fecha o aceptar el valor por omisión.
   - **Cifrar los archivos de anillo de claves privadas del servidor**
     Este diálogo crea un archivo de anillo de claves privadas para cada servidor que haya especificado. Cada archivo de anillo de claves privadas contiene la clave privada de un servidor y por lo tanto se debe mantener siempre protegido. Puede proteger los archivos de anillo de claves privadas cifrándolos. Si selecciona esta opción, se le solicitará una contraseña, que necesitará cuando instale los anillos de claves privadas en los servidores.

   Cuando pulse **OK**, se creará un archivo de anillo de claves privadas para cada servidor que haya especificado.

   También puede generar archivos de anillo de claves públicas desde la línea de mandatos con el mandato **/usr/websm/bin/smgenprivkr**.

3. **Distribuya el archivo de anillo de claves públicas (SM.pubkr) a todos los servidores y clientes**.

   Se debe colocar una copia del archivo de anillo de claves públicas de CA del directorio especificado en el paso 1 en el directorio **/usr/websm/codebase** de sus servidores y clientes de Gestor del sistema basado en la Web.

   > **Nota:** El contenido de este archivo no es secreto. Sin embargo, el hecho de colocarlo en una máquina cliente especifica en qué CA confía el cliente. Por lo tanto, el acceso a este archivo en

la máquina cliente debe estar limitado. En modalidad de applet, el cliente puede confiar en el servidor para enviar este archivo junto con la applet, siempre y cuando se utilice el protocolo **HTTPS**.

4. **Distribuya los archivos de anillo de claves privadas a todos los servidores.**

   El archivo de anillo de claves privadas de cada servidor se debe instalar en el servidor.

   Puede mover los archivos a sus destinos en cualquier modo seguro. Los métodos de directorio compartido y de disquete TAR se describen a continuación:

   - **Directorio compartido:** Coloque todos los archivos de anillo de claves en un directorio compartido (por ejemplo, NFS o DFS) al que pueda acceder cada servidor.

     Nota: Para este método, debe haber elegido la opción de cifrar los archivos de anillo de claves privadas del servidor en el diálogo **Generar archivos de anillo de claves privadas del servidor** porque los archivos se transfieren tal cual, es decir, sin cifrar. También se recomienda restringir los derechos de acceso al directorio compartido al administrador.
   - **Disquete TAR:** Genere un disquete TAR que contenga todos los archivos de anillo de claves privadas del servidor. El archivo TAR debe contener únicamente los nombres de archivos sin vías de acceso. Para hacerlo, cambie al directorio que contiene los archivos de anillo de claves privadas del servidor y ejecute el mandato **tar -cvf /dev/fd0 *.privkr**.

   A continuación, instale los anillos de claves privadas en cada servidor. Inicie una sesión en cada servidor como usuario root, inicie Gestor del sistema basado en la Web y seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**. Desde la lista de tareas, seleccione **Instalar el archivo de anillo de claves privadas para este servidor**. Seleccione el origen de los archivos de anillo de claves privadas del servidor. Si está utilizando un disquete, seleccione `disquete tar`, inserte el disquete y luego pulse **OK**. Si los archivos de anillo de claves están cifrados, se le solicitará la contraseña. La clave privada del servidor se instala en **/var/websm/security/SM.privkr**. Repita este procedimiento en cada servidor.

   También puede distribuir archivos de anillo de claves privadas a todos los servidores desde la línea de mandatos con el mandato **/usr/websm/bin/sminstkey**.

Administración de varios sitios

Utilice este escenario si tiene varios sitios y no desea distribuir archivos de anillo de claves privadas entre sitios. Suponga que tiene un sitio A y un sitio B, y define su Autoridad de certificados (CA) de Gestor del sistema basado en la Web interna en una máquina del sitio A. Consulte el paso 1 de ″Archivos de anillo de claves Ready-to-Go″ para obtener instrucciones sobre cómo configurar una CA.

Nota: Para todos los clientes y para los servidores del sitio A puede seguir las instrucciones del tema “Utilización de archivos de anillo de claves Ready-to-Go” en la página 34.

Para los servidores del sitio B, siga los pasos siguientes:

1. **Genere claves privadas y peticiones de certificados para los servidores de Gestor del sistema basado en la Web.**

   Especifique nombres de TCP/IP completos para todos los servidores de Gestor del sistema basado en la Web del sitio B. Puede entrarlos en el diálogo de uno en uno o puede suministrar un archivo que contenga una lista de servidores, uno por línea.

   En un servidor del sitio B, inicie una sesión localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado la sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o de applet.

   Seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**.

En la lista de tareas correspondiente a **Seguridad del servidor**, seleccione **Generar claves privadas y peticiones de certificados de los servidores**. Especifique la siguiente información:

- **Lista de servidores**
  Añada a la lista los nombres de los servidores de Gestor del sistema basado en la Web del sitio B. Puede entrarlos en el diálogo uno por uno o puede suministrar un archivo que contenga una lista de los servidores, uno por línea. Para obtener nombres de servidores del archivo, entre el nombre del archivo en el campo de entrada **Archivo que contiene lista de servidores** y pulse el botón **Examinar archivo**. Utilice el diálogo **Examinar archivo de lista de servidores** para seleccionar algunos o todos los servidores de la lista.
- **Nombre de organización**
  Entre un nombre descriptivo que identifique su empresa u organización.
- **Código de país ISO**
  Entre su código de país ISO de dos caracteres o selecciónelo en la lista.
- **Ubicación de archivos de anillo de claves privadas**
  Entre el directorio en el que desea que se escriban las peticiones de certificados y los archivos de anillo de claves privadas del servidor. En el paso 2, transfiera los archivos de peticiones de certificados a la CA del sitio A para que los firme. En el paso 3, transfiera los certificados firmados de la CA del sitio A a este directorio.
- **Longitud en bits de claves del servidor**
  Seleccione una **longitud de clave** (este campo sólo aparece si tiene instalado el archivo **sysmgt.websm.security-us**).
- **Cifrar los archivos de anillo de claves privadas del servidor**
  Este diálogo crea un archivo de anillo de claves privadas para cada servidor que haya especificado. Cada archivo de anillo de claves privadas contiene la clave privada del servidor y por lo tanto se debe mantener siempre protegido. Puede proteger los archivos de anillo de claves privadas cifrándolos. Si selecciona esta opción, se le solicitará una contraseña, que necesitará cuando importe los certificados firmados y cuando instale los anillos de claves privadas en los servidores.

Cuando pulse **OK**, se creará un archivo de anillo de claves privadas y una petición de certificado para cada servidor que haya especificado.

