Notas de la version de Sun Java System Access Manager 7 2005Q4

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

Referencia: 819–3480
19 de agosto de 2008

080915@20795

Contenido

Notas de la versión de Sun Java System Access Manager 7 2005Q4 5
Contenido 5
Historial de revisiones 6
Acerca de Sun Java System Access Manager 7 2005Q4 10
Versiones de las revisiones de Access Manager 7 2005Q4 10
- Revisión 7 de Access Manager 7 2005Q4 11
- Consideraciones previas a la instalación 13
- Instrucciones de instalación de las revisiones 15
- Consideraciones posteriores a la instalación 21
- Revisión 6 de Access Manager 7 2005Q4 24
- Access Manager 7 2005Q4 revisión 5 29
- Revisión 4 de Access Manager 7 2005Q4 47
- Revisión 3 de Access Manager 7 2005Q4 49
- Revisión 2 de Access Manager 7 2005Q4 60
- Revisión 1 de Access Manager 7 2005Q4 65

Novedades de esta versión 66
- Modos de Access Manager 67
- Nueva consola de Access Manager 67
- Repositorio de identidades 68
- Árbol de información de Access Manager 68
- Cambios en la conmutación por error de la sesión 68
- Notificación de cambio de propiedad de sesión 69
- Restricciones de cuota de sesión 69
- Autenticación distribuida 70
- Compatibilidad con varias instancias del módulo de autenticación 70
- Espacio de nombre de “cadena” o “configuración con nombre” de autenticación 70
- Mejoras del módulo de directivas 71
- Configuración del sitio 72

Federación en masa 72
Mejoras del registro 72
Requisitos de hardware y software 73
Exploradores compatibles 74
Compatibilidad con la virtualización de sistemas 75
Problemas de compatibilidad 75
Modo tradicional de Access Manager 75
Agentes de directivas de Access Manager 77
Notas sobre la instalación 78
Limitaciones y problemas conocidos 78
Problemas de compatibilidad 78
Problemas de instalación 80
Problemas de actualización 83
Problemas de configuración 85
Problemas de la consola de Access Manager 89
Problemas de SDK y de cliente 92
Problemas de las utilidades de línea de comandos 93
Problemas de autenticación 94
Problemas de sesión y SSO 95
Problemas de directivas 98
Problemas de inicio del servidor 98
Problemas relacionados con el SO Linux 99
Problemas de federación y SAML 99
Problemas de internacionalización (g11n) 101
Problemas de documentación 103
Actualizaciones de la documentación 111
Colección de documentos de Sun Java System Access Manager 7 2005Q4 111
Colección de documentos de Sun Java System Federation Manager 7.0 2005Q4 112
Colección de documentos de Sun Java System Access Manager Policy Agent 2.2 112
Archivos redistribuibles 112
Información sobre problemas y respuestas de los clientes 112
Sun valora sus comentarios 113
Recursos adicionales de Sun 113
Funciones de accesibilidad para usuarios con discapacidades 113
Sitios web de terceros relacionados 114

Notas de la versión de Sun Java System Access Manager 7 2005Q4

19 de agosto de 2008

Número de referencia 819-2134-22

Las Notas de la versión de Sun Java™ System Access Manager (Access Manager) 7 2005Q4 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 obtener información de esta edición de las Notas de la versión, consulte "Historial de revisiones" en la página 6.

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.

Contenido

Las Notas de la versión de Access Manager 7 2005Q4 contienen las siguientes secciones:

- "Historial de revisiones" en la página 6
- "Acerca de Sun Java System Access Manager 7 2005Q4" en la página 10
- "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10
- "Novedades de esta versión" en la página 66
- "Requisitos de hardware y software" en la página 73
- "Problemas de compatibilidad" en la página 75
- "Notas sobre la instalación" en la página 78
- "Limitaciones y problemas conocidos" en la página 78

- "Actualizaciones de la documentación" en la página 111
- "Archivos redistribuibles" en la página 112
- "Información sobre problemas y respuestas de los clientes" en la página 112
- "Recursos adicionales de Sun" en la página 113
- "Sitios web de terceros relacionados" en la página 114

Historial de revisiones

La siguiente tabla muestra el historial de revisiones de las Notas de la versión de Access Manager 7 2005Q4.

TABLA 1 Historial de revisiones

Fecha	Descripción de los cambios
19 de agosto de 2008	Se ha agregado información sobre la revisión 7 para los sistemas Windows y HP-UX en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10.
12 de mayo de 2008	■ Se ha agregado información sobre la revisión 7 en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10. ■ Se ha agregado la sección "Compatibilidad con la virtualización de sistemas" en la página 75.
16 de octubre de 2007	Entre los cambios de esta revisión, se incluyen: ■ Se ha agregado información sobre la revisión 6 en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10. ■ "CR# 6522720: la búsqueda en la ayuda en línea de la consola no funciona con caracteres de varios bytes en los sistemas Windows y HP-UX" en la página 46. La revisión 6 soluciona este problema en los sistemas Windows. Sin embargo, el problema aún persiste en los sistemas HP-UX.
10 de julio de 2007	Entre los cambios de esta revisión, se incluyen: ■ Se ha agregado información sobre la revisión 126371-05 para los sistemas HP-UX en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10. ■ Se ha agregado el siguiente nuevo problema: "La búsqueda LDAP de atributos nulos devuelve un error cuando Access Manager señala a Directory Proxy (6357975)" en la página 93.

TABLA 1 Historial de revisiones *(Continuación)*

Fecha	Descripción de los cambios
16 de marzo de 2007	Entre los cambios de esta revisión, se incluyen: ■ Se ha agregado información sobre la revisión 5 en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10. ■ Se han agregado aclaraciones y nueva información en "Problemas de documentación" en la página 103. ■ Se han hecho varios cambios técnicos y editoriales por parte de los revisores y solicitudes de cambio (CR).
30 de octubre de 2006	Entre los cambios realizados en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10, se incluyen: ■ Se ha agregado información sobre la revisión 4. ■ Se ha corregido el uso inconsistente de *AccessManager-base* . ■ Se ha revisado la descripción de "CR# 6440651: la repetición de las cookies requiere la propiedad `com.sun.identity.session.resetLBCookie`" en la página 57.
25 de agosto de 2006	Entre los cambios realizados en la sección "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10, se incluyen: ■ Se ha agregado información sobre la revisión 3. ■ Se ha revisado la información sobre las revisiones 1 y 2, además de incluir nueva información.

25 de mayo de 2006	Entre los cambios de esta revisión, se incluyen:
	■ Se ha agregado la nueva sección "Revisión 2 de Access Manager 7 2005Q4" en la página 60.
	■ Se ha agregado información sobre la compatibilidad con las plataformas HP-UX y Microsoft Windows en la Tabla 4.
	■ Se han agregado los siguientes problemas en "Problemas de documentación" en la página 103:
	  ■ "Las Notas de la versión presentan una solución incorrecta para un problema conocido. (6422907)" en la página 109
	  ■ "Documento `com.iplanet.am.session.protectedPropertiesList` en `AMConfig.properties` (6351192)" en la página 109

9 de febrero de 2006	Se ha modificado "Actualizaciones de la documentación" en la página 111 para que muestre los nuevos documentos revisados de Access Manager 7 2005Q4 que se han publicado desde el lanzamiento de la versión inicial.

