

# Sun Java™ System Access Manager

## Notas de la versión

### Versión 6 2005Q1

2 de febrero de 2005

Número de pieza 819-1944

---

Estas notas de la versión contienen información importante disponible en el momento del lanzamiento de Sun Java System Access Manager 6 2005Q1 (conocido anteriormente como Sun Java System Identity Server). Aquí se tratan nuevas funciones y mejoras, limitaciones y problemas conocidos e información de otro tipo. Lea este documento antes de instalar y utilizar esta versión.

La versión más actualizada de estas notas de la versión se encuentra en el sitio Web de documentación de Sun Java System:

<http://docs.sun.com/prod/entsys.05q1>

Consulte el sitio Web antes de instalar y configurar el software, así como después, de forma periódica, para ver la documentación del producto y las notas de la versión más actualizadas.

En estas notas de la versión se incluyen los siguientes apartados:

- [Historial de revisiones de las notas de la versión](#)
- [Acerca de Access Manager 6 2005Q1](#)
- [Novedades de esta versión](#)
- [Errores solucionados en esta versión](#)
- [Notas de la instalación](#)
- [Limitaciones y problemas conocidos](#)
- [Archivos que se pueden distribuir](#)
- [Información sobre problemas y respuestas de los clientes](#)
- [Recursos adicionales de Sun](#)

Se hace referencia a las direcciones URL de otros fabricantes para proporcionar información adicional relacionada.

---

**NOTA** Sun no se responsabiliza de que los sitios Web de otros fabricantes aquí mencionados estén disponibles. Sun no respalda ni se hace responsable de ningún contenido, anuncio, producto ni de cualquier otro material disponible en dichos sitios o recursos. Sun declina toda responsabilidad en cuanto a daños reales o alegados o pérdidas que pudieran derivarse o estar relacionadas con el uso de los contenidos, artículos y servicios que estén disponibles en dichos sitios o recursos o a través de ellos.

---

---

## Historial de revisiones de las notas de la versión

**Tabla 1** Historial de revisiones

Fecha	Descripción de los cambios
2 de febrero de 2005	Versión 2005Q1. Primera publicación de estas notas de la versión.

---

---

## Acerca de Access Manager 6 2005Q1

Sun Java System Access Manager es una solución de administración de identidades diseñada para satisfacer las necesidades de empresas en rápida expansión. Access Manager permite obtener identidades para los empleados, los socios y proveedores en un directorio en línea. También permite establecer políticas y permisos relativos al acceso a información determinada en la empresa. Access Manager es la clave de todos los datos, los servicios y de quién tiene acceso a qué: es la clave de todas las relaciones de negocios internas y externas.

---

# Novedades de esta versión

Access Manager 2005Q1 incluye las funciones siguientes. Para obtener más información acerca de estas funciones, consulte la publicación *Visión general técnica de Sun Java System Access Manager*.

- El nombre del producto ha cambiado de Identity Server a Access Manager
- Compatibilidad con Solaris 10
- Compatibilidad con un nuevo contenedor Web: Sun Java System Application Server Enterprise Edition 8 2005Q1 (8.1)
- Módulos de autenticación nuevos o revisados:
  - Java Database Connectivity (JDBC)
  - Mobile Station ISDN (MSISDN)
  - Active Directory
  - Security Assertion Markup Language (SAML): la compatibilidad de autenticación de SAML se ha lanzado como un módulo de autenticación, mediante el cual la autenticación de SAML forma parte de la pila de autenticación.
- Recuperación ante fallos de la sesión
  - Dos o más instancias de Access Manager 6 2005Q1, cada una de las cuales funciona en un contenedor Web compatible en un servidor host diferente.
  - Clúster del intermediario de Message Queue que administra los mensajes de la sesión entre las instancias de Access Manager y la base de datos de almacenamiento de sesiones.
  - Berkeley DB de Sleepycat Software, Inc. (<http://www.sleepycat.com/>) como base de datos de almacenamiento de sesiones. El demonio del cliente de Berkeley DB es `amsessiondb`.
- La sección Administración de políticas incluye un nuevo complemento Resource Name (Nombre de recurso): `HttpURLResourceName`.
- Mejoras en la consola:
  - Capacidad de personalizar la visualización de cada tipo de objeto en el panel de navegación mostrando uno o varios atributos de dicho objeto.
  - Capacidad de agregar nuevos tipos de objetos en el menú desplegable del panel de navegación (por ejemplo, agregar una entrada para impresoras o edificios).

- SDK cliente:
  - Se vuelven a incluir componentes SDK (por ejemplo, componentes de autenticación, administración de servicios, administración de usuarios, SAML, políticas de cliente y sesión) de modo que los desarrolladores de aplicaciones Java pueden integrarse mejor con Access Manager.
  - Se ha eliminado la dependencia del archivo serverconfig.xml y se ha minimizado la huella de los archivos jar.
- Administración de federación
  - Compatibilidad con el protocolo de asignación de identificador de nombres Liberty Alliance Project (LAP)
  - Compatibilidad con la especificación de servicios de detección de LAP Identity Web Services Framework (ID-WSF), versión 1.1
  - Compatibilidad con la especificación de servicios de autenticación de LAP ID-WSF
  - Compatibilidad con la especificación de servicios de detección y descripción de metadatos LAP
  - Compatibilidad con los perfiles ampliados de LAP Liberty Identity Federation Framework (ID-FF):
    - Configuración de proxy de proveedor de identidades dinámico
    - Federación de afiliaciones
    - Federación única
    - Perfil de asignación de identificador de nombres
    - Perfil de cifrado de identificador de nombres
- Una secuencia de órdenes de ajuste de rendimiento está disponible para ajustar Application Server Enterprise Edition 8 2005Q1 (8.1) como un contenedor Web

# Requisitos de software y hardware

A continuación, se muestran el hardware y el software necesarios para esta versión de Access Manager.