También puede generar claves privadas y peticiones de certificados desde la línea de mandatos con el mandato **/usr/websm/bin/smgenkeycr**.

2. **Obtenga los certificados firmados por la CA del sitio A**.

   Transfiera los archivos de peticiones de certificados a la CA del sitio A. Las peticiones de certificados no contienen datos secretos. Sin embargo, se deben asegurar la integridad y la autenticidad durante la transferencia.

   Transfiera una copia de los archivos de peticiones de certificados del servidor del sitio B a un directorio de la máquina CA del sitio A.

   Inicie una sesión en la máquina CA del sitio A localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado la sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o de applet.

   Seleccione **Entorno de gestión—>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Autoridad de certificados**.

   En la lista de tareas correspondiente a **Autoridad de certificados**, seleccione **Firmar peticiones de certificados**. Especifique la siguiente información:

   - **Directorio para peticiones de certificados**
     Entre el directorio que contiene las peticiones de certificados. Luego pulse el botón **Actualizar lista**. Aparece la lista de peticiones de certificados.

- **Seleccionar peticiones de certificados a firmar**
  Para seleccionar peticiones de certificados individuales, pulse sobre las mismas en el recuadro de lista. Para seleccionar todas las peticiones de certificados que aparecen listadas, pulse el botón **Seleccionar todo**.
- **Fecha de caducidad de certificados**
  Una vez caducado el certificado, tiene que repetir este proceso para generar nuevos archivos de anillo de claves privadas para sus servidores. Puede cambiar esta fecha o aceptar la fecha por omisión.

Cuando pulse **OK**, se creará un archivo de certificados para cada servidor seleccionado. Los certificados se graban en el directorio que contiene las peticiones de certificados.

También puede obtener los certificados firmados por la CA ejecutando el siguiente mandato desde la línea de mandatos: **/usr/websm/bin/smsigncert**.

3. **Importe los certificados firmados a los archivos de anillo de claves privadas de los servidores**.
   En este paso, transfiera los certificados de la CA del sitio A de nuevo al servidor del sitio B. Cópielos en el directorio que contiene las peticiones de certificados y los archivos de claves privadas del servidor que ha creado en el paso 1.
   Luego, en el servidor del sitio a B, desde la lista de tareas **Seguridad del servidor**, seleccione **Importar certificados firmados**.
   Especifique la siguiente información:
   - **Directorio para certificados y claves privadas**
     Entre el directorio que contiene los certificados firmados y los archivos de claves privadas del servidor. Luego, pulse el botón **Actualizar lista**. Aparece la lista de servidores para los que hay un certificado firmado y un archivo de claves privadas.
   - **Seleccione uno o más servidores de la lista**
     Para seleccionar servidores individuales, pulse sobre los mismos en el recuadro de lista. Para seleccionar todos los servidores listados, pulse el botón **Seleccionar todos**.

   Cuando pulse **OK**, si los archivos de claves privadas del servidor se cifraron en el paso 1, se le solicitará la contraseña. Luego, para cada servidor que haya seleccionado, el certificado se importa en el archivo de claves privadas y se crea el archivo de anillo de claves privadas.

   Puede importar certificados firmados desde la línea de mandatos con el mandato **/usr/websm/bin/smimpservercert**.
4. **Distribuya los archivos de anillo de claves privadas a todos los servidores**.
   El archivo de anillo de claves privadas de cada servidor se debe instalar en el servidor.
   Puede mover los archivos a sus destinos en cualquier modo seguro. Los métodos de directorio compartido y de disquete TAR se describen a continuación:
   - **Directorio compartido:** Coloque todos los archivos de anillo de claves en un directorio compartido (por ejemplo, NFS o DFS) al que pueda acceder cada servidor.

     Nota: Para este método, debe haber elegido la opción de cifrar los archivos de anillo de claves privadas del servidor en el diálogo **Generar claves privadas y peticiones de certificados para este servidor u otros servidores** porque los archivos se transfieren tal cual, es decir, sin cifrar. También se recomienda restringir los derechos de acceso al directorio compartido al administrador.
   - **Disquete TAR:** Genere un disquete TAR que contenga todos los archivos de anillo de claves privadas del servidor. El archivo TAR debe contener únicamente los nombres de archivos sin vías de acceso. Para hacerlo, cambie al directorio que contiene los archivos de anillo de claves privadas del servidor y ejecute el mandato **tar -cvf /dev/fd0 *.privkr**.

A continuación, instale los anillos de claves privadas en cada servidor. Inicie una sesión en cada servidor como usuario root e inicie Gestor del sistema basado en la Web. Seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**. Luego seleccione **Instalar los archivos de anillo de claves privadas para este servidor**. Seleccione el origen de los archivos de anillo de claves privadas del servidor. Si utiliza un disquete TAR, inserte el disquete antes de pulsar **OK**. Si los archivos de anillo de claves están cifrados, se le solicitará la contraseña. La clave privada del servidor se instala en **/var/websm/security/SM.privkr**. Repita este procedimiento en cada servidor.

También puede distribuir los archivos de anillo de claves privadas desde la línea de mandatos con el mandato **/usr/websm/bin/sminstkey**.

5. **Distribución del archivo de anillo de claves públicas de la CA a todos los servidores y clientes del sitio B**.

   Se debe colocar una copia del archivo de anillo de claves públicas de CA del directorio especificado en el paso 1 en el directorio **/usr/websm/codebase** de sus servidores y clientes de Gestor del sistema basado en la Web.

   > **Nota:** El contenido de este archivo no es secreto. Sin embargo, el hecho de colocarlo en una máquina cliente especifica en qué CA confía el cliente. Por lo tanto, asegúrese de limitar el acceso a este archivo en la máquina cliente. En modalidad de applet, el cliente puede confiar en el servidor para enviar este archivo junto con la applet, siempre y cuando se utilice el protocolo **HTTPS**.

Cómo evitar la transferencia de claves privadas

Utilice este escenario si desea que se genere una clave privada en el servidor al que pertenece, evitando que se transfiera (por red o disquete) a otros sistemas. En este escenario, configurará cada servidor por separado. El proceso se debe repetir en cada servidor.

Antes de continuar con este escenario, configure la CA siguiendo los pasos del tema “Utilización de archivos de anillo de claves Ready-to-Go” en la página 34.

En este escenario se realizan las siguientes tareas:

1. **Genere una petición de clave privada y certificado para su servidor de Gestor del sistema basado en la Web**

   En el servidor, inicie una sesión localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado la sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o de applet.

   Seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**.

