Notas de la versión de Sun Java System Access Manager 7.1

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

Referencia: 820–0361–10
Julio de 2007

070802@18135

Contenido

Notas de la versión de Sun Java System Access Manager 7.1

Julio de 2007

Número de referencia 819-4683-13

Las Notas de la versión de Sun Java™ System Access Manager 7.1 contienen información importante disponible para esta versión de Sun Java Enterprise System (Java ES), incluidas las nuevas funciones de Access Manager y problemas conocidos junto con sus soluciones, si hay alguna disponible. Lea este documento antes de instalar y utilizar esta versión.

Para consultar la documentación del producto Java ES, incluida la recopilación sobre Access Manager, consulte `http://docs.sun.com/prod/entsys.05q4`.

Visite este sitio antes de instalar y configurar el software y, después, de forma periódica para consultar la documentación más reciente.

Estas notas de la versión contienen las siguientes secciones:

Historial de revisiones

La siguiente tabla muestra el historial de revisiones de las Notas de la versión de Access Manager 7.1.

TABLA 1 Historial de revisiones

Fecha	Descripción de los cambios
Julio de 2006	Versión Beta.
Marzo de 2007	Versión Java Enterprise System 5
Mayo de 2007	Actualizado con los nuevos problemas conocidos 6555040, 6550261, 6554379, 6554372, 6480354
Junio de 2007	Actualizado con los nuevos problemas conocidos 6562076, 6490150
Julio de 2007	Actualizado con el nuevo problema conocido 6485695

Acerca de Sun Java System Access Manager 7.1

Sun Java System Access Manager forma parte de la infraestructura de Sun Identity Management que permite a una organización administrar el acceso seguro a aplicaciones web y a otros recursos de una empresa y entre cadenas de valores de empresa a empresa (business-to-business, B2B).

Access Manager proporciona las siguientes funciones principales:

- Servicios de autenticación y autorización centralizados mediante un control de acceso basado en roles y reglas
- Inicio de sesión único (Single sign-on, SSO) para el acceso a las aplicaciones basadas en Web de la organización
- Compatibilidad de identidad federada con Liberty Alliance Project y el Lenguaje de marcas de afirmación de seguridad (Security Assertions Markup Language, SAML)
- Registro de la información vital, incluidas las actividades de los usuarios y el administrador, por parte de los componentes de Access Manager para las consiguientes operaciones de análisis, elaboración de informes y auditoría.

Novedades de esta versión

Esta versión incluye las siguientes funciones nuevas:

Integración de la estructura de supervisión de Java ES

Access Manager 7.1 se integra con la estructura de supervisión de Java Enterprise System mediante extensiones de administración de Java (JMX). La tecnología JMX proporciona las herramientas para crear soluciones dinámicas, modulares y basadas en Web para administrar y supervisar los dispositivos, las aplicaciones y las redes controladas por el servicio. Los usos habituales de la tecnología JMX incluyen: consulta y modificación de la configuración de la aplicación, recopilación de estadísticas acerca del comportamiento de las aplicaciones, y notificación de los cambios de estado y comportamientos incorrectos. Los datos se entregan a una consola de supervisión centralizada.

Access Manager 7.1 utiliza la estructura de supervisión de Java ES para capturar datos relacionados con los servicios y estadísticas, entre los que se incluyen:

- Número de intentos de autenticación, y autenticaciones realizadas con éxito y no satisfactorias
- Estadísticas de almacenamiento en la caché de directivas
- Tiempos de transacción de evaluación de directivas

Seguridad de servicios Web

Access Manager 7.1 amplía las capacidades de autenticación de los servicios Web de la siguiente manera:

- Inserta símbolos en los mensajes salientes.
- Evalúa los mensajes entrantes en busca de símbolos de seguridad
- Habilita la selección mediante clics de los proveedores de autenticación para nuevas aplicaciones

Implementación de un único archivo WAR de Access Manager

Access Manager incluye un único archivo WAR que puede utilizar para implementar los servicios de Access Manager de forma coherente en cualquiera de los contenedores compatibles incluidos en una de las plataformas admitidas. El archivo WAR de Access Manager coexiste con el programa de instalación de Java Enterprise System que implementa varios archivos JAR, XML, JSP, HTML, GIF y de propiedades.

Mejoras de los servicios principales

Contenedores web admitidos

- Sun Java System Web Server 7.0
- Sun Java System Application Server 8.2
- BEA WL 8.1 SP4
- IBM WebSphere 5.1.1.6

Integración con la estructura de supervisión

Access Manager puede utilizar la estructura de supervisión de JES para supervisar lo siguiente:

1. Autenticación
   - Número de intentos de autenticación
   - Número de intentos de autenticación remota (opcional)
   - Número de autenticaciones realizadas con éxito
   - Número de autenticaciones no satisfactorias
   - Número de operaciones de cierre de sesión realizadas con éxito
   - Número de operaciones de cierre de sesión realizadas con éxito
   - Tiempo de transacción para cada módulo, si es posible (en estado de ejecución y de espera)
2. Sesiones
   - Tamaño de la tabla de sesiones (por tanto, número máximo de sesiones)
   - Número de sesiones activas (contador incremental)
3. Servicio de perfiles
   - Tamaño máximo de caché
   - Tiempo de transacción de las operaciones (en ejecución y en espera)
4. Directiva
   - Solicitudes de evaluación de directivas entrantes y salientes

- Estadísticas del conjunto de conexiones de directivas para servidor LDAP del complemento del asunto

Módulo de autenticación

- El servicio de autenticación distribuida no es necesario para utilizar un servidor para las implementaciones de carga equilibrada.
- El servidor y el servicio de autenticación no son necesarios para utilizar un servidor para las implementaciones de carga equilibrada.
- Compatibilidad con los consejos compuestos entre el servicio de autenticación, los agentes de directivas y el servicio de directivas. Incluye la condición `AuthenticateToRealm`, AuthenticateToService y la idoneidad del dominio para todas las condiciones.
- Organización de consejo (condiciones de autenticación cualificadas para el dominio)
- Configuraciones de autenticación / cadenas de autenticación (`AuthServiceCondition`)
- Ahora la autenticación basada en módulos puede desactivarse si se aplica el encadenamiento de autenticación.
- El servicio de autenticación distribuida admite el módulo de autenticación de certificados.
- Se ha agregado `CertAuth` a la IU de autenticación distribuida para convertirla en una presentación de extractor de credenciales con todas las funciones.
- Nuevo módulo de autenticación de almacén de datos como un módulo comercializable que se autentica en el almacén de datos configurado de un dominio concreto
- Ahora la configuración de bloqueo de cuenta se mantiene en varias instancias del servidor AM.
- Encadenamiento de clases SPI de procesamiento posterior

Módulo de directiva

- Se ha agregado una nueva condición de directiva `AuthenticateToServiceCondition` para forzar la autenticación del usuario en una cadena de servicio de autenticación específica.
- Se ha agregado una nueva condición de directiva `AuthenticateToRealmCondition` para forzar la autenticación del usuario en un dominio específico.
- Se ha agregado una nueva condición de directiva `LDAPFilterCondition` para que el usuario coincida obligatoriamente con el filtro ldap especificado.
- Compatibilidad con la comparación de caracteres comodín de un nivel para facilitar la protección del contenido del directorio sin proteger el subdirectorio.
- Se pueden crear directivas en subdominios sin directivas de referencia explícitas desde el dominio principal si la referencia al alias de la organización se ha habilitado en la configuración global de directivas.
- `AuthLevelCondition` puede especificar el nombre del dominio, además del nivel de autenticación.

- `AuthSchemeCondition` puede especificar el nombre del domino, además del nombre del módulo de autenticación.

Módulo de administración de servicios

- Compatibilidad con el almacenamiento de la configuración de administración de servicios/directivas en Active Directory

Access Manager SDK

- Compatibilidad de las API con la autenticación de usuarios en una base de datos de la estructura del depósito de identidades predeterminada

Compatibilidad con los servicios web

- Proveedor SOAP de Liberty ID-WSF: proveedor de autenticación que encapsula el enlace SOAP de Liberty ID-WSF del mismo modo que Access Manager lo implementa. Consta de un cliente y un proveedor de servicios.
- Proveedor SSO de capa HTTP: proveedor de autenticación de capa HttpServlet que encapsula SSO de servidor basado en Access Manager.

Módulo de instalación

- Vuelve a empaquetar Access Manager como una aplicación J2EE, lo que da lugar a un único archivo WAR que se puede implementar en la Web.
- Compatibilidad con SJS Web Server 7.0 de 64 bits, para admitir el JVM de 64 bits

Módulo de delegación

- Compatibilidad con la agrupación de los privilegios de delegación

Actualización

- Admite la actualización a Access Manager 7.1 a partir de las siguientes versiones: Access Manager 7.0 2005Q4, Access Manager 6.3 2005Q1 e Identity Server 6.2 2004Q2.

Registro

- Compatibilidad con la delegación en el módulo de registro, controlando las identidades autorizadas para escribir o leer desde los archivos de registro.
- Compatibilidad con `SecureLogHelper` basado en JCE, lo que permite utilizar JCE (además de JSS) como un proveedor de seguridad para la implementación del registro seguro.