TABLA 1 Historial de revisiones *(Continuación)*

Fecha	Descripción de los cambios
7 de febrero de 2006	Entre los cambios de esta revisión, se incluyen: ■ Se han agregado los siguientes problemas en "Limitaciones y problemas conocidos" en la página 78: ■ "El servicio de autenticación no se inicializa si se instala Access Manager y Directory Server en distintos equipos (6229897)" en la página 82 ■ "La secuencia de comandos `ampre70upgrade` de Access Manager no elimina los paquetes traducidos (6378444)" en la página 83 ■ Se ha actualizado la sección "Actualizaciones de la documentación" en la página 111.

TABLA 1 Historial de revisiones *(Continuación)*

Fecha	Descripción de los cambios
18 de enero de 2006	Entre los cambios de esta revisión, se incluyen: ■ Se ha agregado la nueva sección "Revisión 1 de Access Manager 7 2005Q4" en la página 65. ■ Se ha aclarado la descripción de "Autenticación distribuida" en la página 70. ■ Se ha aclarado el concepto de compatibilidad con las zonas de Solaris 10 y se ha agregado este tipo de compatibilidad para las plataformas AMD64 en "Requisitos de hardware y software" en la página 73. ■ Se han agregado los siguientes problemas en "Limitaciones y problemas conocidos" en la página 78: ■ "Error en la firma de URL en IBM WebSphere al utilizar la clave RSA (6271087)" en la página 88 ■ "Se producen problemas de JVM cuando se ejecuta Access Manager en Application Server (6223676)" en la página 99 ■ "La ejecución de los ejemplos de servicios web devuelve el mensaje "Oferta de recursos no encontrada" (6359900)" en la página 99 ■ "Después de aplicar la revisión 1, el archivo `/tmp/amsilent` concede acceso de lectura a todos los usuarios (6370691)" en la página 81 ■ "Adición del atributo `ContainerDefaultTemplateRole` después de la migración de datos (4677779)" en la página 85 ■ "Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3 (6365196)" en la página 109 ■ "Información sobre las propiedades no utilizadas en el archivo `AMConfig.properties` (6344530)" en la página 109 ■ "Información sobre cómo habilitar el cifrado XML (6275563)" en la página 110 ■ Se ha agregado la nueva sección "Actualizaciones de la documentación" en la página 111.
8 de noviembre de 2005	Se ha modificado la sección "Repositorio de identidades" en la página 68 para que incluya los repositorios compatibles con la versión 3 de LDAP (LDAP v3) admitida.
3 de octubre de 2005	Versión inicial.
30 de junio de 2005	Versión Beta.

Acerca de Sun Java System Access Manager 7 2005Q4

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 las organizaciones
- Compatibilidad de identidad federada con Liberty Alliance Project y el Lenguaje de marcas de aserción 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.

Versiones de las revisiones de Access Manager 7 2005Q4

Las versiones más recientes de las revisiones de Access Manager 7 2005Q4 pueden descargarse en SunSolve Online: `http://sunsolve.sun.com`. Los Id. de revisión más recientes son:

- Sistema operativo Solaris™(SO Solaris) en sistemas basado en SPARC®: **120954-07**
- SO Solaris en plataformas x86: **120955-07**
- Sistemas Linux: **120956-07**
- Sistemas Microsoft Windows: **124296-07**
- Sistemas HP-UX: **126371-07**

Nota – Las revisiones de Access Manager 7 2005Q4 son acumulativas. Puede instalar la revisión 7 sin necesidad de instalar en primer lugar la revisión 1, 2, 3, 4, 5 o 6. Sin embargo, si no ha instalado ninguna revisión anterior, revise las nuevas funciones y problemas de las secciones de la revisión anterior para determinar si alguna de las funciones o problemas se aplican a su implementación.

Entre la información acerca de las revisiones de Access Manager 7 2005Q4, se incluye:

- "Revisión 7 de Access Manager 7 2005Q4" en la página 11
- "Consideraciones previas a la instalación" en la página 13
- "Instrucciones de instalación de las revisiones" en la página 15
- "Consideraciones posteriores a la instalación" en la página 21
- "Revisión 6 de Access Manager 7 2005Q4" en la página 24
- "Access Manager 7 2005Q4 revisión 5" en la página 29

- "Revisión 4 de Access Manager 7 2005Q4" en la página 47
- "Revisión 3 de Access Manager 7 2005Q4" en la página 49
- "Revisión 2 de Access Manager 7 2005Q4" en la página 60
- "Revisión 1 de Access Manager 7 2005Q4" en la página 65

Revisión 7 de Access Manager 7 2005Q4

La revisión 7 (versión 07) de Access Manager 7 soluciona diversos problemas, como se indica en el archivo README (LÉAME) incluido con la revisión.

La revisión 7 incluye estos cambios:

- "CR# 6637806: tras el reinicio, Access Manager envió un token SSO de aplicaciones no válido a un agente" en la página 11
- "CR# 6612609: la conmutación por error de sesión funciona si el cable de red está desconectado del servidor Message Queue" en la página 11
- "CR# 6570409: el servicio de interacción del equilibrador de carga funciona correctamente como proveedor de identidades" en la página 12
- "CR# 6545176: las URL de redirección se pueden establecer de forma dinámica en el complemento SPI de procesamiento posterior a la autenticación" en la página 12

CR# 6637806: tras el reinicio, Access Manager envió un token SSO de aplicaciones no válido a un agente

Tras el reinicio de un servidor Access Manager, el SDK de cliente de Access Manager ahora envía una excepción significativa a un agente, por lo que el agente puede volver a autenticarse para obtener una nueva sesión de aplicaciones. Anteriormente, tras aplicar la revisión 5 de Access Manager 7 2005Q4, el SDK de cliente de Access Manager enviaba un token SSO de aplicaciones no válido al agente tras reiniciar el servidor Access Manager.

Este problema se ha solucionado mediante el duplicado CR 6496155. La revisión 7 también cuenta con una opción (propiedad `comp.iplanet.dpro.session.dnRestrictionOnly`) para enviar el token SSO de aplicaciones en un contexto restrictivo. De forma predeterminada, los agentes envían la dirección IP del servidor en el que están instalados, pero si es necesario realizar una comprobación de DN estricta, establezca esta propiedad en el archivo `AMConfig.properties` de la siguiente manera:

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609: la conmutación por error de sesión funciona si el cable de red está desconectado del servidor Message Queue

En una implementación de conmutación por error de sesión, si todas las instancias de Access Manager y los agentes de Message Queue están instalados en el mismo servidor, la conmutación por error de sesión ahora funciona si el cable de red está desconectado de uno de los servidores.

De forma predeterminada, el atributo de fábrica de conexión `imqAddressListBehavior` de Message Queue está establecido en `PRIORITY`, lo que provoca que Message Queue pruebe las direcciones en el orden en que aparecen en la lista de direcciones del agente (por ejemplo: `localhost:7777,server2:7777,server3:7777`). Si el atributo está establecido en `RANDOM`, las direcciones se prueban en orden aleatorio.

Para establecer este atributo en RANDOM, establezca el siguiente parámetro en la secuencia de comandos `amsessiondb`:

```
-DimqAddressListBehavior=RANDOM
```

Para obtener información acerca de los atributos `PRIORITY` y `RANDOM` de Message Queue, consulte "Broker Address List" de *Sun Java System Message Queue 3.7 UR1 Administration Guide*.