   En la lista de tareas correspondiente a **Seguridad del servidor**, seleccione **Generar claves privadas y peticiones de certificados para este servidor y otros servidores**. Especifique la siguiente información:

   - **Lista de servidores**
     Añada el nombre del servidor de Gestor del sistema basado en la Web que desea listar. El nombre del servidor se muestra por omisión en el primer campo de texto. Pulse el botón **Añadir a la lista** para añadir el servidor a la lista.
   - **Nombre de organización**
     Entre un nombre descriptivo que identifique su empresa u organización.
   - **Código de país ISO**
     Entre su código de país ISO de dos caracteres o selecciónelo en la lista.
   - **Ubicación de archivos de anillo de claves privadas**
     Entre el directorio en el que desea que se escriban las peticiones de certificados y los archivos de

anillo de claves privadas del servidor. En el paso 2, transfiera el archivo de peticiones de certificados a la CA para que los firme. En el paso 3, transfiera el certificado firmado de la CA de nuevo a este directorio.

- **Longitud en bits de claves del servidor**
  Seleccione una **longitud de clave** (este campo sólo aparece si tiene instalado el archivo **sysmgt.websm.security-us**).
- **Cifrar los archivos de anillo de claves privadas del servidor**
  Este diálogo crea un archivo de anillo de claves privadas para el servidor que ha especificado. El archivo de anillo de claves privadas contiene la clave privada del servidor y por lo tanto se debe mantener siempre protegido. Puede proteger el archivo de claves privadas cifrándolo. Si selecciona esta opción, se le solicitará una contraseña, que necesitará cuando importe el certificado firmado y cuando instale el anillo de claves privadas en este servidor.

Cuando pulse **OK**, se creará un archivo de anillo de claves privadas y una petición de certificado para este servidor.

Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/smgenkeycr**.

2. **Obtenga los certificados firmados por la CA**.

   Transfiera el archivo de petición de certificados a la CA. La petición de certificados no contiene datos secretos. Sin embargo, se deben asegurar la integridad y la autenticidad durante la transferencia.

   Transfiera una copia del archivo de petición de certificados del servidor a un directorio de la máquina CA. Para ahorrar tiempo, puede transferir las peticiones de certificados desde todos los servidores y hacer que la CA los firme todos en un solo paso.

   Inicie una sesión en la máquina CA localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado la sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o de applet.

   Seleccione **Entorno de gestión—>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Autoridad de certificados**.

   En la lista de tareas correspondiente a **Autoridad de certificados**, seleccione **Firmar peticiones de certificados**. Especifique la siguiente información:

   - **Directorio para peticiones de certificados**
     Entre el directorio que contiene las peticiones de certificados. Luego pulse el botón **Actualizar lista**. Aparece la petición de certificados.
   - **Seleccionar peticiones de certificados a firmar**
     Pulse las peticiones de certificados del servidor en el recuadro de lista.
   - **Fecha de caducidad de certificado**
     Tras la fecha de caducidad, tiene que repetir este proceso para generar un nuevo archivo de anillo de claves privadas para el servidor. Puede cambiar esta fecha o aceptar la fecha por omisión.

   Cuando pulse **OK**, se creará un archivo de certificados para cada servidor seleccionado. El certificado se graba en el directorio que contiene la petición de certificado.

   Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/smsigncert**.

3. **Importe los certificados a los archivos de claves privadas.**

   Transfiera el certificado desde la CA de nuevo al servidor. Cópielo en el directorio que contiene la petición de certificados y el archivo de claves privadas del servidor que ha creado en el paso 1.

   Luego, en el servidor, desde la lista de tareas correspondiente a **Servidor de seguridad**, seleccione **Importar certificados firmados**.

   Especifique la siguiente información:

- **Directorio para certificados y claves privadas**
  Entre el directorio que contiene el certificado firmado y el archivo de claves privadas del servidor. Luego, pulse el botón **Actualizar lista**. El servidor se muestra en el recuadro de lista.
- **Seleccione uno o más servidores de la lista**
  Pulse el nombre del servidor en el recuadro de lista.

Cuando pulse **OK**, si el archivo de claves privadas del servidor se cifró en el paso 1, se le solicitará la contraseña. El certificado del servidor se importa en el archivo de claves privadas y se crea el archivo de anillo de claves privadas en el directorio que contiene la petición de certificados y el archivo de claves privadas.

Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/smimpservercert**.

4. **Instale la clave privada en el servidor.**

   En la lista de tareas correspondiente a **Seguridad del servidor**, seleccione **Instalar el archivo de anillo de claves privadas para este servidor**. Seleccione el botón **Directorio** y entre el directorio que contiene el archivo de anillo de claves privadas del servidor. Si el archivo de anillo de claves se cifró, se le solicitará la contraseña. La clave privada del servidor se instala en **/var/websm/security/SM.privkr**.

   Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/sminstkey**.

5. **Distribuya el archivo de anillo de claves públicas (SM.pubkr) a todos los servidores y clientes.**

   Se debe colocar una copia de **SM.pubkr** del directorio especificado en el paso 1 en el directorio **/usr/websm/codebase** de sus servidores y clientes de Gestor del sistema basado en la Web.

   > **Nota:** El contenido de este archivo no es secreto. Sin embargo, el hecho de colocarlo en una máquina cliente especifica en qué CA confía el cliente. Por lo tanto, asegúrese de limitar el acceso a este archivo en la máquina cliente. En modalidad de applet, el cliente puede confiar en el servidor para enviar este archivo junto con la applet, siempre y cuando se utilice el protocolo **HTTPS**.

Utilización de otra Autoridad de certificados

Utilice este escenario si no desea utilizar una CA interna de Gestor del sistema basado en la Web y desea utilizar en su lugar otro producto de CA interna que puede estar ya funcionando en su sistema. En este escenario, esta otra CA firma las peticiones de certificados.

1. **Genere claves privadas y peticiones de certificados para los servidores de Gestor del sistema basado en la Web.**

   Especifique nombres de TCP/IP completos de todos los servidores de Gestor del sistema basado en la Web. Puede entrarlos en el diálogo de uno en uno o puede suministrar un archivo que contenga una lista de servidores, uno por línea.

   En un servidor, inicie una sesión localmente como usuario root e inicie Gestor del sistema basado en la Web. No se puede acceder a las aplicaciones de la configuración de seguridad de Gestor del sistema basado en la Web si no ha iniciado la sesión como usuario root o si está ejecutando Gestor del sistema basado en la Web en modalidad de aplicación remota o de applet.

   Seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**.