Notificaciones y avisos de Desaprobación

Las API de administración de identidades de Sun Java(TM) System Access Manager 7.1 y las plantillas XML permiten que los administradores del sistema creen, eliminen y administren entradas de identidades en Sun Java System Directory Server. Access Manager también

proporciona API para la administración de identidades. Los programadores utilizan las interfaces públicas y las clases definidas en el paquete `com.iplanet.am.sdk` para integrar las funciones de administración en las aplicaciones o servicios externos que Access Manager administrará. Las API de Access Manager proporcionan los medios para crear o eliminar objetos relacionados con identidades, así como para obtener, modificar, agregar o eliminar los atributos de objetos desde Directory Server.

El paquete `com.iplanet.am.sdk` de Access Manager, conocido normalmente como AMSDK, no se incluirá en una próxima versión de Access Manager. Esto incluye todas las API y plantillas XML relacionadas. No hay ninguna opción de migración disponible en la actualidad y tampoco se espera que haya ninguna en el futuro. Las soluciones de aprovisionamiento de usuarios proporcionadas por Sun Java System Identity Manager son sustitutos compatibles que puede comenzar a utilizar ya. Para obtener más información acerca de Sun Java System Identity Manager, visite `http://www.sun.com/software/products/identity_mgr/index.xml`.

Requisitos de hardware y software

La siguiente tabla muestra los requisitos de hardware y software para esta versión.

TABLA 2 Requisitos de hardware y software

Componente	Requisito
Sistema operativo (SO)	■ Solaris™ 10 en sistemas basados en SPARC, x86 y x64, incluida la compatibilidad con zonas locales root completas y zonas root dispersas. ■ Solaris 9 en sistemas basados en SPARC y x86. ■ Red Hat™ Enterprise Linux 3 y 4, todas las actualizaciones. Advanced Server (versiones de 32 y 64 bits) y Enterprise Server (versiones de 32 y 64 bits). ■ Windows Windows 2000 Advanced Server, Data Center Server versión SP4 en x86 Windows 2003 Standard (versiones de 32 y 64 bits), Enterprise (versiones de 32 y 64 bits), Data Center Server (versión de 32 bits) en sistemas basados en x86 y x64 Windows XP Professional SP2 en sistemas basados en x86 HP-UX 11i v1 (11.11 de uname), 64 bits en PA-RISC 2.0 Para obtener la lista más actualizada de los sistemas operativos admitidos, consulte "Platform Requirements and Issues" de *Sun Java Enterprise System 5 Release Notes for UNIX* en las *Notas de la versión de Sun Java Enterprise System 5 para UNIX* o "Hardware and Software Platform Information" de *Sun Java Enterprise System 5 Release Notes for Microsoft Windows* en las *Notas de la versión de Sun Java Enterprise System 5 para Windows.*
Java 2 Standard Edition (J2SE)	J2SE platform 6.0, 5.0 actualización 9 (HP-UX: 1.5.0.03) y 1.4.2 actualización 11
Directory Server	Árbol de información de Access Manager: Sun Java System Directory Server 6.0 o Sun Java System Directory Server 5.2 2005Q4 Repositorio de identidades de Access Manager: Sun Java System Directory Server 5.2 y 6.0 y Microsoft Active Directory

TABLA 2 Requisitos de hardware y software *(Continuación)*

Componente	Requisito
Contenedores web	Sun Java System Web Server 7.0 En las combinaciones de SO/plataforma compatibles, puede elegir ejecutar la instancia de Web Server en una JVM de 64 bits. Plataformas compatibles: Solaris 9/SPARC, Solaris 10/SPARC, Solaris 10/AMD64, Red Hat AS o ES 3.0/AMD64, Red Hat AS o ES 4.0/AMD64
	Sun Java System Application Server Enterprise Edition 8.2
	BEA WebLogic 8.1 SP4
	IBM WebSphere Application Server 5.1.1.6
RAM	Prueba básica: 512 Mbytes
	Implementación real: 1 Gbyte para los subprocesos, Access Manager SDK, el servidor HTTP y otros componentes internos
Espacio en el disco	512 Mbytes para Access Manager y las aplicaciones asociadas

Si tiene alguna duda sobre la compatibilidad de otras versiones de estos componentes, póngase en contacto con el representante técnico de Sun Microsystems.

Navegadores compatibles

La siguiente tabla muestra los exploradores compatibles con la versión Sun Java Enterprise System 5.

TABLA 3 Navegadores compatibles

Explorador	Plataforma
Firefox 1.0.7	Windows XP
	Windows 2000
	SO Solaris, versiones 9 y 10
	Red Hat Linux 3 y 4
	Mac OS X
Microsoft Internet Explorer™ 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows™ 2000

TABLA 3 Navegadores compatibles *(Continuación)*

Explorador	Plataforma
Mozilla™ 1.7.12	SO Solaris, versiones 9 y 10
	Windows XP
	Windows 2000
	Red Hat Linux 3 y 4
	Mac OS X
Netscape™ Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	SO Solaris, versiones 9 y 10

Información general de compatibilidad

Incompatibilidad entre sistemas de AMSDK con el servidor de Access Manager

Las siguientes combinaciones son compatibles entre AMSDK y el servidor de Access Manager en las siguientes versiones de Java Enterprise System:

- Java Enterprise System 2004Q2 AMSDK no es compatible con el servidor de Java Enterprise System 5 Access Manager (esta versión).
- Java Enterprise System 5 AMSDK (esta versión) no es compatible con el servidor de Java Enterprise System Access Manager 2004Q2 (anteriormente, Identity Server).

Actualización no admitida para la versión HPUX de Access Manager

No se admite la ruta de actualización de Access Manager 7 2005Q4 a Access Manager 7.1 (esta versión) para la versión HPUX.

Modo tradicional de Access Manager

Si instala Access Manager con cualquiera de los siguientes productos, debe seleccionar el modo tradicional (6.x) de Access Manager:

- Sun Java System Portal Server
- Los servidores de Sun Java System Communications Services, incluidos Messaging Server, Calendar Server, Instant Messaging o Delegated Administrator

Seleccione el modo tradicional (6.x) de Access Manager en función de cómo se ejecute el programa de instalación de Java ES:

- "Instalación silenciosa de Java ES con un archivo de estado " en la página 15
- "Opción de instalación "Configurar ahora" (Configure Now) en el modo gráfico" en la página 16
- "Opción de instalación "Configurar ahora" (Configure Now) en el modo basado en texto" en la página 16
- "Opción de instalación "Configure más tarde" (Configure Later)" en la página 16

Para determinar el modo de instalación de Access Manager 7.1, consulte "Determinar el modo de Access Manager" en la página 16.

Instalación silenciosa de Java ES con un archivo de estado

El modo de instalación silenciosa del programa de instalación de Java ES no permite la interacción. Con él, puede instalar los componentes de Java ES en varios servidores host que tengan configuraciones similares. Primero, debe ejecutar el programa de instalación para generar un archivo de estado (sin instalar realmente los componentes) y, a continuación, editar una copia de este archivo para cada servidor host en el que desee instalar Access Manager y otros componentes.

Para seleccionar Access Manager en el modo tradicional (6.x), establezca el siguiente parámetro (junto con otros) en el archivo de estado antes de ejecutar el programa de instalación en el modo silencioso:

```
...
AM_REALM = disabled
...
```

Para obtener más información sobre cómo ejecutar el programa de instalación de Java ES en el modo silencioso utilizando un archivo de estado, consulte el Capítulo 5, "Installing in Silent Mode" de *Sun Java Enterprise System 5 Installation Guide for UNIX*.

Opción de instalación "Configurar ahora" (Configure Now) en el modo gráfico

Si ejecuta el programa de instalación de Java ES en el modo gráfico con la opción "Configurar ahora" (Configure Now) del panel "Access Manager: Administración (1 de 6)" (Access Manager: Administration [1 of 6]), seleccione el valor predeterminado, "Tradicional (versión estilo 6.x)", (Legacy [version 6.x style]).

Opción de instalación "Configurar ahora" (Configure Now) en el modo basado en texto

Si ejecuta el programa de instalación de Java ES en el modo basado en texto con la opción "Configurar ahora" (Configure Now), seleccione el valor predeterminado `Legacy` en `Install type (Realm/Legacy) [Legacy]`.

Opción de instalación "Configure más tarde" (Configure Later)

Si ha ejecutado el programa de instalación de Java ES con la opción "Configure más tarde" (Configure Later), debe ejecutar la secuencia de comandos `amconfig` para configurar Access Manager tras la instalación. Para seleccionar el modo tradicional (6.x), establezca el siguiente parámetro en el archivo de entrada de la secuencia de comandos de configuración (`amsamplesilent`):

```
...
AM_REALM=disabled
...
```

Para obtener más información sobre cómo configurar Access Manager mediante la ejecución de la secuencia de comandos `amconfig`, consulte la *Sun Java System Access Manager 7.1 Administration Guide* .

Determinar el modo de Access Manager

Para determinar si la instalación de Access Manager 7.1 que se está ejecutando se ha configurado en el modo tradicional o de dominio, ejecute:

`http(s)://`*host*`:`*port*`/amserver/SMSServlet?method=isRealmEnabled`

Se mostrarán los siguientes resultados:

- true: modo de dominio
- false: modo tradicional

Agentes de directivas de Access Manager

La siguiente tabla muestra la compatibilidad de los agentes de directivas con los modos de Access Manager 7.1.