CR# 6570409: el servicio de interacción del equilibrador de carga funciona correctamente como proveedor de identidades

En una implementación con dos servidores conectados con un equilibrador de carga y funcionando como un único proveedor de identidades, debe establecer las siguientes propiedades en el archivo `AMConfig.properties`:

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

La clase `com.sun.identity.liberty.interaction.interactionConfigClass` es la única compatible actualmente. Por lo tanto, de forma predeterminada, la clase de configuración de interacción integrada en Federation Liberty se utiliza para acceder a los parámetros de configuración de interacción.

CR# 6545176: las URL de redirección se pueden establecer de forma dinámica en el complemento SPI de procesamiento posterior a la autenticación

Las URL de redirección se pueden establecer ahora de forma dinámica en los complementos SPI de procesamiento posterior a la autenticación para un inicio de sesión correcto e incorrecto y para el cierre de sesión. Si no se ejecuta un complemento de procesamiento posterior, no se utilizará la URL de redirección establecida en la SPI de procesamiento posterior, y las URL de redirección establecidas a través de otros medios se ejecutarán de la misma forma que antes.

Para obtener más información, consulte el ejemplo `com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java` .

Consideraciones previas a la instalación

- "Copia de seguridad de los archivos" en la página 13
- "Instalación y configuración de Access Manager" en la página 15

Copia de seguridad de los archivos

Importante. Si se ha personalizado alguno de los archivos de la instalación actual, realice una copia de seguridad de éstos antes de instalar la revisión. Después de instalar la revisión, compare los archivos de los que se ha realizado una copia de seguridad con los nuevos archivos instalados por la revisión para identificar los elementos que se han personalizado. Combine las personalizaciones con los nuevos archivos y guárdelos. Para obtener más información sobre cómo administrar los archivos personalizados, lea la siguiente información.

Antes de instalar una revisión, realice también una copia de seguridad de los siguientes archivos.

Sistemas Solaris	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ Archivos del directorio /etc/opt/SUNWam/config/xml/template/: idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml, amAuth.xml , amSession.xml ■ Archivos del directorio *AccessManager-base*/SUNWam/locale/ : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

Sistemas Linux y HP-UX	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ Archivos del directorio /etc/opt/sun/identity/config/xml/template/ : idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Archivos del directorio *AccessManager-base*/identity/locale/ : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties
Sistemas Windows	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ Archivos del directorio *AccessManager-base*\identity\config\xml\template : idRepoService.xml, amSOAPBinding.xml, amDisco.xml, amAuthCert.xml , amAuth.xml, amSession.xml ■ Archivos del directorio *AccessManager-base*\identity\locale : amConsole.properties, amIdRepoService.properties, amAuthUI.properties, amAuth.properties, amPolicy.properties, amPolicyConfig.properties, amSessionDB.properties, amSOAPBinding.properties, amAdminCLI.properties, amSDK.properties, amAuthLDAP.properties, amSession.properties, amAuthContext.properties, amSAML.properties, amAuthCert.properties

AccessManager-base es el directorio base de instalación. El directorio base de instalación predeterminado depende de la plataforma:

- Sistemas Solaris: /opt
- Sistemas Linux y HP-UX: /opt/sun
- Sistemas Windows: *javaes-install-directory*\AccessManager . Por ejemplo: C:\Program Files\Sun\AccessManager

Instalación y configuración de Access Manager

Las revisiones de Access Manager descritas en este documento no instalan Access Manager. Antes instalar la revisión, Access Manager 7 2005Q4 debe instalarse en el servidor. Para obtener más información sobre la instalación, consulte la *Guía de instalación de Sun Java Enterprise System 2005Q4 para UNIX*.

Si instala la revisión en un sistema Windows, consulte la *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Además, debe familiarizarse con la secuencia de comandos `amconfig` para implementar, reimplementar y configurar Access Manager, como se describe en el Capítulo 1, "Access Manager 7 2005Q4 Configuration Scripts" de *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Para obtener una lista de las revisiones de Access Manager obsoletas debido a esta nueva revisión y a todas las revisiones que debe instalar antes de instalar este revisión, consulte el archivo README (LÉAME) incluido con la revisión.

Precaución – Las revisiones de Access Manager (al igual que cualquier otra revisión) debe probarse en un sistema en el que no se haya realizado aún una implementación o en el que se esté iniciando una implementación antes de aplicarlas en un entorno de producción. Además, el programa de instalación de revisiones no actualiza adecuadamente los archivos JSP personalizados, por lo es que es posible que deba realizar cambios manuales en estos archivos para que Access Manager funcione correctamente.

Instrucciones de instalación de las revisiones

- "Instrucciones de instalación de revisiones para los sistemas Solaris" en la página 15
- "Instrucciones de instalación de revisiones para los sistemas Linux" en la página 18
- "Instrucciones de instalación de revisiones para los sistemas Windows" en la página 19
- "Instrucciones de instalación de revisiones para los sistemas HP-UX" en la página 20

Instrucciones de instalación de revisiones para los sistemas Solaris

Antes de instalar la revisión de Solaris, asegúrese de que ha hecho una copia de seguridad de los archivos enumerados en "Consideraciones previas a la instalación" en la página 13.

Para agregar o eliminar revisiones en los sistemas Solaris, utilice los comandos `patchadd` y `patchrm`, que se proporcionan con el SO.

Comando patchadd

Utilice el comando `patchadd` para instalar una revisión en un sistema independiente. Por ejemplo:

```
# patchadd /var/spool/patch/120954-07
```

Nota – Si está instalando la revisión de Solaris en una zona global de Solaris 10, llame al comando `patchadd` con el argumento `-G`. Por ejemplo:

```
patchadd -G /var/spool/patch/120954-07
```

La secuencia de comandos `postpatch` muestra un mensaje acerca de la reimplementación de las aplicaciones de Access Manager, excepto en un sistema con un único componente de SDK de Access Manager instalado.

La secuencia de comandos `postpatch` crea el archivo `amsilent` en el siguiente directorio:

- Sistemas Solaris: *AccessManager-base*`/SUNWam`
- Sistemas Linux: *AccessManager-base*`/identity`

AccessManager-base es el directorio base de instalación. El directorio base de instalación predeterminado es `/opt` en los sistemas Solaris y `/opt/sun` en los sistemas Linux.

El archivo `amsilent` se basa en el archivo `amsamplesilent`, aunque se han establecido algunos parámetros necesarios en función de los archivos de configuración de Access Manager en el sistema. Sin embargo, los parámetros de contraseña contienen valores predeterminados. Elimine el delimitador y modifique el valor de cada parámetro de contraseña, y compruebe atentamente los valores de los demás parámetros de este archivo según las necesidades de su implementación.

El parámetro `COMMON_DEPLOY_URI`, el prefijo URI de la aplicación web de dominio común, también contiene un valor predeterminado. Si ha elegido un valor no predeterminado para este URI, asegúrese de actualizar este valor. De lo contrario, fallará la reimplementación de las aplicaciones web con `amconfig` y el archivo `amsilent` generado por la revisión.