   En la lista de tareas correspondiente a **Seguridad del servidor**, seleccione **Generar claves privadas y peticiones de certificados para este servidor y otros servidores**. Especifique la siguiente información:

   - **Lista de servidores**
     Añada los nombres de los servidores de Gestor del sistema basado en la Web a la lista. Puede entrarlos en el diálogo uno por uno o puede suministrar un archivo que contenga una lista de los servidores, uno por línea. Para obtener nombres de servidores del archivo, entre el nombre del

archivo en el campo de entrada **Archivo que contiene lista de servidores** y pulse el botón **Examinar archivo**. Utilice el diálogo **Examinar archivo de lista de servidores** para seleccionar algunos o todos los servidores de la lista.

- **Nombre de organización**
  Entre un nombre descriptivo que identifique su empresa u organización.
- **Código de país ISO**
  Entre su código de país ISO de dos caracteres o selecciónelo en la lista.
- **Ubicación de archivos de anillo de claves privadas**
  Entre el directorio en el que desea que se escriban las peticiones de certificados y los archivos de anillo de claves privadas del servidor. En el paso 2, transfiera los archivos de peticiones de certificados a la CA para que los firme. En el paso 3, transfiera los certificados firmados de la CA a este directorio.
- **Longitud en bits de claves del servidor**
  Seleccione una **longitud de clave** (este campo sólo aparece si tiene instalado el archivo **sysmgt.websm.security-us**).
- **Cifrar los archivos de anillo de claves privadas del servidor**
  Este diálogo crea un archivo de anillo de claves privadas para cada servidor que haya especificado. Cada archivo de anillo de claves privadas contiene la clave privada de un servidor y por lo tanto se debe mantener siempre protegido. Puede proteger los archivos de anillo de claves privadas cifrándolos. Si selecciona esta opción, se le solicitará una contraseña, que necesitará cuando importe los certificados firmados y cuando instale los anillos de claves privadas en los servidores.

Cuando pulse **OK**, se creará un archivo de claves privadas y una petición de certificado para cada servidor que haya especificado.

Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/smgenkeycr**.

2. **Obtenga los certificados firmados por la CA.**

   Transfiera los archivos de peticiones de certificados a la CA. Las peticiones de certificados no contienen datos secretos. Sin embargo, se deben asegurar la integridad y la autenticidad durante la transferencia.

   Transfiera una copia de los archivos de petición de certificados del servidor a un directorio de la máquina CA.

   Siga las instrucciones de la CA para generar los certificados firmados a partir de las peticiones de certificados.

3. **Importe los certificados firmados en los archivos de anillo de claves privadas del servidor.**

   Transfiera los certificados desde la CA de nuevo al servidor. Cópielos en el directorio que contiene las peticiones de certificados y los archivos de claves privadas del servidor creados en el paso 1. Este paso necesita que el archivo de certificados del servidor *S* se denomine **S.cert**.

   Luego, en el servidor, desde **Servidor de seguridad**, seleccione **Importar certificados firmados**.

   Especifique la siguiente información:

   - **Directorio para certificados y claves privadas**
     Entre el directorio que contiene los certificados firmados y los archivos de claves privadas del servidor. Luego pulse el botón **Actualizar lista**. Aparece la lista de servidores para los que hay un certificado firmado y un archivo de claves privadas.
   - **Seleccione uno o más servidores de la lista**
     Para seleccionar servidores individuales, pulse sobre los mismos en el recuadro de lista. Para seleccionar todos los servidores listados, pulse el botón **Seleccionar todos**.

   Cuando pulse **OK**, si los archivos de claves privadas del servidor se cifraron en el paso 1, se le solicitará la contraseña. Luego, para cada servidor que haya seleccionado, el certificado se importa en el archivo de claves privadas y se crea el archivo de anillo de claves privadas.

Puede realizar la tarea anterior desde la línea de mandatos con el mandato **/usr/websm/bin/smimpservercert**.

4. **Distribuya los archivos de anillo de claves privadas a todos los servidores.**

   El archivo de anillo de claves privadas de cada servidor se debe instalar en el servidor.

   Puede mover los archivos a sus destinos en cualquier modo seguro. Los métodos de directorio compartido y de disquete TAR se describen a continuación:

   - **Directorio compartido:** Coloque todos los archivos de anillo de claves en un directorio compartido (por ejemplo, NFS o DFS) al que pueda acceder cada servidor.

     Nota: Para este método, debe haber elegido la opción de cifrar los archivos de anillo de claves privadas del servidor en el diálogo **Generar claves privadas y peticiones de certificados para este servidor u otros servidores** porque los archivos se transfieren sin cifrar. También se recomienda restringir los derechos de acceso al directorio compartido al administrador.
   - **Disquete TAR:** Genere un disquete TAR que contenga todos los archivos de anillo de claves privadas del servidor. El archivo TAR debe contener únicamente los nombres de archivos sin vías de acceso. Para hacerlo, cambie al directorio que contiene los archivos de anillo de claves privadas del servidor y ejecute el mandato **tar -cvf /dev/fd0 *.privkr**.

   A continuación, instale los anillos de claves privadas en cada servidor. Inicie una sesión en cada servidor como usuario root e inicie Gestor del sistema basado en la Web. Seleccione **Entorno de gestión —>** *nombre sistema principal* **—> Seguridad del Gestor de sistemas —> Seguridad del servidor**. Seleccione **Instalar anillo de claves privadas** y luego seleccione el origen de los archivos de anillo de claves privadas del servidor. Si utiliza un disquete TAR, inserte el disquete antes de pulsar **OK**. Si los archivos de anillo de claves están cifrados, se le solicitará la contraseña. La clave privada del servidor se instala en **/var/websm/security/SM.privkr**. Repita este procedimiento en cada servidor.

   Puede realizar esta tarea desde la línea de mandatos con el mandato **/usr/websm/bin/sminstkey**.

5. **Importe el certificado de la Autoridad de certificados en el archivo de anillo de claves públicas.**

   Reciba el certificado auto-firmado por la CA en su CA. Cópielo en un directorio en el servidor en el que esté trabajando.

   Luego, en el servidor, desde la lista de tareas correspondiente a **Seguridad del servidor**, seleccione **Importar certificado de CA**.

   Especifique la siguiente información:

   - **Directorio que contiene el archivo de anillo de claves públicas**
     Entre un directorio para el archivo de anillo de claves públicas de la CA. Este archivo se tiene que distribuir a todos los servidores y clientes.
   - **Nombre completo de vía de acceso del archivo de certificados de la CA**
     Entre el directorio que contiene el certificado auto-firmado de la CA.

   Cuando pulse **OK**, el archivo de anillo de claves públicas **SM.pubkr** se escribirá en el directorio que ha especificado.

   Puede realizar la tarea anterior desde la línea de mandatos con el mandato **/usr/websm/bin/smimpcacert**.