TABLA 4 Compatibilidad de los agentes de directivas con los modos de Access Manager 7.1

Agente y versión	Modo compatible
Agentes web y J2EE , versión 2.2	Modos tradicional y de dominio
Los agentes web y J2EE, versión 2.1, no se admiten en Access Manager 7.1.	

Limitaciones y problemas conocidos

En esta sección, se describen los siguientes problemas conocidos y sus soluciones (si las hay) en el momento de la publicación de Access Manager 7.1.

Problemas relacionados con la instalación

La información acerca de los problemas de instalación de Java System Enterprise se encuentra en las Notas de la versión de JES5. Consulte la sección "Access Manager Installation Issues" de *Sun Java Enterprise System 5 Release Notes for UNIX*.

Esta sección contiene los siguientes problemas conocidos:

- "Es necesario un archivo .jar adicional para el WAR único generado por el programa de instalación de JES 5 para Websphere 5.1 (6550261)" en la página 19
- "La implementación del archivo WAR único para Webshpere requiere realizar cambios en server.xml para que se comunique con el SDK del cliente (6554379)" en la página 19
- "Es preciso realizar cambios para que la autenticación distribuida trabaje con el archivo WAR único de Access Manager para Weblogic y Webshpere (6554372)" en la página 21

La implementación de un único archivo WAR de Access Manager en WebLogic requiere que los archivos JAR de JAX-RPC 1.0 se comuniquen con el SDK del cliente (6555040)

Existe un problema conocido con el archivo WAR único implementado en Weblogic 8.1 con la inicialización de JAX-RPC. Para que Access Manager se comunique con el SDK del cliente, deberá sustituir los archivos jar de JAX-RCP 1.1 por archivos jar de JAX-RPC 1.0.

Solución:

Existen dos formas de obtener el archivo WAR. Una es mediante el programa de instalación de Java Enterprise System 5 con Access Manager definido en la opción Configurar más tarde; la otra es desde el sitio de descargas de Sun.

Si ha generado el archivo WAR mediante el programa de instalación de JES 5 con la opción Configurar más tarde:

1. Elimine los siguientes archivos `.jar` de JAXRPC 1.1 de *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
2. Copie los siguientes archivos `.jar` desde sus ubicaciones respectivas a *AccessManager-base*`/SUNWam/web-src/WEB-INF/lib` :
   - `jaxrpc-api.jar` desde `/opt/SUNWam/lib/jaxrpc 1.0`
   - `jaxrpc_ri.jar` desde `/opt/SUNWam/lib/jaxrpc 1.0`
   - `commons-logging.jar` desde `/opt/SUNWmfwk/lib`
3. Vaya a *AccessManager-base*`/SUNWam/bin/` y ejecute el siguiente comando:

   `amconfig –s` *samplesilent*

   Para obtener más información sobre cómo configurar Access Manager con la secuencia de comandos amconfig, consulte Running the Access Manager amconfig Script en la *Guía de postinstalación de Access Manager*.

Si ha obtenido el archivo WAR mediante el sitio de descargas de Sun (`http://www.sun.com/download/index.jsp`):

1. Obtenga el archivo *ZIP_ROOT*`/applications/jdk14/amserver.war` y ábralo en un área de ensayo, como `/tmp/am-staging` .

2. Elimine los siguientes archivos `.jar` de JAXRPC 1.1 de `/tmp/am-staging/WEB-INF/lib`:
   - `jaxrpc-api.jar`
   - `jaxrpc-spi.jar`
   - `jaxrpc-impl.jar`
3. Copie los siguientes archivos `.jar` de JAXRPC 1.0 y el archivo `.jar` de registros comunes, que se encuentra en el directorio *ZIP_ROOT*`/applications/jdk14/jarFix` a `/tmp/am-staging/WEB-INF/lib`:
   - `jaxrpc-api.jar`
   - `jaxrpc-ri.jar`
   - `commons-logging.jar`
4. Vuelva a crear e implementar el archivo WAR de Access Manager. Para obtener más información, consulte Deploying Access Manager as a Single WAR File en la *Guía de postinstalación de Access Manager*.

Es necesario un archivo .jar adicional para el WAR único generado por el programa de instalación de JES 5 para Websphere 5.1 (6550261)

Si se genera el archivo WAR único de Access utilizando el programa de instalación de JES 5 con la opción Configurar más tarde, se necesitarán archivos `.jar` adicionales antes de que implemente Websphere 5.1.

Solución:

1. Copie `jsr173_api.jar` desde `/usr/share/lib` al directorio *AcessManager-base*`/opt/SUNWam/web-src/WEB-INF/lib .`
2. Vaya a *AccessManager-base*`/SUNWam/bin/` y ejecute el siguiente comando:

   `amconfig –s` *samplesilent*

   Para obtener más información sobre cómo configurar Access Manager con la secuencia de comandos amconfig, consulte Running the Access Manager amconfig Script en la *Access Manager Post Installation Guide*.

La implementación del archivo WAR único para Webshpere requiere realizar cambios en server.xml para que se comunique con el SDK del cliente (6554379)

Para que la implementación del archivo WAR único de Access Manager con Websphere 5.1 se comunique correctamente con el SDK del cliente deberá realizar cambios en el archivo `server.xml`.

Solución:

Para cambiar correctamente el archivo `server.xml`, lleve a cabo los siguientes pasos:

1. Obtenga el archivo `amserver.war`. Existen dos maneras de obtener el archivo WAR único; mediante el programa de instalación de JES 5 con la opción Configurar más tarde o mediante el sitio de descarga de Sun.

   Nota – Si ha generado el archivo WAR mediante el programa de instalación de JES 5, asegúrese de completar los pasos definidos en el problema conocido nº 6550261.

2. Despliegue el archivo WAR de Access Manager en un área de ensayo, por ejemplo `/tmp/am-staging`.
3. Copie los siguientes archivos `.jar` compartidos de `/tmp/am-staging/WEB-INF/lib` a una ubicación compartida como `/export/jars`:

jaxrpc-api.jar	jaxrpc-spi.jar	jaxrpc-impl.jar	saaj-api.jar
saaj-impl.jar	xercesImpl.jar	namespace.jar	xalan.jar
dom.jar	jax-qname.jar	jaxb-api.jar	jaxb-impl.jar
jaxb-libs.jar	jaxb-xjc.jar	jaxr-api.jar	jaxr-impl.jar
xmlsec.jar	swec.jar	acmecrypt.jar	iaik_ssl.jar
iaik_jce_full.jar	mail.jar	activation.jar	relaxngDatatype.jar
xsdlib.jar	mfwk_instrum_tk.jar	FastInfoset.jar	jsr173_api.jar

4. Elimine los mismos archivos `.jar` de `/tmp/am-staging/WEB-INF/lib` en el área de ensayo.
5. Actualice el archivo `server.xml` de la instancia de Websphere. Realice los cambios a *jvmEntries* en `server.xml` si la ubicación de instancia predeterminada es `/opt/WebSphere/AppServer/config/cells/` *node-name*`/nodes/`*node-name*`/servers/server1` , como se indica a continuación:

   ```
   <classpath>/export/jars/jaxrpc-api.jar:/export/jars/jaxrpc-spi.jar:
       /export/jars/jaxrpc-impl.jar:/export/jars/saaj-api.jar:
       /export/jars/saaj-impl.jar:/export/jars/xercesImpl.jar:
       /export/jars/namespace.jar:/export/jars/xalan.jar:/export/jars/dom.jar:
       /export/jars/jax-qname.jar:/export/jars/jaxb-api.jar:/export/jars/jaxb-impl.jar:
       /export/jars/jaxb-libs.jar:/export/jars/jaxb-xjc.jar:/export/jars/jaxr-api.jar:
       /export/jars/jaxr-impl.jar:/export/jars/xmlsec.jar:/export/jars/swec.jar:
       /export/jars/acmecrypt.jar:/export/jars/iaik_ssl.jar:
       /export/jars/iaik_jce_full.jar:/export/jars/mail.jar:
       /export/jars/activation.jar::/export/jars/relaxngDatatype.jar:
       /export/jars/xsdlib.jar:/export/jars/mfwk_instrum_tk.jar:
       /export/jars/FastInfoset.jar:/export/jars/jsr173_api.jar</classpath>
   ```

6. Reinicie el contenedor.
7. Vuelva a crear e implementar el archivo WAR de Access Manager desde /tmp/am-staging. Para obtener más información, consulte Deploying Access Manager as a Single WAR File en la *Guía de postinstalación de Access Manager*.

Es preciso realizar cambios para que la autenticación distribuida trabaje con el archivo WAR único de Access Manager para Weblogic y Webshpere (6554372)

El archivo WAR de autenticación distribuida requiere archivos jar adicionales para el análisis tanto para Weblogic 8.1 como para Websphere 5.1 porque el contenedor es de la versión JDK14. Los archivos `.jar` de JDK14 se encuentran en el siguiente directorio del archivo `.zip`:

ZIP-ROOT`/applications/jdk14/jarFix`

Solución:

Para Weblogic 8.1:

1. Configure la autenticación distribuida utilizando las secuencias de comandos de configuración. Consulte Deploying a Distributed Authentication UI Server en la *Guía de postinstalación de Access Manager*.
2. Despliegue el archivo WAR de autenticación distribuida actualizado en una ubicación temporal como `/tmp/dist-auth`.
3. Copie `xercesImpl.jar`, `dom.jar` y `xalan.jar` al directorio `/tmp/dist_auth/WEB-INF/lib` desde *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Vuelva a generar el archivo WAR de autenticación distribuida desde la ubicación temporal e impleméntelo. Para obtener más información, consulte Deploying a Distributed Authentication UI Server WAR File en la *Guía de postinstalación de Access Manager*.