**Tabla 2** Requisitos de software y hardware

Componente	Requisito
Sistema operativo	Sistema operativo (SO) Solaris™, SPARC® Platform Edition, versiones 8, 9 y 10 SO Solaris™, x86 Platform Edition, versiones 9 y 10 Red Hat™ Linux, Advanced Server 2.1 Update 2 Red Hat™ Linux, Advanced Server 3.0, 3.0 Update 1, 3.0 Update 2, 3.0 Update 3 Red Hat™ Linux, Advanced Server 3.0 Update 2 para AMD64
RAM	512 Mbytes
Espacio en disco	250 Mbytes para Access Manager y aplicaciones asociadas

## Exploradores compatibles

Esta versión de Access Manager admite los exploradores siguientes:

Explorador	Plataformas
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000, Sun Linux, Red Hat™ Linux 8.0
Microsoft Internet Explorer 6.0	Windows 2000, Windows™ XP, Sun Linux, Red Hat Linux 8.0
Mozilla 1.7.1	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris™ 9 y 10, SO Solaris™, x86 Platform Edition, versiones 9 y 10
Netscape™ 4.79	Windows NT, Solaris 8 y 9
Netscape™ 6.2.1	Windows NT, Windows 98, Sun Linux, Red Hat™ Linux Advanced Server 2.1, SO Solaris™, x86 Platform Edition, versiones 9 y 10
Netscape™ 7.0	Windows 2000, Sun Linux, Red Hat Linux 8.0, Solaris 9 y 10, SO Solaris™, x86 Platform Edition, versiones 9 y 10

# Errores solucionados en esta versión

La siguiente tabla describe los errores solucionados en Access Manager 2005Q1:

**Tabla 3** Errores solucionados en Access Manager 2005Q1

Número de error	Descripción
5050332	En los sistemas Linux, amserver stop no detiene el proceso amunixd
5049218	Error en la consola al buscar usuarios cuando la administración de usuarios está desactivada
5048378	Propiedad smtp server port incorrecta en AMConfig.properties
5043752	Aparece un mensaje de error al ejecutar am2bak
5042100	El administrador de políticas no puede modificar su propio perfil
5041529	Filtro BasicEntitySearch codificado para uid
5038600	No pueden crearse usuarios con el servicio SAML
5037978	Se genera un error al crear roles con permisos de acceso definidos como org admin
5026635	Las muestras de consolas no se compilan
5016725	Modificaciones en la regla de la política de referencia no reflejadas en la suborganización
5013994	Error en el inicio de sesión de Authlevel en exploradores en japonés
5008960	amadmin devuelve un mensaje de error incorrecto
4996479	Los servicios con esquema de política aparecen como susceptibles de ser agregados para un usuario
4961370	La máscara de búsqueda “***” no funciona
4959895	El filtro de búsqueda de descripciones de entidades no funciona correctamente
4959071	Las sesiones inactivas no se limpian
4931907	Los servicios desaparecen al iniciar sesión con un rol de servicio
4931163	Los atributos de nombre deben estar en minúsculas
4930610	Versión de los mensajes am2bak y bak2am sólo en inglés
4922030	Nivel de resolución de conflictos con una configuración regional determinada
4916683	Mensaje para los pares msgid-msgstr no traducido en backup_restore.po
4853809	Problema en el registro de servicios
4853809	El registro de todos los servicios quizá no afecte a todos los servicios disponibles

---

# Notas de la instalación

La secuencia de órdenes `amconfig` ahora admite la implementación de instancias adicionales de Access Manager utilizando Application Server Enterprise Edition 8 2005Q1 (8.1) como un contenedor Web, tras instalar la primera instancia con el instalador de Java Enterprise System.

Para obtener más información acerca de la ejecución de secuencias de órdenes de configuración, consulte la publicación *Access Manager 6 2005Q1 Administration Guide*.

Consulte también [Instalación](#) en [Limitaciones y problemas conocidos](#).

---

## Limitaciones y problemas conocidos

Este apartado contiene una lista de los problemas conocidos más importantes en el momento del lanzamiento de Access Manager 2005Q1. En este apartado se describen los temas siguientes:

- [Instalación](#)
- [Autenticación](#)
- [Muestras de Access Manager](#)
- [Herramientas de línea de comandos](#)
- [Configuración](#)
- [Consola de Access Manager](#)
- [Federación](#)
- [Servicio de registro](#)
- [Política](#)
- [Inicio de sesión único](#)
- [Access Manager SDK](#)
- [Internacionalización \(i18n\)](#)
- [Cookies](#)
- [Secuestro de cookies](#)

# Instalación

## **amadmin en instalaciones SDK con un servidor seguro genera excepciones (5107584)**

En Access Manager 2005Q1, si efectúa una instalación completa de un Access Manager seguro y posteriormente efectúa una instalación SDK para utilizar la instalación completa, es posible que se generen errores. Esto se debe a que la propiedad `com.iplanet.am.admin.sli.cerdb.prefix` presenta un valor incorrecto con Web Server.

### *Solución del problema*

1. Edite el archivo `AMConfig.properties`.
2. Cambie la propiedad `com.iplanet.am.admin.cli.certdb.prefix` a `https-<ws-instance-name>-<ws-hostname>-`.
3. Reinicie el servidor Web.

## **La instalación de AMSDK con contenedores Web contiene enlaces rotos a componentes compartidos en Linux (6199933)**

Si instala el Access Manager SDK en cualquier contenedor Web de la plataforma Linux, aparecerán varios enlaces rotos a componentes compartidos.

### *Solución del problema*

Quite los enlaces incorrectos y cree otros correctos.

Para quitar los enlaces:

```
cd ${AM_INSTALL_DIR}/identity/lib
rm -rf jaxrpc-spi.jar relaxngDatatype.jar xsdlib.jar
```

Para crear enlaces nuevos:

```
ln -s /opt/sun/private/share/lib/jaxrpc-spi.jar
ln -s /opt/sun/private/share/lib/relaxngDatatype.jar
ln -s /opt/sun/private/share/lib/xsdlib.jar
```

## **Una errata en el argumento al complemento de integridad referencial repercute en el rendimiento (5029256)**

Cuando Access Manager habilita el complemento de integridad referencial para Directory Server, en el argumento 11 del complemento, el nombre del atributo presenta una errata. El nombre del atributo aparece como `iplanet-am-modifiable-by`. Por consiguiente, aparecerá una advertencia de búsqueda no indexada en el registro de errores del directorio cuando se elimina una organización.



El complemento de integridad referencial necesita que todos los atributos mencionados en sus argumentos se indexen, y el atributo indexado es `iplanet-am-modifiable-by`. Esto puede repercutir en el rendimiento de Access Manager.

### **xercesImpl.jar de Application Server hace que falle JVM (6223676)**

`xercesImpl.jar` de Application Server 8.1 EE en `/opt/sun/appserver/lib` para RedHat Linux (o `/opt/SUNWappserver/appserver/lib`) para Solaris se carga antes que la versión de los componentes compartidos de `xercesImpl.jar` en `/opt/sun/share/lib` para RedHat Linux (o `/usr/share/lib` para Solaris).

El cargador de clases carga la versión de Application Server antes que la versión de los componentes compartidos. Cuando esto ocurre, la versión no actualizada de Application Server no puede seguir con miles de JSP esperando a ser procesados. JVM se bloquea o deja de funcionar.

### *Solución del problema*

Cambie el nombre de `xercesImpl.jar` en `opt/sun/appserver/lib` para Red Hat AS 2.1 o 3.0 o en `/opt/SUNWappserver/appserve/lib` para Solaris 9 o 10 para SPARC y x86. El cargador de clases de JVM se verá obligado a utilizar el comando `xerceImpl.jar` de los componentes compartidos en `/opt/sun/share/lib` para Red Hat AS 2.1 o 3.0 o en `/usr/share/lib` para Solaris 9 y 10.