6. **Distribuya el archivo de anillo de claves públicas a todos los clientes y servidores.**

   Se debe colocar una copia del archivo de anillo de claves públicas de la CA en el directorio **/usr/websm/codebase** de todos los servidores y clientes de Gestor del sistema basado en la Web.

   Nota: El contenido de este archivo no es secreto. Sin embargo, el hecho de colocarlo en una máquina cliente especifica en qué CA confía el cliente. Por lo tanto, asegúrese de limitar el

acceso a este archivo en la máquina cliente. En modalidad de applet, el cliente puede confiar en el servidor para enviar este archivo junto con la applet, siempre y cuando se utilice el protocolo **HTTPS**.

Configuración para el daemon SMGate

El daemon **SMGate** que se instala con Seguridad de Gestor del sistema basado en la Web le permite ejecutar en modalidad de applet segura sin tener que configurar la seguridad en cada sistema gestionado. **SMGate** sirve como pasarela SSL entre el navegador del cliente y el servidor Web local.

Para utilizar el daemon **SMGate**, instale el certificado que emite la Autoridad de certificados (CA) en el navegador de cada cliente, del modo siguiente:

1. Si utiliza la autoridad de certificados interna de Gestor del sistema basado en la Web, puede obtener el certificado de la CA siguiendo el siguiente procedimiento:
   a. Inicie la sesión en la máquina CA como usuario root.
   b. Inicie Gestor del sistema basado en la Web.
   c. Abra el Entorno de gestión y seleccione el sistema principal local.
   d. Seleccione **Exportar certificado de la Autoridad de certificados** en la lista de tareas.
   e. En el diálogo Exportar certificado de la Autoridad de certificados, entre el nombre completo de la vía de acceso en la que se tiene que escribir el certificado.
   f. Pulse **OK**.

   También puede escribir lo siguiente en la línea de mandatos:
   ```
   /usr/websm/bin/smexpcacert
   ```

   Nota: Si no utiliza la autoridad de certificados interna de Gestor del sistema basado en la Web, utilice los procedimientos de la autoridad de certificados para obtener una copia de su certificado.
2. Copie el certificado en un directorio del Servidor HTTP para poder acceder al mismo desde el navegador del cliente. El tipo MIME que envía el Servidor HTTP debe ser **application/x-x509-ca-cert**.
3. En el navegador de cada uno de sus clientes, dirija el navegador al archivo de certificados de la CA y siga el procedimiento del navegador para aceptarlo como certificado de firmante.

Ahora los navegadores están configurados para conectarse con los servidores a través del daemon **SMGate**. Para obtener información sobre cómo habilitar el daemon **SMGate**, consulte el tema “Habilitación del daemon SMGate” en la página 45. Para obtener información sobre cómo ejecutar a través del SMGate, consulte el tema “Modalidad de applet” en la página 46.

Cómo ver las propiedades de configuración

Una vez realizada la configuración de seguridad, puede ver las propiedades de la Autoridad de certificados (CA), cualquier servidor y el anillo de claves públicas de cualquier cliente.

Para ver propiedades de la CA, siga los pasos siguientes:

1. Abra el Entorno de gestión y seleccione el sistema principal local.
2. Seleccione el objeto **Seguridad** de Gestor del sistema basado en la Web.
3. Seleccione el objeto **Autoridad de certificados**.
4. Seleccione **Propiedades** en la lista de tareas.
5. Entre la contraseña.

   Nota: El diálogo ofrece información de sólo lectura sobre la CA.

Encontrará información detallada sobre todas las operaciones ejecutadas por la CA (por ejemplo, generación de anillos de claves o firma de certificados) en el archivo de registro de la CA **/var/websm/security/SMCa.log**.

Puede realizar esta tarea desde la línea de mandatos mediante el mandato **/usr/websm/bin/smcaprop**.

Para ver las propiedades de un servidor, siga los pasos siguientes:

1. Abra el Entorno de gestión y seleccione el sistema principal local.
2. Seleccione el objeto **Seguridad** de Gestor del sistema basado en la Web.
3. Seleccione **Seguridad del servidor**.
4. Seleccione **Ver propiedades de este servidor** en la lista de tareas.
5. Entre la contraseña.

   Nota: El diálogo ofrece información de sólo lectura sobre el servidor.

Puede realizar esta tarea desde la línea de mandatos utilizando el mandato **/usr/websm/bin/smserverprop**.

Contenido del anillo de claves públicas

Para ver el certificado de la CA que se incluye en el anillo de claves públicas de la CA, utilice el mandato **/usr/websm/bin/smlistcerts**.

Habilitación de Seguridad de Gestor del sistema basado en la Web

En cada sistema gestionado, puede habilitar la opción de seguridad que desee hacer cumplir.

Para habilitar la seguridad de modo que el sistema gestionado acepte conexiones seguras o no seguras, ejecute el mandato **wsmserver -ssloptional**. En esta modalidad, el usuario del cliente puede seleccionar una opción en el diálogo de inicio de sesión de Gestor del sistema basado en la Web para especificar una conexión segura o no segura.

Para habilitar un sistema gestionado de modo que sólo acepte conexiones seguras, ejecute el mandato **/usr/websm/bin/wsmserver -sslalways**.

Habilitación del daemon SMGate

El daemon SMGate sólo se puede habilitar una vez instalado el anillo de claves privadas del servidor.

Para habilitar SMGate, escriba el siguiente mandato:

```
/usr/websm/bin/wsmserver -enablehttps
```

Este mandato inicia SMGate y añade una entrada en el archivo **/etc/inittab** de modo que se active automáticamente cuando se vuelva a iniciar el sistema. El puerto por omisión para SMGate es 9092. Revise el archivo **/etc/services** para asegurarse de que ningún otro servicio utilice este puerto. Puede configurar SMGate de modo que utilice otro puerto escribiendo:

```
/usr/websm/bin/wsmserver -enablehttps puerto
```

donde *puerto* es el número de puerto que desea que utilice.

Si cambia la configuración de seguridad del servidor, debe inhabilitar SMGate. Para inhabilitar SMGate, escriba:

```
/usr/websm/bin/wsmserver -disablehttps
```

Para configurar el navegador de modo que funcione a través de SMGate, consulte el tema “Configuración para el daemon SMGate” en la página 44.

Ejecución de Seguridad de Gestor del sistema basado en la Web

Gestor del sistema basado en la Web se ejecuta en modalidad de aplicación cuando el usuario utiliza una máquina como un cliente para gestionar otra máquina.

Modalidad de aplicación

Para activar la modalidad de aplicación, escriba el siguiente mandato en el cliente:

```
wsm -host nombre sistema principal
```

donde *nombre sistema principal* es el nombre de la máquina remota que desea gestionar.