Para Websphere 5.1:

1. Configure la autenticación distribuida utilizando las secuencias de comandos de configuración. Consulte Deploying a Distributed Authentication UI Server en la *Guía de postinstalación de Access Manager*.
2. Despliegue el archivo WAR de autenticación distribuida actualizado en una ubicación temporal como `/tmp/dist-auth`.
3. Copie `xercesImpl.jar`, `dom.jar` y `xalan.jar` al directorio `/tmp/dist_auth/WEB-INF/lib` desde *ZIP-ROOT*`/applications/jdk14/jarFix`.
4. Edite el archivo `WEB-INF/web.xml` y sustituya `jar://web-app_2_3.dtd` por `http://java.sun.com/dtd/web-app_2_3.dtd` .
5. Vuelva a generar el archivo WAR de autenticación distribuida desde la ubicación temporal e impleméntelo. Para obtener más información, consulte Deploying a Distributed Authentication UI Server WAR File en la *Guía de postinstalación de Access Manager*.

El programa de configuración del archivo WAR único produce un error con DS (6562076)

Access Manager implementado como un archivo WAR único no se configura correctamente en Directory Server 6 con un sufijo raíz de un único componente, por ejemplo. `dc=example`. Sin embargo, funciona con un sufijo raíz de varios componentes, como `dc=example,dc=com` .

Solución: Use el sufijo raíz de varios componentes, por ejemplo `dc=example,dc=com`.

La configuración de multiservidor del archivo WAR único de AM en el mismo host presenta una excepción (6490150)

Cuando se configura la segunda instancia del archivo WAR único de Access Manager en el mismo host con Directory Server, presenta una excepción mientras se actualiza el Alias de organización. Este problema no se produce si la segunda instancia configurada se encuentra en un host distinto.

Problemas relacionados con la actualización

Puede encontrar información sobre los problemas de actualización en la sección "Upgrade Issues" de *Sun Java Enterprise System 5 Release Notes for UNIX* en las *Notas de la versión de Sun Java Enterprise System 5 para UNIX*.

Problemas de compatibilidad

Se produce un error en el inicio de sesión único de Access Manager en un cliente Web universal (6367058, 6429573)

El problema se produce después de instalar Access Manager, Messaging Server y Calendar Server, configurarlos para que trabajen juntos e instalar a continuación la revisión 120955-01 de JES5. El usuario encontrará un error de inicio de sesión. Este error se debe a una incompatibilidad entre las propiedades de Policy Agent 2.1 y AMSDK. No hay una solución para este error por el momento.

Se produce el error StackOverflowError en Web Server 7.0 al ejecutarse en el modo de 64 bits (6449977)

Si Access Manager se ha configurado en una instancia de Web Server 7.0 que utiliza una JVM de 64 bits, el usuario encontrará un mensaje de error de servidor al acceder a la página de inicio de sesión de la consola. El registro de errores de Web Server contiene una excepción `StackOverflowError`.

Solución: modifique la configuración de Web Server siguiendo estos pasos:

1. Inicie una sesión en la consola de administración de Web Server como administrador de Web Server.
2. Haga clic en "Edit Configuration".

   En el campo "Plataform", seleccione 64 y haga clic en "Save".
3. Haga clic en la ficha "Java" y a continuación en la ficha "JVM Settings".
   - En "Options", busque la entrada de menor tamaño de pila (por ejemplo: -Xms). El valor de tamaño mínimo de pila debe ser, al menos, 512m. Por ejemplo, si el valor de tamaño de pila no es -Xms512m o superior, cambie el valor a, al menos, -Xms512m.
   - El valor de tamaño máximo de pila debe ser, al menos, 768m. Si el tamaño máximo de pila no es -Xmx768m o superior, cambie el valor a, al menos, -Xmx768m.
   - Defina el tamaño de pila Java en 512 k o 768 k utilizando `-Xss512k` o `-Xss768k`. Puede utilizar el tamaño predeterminado para la JVM de 64 bits en Solaris Sparc (1024k) dejándolo en blanco.
4. Haga clic en la ficha "Performance" y, a continuación, en el vínculo "Thread Pool Settings"

   Cambie el valor de tamaño de pila a, al menos, 261144 y haga clic en Guardar.
5. Haga clic en el vínculo "Deployment Pending" en la esquina superior de la pantalla.

   En la página "Configuration Deployment", haga clic en el botón "Deploy".
6. En la ventana "Results", haga clic en OK para reiniciar la instancia de Web Server.

   Haga clic en "Close" en la ventana "Results" después de que se haya reiniciado Web Server.

Existen incompatibilidades en el módulo de autenticación principal para el modo tradicional (6305840)

El modo tradicional de Access Manager 7.1 presenta las siguientes incompatibilidades en el módulo de autenticación principal a partir de la versión Access Manager 6 2005Q1:

- Los módulos de autenticación de la organización se eliminan en el modo tradicional.
- Se ha modificado la presentación de la “Configuración de autenticación del administrador” y la “Configuración de autenticación de la organización”. En la consola de Access Manager 7.1, la lista desplegable tiene seleccionada de forma predeterminada la opción `ldapService`. En la consola de Access Manager 6 2005Q1, se mostraba el botón de edición y el módulo LDAP no aparecía seleccionado de forma predeterminada.

Solución: ninguna.

La utilidad `commadmin` de Delegated Administrator no crea un usuario (6294603)

La utilidad `commadmin` de Delegated Administrator, junto con la opción `-S mail,cal`, no crea un usuario en el dominio predeterminado.

Solución: este problema se produce al actualizar Access Manager a la versión 7.1 sin actualizar Delegated Administrator.

Si no desea actualizar Delegated Administrator, siga estos pasos:

1. En el archivo `UserCalendarService.xml`, marque los atributos `mail`, `icssubcribed` e `icsfirstday` como opcionales en lugar de obligatorios. Este archivo se encuentra de forma predeterminada en el directorio `/opt/SUNWcomm/lib/services/` de los sistemas Solaris.
2. En Access Manager, elimine el archivo XML existente. Para ello, ejecute el comando `amadmin` de la siguiente forma:

   ```
   # ./amadmin -u amadmin -w password -r UserCalendarService
   ```

3. En Access Manager, agregue el archivo XML actualizado como se muestra a continuación:

   ```
   # ./amadmin -u amadmin -w password
   -s /opt/SUNWcomm/lib/services/UserCalendarService.xml
   ```

4. Reinicie el contenedor web de Access Manager.

La utilidad `commadmin` de Delegated Administrator no crea una organización (6292104)

La utilidad `commadmin` de Delegated Administrator, junto con la opción `-S mail,cal`, no crea una organización.

Solución: consulte la solución del problema anterior.

Problemas de configuración

- "La secuencia de comandos amconfig no actualiza los alias de dominio/DNS ni las entradas de la lista de servidores de plataforma (6284161)" en la página 27
- "El modo de dominio es el modo predeterminado de Access Manager en la plantilla del archivo de estado de la configuración (6280844)" en la página 27

Redirección incorrecta de la consola detrás de un equilibrador de carga (6480354)

Si cuenta con instancias de Access Manager implementadas detrás de un equilibrador de carga, el inicio de sesión en Access Manager Console puede redirigirse a una de las instancias de Access Manager en vez de al equilibrador de carga. La dirección URL en el explorador también cambia a la instancia de Access Manager. Por ejemplo, este problema se puede producir si inicia la sesión en Console usando esta dirección URL:

```
http://loadbalancer.example.com/amserver/realm
```

Esta redirección se puede producir tanto en la implementación de los modos Realm como Legacy.

Existen dos soluciones para este problema. Puede utilizar cualquiera de ellas:

1. Inicie la sesión con cualquiera de las siguientes direcciones URL:

   `http://` *loadbalancer*`/amserver/UI/Login`

   `http://` *loadbalancer*`/amserver`

2. En `AMConfig.properties`, defina la propiedad `com.sun.identity.loginurl` como el nombre del equilibrador de carga. Esto debe realizarse en cada instancia de Access Manager detrás del equilibrador de carga.

Debe actualizarse la URL de notificación para la instalación de Access Manager SDK sin contenedor web (6491977)

Si instala Access Manager SDK sin un contenedor web ejecutando el programa de instalación de Java ES 5 con la opción "Configurar ahora", la propiedad `com.iplanet.am.notification.url` del archivo AMConfig.properties se establece en `NOTIFICATION_URL`. Si no se realiza ninguna configuración adicional del contenedor web, los usuarios no recibirán ninguna notificación desde el servidor remoto de Access Manager.