### **El instalador no permite que el usuario introduzca un protocolo durante la instalación de AM SDK (6180090)**

Si instala Access Manager SDK, el panel “Access Manager: Web Container for running Sun Java System Access Manager Services” (Access Manager: contenedor Web para ejecutar los servicios de Sun Java System Access Manager) no solicitará el protocolo del contenedor Web que ejecuta los servicios de Access Manager. El instalador asume que el contenedor Web utiliza el protocolo `http`. Sin embargo, es posible que deba especificar el protocolo `https` para acceder a una instalación SDK que utiliza una instalación Access Manager habilitada para SSL.

### *Solución del problema*

En el archivo `AMConfig.properties`, establezca el protocolo asociado a la instalación del servidor de Access Manager en `https`. Por ejemplo:

```
com.iplanet.am.server.protocol=https
com.iplanet.am.console.protocol=https
```

### **Access Manager agrega servlet.jar a la variable CLASSPATH del servidor (5016348)**

Access Manager coloca un comando `servlet.jar` en la variable `CLASSPATH` del servidor para los contenedores Web compatibles. Este archivo puede provocar resultados inesperados porque cada contenedor Web agrupa un archivo `servlet.jar` en su implementación.

### *Solución del problema*

Quite el archivo `servlet.jar` de la variable `CLASSPATH`.

## Muestras de Access Manager

### **Las muestras devuelven advertencias al compilarse con JDK 1.5 (5102149)**

Las muestras que se incluyen con Access Manager devuelven advertencias si se compilan con JDK 1.5.

#### *Solución del problema*

Tome las medidas siguientes para evitar que aparezcan estas advertencias:

- Cuando utilice JDK 1.5, agregue `encoding="ISO-8859-1"` en la línea de comandos de compilación
  - o
- utilice JDK 1.4 para compilar las muestras.

### **Las omisiones en la muestra `xmlsig` de SAML provocan fallos en la compilación (5090925)**

Las omisiones en las muestras `xmlsig` de SAML provocan fallos en la compilación si se realiza con JDK 1.5. Este problema se puede evitar si se compila con JDK 1.4.2.

#### *Solución del problema*

Si compila con JDK 1.5, siga estos pasos para configurar `LD_LIBRARY_PATH`:

1. Busque el archivo `Readme.html` o `Readme.txt` para las muestras SAML en el directorio `xmlsig`.
2. En la sección 3 “Instructions to set up the XMLSIG sample on Solaris” (Instrucciones para configurar la muestra XMLSIG en Solaris), en el paso 4, defina `LD_LIBRARY_PATH` en `web-server-install-directory/bin/https/lib`.
3. Agregue `/usr/lib/mps/secv1` a `LD_LIBRARY_PATH` para seleccionar la biblioteca JSS y sus dependencias.

## Autenticación

### **La notificación de modificación de usuario enviada por correo electrónico no funciona (6212964)**

La notificación de modificación de usuario enviada por correo electrónico, que se encuentra en el servicio de administración, no funciona en estos momentos.

**Las conexiones SafeWord no están cerradas (5073718)**

Si intenta iniciar sesión en Access Manager, vaya a la página de respuesta de desafío SafeWord y no introduzca nunca una contraseña. No hay tiempo de espera en la conexión. Si cierra el explorador, la conexión nunca se cierra con el servidor SafeWord.

**La autenticación LDAP realiza una conexión anónima para conectarse con el servidor de directorio LDAP (5090018)**

Access Manager no transfiere el DN de conexión ni la contraseña al servidor de directorio para una conexión LDAP, lo cual afecta a la autenticación cuando se desactiva la conexión anónima en el servidor de directorio LDAP.

*Solución del problema*

Active la conexión anónima para el servidor de directorio.

**La propiedad del modo de cookies persistentes es incoherente (5038544)**

En este modo, la propiedad UserId configurada en el testigo es incoherente. Por este motivo, puede dar error el agente de políticas, que depende de la propiedad UserID.

*Solución del problema*

Use UserToken para un valor que no sea DN y Principal para el valor DN.

**La recarga de la página de tiempo de espera de sesión autenticará al usuario con un nombre de usuario y una contraseña válidos (4697120)**

En la página de inicio de sesión, si el usuario aguarda a que se agote el tiempo de espera de carga de la página y, a continuación, introduce un nombre de usuario y una contraseña válidos, verá la página de tiempo de espera de sesión. El usuario se autenticará en Access Manager si vuelve a cargar la página sin volver a introducir el nombre de usuario y la contraseña.

**Se deben especificar diferentes directorios para varios servidores de SafeWord (4756295)**

Una configuración con varias organizaciones que utilicen sus propios servidores SafeWord debe especificar sus propios directorios `.../serverVerification` en las plantillas de servicio de autenticación de SafeWord. Si deja el valor predeterminado y todos los servidores utilizan el mismo directorio, la primera organización que realice una autenticación con su servidor SafeWord será la única que funcione.

## Herramientas de línea de comandos

### Las utilidades `ldapsearch` y `ldapmodify` en el directorio `/opt/SUNWam/bin` no funcionan correctamente (4954779)

Las utilidades `ldapsearch` y `ldapmodify` en el directorio `/opt/SUNWam/bin` devuelven errores graves.

#### *Solución del problema*

Agregue la ruta `DirectoryServer-base/lib/` a la variable de entorno `LD_LIBRARY_PATH`.

### Las secuencias de órdenes `am2bak` y `bak2am` no funcionan en Linux (5053866)

Las secuencias de órdenes de restauración `am2bak` y `bak2am` no funcionan si Access Manager se ejecuta en un sistema Linux.

#### *Solución del problema*

1. Corrija la ruta de los siguientes comandos:

- o `ECHO=/usr/bin/echo` debe ser `ECHO=/bin/echo`
- o `uid='/usr/xpg4/bin/id -un'` debe ser `uid='/usr/bin/id -un'`
- o `/usr/bin/tar` debe ser `/bin/tar`
- o `/usr/bin/rm` debe ser `/bin/rm`
- o `/usr/bin/grep` debe ser `/bin/grep`
- o `/usr/bin/ps` debe ser `/bin/ps`
- o `/usr/bin/ls` debe ser `/bin/ls`

2. Modifique la función `check_for_invalid_chars()`. Por ejemplo:

```
check_for_invalid_chars() {  
echo "$1" | grep '[^/_.a-zA-Z0-9a-]' > /dev/null  
if [ $? = 0 ]; then  
return 1  
else  
return 0  
fi  
}
```

### `amadmin` devuelve un mensaje de error incorrecto (5008960)

La opción `import` de `amadmin` produce de forma incorrecta el mismo mensaje de error para todos los errores relacionados.