Si la máquina que se va a gestionar está configurada de modo que sólo permite las conexiones seguras (consulte el tema “Habilitación de Seguridad de Gestor del sistema basado en la Web” en la página 45), el cliente debe tener el archivo **sysmgt.websm.security** instalado y debe tener una copia del archivo de anillo de claves públicas de CA en el directorio **/usr/websm/codebase**. En esta modalidad, el diálogo de inicio de sesión de Gestor del sistema basado en la Web indica que se necesita seguridad.

Si la máquina que se va a gestionar está configurada de modo que permite conexiones seguras y no seguras (consulte el tema “Habilitación de Seguridad de Gestor del sistema basado en la Web” en la página 45) y el cliente tiene una copia del archivo de anillo de claves públicas de CA en el directorio **/usr/websm/codebase**, el diálogo de inicio de sesión de Gestor del sistema basado en la Web permite al usuario del cliente especificar una conexión segura o no segura.

Cuando se ejecuta en modalidad de aplicación, la seguridad se indica mediante un mensaje `conexión segura` en la línea de estado que hay en la parte inferior de la ventana.

Modalidad de applet

Gestor del sistema basado en la Web se ejecuta en modalidad de applet cuando utiliza un navegador para conectarse a la máquina que desea gestionar. La modalidad de applet añade otra consideración sobre seguridad para la trasferencia segura del archivo de anillo de claves públicas CA y de los archivos **.class** de la applet. Para disponer de una seguridad completa en modalidad de applet, el cliente debe utilizar las posibilidades SSL de su navegador y sólo ponerse en contacto con el servidor con el protocolo **HTTPS**. Para ello, el Servidor HTTP debe estar configurado para seguridad o SMGate debe estar configurado mediante una de las siguientes opciones:

- Una opción es utilizar la función SSL del servidor Web en la máquina gestionada. Para esta opción, el servidor Web debe estar configurado para seguridad. Siga las instrucciones suministradas con su servidor Web. Luego podrá acceder a Gestor del sistema basado en la Web en la máquina gestionada con la siguiente dirección Web: **https://*nombre sistema principal*/wsm.html**, donde *nombre sistema principal* es el nombre de la máquina remota que desea gestionar. En esta opción, la applet y el anillo de claves públicas **SM.pubkr** se transfieren de forma segura del servidor Web de la máquina gestionada al cliente.
- Otra opción es utilizar el daemon **SMGate**.**SMGate** se ejecuta en máquinas gestionadas y sirve como una pasarela SSL entre el navegador del cliente y el servidor Web local. **SMGate** responde a la petición **HTTPS** del navegador del cliente y crea una conexión SSL con el mismo utilizando la clave privada y el certificado del servidor de Gestor del sistema basado en la Web. Dentro de la máquina gestionada, **SMGate** crea una conexión no segura con el servidor Web local.

  En esta opción, la applet y el anillo de claves públicas **SM.pubkr** se transfieren de forma segura desde **SMGate** en la máquina gestionada al navegador del cliente. Las comunicaciones entre la máquina gestionada y el cliente ser realizan sobre SSL. Cuando utiliza **SMGate**, puede acceder a Gestor del

sistema basado en la Web en la máquina gestionada con la siguiente dirección Web: https://*nombre sistema principal*:9092/wsm.html, donde *nombre sistema principal* es el nombre de la máquina remota que desea gestionar.

> **Nota:** `9092` es el número de puerto por omisión para **SMGate**. Si ha habilitado **SMGate** con otro número de puerto, especifique dicho número.

Cuando esté ejecutando en modalidad de applet, asegúrese de que estén presentes los siguientes indicadores de seguridad:

- La indicación **HTTPS** del navegador
- El mensaje `conexión segura` en la línea de estado situada en la parte inferior de las ventanas de Gestor del sistema basado en la Web.

Si falta alguno de estos indicadores, la conexión no es completamente segura.

Capítulo 6. Accesibilidad de Gestor del sistema basado en la Web

Gestor del sistema basado en la Web ofrece características de accesibilidad de teclado y la implantación del Self Voicing Kit (SVK). Ambas características se describen en detalle en las secciones siguientes.

Accesibilidad de teclado

El objetivo de las funciones de accesibilidad de teclado es permitir al usuario utilizar Gestor del sistema basado en la Web sin tener que utilizar un ratón. Dispone de las siguientes características de accesibilidad de teclado:

- Mnemotécnicos de menús: todas las opciones de menú se pueden seleccionar desde el teclado escribiendo la letra indicada en el título del menú. Por ejemplo, para un menú con la opción **Propiedades**, abra el menú y escriba `r` para seleccionar la opción Propiedades.
- Aceleradores de menús o teclas de atajo: dispone de combinaciones de teclas para acciones habituales. Por ejemplo, Control + S para salir y F9 para Ayuda sobre teclas.
- Características de accesibilidad de diálogos: dispone de mnemotécnicos y aceleradores para botones de diálogo. Por ejemplo, al pulsar la tecla Intro se activa el botón OK y al pulsar Esc se activa el botón Cancelar.

Ayuda sobre teclas (F9) ofrece una descripción de todos los atajos y teclas aceleradoras del teclado. Otros tipos de atajos incluyen teclas especiales para moverse entre áreas de la consola y ampliar ramas de un árbol.

Soporte de texto a voz

El Self Voicing Kit (SVK) ofrece un enlace entre el código Java y un sintetizador de voz que convierte la GUI de Gestor del sistema basado en la Web en salida hablada. Esta sección describe cómo el SVK da soporte a la salida hablada para aplicaciones Java, como Gestor del sistema basado en la Web, sin necesidad de modificar el código base.

Se necesita el siguiente archivo para poder ejecutar el SVK dentro de Gestor del sistema basado en la Web: **sysmgt.websm.accessibility**. Este archivo está disponible en el CD de instalación de AIX base.

El SVK está disponible en el sitio web de IBM AlphaWorks en:

http://www.alphaworks.ibm.com

Utilización de Gestor del sistema basado en la Web con el Self-Voicing Kit

El SVK, basado en la nueva tecnología Access Engine de IBM, se ejecuta como una tecnología de ayuda de la clase del programa de utilidad de accesibilidad a Java de Sun EventQueueMonitor. El motor se comunica con los componentes a los que se puede acceder de Gestor del sistema basado en la Web y gestiona la información desde Gestor del sistema basado en la Web de modo que las extensiones de presentación de interfaz de usuario pueden acceder rápidamente a la información a través de la biblioteca de clases de SVK Toolkit. La biblioteca de clases de SVK contiene muchas funciones de programas de utilidad que incluyen, aunque sin limitarse a las mismas, pronunciación de texto, lectura de texto de aplicaciones y activación de componentes a los que se puede acceder.