Solución: restablezca esta propiedad de la siguiente forma:
`com.iplanet.am.notification.url=""`

El servicio de restablecimiento de contraseñas indica errores de notificaciones cuando se cambia una contraseña (6455079)

Cuando se modifica una contraseña, Access Manager envía una notificación por correo electrónico utilizando un nombre de remitente inadecuado `Identity-Server` que da lugar a entradas de errores en los registros de `amPasswordReset`. Ejemplo:

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

Solución: Cambie la configuración en `/opt/SUNWam/locale/amPasswordResetModuleMsgs.properties`.

- Cambie la dirección del remitente. Cambie `fromAddress.label=<Identity-Server>` por `fromAddress.label=<IdentityServer@myhost.company.com>`
- Cambie la propiedad `lockOutEmailFrom` para garantizar que las notificaciones de bloqueo utilicen la dirección del remitente (`from`) correcta.

No se actualizan la lista de servidores de plataforma ni el atributo de alias FQDN (6309259, 6308649)

En una implementación con varios servidores, no se actualizan la lista de servidores de plataforma ni el atributo de alias FQDN cuando se instala Access Manager en el segundo servidor (y en los siguientes).

Solución: agregue manualmente los alias de dominio/DNS y las entradas de la lista de servidores de plataforma. Para obtener información sobre los pasos de este proceso, consulte "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" de *Sun Java System Access Manager 7.1 Postinstallation Guide*.

Validación de datos para los atributos necesarios en los servicios (6308653)

En Access Manager 7.1, los atributos necesarios para los archivos XML de los servicios deben establecerse obligatoriamente en los valores predeterminados.

Solución: si tiene servicios con atributos necesarios sin valores, agregue los valores para dichos atributos y, a continuación, vuelva a cargar el servicio.

Solución para la implementación en una instancia de WebLogic 8.1 segura (6295863)

Si se implementa Access Manager 7.1 en una instancia de BEA WebLogic 8.1 SP4 segura (con SSL habilitado), se producirá una excepción durante la implementación de cada aplicación web de Access Manager.

Solución: siga estos pasos:

1. Aplique el archivo JAR de la revisión de WebLogic 8.1 SP4, `CR210310_81sp4.jar`, disponible en BEA.

2. En la secuencia de comandos `/opt/SUNWam/bin/amwl81config` (sistemas Solaris) o `/opt/sun/identity/bin/amwl81config` (sistemas Linux), actualice las funciones `doDeploy` y `undeploy_it` para especificar la ruta del archivo JAR de la revisión al principio de `wl8_classpath` , que es la variable que contiene la ruta `classpath` empleada para implementar las aplicaciones Web de Access Manager y anular la implementación.

   Busque la línea que contiene `wl8_classpath`:

   ```
   wl8_classpath= ...
   ```

3. Justo detrás de la línea indicada en el paso 2, agregue la siguiente línea:

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

La secuencia de comandos `amconfig` no actualiza los alias de dominio/DNS ni las entradas de la lista de servidores de plataforma (6284161)

En una implementación con varios servidores, la secuencia de comandos `amconfig` no actualiza los alias de dominio/DNS ni las entradas de la lista de servidores de plataforma para las instancias de Access Manager adicionales.

Solución: agregue manualmente los alias de dominio/DNS y las entradas de la lista de servidores de plataforma. Para obtener información sobre los pasos de este proceso, consulte "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" de *Sun Java System Access Manager 7.1 Postinstallation Guide*.

El modo de dominio es el modo predeterminado de Access Manager en la plantilla del archivo de estado de la configuración (6280844)

El modo de Access Manager (variable `AM_REALM`) se activa de forma predeterminada en la plantilla del archivo de estado de la configuración.

Solución: para instalar o configurar Access Manager en el modo tradicional, restablezca la variable en el archivo de estado:

```
AM_REALM = disabled
```

Problemas de rendimiento

En el modo Realm, la creación de un grupo nuevo genera una administración de grupo con ACIs que nunca se utilizan (6485695)

Si Access Manager se instala en el modo Realm, siempre que se cree un grupo nuevo, Access Manager creará dinámicamente una nueva administración de grupo con las ACIs necesarias para administrar el grupo. En el modo Realm, estas ACIs de administración de grupo no se utilizan. Sin embargo, Directory Server todavía las evalúa al procesar entradas bajo el sufijo, lo que puede reducir el rendimiento de Access Manager, especialmente si la implementación crea un gran número de grupos.

Solución: La solución para este problema implica dos partes:

- Evitar que Access Manager cree una administración de grupo y las ACIs correspondientes cada vez que se cree un grupo nuevo
- Eliminar cualquier ACI de administración de grupo de Directory Server

Evitar que se creen ACIs de administración de grupos

El siguiente procedimiento impide que Access Manager cree una administración de grupo y las ACIs correspondientes cada vez que se cree un grupo nuevo.

Nota – Este procedimiento evita permanentemente la creación de administraciones de grupo y las ACI correspondiente siempre que se cree un grupo nuevo. Use este procedimiento únicamente si este comportamiento es adecuado para su implementación específica.

---

1. Realice una copia de seguridad del archivo `amAdminConsole.xml`. Este archivo se encuentra en el siguiente directorio, en función de su plataforma:
   - Sistemas Solaris: `/etc/opt/SUNWam/config/xml`
   - Sistemas Linux y HP-UX: `/etc/opt/sun/identity/config/xml`
   - Sistemas Windows: *javaes-install-dir*`\identity\config\xml`

     javaes-install-dir representa el directorio de instalación de Java ES 5. El valor predeterminado es `C:\Program Files\Sun\JavaES5`.
2. En el archivo `amAdminConsole.xml`, elimine la siguiente entrada de administración de grupo que se muestra entre líneas de comentario:

```
<AttributeSchema name="iplanet-am-admin-console-dynamic-aci-list"
    type="list"
    syntax="string"
    i18nKey="g111">
    <DefaultValues>
...
```

```
# Beginning of entry to delete
                <Value>Group Admin|Group Admin Description|ORGANIZATION:aci:
(target="ldap:///GROUPNAME")(targetattr = "*")
(version 3.0; acl "Group and people container admin role";
allow (all) roledn = "ldap:///ROLENAME";)##ORGANIZATION:aci:
(target="ldap:///ORGANIZATION")
(targetfilter=(&amp;FILTER(!(|(nsroledn=cn=Top-level Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Help Desk Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Top-level Policy Admin Role,dc=iplanet,dc=com)
(nsroledn=cn=Organization Admin Role,ORGANIZATION)
(nsroledn=cn=Container Admin Role,ORGANIZATION)
(nsroledn=cn=Organization Policy Admin Role,ORGANIZATION)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members"; allow (read,write,search)
roledn = "ldap:///ROLENAME";)</Value>
# End of entry to delete
...
    </DefaultValues>
</AttributeSchema>
```

3. Use `amadmin` para eliminar el servicio de Consola de administración de Access Manager. Por ejemplo, en sistemas Solaris:

   ```
   # cd /opt/SUNWam/bin
   # ./amadmin -u amadmin -w amadmin_password
   --deleteService iPlanetAMAdminConsoleService
   ```

4. Use `amadmin` para volver a cargar el servicio de Consola de administración en Access Manager del archivo `amAdminConsole.xml` editado en el paso 2. Por ejemplo:

   ```
   # ./amadmin -u amadmin -w amadmin_password
   -t /etc/opt/SUNWam/config/xml/amAdminConsole.xml
   ```

5. Reinicie el contenedor web de Access Manager. (Si tiene previsto eliminar ACIs de Directory Server, como se describe en el siguiente procedimiento, espere y reinicie el contenedor web una vez haya finalizado dicho procedimiento.)

Eliminar las ACIs de administración de grupos existentes

Nota – El siguiente procedimiento emplea las utilidades `ldapsearch` y `ldapmodify` para buscar y eliminar las ACIs de administración de grupos. Si su implementación utiliza Directory Server 6.0, también puede utilizar Directory Server Control Center (DSCC) o el comando `dsconf` para realizar estas funciones. Para obtener más información, consulte la documentación de Directory Server 6.0:

http://docs.sun.com/app/docs/coll/1224.1

El siguiente procedimiento elimina las ACIs de administración de grupos que ya existen en Directory Server.

1. Cree un archivo LDIF para utilizarlo con `ldapmodify` para eliminar las ACIs de administración de grupos. Para buscar estas ACIs, use `ldapsearch` (o cualquier otra herramienta de búsqueda en directorios si lo prefiere).