A continuación, ejecute el siguiente comando (que se muestra con Access Manager instalado en el directorio predeterminado):

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

Precaución – El archivo `amsilent` contiene datos confidenciales como por ejemplo las contraseñas de administrador en texto sencillo, así que asegúrese de que protege el archivo adecuadamente para su implementación.

Tras ejecutar la secuencia de comandos `amconfig`, ejecute la secuencia de comandos `updateschema.sh` para cargar los archivos XML y LDIF. La secuencia de comandos `updateschema.sh` está disponible tras la instalación de la revisión 7 en el siguiente directorio:

- Sistemas Solaris SPARC: *patch-home-directory* /120954-07
- Sistemas Solaris x86: *patch-home-directory*/120955-07

Después de ejecutar la secuencia de comandos `updateschema`, reinicie los procesos de Access Manager. Por ejemplo:

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

A continuación, reinicie el contenedor web de Access Manager.

Comando patchrm

Utilice el comando `patchrm` para eliminar una revisión de un sistema independiente. Por ejemplo:

```
# patchrm 120954-03
```

La secuencia de comandos `backout` muestra un mensaje parecido al del comando `patchadd`, excepto en un sistema con un único componente de SDK de Access Manager instalado.

Tras eliminar la revisión, vuelva a implementar las aplicaciones de Access Manager utilizando el archivo `amsilent` del directorio *AccessManager-base* `/SUNWam`, donde *AccessManager-base* es el directorio base de instalación. El directorio base de instalación predeterminado es `/opt` en los sistemas Solaris.

Establezca los parámetros del archivo `amsilent` según las necesidades de su implementación.

A continuación, ejecute el siguiente comando, que aparece con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

Para obtener información y ejemplos adicionales sobre los comandos `patchadd` y `patchrm`, consulte las páginas de comando `man` correspondientes de Solaris.

Consulte también “Consideraciones posteriores a la instalación” en la página 21 para obtener más información.

Zonas de Solaris 10

El sistema operativo Solaris 10 introdujo el nuevo concepto de “zonas”. Por lo tanto, el comando patchadd incluye la nueva opción `-G`, que permite agregar una revisión sólo a la zona global. Este comando busca de forma predeterminada la variable `SUNW_PKG_ALLZONES` en el elemento pkginfo de los paquetes a los que se va a aplicar la revisión. Sin embargo, la variable

SUNW_PKG_ALLZONES no se ha establecido para todos los paquetes de Access Manager y la opción -G es necesaria si Access Manager 7 2005Q4 se ha instalado en la zona global. Si Access Manager se ha instalado en una zona local, la opción patchadd -G no tiene ningún efecto.

Si va a instalar las revisiones de Access Manager 7 2005Q4 en un sistema Solaris, se recomienda que utilice la opción -G. Por ejemplo:

```
# patchadd -G AM7_patch_dir
```

Del mismo modo, si Access Manager se ha instalado en la zona global, la opción -G es necesaria para ejecutar el comando patchrm. Por ejemplo:

```
# patchrm -G 120954-07
```

Instrucciones de instalación de revisiones para los sistemas Linux

Antes de instalar la revisión de Linux, asegúrese de que ha hecho una copia de seguridad de los archivos enumerados en "Consideraciones previas a la instalación" en la página 13.

El comando installpatch instala una revisión en sistema Linux independiente. Por ejemplo:

```
# ./installpatch
```

La secuencia de comandos postpatch imprime mensajes similares a los mensajes del sistema Solaris. Sin embargo, el procedimiento para deshacer una revisión en un sistema Linux es diferente al de un sistema Solaris. No existe ninguna secuencia de comandos genérica para deshacer una revisión de Linux. Si se ha instalado anteriormente una versión inferior de la revisión, puede reinstalar esa versión y, a continuación, seguir las instrucciones posteriores a la aplicación de las revisiones para reimplementar las aplicaciones de Access Manager ejecutando la secuencia de comandos amconfig.

Tras ejecutar la secuencia de comandos amconfig, ejecute la secuencia de comandos updateschema.sh (revisión 5 y posteriores) para cargar los archivos XML y LDIF. La secuencia de comandos updateschema.sh está disponible tras la instalación de la revisión 7 en el directorio *patch-home-directory*/120956-07/scripts .

Tras ejecutar las secuencias de comandos amconfig y updateschema.sh , reinicie el contenedor web de Access Manager.

Si la revisión se ha instalado en la versión Access Manager 7 2005Q4 RTM, y desea eliminarla y restablecer el sistema al estado de RTM, debe reinstalar los bits de RTM de Access Manager mediante la secuencia de comandos reinstallRTM. La secuencia de comandos utiliza la ruta en la que se han almacenado los RPM de RTM de Access Manager e instala los RPM de RTM sobre los RPM a los que se les ha aplicado la revisión. Por ejemplo:

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

Tras ejecutar la secuencia de comandos `reinstallRTM`, vuelva a implementar las aplicaciones de Access Manager ejecutando la secuencia de comandos `amconfig` y reinicie el contenedor web.

Consulte también "Consideraciones posteriores a la instalación" en la página 21 para obtener más información.

Instrucciones de instalación de revisiones para los sistemas Windows

Entre los requisitos para instalar la revisión de Windows se encuentran:

- Debe estar instalado Access Manager 7 2005Q4 en el sistema Windows. Para obtener más información sobre la instalación, consulte la *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .
- Para ejecutar las secuencias de comandos de las revisiones, es necesario disponer de ActivePerl 5.8 (o posterior) en el sistema Windows.

Instalación de la revisión de Windows

Antes de instalar la revisión de Windows, asegúrese de que ha hecho una copia de seguridad de los archivos enumerados en "Consideraciones previas a la instalación" en la página 13.

En la ruta de entrada del directorio base a las secuencias de comandos de revisión, utilice una barra diagonal (`/`). Por ejemplo: `c:/sun`

Para instalar la revisión de Windows:

1. Inicie una sesión en el sistema Windows como miembro del grupo de administradores.
2. Cree un directorio para descargar y descomprimir el archivo de revisión de Windows. Por ejemplo: `AM7p7`
3. Descargue y descomprima el archivo `124296-07.zip` en el directorio indicado en el paso anterior.
4. Detenga todos los servicios de Java ES 2005Q4.
5. Ejecute la secuencia de comandos `AM7p7\scripts\prepatch.pl`.
6. Ejecute `AM7p7\124296-07.exe` para instalar la revisión.
7. Ejecute la secuencia de comandos `AM7p7\scripts\postpatch.pl`.
8. Reinicie los servicios de Java ES 2005Q4.
9. Vuelva a implementar las aplicaciones de Access Manager. Consulte "Consideraciones posteriores a la instalación" en la página 21 para obtener más información.
10. Ejecute la secuencia de comandos `AM7p7\scripts\updateschema.pl` para actualizar el esquema de servicios de Directory Server. La secuencia de comandos valida sus entradas y, a continuación, carga los archivos. La secuencia de comandos también escribe el siguiente archivo de registro:

javaes-install-directory\AccessManager\AM70Patch-upgrade-schema- *timestamp*

11. Reinicie los servicios de Java ES 2005Q4.

Cómo deshacer la revisión de Windows

Para deshacer la revisión de Windows:

1. Inicie una sesión en el sistema Windows como miembro del grupo de administradores.
2. Ejecute el archivo `Uninstall_124296-07.bat`.
3. Ejecute la secuencia de comandos `AM7p7\scripts\postbackout.pl`.
4. Vuelva a implementar las aplicaciones de Access Manager.
5. Reinicie los servicios de Java ES 2005Q4.