**amverifyarchive en instalaciones sólo en consolas tiene etiquetas sin intercambiar (4993375)**

Si realiza una instalación sólo en la consola de Access Manager, la utilidad `amverifyarchive` no tendrá las siguientes etiquetas intercambiadas en esta secuencia de órdenes: `JSSHOME`, `JDK_HOME`, `BASEDIR` y `PRODUCT_DIR`.

## Configuración

**WebSphere Application Server 5.1 no se puede iniciar tras realizar correctamente la configuración en Linux (6204646)**

Si instala el componente Access Manager SDK para WebSphere en Linux y posteriormente ejecuta `amwas51config` con el archivo correcto `amsamplesilent`, WebSphere no se podrá iniciar.

*Solución del problema*

Agregue `/opt/sun/private/lib` en la variable `LD_LIBRARY_PATH` como se muestra a continuación:

```
LD_LIBRARY_PATH="$WAS_LIBPATH":$LD_LIBRARY_PATH:/opt/sun/private/lib
export LD_LIBRARY_PATH ;;
```

En `server.xml`, quite `"/:` antes de la opción `the -Djava.util.logging.config.class`.

**El alias certdb no se ha definido correctamente para Web Server (6212532)**

Si habilita SSL para Web Server con Access Manager y posteriormente ejecuta `amadmin`, generará el error `"namingservice not available"` (`namingservice` no disponible). Si usa el explorador, éste funcionará como era de esperar.

**Los índices siempre se crean para userRoot independientemente del nombre del servidor (5002886)**

`index.ldif` codifica `userRoot` y crea el índice para los atributos. Es posible instalar Access Manager en un sufijo raíz que resida en cualquier nombre de base de datos secundaria arbitraria. El nombre de este servidor puede obtenerse mediante `ldapsearch` con la base `cn=config` utilizando `nsslapd-suffix=SUFFIX_NAME` como filtro.

## Federación

**La persona de contacto de la administración de federación genera una excepción (6213102)**

Si crea un nuevo proveedor y agrega una nueva persona de contacto a ese proveedor, es posible que reciba el siguiente error:

```
El servidor encontró un error interno () que impide satisfacer la solicitud
```

### **El registro remoto no funciona para los registros amFederation.access (6197608)**

Una vez configurado el registro remoto, todos los registros se escriben de forma correcta en la instancia remota de Access Manager, con la excepción de amFederation.access. La entrada de registro no se escribe.

#### *Solución del problema*

Utilice `AccessController.doPrivileged(AdminTokenAction.getInstance());` en `LogUtils`.

### **El estado fedCookie no cambia (6202574)**

Si realiza una terminación de federación para usuarios federados en SP e IDP, el estado de `fedCookie` seguirá mostrando YES (Sí). Debería mostrar NO.

### **Se ha producido un error en los contenedores de perfil personal al realizar una consulta o una modificación (6189808)**

Se produce un error en los siguientes contenedores de perfil personal al realizar una consulta o una modificación:

`LegalIdentity/Gender`

`EmploymentIdentity/AltO`

### **Excepción producida para modificar PP si el valor del atributo está vacío (5047103)**

Access Manager genera una excepción cuando se realiza una modificación de PP con un valor de atributo vacío. Por ejemplo, si crea la configuración para probar la muestra `sis-ep` y después envía la página EP Modify y hace clic en el botón sin escribir un valor para el atributo, la excepción se producirá incorrectamente.

### **Para que surta efecto la política debe reiniciar el servidor (5045036)**

La implementación de políticas de federación no surte efecto hasta que reinicie el servidor. Esto es válido para Application Server y para Web Server. Debe reiniciar el servidor sólo tras una instalación nueva y cuando se implemente por primera vez la política.

## Consola de Access Manager

### **No se pueden crear usuarios con un número considerable de contenedores de personas en el DIT (5079609)**

Si crea un número considerable de contenedores de personas (más de mil) y posteriormente inicia la sesión en la consola de Access Manager y crea un nuevo usuario, el usuario no se creará porque no se encontrarán dichos contenedores.

Esto se debe a que se produce un error en `UMCreateUserModelImpl.getPeopleContainers()` con errores de límite de tiempo de búsqueda, a pesar de que Directory Server encuentra un gran número de contenedores de personas antes de alcanzar el límite de tiempo.

### *Solución del problema*

Active la opción Mostrar contenedores de personas en la consola de Access Manager, vaya al contenedor de personas específico y cree usuarios en él.

### **El rol de Administrador del centro de ayuda de nivel superior con acceso de sólo lectura puede crear usuarios nuevos (5109348)**

En estos momentos, el valor predeterminado para el rol de Administrador del centro de ayuda está ajustado en Acceso completo. Si lo cambia a Modificar desactivará los botones Nuevo y Eliminar del marco de navegación, pero el administrador todavía podrá modificar las propiedades de entrada del usuario.

### *Solución del problema*

Abra la página de propiedades Administrador del centro de ayuda y cambie la visualización a las acciones disponibles. Localice la fila Usuario y cambie la configuración de Acceso completo a Modificar.

### **Generación de error al seleccionar la opción Afiliado de una entidad afiliada (6203563)**

En el módulo Administración de federación, se generará una excepción cuando seleccione Ver>Afiliados en la página de la entidad afiliada.

### *Solución del problema*

Modifique JSP para que el atributo de altura esté fuera de la etiqueta de cierre JATO. En `FSAffiliateProfile.jsp`, la línea 104 cambia a:

```
<td width="1%"> height="1" alt=""></td>
```

Tenga en cuenta que `/>` precede al atributo de altura.

### **Error en la opción Affiliates Display (Pantalla de afiliaciones) (6194139)**

Access Manager devolverá una página de error cuando la opción Affiliates Display (Pantalla de afiliaciones), en el módulo Administración de federación, sea la única opción del menú y esté definida como predeterminada.

### **No se pueden modificar servicios de usuarios como rol de Administrador de personas (6174652)**

Si ha iniciado sesión con el rol de Administrador de personas de nivel superior, puede agregar un nuevo servicio a un usuario, pero no puede modificar los servicios.

### *Solución del problema*

Edite el perfil de visualización para el rol de Administrador de personas y otórguele los menús de visualización necesarios y las acciones disponibles.

#### **Valores no conservados al hacer clic en el botón “Atrás” (4992972)**

Siempre que haya un proceso de varias páginas, como crear un grupo, un rol o añadir una condición a una política, y siempre que se pulse el botón “Atrás”, los valores de la página anterior no se restaurarán.

#### **Problemas de actualización para los proveedores alojados del módulo Administración de federación (4915894)**

En el módulo Administración de federación, si modifica y guarda cualquier atributo en la vista del proveedor de identidades de un proveedor alojado, los cambios se guardarán, pero no se actualizarán automáticamente en la pantalla.