   Por ejemplo, las siguientes entradas en el archivo LDIF de muestra llamado `Remove_Group_ACIs.ldif` eliminarán las ACIs de un grupo que se llama Grupo nuevo:

```
dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///cn=New Group,ou=Groups,o=isp")(targetattr = "*")
(version 3.0; acl "Group and people container admin role"; allow (all)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///ou=People,o=isp")(targetattr="nsroledn")
(targattrfilters="add=nsroledn:(!(nsroledn=*)),
del=nsroledn:(!(nsroledn=*))") (version 3.0;
acl "Group admin's right to add user to people container"; allow (add)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)

dn: ROOT_SUFFIX
changetype: modify
delete: aci
aci: (target="ldap:///o=isp")
(targetfilter=(&(|(memberof=*cn=New Group,ou=Groups,o=isp)
(iplanet-am-static-group-dn=*cn=New Group,ou=Groups,o=isp))
(!(|(nsroledn=cn=Top-level Admin Role,o=isp)
(nsroledn=cn=Top-level Help Desk Admin Role,o=isp)
(nsroledn=cn=Top-level Policy Admin Role,o=isp)
(nsroledn=cn=Organization Admin Role,o=isp)(
nsroledn=cn=Container Admin Role,o=isp)
(nsroledn=cn=Organization Policy Admin Role,o=isp)))))
(targetattr != "iplanet-am-web-agent-access-allow-list ||
iplanet-am-web-agent-access-not-enforced-list ||
iplanet-am-domain-url-access-allow ||
iplanet-am-web-agent-access-deny-list ||nsroledn")
(version 3.0; acl "Group admin's right to the members";
allow (read,write,search)
roledn = "ldap:///cn=cn=New Group_ou=Groups_o=isp,o=isp";)
aci: (target="ldap:///o=isp")(targetattr="*")
```

```
(version 3.0; acl "S1IS special dsame user rights for all under the root suffix";
allow (all) userdn = "ldap: ///cn=dsameuser,ou=DSAME Users,o=isp"; )
```

2. Use `ldapmodify` con el archivo LDIF del paso anterior para eliminas las ACIs de grupo de Directory Server. Por ejemplo:

```
# ldapmodify -h ds-host -p 389 -D "cn=Directory Manager"
-w ds-bind-password -f Remove_Group_ACIs.ldif
```

3. Reinicie el contenedor web de Access Manager.

Problemas de la consola de Access Manager

La nueva consola de Access Manager no puede establecer las prioridades de plantilla de CoS (6309262)

La nueva consola de Access Manager 7.1 no puede establecer ni modificar una prioridad de plantilla de Clase de servicio (CoS).

Solución: inicie una sesión en la consola de Access Manager 6 2005Q1 para establecer o modificar la prioridad de plantilla de CoS.

Aparece la antigua consola al agregar servicios relacionados con Portal Server (6293299)

Portal Server y Access Manager se instalan en el mismo servidor. Con Access Manager instalado en el modo tradicional, inicie una sesión en la nueva consola mediante `/amserver`. Si se selecciona un usuario existente y se intentan agregar servicios (como NetFile o Netlet), aparecerá la antigua consola de Access Manager (`/amconsle`).

Solución: ninguna. La versión actual de Portal Server requiere la consola de Access Manager 6 2005Q1.

La consola no devuelve el conjunto de resultados de Directory Server una vez alcanzado el límite de recursos (6239724)

Instale Directory Server y, a continuación, Access Manager con la opción de DIT existente. Inicie una sesión en la consola de Access Manager y cree un grupo. Edite los usuarios de dicho grupo. Por ejemplo, agregue usuarios con el filtro `uid=*999*`. La lista resultante estará vacía y la consola no mostrará ningún mensaje de error, advertencia ni informativo.

Solución: los miembros del grupo no deben superar el límite de tamaño de búsqueda de Directory Server. En caso contrario, cambie el límite de tamaño de búsqueda proporcionalmente.

Adición del atributo `ContainerDefaultTemplateRole` después de la migración de datos (4677779)

En el modo tradicional, el rol del usuario no se muestra en una organización que no se haya creado en Access Manager. En el modo de depuración, aparece el siguiente mensaje:

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

Este error se muestra después de que se ejecuten las secuencias de comandos de migración del programa de instalación de Java ES. El atributo `ContainerDefaultTemplateRole` no se agrega automáticamente a la organización cuando ésta se migra desde un árbol de información de directorio (DIT, Directory Information Tree) o desde otro origen.

Solución: utilice la consola de Directory Server para copiar el atributo `ContainerDefaultTemplateRole` desde otra organización de Access Manager y agréguelo a continuación a la organización en cuestión.

Problema de la línea de comandos

El rol de administrador de organización no puede crear un nuevo usuario con la utilidad de línea de comandos amadmin (6480776)

Un administrador asignado al rol de administrador de organización no puede crear un nuevo usuario con la utilidad de línea de comandos debido a privilegios de registro incorrectos.

Solución: Tanto el administrador de organización como el administrador de nivel superior deben establecer los permisos. Para realizar esta tarea mediante la consola de administración:

1. Acceda a la organización a la que pertenece el administrador.
2. Haga clic en la ficha Privilegios.

3. Haga clic en el vínculo Rol de administrador de organización.
4. Seleccione `Read and write access to all log files` o `Write access to all log files`.
5. Haga clic en Guardar.

Problemas de SDK y de cliente

Los clientes no reciben notificaciones después de reiniciarse el servlet (6309161)

Las aplicaciones escritas con el cliente SDK (`amclientsdk.jar`) no reciben notificaciones si se reinicia el servidor.

Solución: ninguna.

Los clientes de SDK deben reiniciarse después del cambio de esquema de servicio. (6292616)

Si se modifica un esquema de servicio, `ServiceSchema.getGlobalSchema` devuelve el antiguo esquema en lugar del nuevo.

Solución: reinicie el cliente tras modificar un esquema de servicio.

Este problema se ha solucionado en la revisión 1.

Problemas de autenticación

Se produce una reducción del rendimiento del servidor de la IU de autenticación distribuida cuando el usuario de la aplicación no cuenta con privilegios suficientes (6470055)

Al implementar el servidor de la IU de autenticación distribuida utilizando el usuario predeterminado de la aplicación, el rendimiento se reduce significativamente debido a los privilegios restringidos del usuario de la aplicación predeterminado.

Solución: cree un nuevo usuario con los privilegios adecuados.

Para crear un nuevo usuario con las ACI adecuadas:

1. Cree un nuevo usuario en la consola de Access Manager. Por ejemplo, cree un usuario que se llame `AuthUIuser`.
2. En la consola de Directory Server, agregue la siguiente ACI.

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>
   changetype:modifyadd:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,<ROOT_SUFFIX>")
   (targetattr = "*"(version 3.0; acl "SunAM client data anonymous access";
   allow (read, search, compare) userdn = "ldap:///<AuthUIuser's DN>";)
   ```

   Observe que `userdn` se ha definido en `"ldap:///<AuthUIuser's DN>"`.
3. Consulte las instrucciones incluidas en "To Install and Configure a Distributed Authentication UI Server" de *Sun Java System Access Manager 7.1 Postinstallation Guide* para editar el archivo `amsilent` y ejecutar el comando `amadmin`.
4. En el archivo `amsilent`, defina las siguientes propiedades:

   APPLICATION_USER Introduzca `AuthUIuser`.

   APPLICATION_PASSWD Introduzca una contraseña para `AuthUIuser`.
5. Guarde el archivo.
6. Ejecute la secuencia de comandos `amconfig` utilizando el nuevo archivo de configuración. Por ejemplo, en un sistema Solaris con Access Manager instalado en el directorio predeterminado:

   ```
   # cd /opt/SUNWam/bin
   ```

   ```
   # ./amconfig -s ./DistAuth_config
   ```
7. Reinicie el contenedor Web en el servidor de la IU de autenticación distribuida.

Incompatibilidad de la configuración predeterminada del servicio de estadísticas de Access Manager en el modo tradicional (compatible) (6286628)

Al instalar Access Manager en el modo tradicional, se modifica la configuración predeterminada del servicio de estadísticas:

- El servicio se activa de forma predeterminada (`com.iplanet.services.stats.state=file`). Anteriormente, estaba desactivado.
- El intervalo predeterminado (`com.iplanet.am.stats.interval`) cambia de 3600 a 60.
- El directorio de estadísticas predeterminado (`com.iplanet.services.stats.directory`) cambia de `/var/opt/SUNWam/debug` a `/var/opt/SUNWam/stats`.

Solución: ninguna.

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

Después de instalar Access Manager, inicie una sesión como `amadmin` y agregue los atributos `o`, `sunPreferredDomain`, `associatedDomain` , `sunOrganizationAlias`, `uid` y `mail` a la lista de atributos exclusivos. Si crea dos nuevas organizaciones con el mismo nombre, la operación fallará, aunque Access Manager mostrará un mensaje en el que se indica que la organización ya existe y no el mensaje previsto, en el que se indica que se ha infringido la unicidad del atributo.

Solución: ninguna. No haga caso del mensaje incorrecto. Access Manager funciona correctamente.

Problemas de sesión y SSO

El sistema crea un nombre de host de servicio no válido cuando el equilibrador de carga tiene una finalización SSL (6245660)

Si Access Manager se implementa con Web Server como contenedor web mediante un equilibrador de carga con finalización SSL, los clientes no se envían a la página correcta de Web Server. Al hacer clic en la ficha Sesiones (Sessions) de la consola de Access Manager, se devuelve un error debido a que el host no es válido.

Solución: en los siguientes ejemplos, Web Server escucha en el puerto 3030, mientras que el equilibrador de carga lo hace en el puerto 80 y redirecciona las solicitudes a Web Server.

En el archivo *web-server-instance-name*/config/server.xml , edite el atributo servername para que señale al equilibrador de carga en función de la versión de Web Server que esté utilizando.

Para las versiones Web Server 6.1 Service Pack (SP), edite el atributo servername de la siguiente forma:

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Web Server 6.1 SP2 (o superior) permite el cambio de protocolo de http a https o de https a http. Por lo tanto, edite servername de la siguiente forma:

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

Utilización de HttpSession con contenedores Web de terceros

El método predeterminado para mantener las sesiones de autenticación es "sesión interna" en lugar de HttpSession. El valor predeterminado de tiempo máximo de sesión no válida de tres minutos es suficiente. La secuencia de comandos amtune define este valor en un minuto para Web Server o Application Server. Sin embargo, si utiliza un contenedor web de otros fabricantes (IBM WebSphere o el servidor BEA WebLogic) y el elemento opcional HttpSession, es posible que necesite limitar el tiempo máximo de HttpSession del contenedor web para evitar problemas de rendimiento.

Problemas de directivas

La eliminación de atributos dinámicos en el servicio de configuración de directivas provoca problemas de edición de directivas (6299074)

La eliminación de atributos dinámicos en el servicio de configuración de directivas provoca problemas al editar las directivas, como se muestra a continuación:

1. Cree dos atributos dinámicos en el servicio de configuración de directivas.
2. Cree una directiva y seleccione los atributos dinámicos del paso 1 en el proveedor de respuesta.

3. Elimine los atributos dinámicos en el servicio de configuración de directivas y cree dos atributos adicionales.
4. Intente editar la directiva creada en el paso 2.

Se mostrarán los siguientes resultados: "Error, se está estableciendo una propiedad dinámica no válida" (Error Invalid Dynamic property being set).No se muestra de forma predeterminada ninguna directiva en la lista. Después de realizar la búsqueda, se mostrarán las directivas, pero no se podrán editar o eliminar las directivas existentes ni crear una nueva.

Solución: antes de eliminar los atributos dinámicos del servicio de configuración de directivas, elimine las referencias a dichos atributos en las directivas.

Problemas de inicio del servidor

Error de depuración al iniciar Access Manager (6309274, 6308646)

Al iniciar Access Manager 7.1, se devuelven los siguientes errores de depuración en los archivos `amDelegation` y `amProfile`:

- `amDelegation`: no se puede obtener una instancia del complemento para la delegación.
- `amProfile`: se recibió una excepción de delegación.

Solución: ninguna. Puede hacer caso omiso de estos mensajes.

Problemas de AMSDK

Se muestra un error al realizar la operación AMIdentity.modifyService (6506448)

Al utilizar `AMIdentity.modifyService` para establecer el atributo dinámico del servicio de escritorio en un dominio, Access Manager devuelve una excepción de puntero nulo.

Solución:agregue la siguiente propiedad a `AMConfig.properties` y, a continuación, reinicie el servidor:

```
com.sun.am.ldap.connnection.idle.seconds=7200
```

Los miembros del grupo no se muestran en la lista seleccionada (6459598)

Este problema tiene lugar al realizar las siguientes acciones:

1. Defina un dominio con la siguiente configuración:
   - El dominio de nivel superior es `amroot`. El subdominio es `example.com`.
   - El subdominio `example.com` tiene dos almacenes de datos: `exampleDB` y `exampledminDB`.
   - El almacén de datos `exampleDB` contiene todos los usuarios a partir de `dc=example,dc=com`. Las operaciones LDAPv3 admitidas se definen en `user=read,write,create,delete,service.`
   - El almacén de datos `exampleadminDB` contiene un grupo de administración para el dominio. El grupo de administración es `DN: cn=example.com Realm Administrators,ou=Groups,dc=example,dc=com`. Este grupo tiene un único miembro, `scarter`. Las operaciones LDAPv3 admitidas se definen en `group=read,write,create,delete,service.`
2. Haga clic en la ficha "Subjects", luego en "Groups" y en la entrada de `administradores de dominio de example.com`.
3. Haga clic en la ficha "Users".

Todos los usuarios del almacén de datos `exampleDB` se mostrarán como disponibles, pero `scarter` no se mostrará en el campo Seleccionado.

Solución: agregue la operación `user=read` a las operaciones LDAPv3 admitidas en el almacén de datos `exampleadminDB` .

La dirección URL de inicio de sesión de Access Manager devuelve el mensaje "No such Organization found" (No se encuentra esa organización) (6430874)

Es posible que el problema se deba a la utilización de mayúsculas y minúsculas en el nombre de dominio completo (FQDN).

Ejemplo: `HostName.PRC.Example.COM`

Solución: tras la instalación, no utilice la dirección URL predeterminada de inicio de sesión de Access Manager. En su lugar, en la URL de inicio de sesión, incluya la ubicación LDAP de la organización predeterminada. Por ejemplo:

```
http://HostName.PRC.Example.COM/amserver/UI/Login?org=dc=PRC,dc=Example,dc=COM
```

Una vez que haya iniciado la sesión correctamente en Access Manager, ya no es necesario introducir la ruta completa a la organización del usuario cada vez que inicie una sesión en Access Manager. siga estos pasos:

1. Vaya a la ficha Dominio en el modo de dominio o vaya a la ficha Organización en el modo tradicional.
2. Haga clic en el nombre de organización o dominio predeterminado.

   En este ejemplo, haga clic en `prc`.
3. Cambie todos los caracteres en mayúsculas del valor de `dominio/alias de DNS` a caracteres en minúsculas.

   En este ejemplo, agregue el valor con letras minúsculas `hostname.prc.example.com` a la lista y elimine el valor `HostName.PRC.Example.COM` en mayúsculas y minúsculas de la lista.
4. Haga clic en Guardar y cierre la sesión en la consola de Access Manager.

Ahora puede iniciar la sesión utilizando cualquiera de las siguientes direcciones URL:

- `http://hostname.PRC.Example.COM/amserver/UI/Login`
- `http://hostname.PRC.Example.COM/amserver`
- `http://hostname.PRC.Example.COM/amserver/console`

No se pueden crear organizaciones secundarias desde Access Manager al utilizar `amadmin` (5001850)

Este problema se produce cuando se activa la repetición de varias réplicas principales entre dos servidores de Directory Server y se intenta crear una organización secundaria mediante la utilidad `amadmin`.

Solución: en ambos servidores de Directory Server, defina la propiedad `nsslapd-lookthroughlimit` en `-1`.

Problema con SSL

- "La secuencia de comandos amconfig genera un error cuando el certificado SSL está caducado. (6488777)" en la página 40

La secuencia de comandos amconfig genera un error cuando el certificado SSL está caducado. (6488777)

Si el contenedor de Access Manager se está ejecutando en modo SSL y el certificado SSL de contenedor está caducado, `amconfig` genera un error, que puede provocar daños en la ruta de clase.

Solución: si ya ha ejecutado `amconfig` con un certificado caducado y la ruta de clase está dañada, obtenga primero un certificado SSL válido. Restablezca el archivo `domain.xml` original o una copia del archivo `domain.xml` en el que la ruta de clase no esté dañada. A continuación, vuelva a ejecutar el comando `amconfig` :

```
/opt/SUNWam/bin/amconfig -s $PWD/amsamplesilent
```

Problemas de muestras

El directorio de muestras "clientsdk" contiene archivos makefile no deseados (6490071)

Los archivos de muestra se incluyen en el SDK de cliente y muestran cómo escribir programas independientes y aplicaciones web. Las muestras se encuentran en el directorio en el que se haya generado el archivo `Makefile.clientsdk` y en los siguientes subdirectorios:

```
.../clientsdk-samples/

.../clientsdk-webapps/
```

En el directorio "clientsdk-samples", se incluyen muestras de autenticación, registro, y programas independientes SAML y de directivas. En el directorio "clientsdk-webapps", se incluyen muestras para la administración de usuarios y servicios, y programas de directivas. Cada muestra incluye un archivo Léame (Readme.html) con instrucciones sobre cómo compilar y ejecutar el programa de muestra.

Para compilar las muestras, el archivo makefile debe ejecutarse en el subdirectorio correspondiente. El archivo makefile de nivel superior no compila las muestras en los subdirectorios.

Problemas relacionados con el SO Linux

Se producen problemas de JVM cuando se ejecuta Access Manager en Application Server (6223676)

Si ejecuta Application Server 8.1 en Red Hat Linux, el tamaño de pila de los subprocesos creados por el SO Red Hat para Application Server es de 10 Mbytes, lo que puede provocar problemas en los recursos de JVM cuando el número de sesiones de usuario de Access Manager alcance las 200.

Solución: establezca el tamaño de pila del SO Red Hat con un valor inferior como, por ejemplo, 2048 o, incluso, 256 Kbytes, ejecutando el comando `ulimit` antes de iniciar Application Server. Ejecute el comando `ulimit` en la misma consola que utilizará para iniciar Application Server. Por ejemplo:

```
# ulimit -s 256;
```

Problemas de Windows y HP-UX

Error en la configuración automática de Access Manager al realizar la instalación con las configuraciones regionales zh_TW y es (6515043)

Solución: Si se usan las configuraciones regionales `zh_TW` y `es` en la plataforma HP-UX, Access Manager debe configurarse únicamente en el modo "Configurar más tarde". Inicie el programa de instalación de JavaES, instale el producto Access Manager y salga del programa. A continuación, ejecute el programa de configuración de Access Manager, como se muestra a continuación:

1. `LANG=C`
2. `export LANG`
3. Edite *accessmanager-base*`/bin/amsamplesilent file`.
4. Ejecute *accessmanager-base*`/bin/amconfig -s amsamplesilent`.

HP-UX necesita el archivo binario gettext con AM al instalar la pila completa de JES (6497926)

Actualmente no existe ninguna solución para este problema.

Problemas de federación y SAML

Error de cierre de sesión en la federación (6291744)

En el modo de dominio, si se intenta realizar la federación de cuentas de usuario en un proveedor de identidades (IDP) y un proveedor de servicios (SP), se finaliza la federación y, a continuación, se cierra la sesión, se producirá un error: Error: no se ha encontrado ninguna suborganización (Error: No sub organization found.)

Solución: ninguna.

Problemas de internacionalización (g11n)

Los componentes de la consola de administración se muestran en inglés con la configuración regional zh (6470543)

Al establecer la configuración regional del explorador en `zh`, los componentes de la consola de administración se muestran en inglés como, por ejemplo, los botones "Version" (Versión), "Help" (Ayuda) y "Logout " (Cerrar la sesión).

Solución: establezca la configuración regional en `zh-cn` en lugar de en `zh`.

El valor actual y el nuevo valor se muestran incorrectamente en la consola (6476672)

En la versión traducida de la consola de administración, las etiquetas de los atributos de valor actual y nuevo valor se muestran incorrectamente como "label.current.value" y "label.new.value" respectivamente.

La fecha de la condición de directiva debe especificarse con el formato inglés (6390856)

Las etiquetas de formato de fecha de la condición de directiva en la configuración regional china no se muestran de acuerdo con la manera habitual china. La etiquetas proponen un formato de fecha inglés. Los campos relacionados también aceptan los valores de formato de fecha inglés.

Solución: para cada campo, siga el ejemplo de formato de fecha que se indica en la etiqueta del campo.

No se puede eliminar UTF-8 en la sección de detección de cliente. (5028779)

La función de detección de cliente no funciona correctamente. Los cambios realizados en la consola de Access Manager 7.1 no se transfieren automáticamente al explorador.

Solución: existen dos soluciones:

- Reinicie el contenedor web de Access Manager después de realizar un cambio en la sección de detección de cliente.

  o

- Siga estos pasos en la consola de Access Manager:
  1. Haga clic en `Client Detection` en la ficha `Configuration`.
  2. Haga clic en el vínculo `Edit` para `genericHTML`.
  3. En la ficha HTML, haga clic en el vínculo `genericHTML`.
  4. Introduzca la siguiente entrada en la lista de juegos de caracteres: `UTF-8;q=0.5` (Asegúrese de que el factor `q` de UTF-8 sea inferior al de otros juegos de caracteres de su configuración regional.)
  5. Guarde el cambio, cierre la sesión y vuelve a iniciarla.

Los caracteres de varios bytes se muestran en forma de signos de interrogación en los archivos de registro (5014120)

Los mensajes de varios bytes de los archivos de registro del directorio `/var/opt/SUNWam/logs` se muestran en forma de signos de interrogación (`?`). Los archivos de registro suelen presentar

una codificación nativa y, no siempre, UTF-8. Cuando una instancia del contenedor web se inicia con una determinada configuración regional, los archivos de registro presentarán una codificación nativa para dicha configuración regional. Si se cambia a otra configuración regional y se reinicia la instancia del contenedor web, los mensajes actuales presentarán la codificación nativa para dicha configuración regional, pero los mensajes de codificaciones anteriores se mostrarán en forma de signos de interrogación.

Solución: asegúrese de iniciar siempre las instancias del contenedor web con la misma codificación nativa.

Problemas de documentación

Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3 (6365196)

Después de aplicar la respectiva revisión, puede configurar los roles y los roles filtrados del complemento LDAPv3, si los datos se han almacenado en Sun Java System Directory Server (soluciona el Id. de problema 6349959). En la consola de administración de Access Manager 7.1, en la configuración de LDAPv3 del campo "Operaciones y tipos admitidos del complemento LDAPv3", introduzca los valores de la siguiente forma:

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

Puede introducir una de las entradas anteriores o ambas en función de los roles y los roles filtrados que desee utilizar en la configuración de LDAPv3.

Información sobre las propiedades no utilizadas en el archivo `AMConfig.properties` (6344530)

Las siguientes propiedades del archivo `AMConfig.properties` no se utilizan:

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

Información sobre cómo habilitar el cifrado XML (6275563)

Para habilitar el cifrado XML para Access Manager o Federation Manager mediante el archivo JAR de Bouncy Castle con el fin de generar una clave de transporte, siga estos pasos:

1. Si utiliza una versión de JDK anterior a JDK 1.5, descargue el proveedor JCE de Bouncy Castle desde el sitio de Bouncy Castle (`http://www.bouncycastle.org/`). Por ejemplo, para JDK 1.4, descargue el archivo `bcprov-jdk14-131.jar`.
2. Si ha descargado un archivo JAR en el paso anterior, cópielo en el directorio *jdk_root*`/jre/lib/ext`.
3. Para la versión interna de JDK, descargue los archivos de "Unlimited Strength Jurisdiction Policy" de JCE para la versión de JDK en el sitio de Sun (`http://java.sun.com`). Para IBM WebSphere, acceda al sitio correspondiente de IBM para descargar los archivos necesarios.
4. Copie los archivos descargados `US_export_policy.jar` y `local_policy.jar` en el directorio *jdk_root*`/jre/lib/security` .
5. Si utiliza una versión de JDK anterior a JDK 1.5, edite el archivo *jdk_root*`/jre/lib/security/java.security` y agregue Bouncy Castle como uno de los proveedores. Por ejemplo:

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. Defina la siguiente propiedad en el archivo `AMConfig.properties` como "true" (verdadera):

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. Reinicie el contenedor web de Access Manager.

Para obtener más información, consulte el Id. de problema 5110285 (El cifrado XML requiere el archivo JAR de Bouncy Castle).

Actualizaciones de la documentación

Para acceder a estos documentos, consulte la colección de documentos de Access Manager 7.1:

`http://docs.sun.com/coll/1292.1`

Se ha agregado un nuevo documento titulado Capítulo 1, “Technical Note: Deploying Access Manager Instances to an Application Server Cluster” de *Technical Note: Deploying Access Manager to an Application Server Cluster* a la colección de Access Manager 7 2005Q4.

La colección de Sun Java System Access Manager Policy Agent 2.2 también se ha revisado para documentar nuevos agentes:

`http://docs.sun.com/coll/1322.1`

Archivos que se pueden distribuir

Sun Java System Access Manager 7.1 no contiene ningún archivo que se pueda distribuir 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 asistencia técnica de Sun usando uno de estos procedimientos:

- Servicios de recursos de asistencia técnica de Sun (SunSolve) en `http://sunsolve.sun.com/`.

  Este sitio dispone de vínculos a la base de datos de soluciones, al centro de asistencia en línea y al rastreador de productos, así como a programas de mantenimiento y números de contacto de asistencia técnica.
- El número de teléfono del distribuidor asociado al contrato de mantenimiento.

Para poder ayudarle lo mejor posible a resolver problemas, tenga disponible la siguiente información cuando se ponga en contacto con el servicio de asistencia:

- Descripción del problema, incluida la situación en la que éste se produce y la forma en que afecta al funcionamiento
- Tipo de equipo, versión del sistema operativo y versión del producto, incluido cualquier parche del producto y otro software que pudiera influir en el problema
- Pasos detallados de los métodos que haya usado para reproducir el problema
- Cualquier registro de errores o volcados del núcleo

Sun valora sus comentarios

Sun tiene interés en mejorar su documentación y valora sus comentarios y sugerencias. Vaya a `http://docs.sun.com/` y haga clic en Send Comments (Enviar comentarios).

Indíquenos el título completo de la documentación y el número de referencia en los campos pertinentes. El número de referencia 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 referencia de las *Access Manager Notas de la versión* es 819-4683-13.

Recursos adicionales de Sun

Puede encontrar información útil y recursos de Access Manager en las siguientes direcciones de Internet:

- Documentación de Sun Java Enterprise System: `http://docs.sun.com/prod/entsys.05q4`
- Servicios de Sun: `http://www.sun.com/service/consulting/`
- Servicios y productos de software: `http://wwws.sun.com/software/`
- Recursos de asistencia técnica: `http://sunsolve.sun.com/`
- Información para programadores: `http://developers.sun.com/`
- Servicios de asistencia para programadores de Sun: `http://www.sun.com/developers/support/`

Funciones de accesibilidad para usuarios con discapacidades

Si desea disfrutar de las funciones de accesibilidad que se han comercializado tras la publicación de este medio, consulte la Sección 508 de las evaluaciones de productos, que se pueden obtener de Sun previa solicitud, para determinar las versiones más adecuadas para implementar soluciones accesibles. Puede obtener versiones actualizadas de las aplicaciones en `http://sun.com/software/javaenterprisesystem/get.html`.

Para obtener información sobre el compromiso de Sun con respecto a la accesibilidad, visite `http://sun.com/access`.

Sitios web de terceros relacionados

Se hace referencia a las direcciones URL de terceras partes para proporcionar información adicional relacionada.

Nota – Sun no se responsabiliza de la disponibilidad de las sedes Web de otras empresas que se mencionan en este documento. Sun no garantiza ni se hace responsable de los contenidos, la publicidad, los productos u otros materiales que puedan estar disponibles a través de dichos sitios o recursos. Sun no será responsable de daños o pérdidas, supuestos o reales, provocados por o a través del uso o confianza del contenido, bienes o servicios disponibles en dichos sitios o recursos, o a través de ellos.