Nota: si deshace la revisión, los cambios de esquema agregados por la secuencia de comandos `AM7p7\scripts\updateschema.pl` no se eliminan de Directory Server. Sin embargo, no es necesario eliminar esos cambios manualmente porque no afectarán a la funcionalidad ni a la facilidad de uso de Access Manager una vez eliminada la revisión.

Instrucciones de instalación de revisiones para los sistemas HP-UX

Para instalar o eliminar la revisión HP-UX, utilice los comandos `swinstall` y `swremove`. Por ejemplo, para instalar la revisión en un sistema independiente:

```
# swinstall /var/spool/patch/126371-07
```

O bien, para eliminar la revisión de un sistema independiente:

```
# swremove 126371-07
```

Para obtener información sobre los comandos `swinstall` y `swremove` , consulte las páginas de comando man `swinstall` y `swremove` .

Tras instalar o eliminar la revisión, debe volver a implementar las aplicaciones de Access Manager, tal y como se describe en la sección “Consideraciones posteriores a la instalación” en la página 21.

Tras volver a implementar las aplicaciones de Access Manager, ejecute la secuencia de comandos `updateschema.sh` (revisión 5 y revisiones posteriores) para cargar los archivos XML y LDIF. La secuencia de comandos `updateschema.sh` está disponible tras la instalación de la revisión 7 en el directorio *patch-home-directory*`/120956-07/scripts` . Tras ejecutar las secuencias de comandos `amconfig` y `updateschema.sh` , reinicie el contenedor web de Access Manager.

Nota: si elimina la revisión, los cambios realizados en el esquema agregados por la secuencia de comandos `updateschema.sh` no se eliminan de Directory Server. Sin embargo, no es necesario

eliminar estos cambios de esquema manualmente, pues la funcionalidad y la facilidad de uso de Access Manager no se verán afectadas una vez que se haya eliminado la revisión.

Para obtener más información sobre la implementación de Access Manager en los sistemas HP-UX, consulte *Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX*.

Consideraciones posteriores a la instalación

Entre las consideraciones posteriores a la instalación de la revisión de Access Manager 7 2005Q4, se incluyen:

- "CR# 6254355: las revisiones de Access Manager no implementan las aplicaciones de Access Manager en las secuencias de comandos posteriores a la aplicación de las revisiones." en la página 21
- "CR# 6436409: reimplementación de los archivos WAR de autenticación distribuida y SDK de cliente." en la página 24

CR# 6254355: las revisiones de Access Manager no implementan las aplicaciones de Access Manager en las secuencias de comandos posteriores a la aplicación de las revisiones.

Es posible que el programa de instalación de revisiones no conserve algunos de los archivos WAR personalizados y los sustituya por versiones no personalizadas. Para ayudarle a identificar y, a continuación, actualizar manualmente el contenido personalizado de un archivo WAR, tenga en cuenta el siguiente procedimiento.

En los siguientes ejemplos, *AccessManager-base* es el directorio base de instalación. El directorio base de instalación predeterminado es `/opt` en los sistemas Solaris y `/opt/sun` en los sistemas Linux.

En los sistemas Windows, *AccessManager-base* es *javaes-install-directory*`\AccessManager`. Por ejemplo: `C:\Program Files\Sun\AccessManager`

Los archivos WAR en los que se aplica la revisión son:

- `console.war`
- `password.war`
- `services.war`

Estos archivos se encuentran en *AccessManager-base*`/SUNWam` en los sistemas Solaris y *AccessManager-base*`/identity` en los sistemas Linux.

En los sistemas Windows: los archivos WAR en los que se aplica la revisión se ubican en *AccessManager-base*`\`.

Entre el contenido modificable de un archivo WAR, se incluye:

- Archivos de propiedades:
  - Sistemas Solaris: *AccessManager-base*/SUNWam/locale/*.properties
  - Sistemas Linux: *AccessManager-base*/identity/locale/*.properties
  - Sistemas Windows: *AccessManager-base*\locale*.properties
- Descriptores de bibliotecas de etiquetas:
  - Sistemas Solaris: *AccessManager-base*/SUNWam/web-src/applications/WEB-INF/*.tld
  - Sistemas Linux: *AccessManager-base*/identity/web-src/applications/WEB-INF/*.tld
  - Sistemas Windows: *AccessManager-base*\web-src\applications\WEB-INF*.tld
- El archivo web.xml y los archivos utilizados para crearlo (WEB-INF/web.xml y WEB-INF/*.xml)
- Archivos específicos de la aplicación: archivos JSP (*.jsp), archivos de imagen (*.gif), hojas de estilo, y archivos de colores de fondo, tamaños de fuente (*.css), etc.

Para asegurarse de que se conserven todos los cambios personalizados, siga estos pasos. Antes de realizar cambios en un archivo, realice siempre antes una copia de seguridad del mismo.

1. Instale la revisión.
2. Expanda los archivos WAR en un directorio temporal. Por ejemplo, con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

   ```
   # cd temporary-directory
   # jar -xvf /opt/SUNWam/console.war
   # jar -xvf /opt/SUNWam/services.war
   # jar -xvf /opt/SUNWam/password.war
   ```

3. Compruebe los archivos expandidos para ver si el programa de instalación de revisiones ha realizado algún cambio en los archivos personalizados y agregue manualmente los cambios personalizados originales a aquéllos que han sufrido modificaciones en el directorio temporal. No es necesario rehacer los cambios para los archivos que se encuentran en el directorio *AccessManager-base*/web-src/ , pero que no se han incluido en los archivos WAR a los que se ha aplicado la revisión.
4. Actualice los archivos WAR con los archivos modificados. Por ejemplo, con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

   Por ejemplo, para los pasos 2-4:

   ```
   # mkdir /tmp/war.tmp
   # cd /tmp/war.tmp
   # jar -xvf /opt/SUNWam/services.war
   ```

```
# vi index.html
# jar -uvf /opt/SUNWam/services.war index.html
```

5. Reutilice el archivo de configuración silenciosa (`amsilent`) generado por la revisión o cree uno nuevo basado en el archivo de plantilla `amsamplesilent` y, a continuación, establezca las variables de configuración adecuadas en el archivo, incluidas:
   - `DEPLOY_LEVEL=21`
   - `DIRECTORY_MODE=5`
   - Las contraseñas de `DS_DIRMGRPASSWD`, `ADMINPASSWD` y `AMLDAPUSERPASSWD`
   - Las variables del contenedor Web de Access Manager

   En los sistemas Windows, reutilice el archivo de configuración silenciosa (`amsilent`) generado por la secuencia de comandos `postpatch.pl` y asegúrese de que los valores de *AccessManager-base*`\setup\AMConfigurator.properties-tmp` son válidos. A continuación cambie el nombre de este archivo a *AccessManager-base* `\setup\AMConfigurator.properties`.

   Para obtener más información sobre las variables del contenedor Web, consulte el archivo `amsamplesilent` en el directorio `/opt/SUNWam/bin` en los sistemas Solaris o en el directorio `/opt/sun/identity/bin` en los sistemas Linux.