Una vez instalado, el SVK se carga automáticamente en Java Virtual Machine (JVM) con Gestor del sistema basado en la Web. De forma opcional, se puede conectar un teclado externo al otro puerto serie para ofrecer funciones de navegación para usuarios ciegos. Si el teclado no está instalado, hay una

secuencia de teclas que permite al usuario colocarse en *modalidad de revisión*. En *modalidad de revisión*, las pulsaciones de teclas se dirigen al SVK para ofrecer funciones similares a las de un teclado externo.

Para obtener más información sobre el Self Voicing Kit, consulte el manual *IBM Self Voicing Kit User's Guide*.

Apéndice A. Resolución de problemas

Dispone de los siguientes temas sobre la resolución de problemas:

- "Resolución de problemas de máquinas remotas"
- "Resolución de problemas de Gestor del sistema basado en la Web en modalidad de applet" en la página 52
- "Resolución de problemas de Gestor del sistema basado en la Web en modalidad PC Client" en la página 53
- "Resolución de problemas de seguridad" en la página 53

Resolución de problemas de máquinas remotas

Problema	Acción
No puede gestionar un sistema principal remoto como una máquina gestionada por Web-based System Manager.	Verifique lo siguiente: • El sistema principal que intenta gestionar tiene un sistema operativo anterior a AIX 5.0. Los sistemas con niveles anteriores a AIX 5.0 sólo se pueden gestionar mediante sistemas que estén al mismo nivel. Por lo tanto, para gestionar este sistema se debe utilizar un sistema que esté al mismo nivel, el sistema se debe actualizar a AIX 5.1 o posterior o el sistema se debe gestionar de forma local. • El sistema principal que intenta gestionar tiene instalado un **sysmgt.websm.framework** a un nivel anterior a AIX 5.0. Las máquinas con niveles de **sysmgt.websm.framework** anteriores a AIX 5.0 sólo se pueden gestionar mediante sistemas que estén al mismo nivel. Por lo tanto, para gestionar este sistema se debe utilizar un sistema con **sysmgt.websm.framework** que esté al mismo nivel, el sistema se debe actualizar a AIX 5.1 o posterior o el sistema se debe gestionar de forma local.

Problema	Acción

No puede gestionar un sistema principal remoto como una máquina gestionada por Web-based System Manager.(continuación)	• El sistema que intenta gestionar escucha un puerto inetd 9090. Si es este el caso, habrá una línea en el archivo **/etc/services** parecida a la siguiente:
	`wsmserver 9090/tcp`
	
	Además, habrá una línea en el archivo **/etc/inetd.conf** parecida a la siguiente:
	`wsmserver stream tcp nowait root \`
	`/usr/websm/bin/wsmserver wsmserver -start`
	
	Si no es este el caso, utilice el siguiente mandato:
	`/usr/websm/bin/wsmserver -enable`
	
	Esto se puede probar mediante el siguiente mandato:
	`tn hostname 9090`
	
	Si el sistema principal remoto está correctamente configurado, responderá con un mensaje parecido al siguiente:
	`Intentando...`
	
	`Conectado a saga.austin.ibm.com.`
	`El carácter de escape es '|T'.`
	`Idioma recibido del cliente:`
	`Entorno nacional definido: en_US`
	`WServer.HANDSHAKING 41292 WServer.HANDSHAKING`
	`en_US`
	
	donde *en_US* se sustituye por el archivo de idioma instalado en la máquina.
	
	Si no responde con la salida anterior, significa que hay un proceso del servidor desocupado en ejecución en la máquina que está consumiendo recursos del sistema. Inicie una sesión en el servidor remoto y utilice el mandato **kill** en el proceso de WServer desocupado.

El conector instalado en un sistema principal remoto no aparece cuando se gestiona desde un cliente.	• El conector del sistema principal remoto puede estar a un nivel que no puede gestionar el nivel **sysmgt.websm.framework** instalado en el sistema cliente. En este caso, aparece un mensaje de error cuando se realiza la conexión con el sistema principal remoto que lista el conector, la versión del mismo y la versión de **sysmgt.websm.framework** necesaria para gestionar el conector. Para gestionar este conector, tendrá que buscar un sistema en el que la versión de **sysmgt.websm.framework** esté al nivel correcto para el conector o tendrá que gestionar el conector de forma local en dicho sistema principal. • El archivo **App*.db** del sistema principal remoto no está correctamente formateado. Aparece un mensaje de error correspondiente al conector que indica que el archivo **App*.db** no está en el formato correcto para dicho conector y que no se ha podido cargar el conector. Si esto sucede, póngase en contacto con el representante del servicio al cliente para tomar la acción adecuada.

Resolución de problemas de Gestor del sistema basado en la Web en modalidad de applet

Problema	Acción

Cuando se utiliza Netscape Communicator en un PC, el navegador le solicita que baje el conector Java. Netscape Communicator abre la página, pero no encuentra el conector Java.	1. Verifique que está utilizando Netscape Communicator 4.7 ó 4.7x. No se da soporte a Netscape Communicator 6.0. 2. Netscape Communicator no siempre encuentra el conector correcto. Baje e instale el conector de forma manual.
El navegador se queda bloqueado después de pulsar el botón Renovar o Volver a cargar, mostrando de nuevo Gestor del sistema basado en la Web.	A veces los navegadores no vuelven a cargar las applets correctamente. Puede intentar lo siguiente: • Renueve o suprima la antememoria del navegador. • Vuelva a iniciar el navegador. Esto hace que el navegador vuelva a cargar las applets.
Al intentar conectar con http://*sumáquina*/wsm.html, sólo se muestra la página de presentación del servidor Web.	Los archivos html no se han enlazado con el directorio **pub** del servidor Web. Para corregir este problema: 1. Ejecute **configassist**. 2. Configure un servidor Web de modo que ejecute Gestor del sistema basado en la Web. 3. Verifique que hay archivos de Gestor del sistema basado en la Web en el directorio **pub** del servidor Web.

Resolución de problemas de Gestor del sistema basado en la Web en modalidad PC Client

Problema	Acción
Al efectuar una doble pulsación en el icono PC Client no se ejecuta la aplicación	Durante la instalación se crean o modifican variables de entorno del sistema. Desde la pestaña **Entorno** del **Panel de control**, compruebe que el valor de la variable **WSMDIR** sólo contenga el valor del directorio de instalación, por ejemplo **C:\ProgramFiles\websm**. Este directorio también debe estar contenido en la variable **PATH**.
La instalación falla	Es posible que la instalación haya fallado por una de las siguientes razones: • Debe haber 60 MB de espacio libre en la unidad por omisión. • Debe haber 50 MB de espacio libre en la unidad de destino. • Se debe utilizar la versión correcta del navegador. No se da soporte a Netscape Communicator 6.0. • El servidor de AIX debe estar correctamente configurado para poder instalar PC Client. Para obtener más información, consulte el tema “Instalación de PC Client de Gestor del sistema basado en la Web” en la página 10.