### *Solución del problema*

Seleccione un módulo diferente para salir del módulo Administración de federación (por ejemplo, Configuración de servicio) y, a continuación, vuelva al módulo Administración de federación. De esta forma, se actualizará la pantalla.

#### **La consola no actualiza los cambios de atributo del usuario (4931455)**

El marco de navegación de la consola de Access Manager no se actualiza para reflejar los cambios en los valores de atributos del usuario realizados en el marco de datos. Actualice manualmente la página para mostrar los valores modificados.

#### **Problemas de puerto con Internet Explorer (4864133)**

Debido a una incompatibilidad con Internet Explorer, no debería utilizar el número de puerto 80 como puerto de Access Manager al ejecutar http o 443 al ejecutar https.

## Servicio de registro

#### **Problema de registro cuando Java Security está activo (4926520)**

Puede que `jdk_logging.jar` no funcione si Java Security está activo.

### *Solución del problema*

Si Java Security está activo y tiene una versión de JDK anterior a la 1.4, incluya la siguiente autorización en el archivo de seguridad de Java:

```
permission java.lang.RuntimePermission shutdownHooks
```



# Política

## **Las entradas coincidentes no se devuelven cuando se alcanza el límite definido en nslookthrough (5013538)**

Las entradas coincidentes no se devuelven a la consola de Access Manager, ni siquiera tras alcanzar los límites de administración definidos en nslookthrough.

### *Solución del problema*

Ajuste el parámetro nslookthroughlimit para compensar el número de entradas.

## **Política no aplicada para testigos con alias (4985823)**

Si utiliza un alias de usuario para iniciar sesión en Access Manager en un módulo de autorización distinto de LDAP o Condición de miembro y después intenta acceder a un recurso protegido, se le denegará el acceso.

## **Problema con la política de muestra (4923898)**

El archivo `Readme.html` ubicado en la política de muestra excluye información que provoca que la muestra no funcione.

### *Solución del problema*

Para que funcione la muestra, la variable de entorno `LD_LIBRARY_PATH` debe incluir la ruta a las bibliotecas compartidas `NSPR`, `NSS` y `JSS`. Ajuste `LD_LIBRARY_PATH` para que incluya `/usr/lib/mps/secv1` para los sistemas Solaris o `/opt/sun/private/lib` para los sistemas Linux.

# Access Manager SDK

## **La unicidad del atributo se ha interrumpido en las organizaciones de nivel superior para los atributos de nombre (6204537)**

La unicidad del atributo para los atributos de nombre no funciona en la organización de nivel superior. Sin embargo, la unicidad del atributo de usuario y organización se aplica correctamente.

## **EventService funciona en un bucle estrecho cuando no obtiene una conexión de búsqueda persistente (6205443)**

El subproceso EventService (ES) agrega correctamente las escuchas (LDAP JDK agrega correctamente la escucha), incluso cuando el número de búsquedas persistentes está conectado. Sin embargo, cuando un subproceso ES intenta obtener una respuesta, una respuesta LDAP notifica (código de error 51) que las conexiones de búsquedas persistentes no están disponibles. A continuación, el subproceso ES intenta volver a establecer las escuchas, por lo que se convierte en un bucle estrecho.

## Uso de certutil para instalaciones de Access Manager SDK que utilizan servidores SSL (5027614)

Los usuarios experimentan errores y excepciones relacionados con la seguridad al intentar establecer comunicación desde equipos sólo SDK con servidores de Access Manager habilitados para SSL. En esta situación, la instalación de Access Manager SDK no se implementa en ningún contenedor Web o se implementa en un contenedor Web de terceros, como BEA WebLogic Server o IBM WebSphere Application Server.

### *Solución del problema*

Cree una base de datos de certificados en el equipo sólo SDK e instale el certificado de CA raíz del servidor de Access Manager en esta base de datos:

1. Inicie sesión en el equipo sólo SDK como superusuario (root).
2. Compruebe que el paquete NSS (Netscape Security Services) necesario está instalado:
  - o En los sistemas Solaris: SUNWtlsu
  - o En los sistemas Linux: sun-nss RPM
3. Si el paquete no está instalado, instálelo. Por ejemplo:

En los sistemas Solaris:

```
cd JavaEnterpriseSystem_base/Solaris_arch/Product/shared_components/Packages
pkgadd -d . SUNWtlsu
```

En los sistemas Linux:

```
cd JavaEnterpriseSystem_base/Linux_x86/Product/shared_components/Packages
rpm -Uvh sun-nss-3.3.10-1.i386.rpm
```

4. Cree el archivo para la contraseña del testigo de la base de datos de certificados.  
Por ejemplo:

En los sistemas Solaris:

```
echo "cert-database-password" > /etc/opt/SUNWam/config/.wtpass
chmod 700 /etc/opt/SUNWam/config/.wtpass
```

En los sistemas Linux:

```
echo "cert-database-password" > /etc/opt/sun/identity/config/.wtpass
chmod 700 /etc/opt/sun/identity/config/.wtpass
```

donde *cert-database-password* es la contraseña del testigo.

5. Compruebe la variable LD\_LIBRARY\_PATH:

En los sistemas Solaris, compruebe LD\_LIBRARY\_PATH para ver si están presentes los directorios /usr/lib, /usr/lib/mps/secv1 y /usr/lib/mps. Si no están presentes, añada los directorios que faltan.

En los sistemas Linux, compruebe LD\_LIBRARY\_PATH para ver si está presente el directorio /opt/sun/private/lib. Si no lo encuentra, añádalo.

6. Utilice la herramienta de base de datos de certificados (certutil) para crear las bases de datos de certificados y claves. Para obtener información sobre certutil, consulte el siguiente sitio Web:

<http://mozilla.org/projects/security/pki/nss/tools/certutil.html>

Por ejemplo:

```
certutil-home/certutil -N -d cert-database-dir -f config-home/.wtpass
```

donde:

*certutil-home* es la ubicación de certutil:

- o En los sistemas Solaris: /usr/sfw/bin
- o En los sistemas Linux: /opt/sun/private/bin

*cert-database-dir* es el directorio de las bases de datos de certificados y claves.

*config-home* es la ubicación de los archivos de configuración de Access Manager:

- o En los sistemas Solaris: /etc/opt/SUNWam/config
- o En los sistemas Linux: /etc/opt/sun/identity/config

7. En la base de datos de certificados recién creada, añada el certificado de CA raíz para el certificado SSL instalado en el servidor de Access Manager. Por ejemplo:

```
certutil-home/certutil -A -n "certificate-nickname" -t "TCu,TCu,TCuw" -d
cert-database-dir -a -i path-to-file-containing-cert -f config-home/.wtpass
```

8. Utilice un editor para ver el archivo AMConfig.properties y compruebe los siguientes valores:

- o Directorio de base de datos de certificados: com.iplanet.am.admin.cli.certdb.dir
- o Prefijo: com.iplanet.am.admin.cli.certdb.prefix
- o Archivo de contraseñas: com.iplanet.am.admin.cli.certdb.passfile

Si no son correctos, edite las preferencias como sea necesario. Por ejemplo, la preferencia de prefijo debería estar vacía (es decir, igual a "").