   En los sistemas Windows, el archivo de configuración es *AccessManager-base*`\setup\AMConfigurator.properties`.
6. Ejecute la secuencia de comandos `amconfig` como se muestra a continuación. Antes de ejecutar `amconfig`, deben estar en ejecución Directory Server y el contenedor Web de Access Manager. Por ejemplo, para ejecutar `amconfig` en un sistema Solaris con Access Manager instalado en el directorio base de instalación predeterminado:

   ```
   # cd /opt/SUNWam/bin
   # ./amconfig -s /opt/SUNWam/amsilent
   ```
7. Después de ejecutar `amconfig`, reinicie los procesos de Access Manager. Por ejemplo:

   ```
   # cd /opt/SUNWam/bin
   # ./amserver stop
   # ./amserver start
   ```
8. Asegúrese de que todos los archivos JSP personalizados se encuentren en los subdirectorios adecuados en el directorio *AccessManager-base*`/SUNWam/web-src/` en los sistemas Solaris o *AccessManager-base* `/identity/web-src/` en los sistemas Linux, y de que haya realizado una copia de seguridad de todos los archivos personalizados.

   En los sistemas Windows, los archivos se encuentran en *AccessManager-base*`\web-src\` .
9. Reinicie el contenedor Web de Access Manager.

Para obtener más información acerca de la ejecución de la secuencia de comandos `amconfig`, consulte el Capítulo 1, "Access Manager 7 2005Q4 Configuration Scripts" de *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6436409: reimplementación de los archivos WAR de autenticación distribuida y SDK de cliente.

Si utiliza la autenticación distribuida o el SDK de cliente, vuelva a crear e implementar los archivos WAR de autenticación distribuida y de SDK de cliente después de instalar la revisión. Para obtener información, consulte los siguientes documentos:

- Creación del archivo WAR de autenticación distribuida: *Technical Note: Using Access Manager Distributed Authentication*
- Creación del archivo WAR de SDK de cliente: "Installing the Client SDK" de *Sun Java System Access Manager 7 2005Q4 Developer's Guide*
- Implementación del archivo WAR de SDK de cliente: "To Deploy amclientwebapps.war" de *Sun Java System Access Manager 7 2005Q4 Developer's Guide*

Revisión 6 de Access Manager 7 2005Q4

La revisión 6 de Access Manager 7 (versión 06) soluciona diversos problemas, como se indica en el archivo README (LÉAME) incluido con la revisión. La revisión 6 también incluye las siguientes nuevas funciones, problemas y actualizaciones de documentación.

Nuevas funciones de la revisión 6

- "Access Manager es compatible con el método JDK 1.5 `HttpURLConnection setReadTimeout`" en la página 25
- "Access Manager SDK conmuta por error a la instancia principal de Directory Server una vez que el servidor principal vuelve a estar activo." en la página 25
- "Las diferentes instancias de Access Manager se registran en varios archivos." en la página 26
- "Access Manager 7 permite varios dominios de cookies." en la página 27
- "El complemento posterior a la autenticación de Microsoft IIS 6.0 admite SharePoint Server" en la página 27
- "Access Manager es compatible con Internet Explorer 7" en la página 28

Problemas conocidos y limitaciones de la revisión 6

- "CR# 6379325: el acceso a la consola durante una conmutación por error de una sesión genera una excepción de puntero nulo" en la página 28
- "CR# 6508103: en Windows, al hacer clic en Ayuda en la consola de administración, se devuelve un error de aplicación" en la página 28
- "CR# 6564877: la instalación de la revisión de Access Manager 7 sobrescribe los archivos de SAML v2" en la página 29

Nota – Antes de instalar la revisión 6, se recomienda que actualice o revise los siguientes componentes:

- Si está utilizando Sun Java System Web Server 6.1 SP5 o anterior, actualice a Web Server 6.1 SP7, que puede descargar desde este sitio:

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  Siga el proceso de actualización que se describe en "Modernización" de *Notas de la versión de Sun Java System Web Server 6.1 SP8*.
- Descargue e instale la última revisión de seguridad para NSS, JSS y NSPR en SunSolve Online: `http://sunsolve.sun.com`.
  - Plataformas Solaris 8 SPARC: 119209
  - Plataformas Solaris 8 x86: 119210
  - Plataformas Solaris 9 SPARC: 119211
  - Plataformas Solaris 9 x86: 119212
  - Plataformas Solaris 10 SPARC: 119213
  - Plataformas Solaris 10 x86 y AMD64: 119214
  - Sistemas Windows: 124392
  - Sistemas HP-UX: 124379

Access Manager es compatible con el método JDK 1.5 `HttpURLConnection setReadTimeout`

Para admitir el método `setReadTimeout`, el archivo`AMConfig.properties` cuenta con la siguiente nueva propiedad para que establezca el valor de tiempo de espera de lectura:

```
com.sun.identity.url.readTimeout
```

Si el contenedor web está utilizando JDK 1.5, establezca esta propiedad en un valor adecuado para que se agote el tiempo de espera de las conexiones y evitar así la presencia de demasiadas conexiones `HttpURLConnections` abiertas, lo que podría provocar que el servidor se bloquease. El valor predeterminado es de 30.000 milisegundos (30 segundos).

El método `setReadTimeout` se omitirá si `com.sun.identity.url.readTimeout` no está presente en el archivo `AMConfig.properties` o si se ha establecido en una cadena vacía.

Access Manager SDK conmuta por error a la instancia principal de Directory Server una vez que el servidor principal vuelve a estar activo.

Si Sun Java System Directory Server se ha configurado para la repetición de varias réplicas principales (MMR), Access Manager SDK conmutará ahora por error a la instancia principal de Directory Server después de que el servidor principal deje de funcionar y vuelva a estar activo a continuación. Anteriormente, Access Manager SDK seguía accediendo a la instancia secundaria de Directory Server una vez que el servidor principal volvía a estar activo.

Para admitir este nuevo comportamiento, Access Manager incluye la siguiente nueva propiedad en el archivo `AMConfig.properties`:

```
com.sun.am.ldap.fallback.sleep.minutes
```

Esta propiedad establece el tiempo en minutos que la instancia secundaria de Directory Server permanece inactiva antes de que conmute por error al servidor principal una vez que éste vuelve a estar activo. El valor predeterminado es de 15 minutos.

La propiedad `com.sun.am.ldap.fallback.sleep.minutes` está oculta. Para establecer esta propiedad en un valor distinto del predeterminado (15 minutos), agréguela de forma explícita al archivo `AMConfig.properties`. Por ejemplo, establezca el valor en 7 minutos:

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

Para que el nuevo valor se aplique, reinicie el contenedor web de Access Manager.

Las diferentes instancias de Access Manager se registran en varios archivos.

Las diversas instancias de Access Manager que se ejecutan en el mismo host pueden registrarse ahora en distintos archivos de registro ubicados en diferentes subdirectorios. Para ello, establezca la siguiente nueva propiedad en el archivo `AMConfig.properties`:

```
com.sun.identity.log.logSubdir
```

A menos que cambie el directorio de registro predeterminado en la consola de administración, los directorios de registro predeterminados son:

- Sistemas Solaris: `/var/opt/SUNWam/logs`
- Sistemas Linux y HP-UX: `/var/opt/sun/identity/logs`
- Sistemas Windows: `C:\Sun\JavaES5\identity\logs`

La primera instancia de Access Manager siempre se registra en el directorio de registro predeterminado. Para especificar subdirectorios de registro diferentes para las instancias adicionales de Access Manager, establezca la propiedad `com.sun.identity.log.logSubdir` en el archivo `AMConfig.properties` para cada instancia de Access Manager adicional.