Resolución de problemas de seguridad

Problema	Acción
Las funciones de seguridad no funcionan.	Asegúrese de haber iniciado la sesión como usuario root y de estar ejecutando Gestor del sistema basado en la Web en la máquina local.
Cuando se intenta utilizar la Autoridad de certificados (CA) para generar anillos de claves o firmar peticiones de certificados, aparece un mensaje que indica que la Autoridad de certificados se está utilizando.	Si está seguro de que no hay ningún otro administrador que esté utilizando la CA en este momento, elimine el archivo de bloqueo de la CA **/var/websm/security/SMCa.lock**.

En configuración de SMGate, el navegador no reconoce el archivo de certificados de la CA como un certificado de la CA.	Compruebe que el tipo MIME que envía el servidor Web para el archivo de certificados sea **application/x-x509-ca-cert**.
La activación remota segura de Gestor del sistema basado en la Web falla.	• Verifique que Gestor del sistema basado en la Web funciona en modalidad remota no segura. Es posible que tenga que cambiar el valor del servidor si no da soporte a conexiones no seguras. • Coincidencia y caducidad de certificados: – Inicie una sesión en el servidor como usuario root y utilice el diálogo Propiedades del servidor del icono **Servidor** (o el mandato **smserverprop**) para verificar la fecha de caducidad de certificados del servidor. Anote el nombre de la CA. – Si el problema se ha producido en modalidad de aplicación, escriba: `/usr/websm/bin/smlistcerts /usr/websm/codebase` en el cliente y verifique que el cliente incluye un certificado de la CA que ha firmado el certificado del servidor (anterior) y que este certificado no ha caducado. Si el problema se ha producido en modalidad de applet, ejecute lo siguiente: `/usr/websm/bin/smlistcerts /usr/websm/codebase` en el servidor, porque el anillo de claves públicas reside en el servidor y se transfiere al cliente.

Apéndice B. Avisos

Esta información se ha desarrollado para productos y servicios que se ofrecen en EE.UU.
Es posible que IBM no ofrezca los productos, servicios o características que se describen en este documento en otros países. Consulte con el representante local de IBM para obtener información sobre los productos y servicios que están actualmente disponibles en su área. Cualquier referencia a un producto, programa o servicio IBM no pretende afirmar ni implica que sólo se pueda utilizar dicho producto, programa o servicio IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja los derechos de propiedad intelectual de IBM. Sin embargo, es responsabilidad del usuario la evaluación y la verificación del funcionamiento de cualquier producto, programa o servicio que no sea de IBM.
IBM puede tener patentes o solicitudes de patentes pendientes que afecten a los temas que se describen en este documento. El suministro de este documento no proporciona ninguna licencia sobre estas patentes. Puede enviar consultas sobre patentes a:
IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.

Para consultas sobre licencias relacionadas con información de doble byte (DBCS), póngase en contacto con el Departamento de Propiedad Intelectual de IBM de su país o envíe las consultas, por escrito a:
IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokio 106, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en el que tales disposiciones entren en contradicción con la ley local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUYENDO, PERO SIN LIMITARSE A, LAS GARANTÍAS IMPLÍCITAS DE NO INCUMPLIMIENTO, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO.
Algunos países no permiten la exclusión de garantías expresas o implícitas en determinadas operaciones comerciales, por lo que es posible que este párrafo no se aplique en su caso.
Esta información puede contener incorrecciones técnicas o errores tipográficos. Periódicamente se realizarán modificaciones en la información aquí contenida; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar en cualquier momento cambios y/o mejoras en el(los) producto(s) y/o programa(s) que se describen en esta publicación sin previo aviso.

IBM puede utilizar o distribuir cualquier información que se le suministre del modo que considere más adecuado sin incurrir por ello en ninguna obligación con el remitente.

Los titulares de una licencia de este programa que deseen obtener información sobre el mismo con la finalidad de habilitar: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) la utilización mutua de la información que se ha intercambiado, deben ponerse en contacto con:
IBM Corporation
Dept. LRAS/Bldg. 003
11400 Burnet Road
Austin, TX 78758-3498
EE.UU.
Esta información puede estar disponible, sujeta a los términos y condiciones apropiados, incluyendo en algunos casos, el pago de una tarifa.
El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible

para el mismo los proporciona IBM bajo los términos del IBM Customer Agreement, el IBM International Program License Agreement o cualquier acuerdo entre IBM y el usuario.

La información sobre productos no IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados u otras fuentes disponibles públicamente. IBM no ha probado dichos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad o cualquier otra información relacionada con productos no IBM. Las preguntas sobre las posibilidades de los productos no IBM deben dirigirse a los suministradores de dichos productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas del modo más completo posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier semejanza con los nombres y direcciones utilizados en una empresa real es una mera coincidencia.

Hoja de Comentarios

AIX 5L Versión 5.1
Guía de administración del Gestor del sistema basado en la Web

Por favor, sírvase facilitarnos su opinión sobre esta publicación, tanto a nivel general (organización, contenido, utilidad, facilidad de lectura,...) como a nivel específico (errores u omisiones concretos). Tenga en cuenta que los comentarios que nos envíe deben estar relacionados exclusivamente con la información contenida en este manual y a la forma de presentación de ésta.

Para realizar consultas técnicas o solicitar información acerca de productos y precios, por favor diríjase a su sucursal de IBM, business partner de IBM o concesionario autorizado.

Para preguntas de tipo general, llame a ″IBM Responde″ (número de teléfono 901 300 000).

Al enviar comentarios a IBM, se garantiza a IBM el derecho no exclusivo de utilizar o distribuir dichos comentarios en la forma que considere apropiada sin incurrir por ello en ninguna obligación con el remitente.

Comentarios:

Gracias por su colaboración.

Para enviar sus comentarios:
- Envíelos por correo a la dirección indicada en el reverso.
- Envíelos por correo electrónico a: aix6koub@austin.ibm.com

Si desea obtener respuesta de IBM, rellene la información siguiente:

Nombre	Dirección
Compañía	
Número de teléfono	Dirección de e-mail

Hoja de Comentarios

IBM S.A.
National Language Solutions Center
Avda. Diagonal, 571
Edif. ″L'Illa″
Barcelona 08029
España