9. Si se han realizado cambios en `AMConfig.properties` y se ha implementado Access Manager SDK en un contenedor Web, reinicie el contenedor.

### **El protocolo de enlace SSL falla con DNSAlias con el proveedor JCE (5038876)**

El protocolo de enlace SSL falla cuando se utilizan certificados con nombres `DNSAlias` válidos en `subjectAltname` con un proveedor JCE.

### **Los métodos de identidad en Init() de los filtros hacen que falle WebLogic (5016283)**

Un servidor WebLogic no se inicia cuando los métodos de `init()` de filtros tienen código relativo a Access Manager. Se llama a la API de Access Manager en el método `init` del servlet `ServletFilter`.

Access Manager usa JSS como proveedor de seguridad, pero WebLogic utiliza JCE de forma predeterminada. Cuando se ejecuta el método `init`, WebLogic intenta validar su licencia utilizando JCE, pero JSS se está inicializando.

#### *Solución del problema*

Cambie el cifrado de seguridad predeterminado de `JSSEncryption` a `JCEEncryption` en el archivo `AMConfig.properties`.

### **No se puede utilizar ninguna contraseña que empiece por los símbolos “{SSHA}” (4966191)**

Access Manager no es compatible con el uso de símbolos en hash `{SSHA}` en contraseñas.

### **La opción para crear grupos añade solamente un atributo memberURL (4931958)**

Si crea un grupo con la opción de filtro de LDAP múltiple (`-f`), el grupo se creará incorrectamente con un solo atributo `memberURL`.

## Ajuste

### **amtune y los archivos asociados no se entregan para Solaris-x86 (6213019)**

En esta versión, la secuencia de órdenes `amtune` y los archivos asociados correspondientes no se instalan en el directorio apropiado para Solaris-x86.

#### *Solución del problema*

Utilice los archivos `amtune` entregados para Sparc-Solaris.

### **La secuencia de órdenes amtune-as8 contiene un error para el archivo de contraseña (6212380)**

El ajuste automatizado para Application Server 8 (`amtune-as8`) con la secuencia de órdenes `amtune` no funciona porque se ha creado un archivo de contraseña temporal con la contraseña `asadmin`. En estos momentos, el archivo sólo incluye la contraseña.

### *Solución del problema*

En `amtune-as8`, utilice la sintaxis siguiente para introducir la cadena:

```
"TOKEN=Value"
```

Por ejemplo:

```
"AS_ADMIN_PASSWORD=11111111"
```

Introduzca este cambio `amtune-env`:

```
#ASADMIN=$CONTAINER_BASE_DIR/bin/asadmin
```

```
ASADMIN=/opt/SUNWappserver/appserver/bin/asadmin
```

## Inicio de sesión único

### **No es posible ejecutar SSO con diferentes URI de implementación (4770271)**

Si los URI de implementación son diferentes en dos instancias distintas de Access Manager, el inicio de sesión único no funcionará correctamente.

## Internacionalización (i18n)

### **Los miembros del grupo no aparecen enumerados si el nombre del grupo contiene caracteres de varios bytes (6197041)**

En la versión internacionalizada de Access Manager 6 2005Q1, los miembros de los grupos no aparecen enumerados en la consola de Access Manager si el nombre del grupo contiene caracteres de varios bytes.

### **Los mensajes de inicio y detención no se pueden leer en Linux (6207421)**

Los mensajes de inicio y detención de Access Manager para el conjunto de caracteres `zh/zh_TW` no se pueden leer. Esto ocurre en la plataforma Linux.

### **No se puede iniciar sesión con los módulos HTTPBasic y WindowsDesktopSSO en una configuración regional diferente del inglés (6209324)**

No puede iniciar sesión en los módulos de autenticación HTTPBasic y WindowsDesktopSSO con una configuración regional diferente del inglés.

### *Solución del problema*

Restablezca estos parámetros al inglés en los archivos XML:

```
HTTPBasic.xml: <HTTPHeader>Authorization</HTTPHeader>
```

```
WindowsDesktopSSO.xml: <HTTPHeader>Authorization</HTTPHeader>
```

Estos archivos se instalan normalmente en el directorio siguiente cuando Access Manager se implementa en Application Server:

```
/var/opt/sun/appserver/domains/domain1/applications/j2ee-modules/amserver/config/auth/default_<lang>
```

Estos archivos se instalan normalmente en el directorio siguiente cuando Access Manager se implementa en Web Server:

```
/opt/sun/webserver/https-<host>/is-web-apps/services/config/auth/default_<lang>
```

### **La ayuda en pantalla en japonés aparece incorrectamente (5024138)**

Si está ejecutando la versión en japonés de Access Manager y cambia el idioma a en\_US, se seguirá viendo el contexto de la ayuda en japonés.

### *Solución del problema*

Cree un enlace simbólico de docs\_en a docs\_en\_US.

### **La función Client Detection no opera correctamente (5028779)**

En el servicio Client Detection, la eliminación de UTF-8 no funciona correctamente.

### *Solución del problema*

Si quita el conjunto de caracteres UTF-8, reinicie el contenedor Web tras haber realizado el cambio.

### **G11NSetting no gestiona un espacio en el factor Q (5008860)**

Cuando los datos del cliente tienen un espacio en el factor q o a su alrededor, el código G11NSettings no lo analiza correctamente y devuelve el siguiente error:

```
ERROR: G11NSettings::Fetchcharset() Unable to parse charset entry invalid Q q
```

### **La página de inicio de sesión falla con el parámetro de rol de varios bytes en la dirección URL para el conjunto de caracteres ja (4905708)**

Si crea un rol de varios bytes y después intenta iniciar una sesión con una dirección URL como usuario registrado en este rol, la página de inicio generará un error.

### *Solución del problema*

Para que el marco de autenticación pueda decodificar un valor de rol de varios bytes especificado en la URL, debe especificar `gx_charset` junto con el parámetro. Por ejemplo:

```
http://hostname:port/amserver/UI/Login?role=manager?role=%E3%81%82%&gx_charset=utf-8
```

### **Los archivos de registro están distorsionados en la configuración regional en japonés (4882286)**

El siguiente archivo de registro contiene caracteres japoneses y se distorsionan al abrirlos:

Todos los archivos incluidos en el directorio `/var/opt/SUNWam/debug`, excepto `deploy.log` y `undeploy.log`.

### **El parámetro de configuración regional de la dirección URL muestra páginas de inicio con caracteres mezclados (4915137)**

Si utiliza un navegador que no esté en inglés con una instancia de Access Manager instalada con Web Server e inicia la sesión en `http://host:port/amserver/UI/Login?locale=en`, la página de inicio se abrirá con caracteres ingleses y no ingleses mezclados.