Por ejemplo, si tiene tres instancias, `am-instance-1`, `am-instance-2` y `am-instance-3`, que se ejecutan en el mismo servidor host de Solaris, establezca la propiedad de la siguiente forma:

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

La propiedad `com.sun.identity.log.logSubdir` está oculta. Debe agregar de forma explícita esta propiedad al archivo `AMConfig.properties` según sea pertinente y reiniciar el contenedor web de Access Manager para que se apliquen los valores del subdirectorio.

Las instancias de Access Manager se registrarán a continuación en los siguientes directorios:

`/var/opt/SUNWam/logs/`*log-files-for-am-instance-1*
`/var/opt/SUNWam/logs/am-instance-2/`*log-files-for-am-instance-2*
`/var/opt/SUNWam/logs/am-instance-3/`*log-files-for-am-instance-3*

Access Manager 7 permite varios dominios de cookies.

Para admitir varios dominios de cookies, Access Manager presenta la siguiente nueva propiedad:

```
com.sun.identity.authentication.setCookieToAllDomains
```

El valor predeterminado es `true` (verdadero). Esta nueva propiedad está oculta. Para establecer el valor en `false` (falso), agregue de forma explícita esta propiedad al archivo `AMConfig.properties` y reinicie el contenedor web de Access Manager.

El complemento posterior a la autenticación de Microsoft IIS 6.0 admite SharePoint Server

El complemento de autenticación de los Servicios de Internet Information Server (IIS) 6.0 de Microsoft admite ahora Microsoft Office SharePoint Server. Un usuario puede iniciar una sesión en Access Manager con un Id. de usuario o un nombre de inicio de sesión. Sin embargo, SharePoint Server sólo acepta un nombre de inicio de sesión, lo que puede provocar problemas cuando el usuario especifique un Id. de usuario.

Para permitir el inicio de sesión en SharePoint Server, el complemento posterior a la autenticación (`ReplayPasswd.java`) utiliza ahora la siguiente nueva propiedad:

```
com.sun.am.sharepoint_login_attr_name
```

Esta nueva propiedad indica el atributo de usuario que usa SharePoint Server para la autenticación. Por ejemplo, la siguiente propiedad especifica el nombre común (`cn`) para la autenticación:

```
com.sun.am.sharepoint_login_attr_name=cn
```

El complemento posterior a la autenticación lee la propiedad `com.sun.am.sharepoint_login_attr_name` y obtiene el valor de atributo correspondiente para el usuario de Directory Server. A continuación, el complemento establece los encabezados de autorización para permitir el acceso del usuario a SharePoint Server.

Esta propiedad está oculta. Para establecer la propiedad, agréguela de forma explícita al archivo `AMConfig.properties` y, a continuación, reinicie el contenedor web de Access Manager para que se aplique el valor.

Access Manager es compatible con Internet Explorer 7

El parche 6 de Access Manager 7 2005Q4 admite ahora Microsoft Windows Internet Explorer 7.

CR# 6379325: el acceso a la consola durante una conmutación por error de una sesión genera una excepción de puntero nulo

En este escenario, varios servidores de Access Manager se implementan en el modo de conmutación por error de sesión detrás de un equilibrador de carga configurado para el enrutamiento de solicitudes persistentes basadas en cookies. El administrador de Access Manager accede a la consola de Access Manager mediante el equilibrador de carga. Cuando el administrador inicie una sesión en la consola, ésta se creará en uno de los servidores de Access Manager. Si el servidor deja de funcionar, se efectuará una conmutación por error de la sesión de la consola en otro servidor de Access Manager según lo previsto. Sin embargo, a veces, el administrador obtiene excepciones de puntero nulo intermitentes en el navegador y en el registro de errores del contenedor web.

Este problema sólo afecta a la sesión activa de la consola de Access Manager durante la conmutación por error y no al funcionamiento de los servidores de Access Manager.

Solución: para evitar que se generen excepciones de puntero nulo intermitentes:

- Para solucionar el problema de forma temporal, actualice el navegador o cierre la sesión y vuelva a iniciarla en la consola.
- Para solucionar el problema de forma permanente, implemente la consola de Access Manager en una instancia independiente de esta aplicación que no participe en la conmutación por error de la sesión.

CR# 6508103: en Windows, al hacer clic en Ayuda en la consola de administración, se devuelve un error de aplicación

En Windows 2003 Enterprise Edition con una instancia de Access Manager implementada en Sun Java System Application Server que utiliza una configuración regional distinta al inglés, al hacer clic en Ayuda en el modo de dominio de administración, la consola devuelve un error de aplicación.

Solución:

1. Copie el archivo *javaes-install-dir*`\share\lib\jhall.jar` en el directorio `%JAVA_HOME%\jre\lib\ext`,

   donde *javaes-install-dir* es el directorio de instalación de Windows.
2. Reinicie la instancia de Application Server.

CR# 6564877: la instalación de la revisión de Access Manager 7 sobrescribe los archivos de SAML v2

Si se ha instalado el complemento SAML v2, al instalar la revisión, se sobrescribirán los archivos de SAML v2 relacionados y la secuencia de comandos `postpatch` mostrará el siguiente mensaje:

```
La secuencia de comandos posterior a la aplicación de la revisión ha detectado
que el complemento SAML v2 se ha instalado en el entorno. Al ejecutar la
secuencia de configuración "amconfig" para volver a implementar las aplicaciones
de Access Manager, la secuencia de comandos volverá a crear el archivo
amserver.war y los archivos de SAML v2 relacionados se perderán. Por lo tanto,
después de ejecutar "amconfig", vuelva a crear e implementar el archivo
"amserver.war", tal y como se describe en "Sun Java System SAML v2 Plug-in for
Federation Services User's Guide".
```

Solución: después de instalar la revisión y ejecutar la secuencia de comandos `amconfig`, vuelva a crear e implementar el archivo `amserver.war` para las implementaciones de Federation Manager o Access Manager que utilicen el complemento SAML v2.

Para conocer los pasos específicos, consulte el Capítulo 2, "Installing the SAML v2 Plug-in for Federation Services" de *Sun Java System SAML v2 Plug-in for Federation Services User's Guide*.

Access Manager 7 2005Q4 revisión 5

Access Manager 7 revisión 5 (versión 05) soluciona diversos problemas, como se indica en el archivo README incluido con la revisión. La revisión 5 también incluye las siguientes nuevas funciones, problemas y actualizaciones de documentación.