### *Solución del problema*

Cambie el siguiente enlace simbólico:

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default
```

por

```
AccessManager-base/SUNWam/web-apps/services/config/auth/default_en
```

### **Configuraciones regionales mezcladas en la ventana de inicio cuando Application Server es ja (4932089)**

La ventana de inicio de sesión de Access Manager no volverá a su configuración predeterminada en inglés cuando la preferencia de idioma del navegador sea `en` y la configuración regional de Application Server se defina en `ja`.

### *Solución del problema*

Ejecute Application Server con la configuración regional `en`.

### **La notificación de bloqueo envía un mensaje de correo electrónico ilegible (4938511)**

Si ejecuta Access Manager con un contenedor Web que tenga como configuración regional preferida alguna distinta a `c` y si se bloquea el acceso de un usuario en el servidor, se enviará un mensaje de correo electrónico con la notificación de bloqueo, pero éste será ilegible.

### *Solución del problema*

Defina `email|local|charset` (en lugar de únicamente el parámetro `email`) en la dirección de correo electrónico para el atributo de envío de notificación de bloqueo. Por ejemplo:

```
usuario1@ejemplo.com|zh|GB2312
```

### **Los nombres de varios bytes no funcionan en el autorregistro (4732470)**

Si crea un usuario en el módulo de autorregistro (servicio de autenticación de condición de miembro) con un identificador de usuario duplicado y un nombre y apellido de varios bytes, se generará un error. Los identificadores de usuarios de varios bytes no son compatibles.

### *Solución del problema*

Si un usuario inicia la sesión utilizando el autorregistro en un entorno de varios bytes, el administrador debe asegurarse de que el atributo User Generator Mode de Core Authentication no se seleccione.

Otra opción es

El usuario puede seleccionar la opción “Crear el mío” en la página de inicio de sesión del autorregistro.

### **La versión en japonés de Access Manager no funciona con Netscape 6.22 ni 6.23 (4902421)**

En la versión en japonés de Access Manager, no puede iniciar sesión en la consola con Netscape 6.22 ni 6.23.

### **El formato de las condiciones de hora no varía (4888416)**

En las condiciones de hora para las definiciones de la política, la visualización de la hora sigue siendo la siguiente, independientemente de la configuración regional:

```
Hora:Minuto a.m./p.m.
```

### **Pantalla de detección de cliente no traducida (4922013)**

Algunas partes de la pantalla de propiedades del estilo actual de la interfaz de detección de cliente no están traducidas en esta versión.

### **Las propiedades de cliente genericHTML actualizadas no se han aplicado (4922348)**

Si elimina UTF-8 de la lista de conjuntos de caracteres de la propiedad de cliente genericHTML del servicio de detección de cliente, guarda los cambios y activa “Detección de cliente” y, a continuación, cierra la sesión y vuelve a iniciarla, la página de inicio seguirá teniendo el conjunto de caracteres UTF-8.



### *Solución del problema*

Reinicie el servidor manualmente con `amserver`.

#### **Encabezados de archivos de registro no traducidos (4923536)**

Las dos primeras líneas de los archivos de registro no están traducidas, en concreto, las secciones `Version` y `Fields` y sus listas de campos.

#### **Valores del campo Data no traducidos en amSSO.access (4923549)**

En el archivo de registro `amSSO.access`, no aparece traducido ningún valor del campo `Data`.

#### **Exception.jsp tiene mensajes codificados (4772313)**

`Exception.jsp` no está traducido y contiene títulos, mensajes de error e información de copyright codificados. Esta página jsp de error de excepción se ejecuta sólo en casos extremos, por ejemplo, cuando está desconectado Directory Server o cuando no se puede acceder a servicios de Access Manager y no hay traducción disponible para esta página jsp.

## Cookies

#### **El modo sin cookies no funciona (4967866)**

Si un navegador que admite cookies accede a Access Manager y se desactiva la admisión de cookies, éste seguirá enviando la cookie más antigua de Access Manager. Esto hace que se deniegue el acceso a los recursos de Access Manager.

### *Solución del problema*

Opte por una de estas soluciones:

- Borre la memoria caché de las cookies del navegador para quitar todas las cookies de Access Manager.
- Desactive las cookies del navegador.

## Secuestro de cookies

**La seguridad puede estar en peligro cuando no son fiables las aplicaciones que utilizan las cookies de sesión.**

Cuando se activa el inicio de sesión único (SSO) o el inicio de sesión único entre dominios (CDSSO) en la implementación de Access Manager, las cookies de sesión `http(s)` se configuran en el navegador del usuario. Estas cookies se validan en varias aplicaciones. Cuando Access Manager se implementa en varios dominios DNS, el protocolo Liberty transfiere las cookies de sesión `http(s)` desde el dominio DNS autenticado al dominio de destino de la aplicación Web.

Aunque el usuario inicia la sesión automáticamente en los recursos Web, existe un problema de seguridad conocido cuando no son fiables las aplicaciones que utilizan las cookies de sesión. El problema puede existir cuando un proveedor de identidades ofrece información de autenticación, autorización y perfil sobre un usuario a aplicaciones (o proveedores de servicio) que desarrollan otros fabricantes o grupos no autorizados de la empresa. Los posibles problemas de seguridad son:

- Todas las aplicaciones comparten la misma cookie de sesión `http`. Esto permite que una aplicación camuflada secuestre la cookie de sesión y suplante al usuario en otra aplicación.
- Si la aplicación no utiliza el protocolo `https`, la cookie de sesión es propensa al espionaje en la red.
- Aunque sólo pueda secuestrarse una aplicación, se pondrá en peligro la seguridad de toda la infraestructura.
- Una aplicación camuflada puede utilizar la cookie de sesión para obtener y, posiblemente, modificar los atributos del perfil de un usuario. Si el usuario tiene privilegios administrativos, la aplicación podría causar mucho más daño.

### *Solución del problema*

Siga estos pasos:

1. Use la consola de administración de Access Manager para crear una entrada para cada agente.
  - a. En la organización que contiene el agente que se va a crear, elija “Agentes” en el menú “Ver” y, después, haga clic en “Nuevo”.

- b. Escriba la siguiente información:

**Nombre.** Escriba el nombre o la identidad del agente. Ejemplo: agente123

**Contraseña.** Introduzca la contraseña del agente. Ejemplo: agente123

**Confirmar contraseña.** Confirme la contraseña.

**Descripción.** Escriba una breve descripción del agente. Por ejemplo, puede escribir el nombre de la instancia de agente o el de la aplicación que está protegiendo.

**Valor de clave de agente.** Configure las propiedades del agente con un par valor/clave. Esta propiedad la utiliza Access Manager para recibir solicitudes de los agentes para aserciones de credenciales acerca de los usuarios.

Escriba un valor de propiedad para agentRootURL con un valor equivalente a la dirección URL del agente con número de puerto. Tenga en cuenta que el valor de agentRootURL distingue entre mayúsculas y minúsculas.

Ejemplo: agentRootURL=http://nombre\_servidor:99/

**Estado de dispositivo.** Escriba el estado del dispositivo del agente. Si se configura como activado, el agente podrá autenticar Access Manager y comunicarse con él. Si se configura como inactivo, el agente no podrá autenticar Access Manager.

- c. Haga clic en "Aceptar".

2. Ejecute el siguiente comando en la contraseña que se escribió en el paso 1b.

```
AccessManager-base/SUNWam/agents/bin/crypt_util agente123
```

Esto producirá el siguiente resultado:

```
WnmKUCg/y3l404ivWY6HPQ==
```

3. Cambie `AMAgent.properties` para reflejar el nuevo valor y después reinicie el agente. Ejemplo:

```
# El nombre de usuario y la contraseña que utilizará para el módulo de autenticación
de la aplicación.

com.sun.am.policy.am.username = agente123
com.sun.am.policy.am.password = WnmKUCg/y31404ivWY6HPQ==

# URL de inicio de sesión único entre dominios
# Está habilitado para CDSSO.
com.sun.am.policy.agents.cdsso-enabled=true

# Ésta es la dirección URL a la que se dirigirá el usuario tras iniciar la sesión
correctamente
# en un escenario de CDSSO.
com.sun.am.policy.agents.cdcervletURL =
http://servidor.ejemplo.com:puerto/amserver/cdcervlet
```

4. Cambie `AMConfig.properties` para reflejar los nuevos valores y después reinicie Access Manager. Ejemplo:

```
com.sun.identity.enableUniqueSSOTokenCookie=true
com.sun.identity.authentication.uniqueCookieName=sunIdentityServerAuthNServer

com.sun.identity.authentication.uniqueCookieDomain=ejemplo.com
```

5. En la consola de administración de Access Manager, elija Configuración de servicio>Plataforma.
6. En la lista de dominio de cookies, cambie el nombre de dominio de las cookies:
  - a. Seleccione el dominio `iplanet.com` predeterminado y después haga clic en “Eliminar”.
  - b. Escriba el nombre de host de la instalación de Access Manager y después haga clic en “Agregar”.

Ejemplo: `server.ejemplo.com`

Debería ver dos cookies configuradas en el navegador:

<b>Cookie</b>	<b>Nombre de host</b>
<code>iPlanetDirectoryPro</code>	<code>server.ejemplo.com</code>
<code>sunIdentityServerAuthNServer</code>	<code>ejemplo.com</code>

---

## Archivos que se pueden distribuir

Sun Java System Access Manager 2005Q1 no contiene ningún archivo que pueda redistribuir a usuarios sin licencia de este producto.

# Información sobre problemas y respuestas de los clientes

Si experimenta problemas con Sun Java System Access Manager, póngase en contacto con el servicio de atención al cliente de Sun usando uno de estos procedimientos:

- Los servicios en línea para la atención al usuario del software de Sun  
<http://www.sun.com/supporttraining>

Este sitio incluye vínculos a la base de conocimiento, al centro de asistencia en línea y al buscador de productos, así como a los programas de mantenimiento y los números de teléfono del servicio de asistencia técnica.

- El número de teléfono del distribuidor asociado al contrato de mantenimiento.

Para que podamos ayudarle de forma óptima en la resolución de problemas, tenga a mano la siguiente información cuando se ponga en contacto con la asistencia:

- Descripción del problema, incluida la situación en la que éste se produce y la forma en que afecta al funcionamiento
- Tipo de máquina, versión del sistema operativo y versión del producto, incluida cualquier revisión del producto y otro software que pueda influir en el problema
- Pasos detallados de los métodos que haya seguido para solucionar el problema
- Cualquier registro de error o volcado del núcleo

## Sun valora sus comentarios

Sun tiene interés en mejorar su documentación y valora sus comentarios y sugerencias. Para enviar sus comentarios a Sun, use el formulario basado en Web que aparece en:

<http://www.sun.com/hwdocs/feedback/>

Indíquenos el título completo de la documentación y el número de pieza en los campos pertinentes. El número de pieza consta de siete o de nueve dígitos y se encuentra en la página que contiene el título de la guía o al principio del documento. Por ejemplo, el número de pieza correspondiente a estas notas de la versión es 819-1944.

---

# Recursos adicionales de Sun

Puede encontrar información útil de Sun Java System en las siguientes direcciones de Internet:

- Documentación de Sun Java System  
<http://docs.sun.com/prod/entsys.05q1>
- Servicios profesionales de Sun Java System  
<http://www.sun.com/service/products/software/javaenterprisesystem/>
- Servicio y productos de software de Sun Java System  
<http://www.sun.com/software/>
- Servicios de asistencia al usuario del software de Sun Java System  
<http://www.sun.com/supporttraining>
- Base de datos de conocimiento y asistencia al cliente de Sun Java System  
<http://sunsolve.sun.com>
- Servicios profesionales y de consultoría de Sun Java System  
<http://www.sun.com/service/products/software/javaenterprisesystem>
- Información para programadores de Sun Java System  
<http://developers.sun.com/>
- Servicios de asistencia de programadores de Sun  
<http://www.sun.com/developers/support>

Copyright © 2005 Sun Microsystems, Inc. Reservados todos los derechos.

Sun Microsystems, Inc. tiene derechos de propiedad intelectual relacionados con la tecnología del producto que se describe en este documento. Especialmente, aunque sin limitarse a ello, estos derechos de propiedad intelectual pueden incluir una o varias patentes en los Estados Unidos, las cuales figuran en <http://www.sun.com/patents>, así como una o varias patentes adicionales (o patentes pendientes de adjudicación) en los Estados Unidos y en otros países.

#### PROPIEDAD/CONFIDENCIAL DE SUN

Derechos del gobierno de Estados Unidos: software comercial. Los usuarios gubernamentales están sujetos al acuerdo de licencia estándar de Sun Microsystems, Inc. y a las disposiciones aplicables de la regulación FAR y sus suplementos.

El uso está sujeto a las condiciones de la licencia.

La distribución puede incluir materiales desarrollados por terceras partes.

Algunas de sus partes pueden proceder de sistemas Berkeley BSD, con licencia de la Universidad de California.

Sun, Sun Microsystems, el logotipo de Sun, Java y Solaris son marcas comerciales o marcas comerciales registradas de Sun Microsystems, Inc. en Estados Unidos y otros países. Todas las marcas comerciales de SPARC se utilizan bajo licencia y son marcas comerciales o marcas comerciales registradas de SPARC International, Inc. en Estados Unidos y en otros países.