Nuevas funciones de la revisión 5

- "Compatibilidad con los sistemas HP-UX" en la página 31
- "Compatibilidad con sistemas de Microsoft Windows" en la página 31
- "Nueva secuencia de comandos `updateschema.sh` para cargar archivos LDIF y XML" en la página 32
- "Compatibilidad con valores de tiempo de espera inactivo de sesión de aplicaciones específicas " en la página 33
- "CDC Servlet puede implementarse en un servidor de la IU de autenticación distribuida" en la página 34
- "Se puede especificar un dominio cuando el servlet de CDC redirige a la URL de inicio de sesión de Access Manager" en la página 34
- "El certificado de autenticación puede utilizar un valor UPN para asignar un perfil de usuario. " en la página 35
- "El proceso de cierre de la sesión posterior a la autenticación se produce en un entorno de varios servidores." en la página 35
- "SAML es compatible con una nueva SPI de identificador de nombres." en la página 35

- "Nuevas propiedades de configuración para la supervisión de sitios" en la página 35
- "El usuario ya no tiene que autenticarse dos veces en la cadena de autenticación." en la página 36
- "Cambios en las secuencias de comandos de ajuste del rendimiento" en la página 36
- "Autenticación básica en el agente de directivas de IIS 6.0" en la página 40

Problemas conocidos y limitaciones de la revisión 5

- "CR# 6567746: en los sistemas HP-UX, la revisión 5 de Access Manager informa de un valor incorrecto de "errorCode" si se supera el recuento de reintentos de introducción de la contraseña" en la página 41
- "CR# 6527663: el valor predeterminado de la propiedad `com.sun.identity.log.resolveHostName` debe ser `false` en lugar de `true`" en la página 41
- "CR# 6527528: la eliminación de la revisión deja los archivos XML con la contraseña `amldapuser` en texto sin formato" en la página 42
- "CR# 6527516: el servidor completo en WebLogic necesita archivos JAR JAX-RPC 1.0 para comunicarse con el SDK de cliente" en la página 42
- "CR # 6523499: el archivo `amsilent` de la revisión 5 puede ser leído por todos los usuarios en los sistemas Linux" en la página 43
- "CR# 6520326: la aplicación de la revisión 5 a una segunda instancia de Access Manager en un servidor sobrescribe `serverconfig.xml` en la primera instancia" en la página 43
- "CR# 6520016: la instalación sólo de SDK de la revisión 5 sobrescribe los archivos MAKE de ejemplos" en la página 44
- "CR#6515502: el complemento de depósito LDAPv3 no siempre administra correctamente el atributo de búsqueda de alias" en la página 44
- "CR# 6515383: la autenticación distribuida y el agente J2EE no funcionan en el mismo contenedor web" en la página 44
- "CR# 6508103: la ayuda en línea devuelve un error de aplicación con Application Server en los sistemas Windows" en la página 45
- "CR# 6507383 and CR# 6507377: la autenticación distribuida necesita el parámetro de URL `goto` explícito" en la página 45
- "CR# 6402167: LDAP JDK 4.18 causa problemas en el cliente LDAP/Directory Server" en la página 45
- "CR# 6352135: los archivos del servidor de la IU de autenticación distribuida se instalan en una ubicación incorrecta" en la página 45
- "CR# 6513653: problema con la configuración de la propiedad `com.iplanet.am.session.purgedelay` " en la página 47

Problemas de internacionalización (g11n)

- "CR# 6522720: la búsqueda en la ayuda en línea de la consola no funciona con caracteres de varios bytes en los sistemas Windows y HP-UX" en la página 46
- "CR# 6524251: los caracteres de varios bytes en los mensajes de salida están distorsionados durante la configuración de Access Manager en los sistemas Windows" en la página 46

- "CR# 6526940: las claves de propiedad aparecen en lugar del texto del mensaje durante la instalación de la revisión 5 en idiomas diferentes del inglés en los sistemas Windows" en la página 46

Actualizaciones de la documentación

- "Access Manager no puede pasar del modo tradicional al modo de dominio (6508473)" en la página 104
- "Información acerca de la deshabilitación de búsquedas persistentes (6486927)" en la página 104
- "Información sobre privilegios admitidos y no admitidos de Access Manager (2143066)" en la página 105
- "Información sobre encaminamiento de solicitudes persistentes basadas en cookies (6476922)" en la página 106
- "Información sobre configuración de inicio de sesión único (SSO) de Windows Desktop para Windows 2003 (6487361)" en la página 107
- "Información sobre los pasos para configurar las contraseñas del servidor de la IU de autenticación distribuida (6510859)" en la página 107
- "La ayuda en línea "To create new site name" ("Para crear un nuevo nombre de sitio") necesita más información (2144543)" en la página 108
- "El parámetro de configuración de contraseña de administrador es `ADMIN_PASSWD` en los sistemas Windows (6470793)" en la página 108

Compatibilidad con los sistemas HP-UX

La revisión **126371** cuenta con compatibilidad con los sistemas HP-UX. Para obtener más información, consulte:

- "Instrucciones de instalación de revisiones para los sistemas HP-UX" en la página 20
- "Consideraciones posteriores a la instalación" en la página 21

Para obtener información sobre la instalación en sistemas HP-UX, consulte *Guía de instalación de Sun Java Enterprise System 2005Q4 para UNIX*.

Compatibilidad con sistemas de Microsoft Windows

La revisión **124296** proporciona compatibilidad con los sistemas Windows. Para obtener más información, consulte:

- "Instrucciones de instalación de revisiones para los sistemas Windows" en la página 19
- "Consideraciones posteriores a la instalación" en la página 21
- "Las secuencias de comandos de ajuste están disponibles para sistemas Windows" en la página 39

Para obtener información sobre la instalación en sistemas Windows, consulte la *Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows* .

Nueva secuencia de comandos `updateschema.sh` para cargar archivos LDIF y XML

La revisión 5 (y posteriores) incluye la secuencia de comandos `updateschema.sh`, que carga los archivos siguientes para actualizar el esquema de servicio de Directory Server:

- `AddLDAPFilterCondition.xml`
- `amPolicyConfig_mod_ldfc.xml`
- `accountLockoutData.xml`
- `accountLockout.ldif`
- `idRepoServiceAddAttrSchemaRequest_Cache.xml`
- `wsf1.1_upgrade.xml`
- `amAuth_mod.xml`
- `amAuthCert_mod.xml`

En versiones de revisiones anteriores de Access Manager, se le solicitó que cargara estos archivos manualmente.

Para ejecutar la secuencia de comandos `updateschema.sh`:

1. Inicie una sesión como superusuario o conviértase en uno (`root`).
2. Cambie al directorio de la revisión.
3. Ejecute la secuencia de comandos. Por ejemplo, en sistemas Solaris:

   ```
   # cd /120954-07
   # ./updateschema.sh
   ```

   En sistemas Windows, la secuencia de comandos es `updateschema.pl`.
4. Cuando la secuencia de comandos se lo solicite, introduzca estos elementos:
   - Nombre de host y número de puerto de Directory Server
   - DN y contraseña de usuario administrativo de Directory Server
   - DN y contraseña `amadmin`
5. La secuencia de comandos valida sus entradas y, a continuación, carga los archivos. La secuencia de comandos también escribe el siguiente archivo de registro:
   - Sistemas Solaris: `/var/opt/SUMWam/logs/AM70Patch.upgrade.schema.` *timestamp*
   - Sistemas Linux: `/var/opt/sun/identity/logs/AM70Patch.upgrade.schema.` *timestamp*
6. Una vez finalizada la secuencia de comandos, reinicie el contenedor web de Access Manager.

Nota si elimina la revisión 5, los cambios realizados en el esquema agregados por la secuencia de comandos `updateschema.sh` no se eliminan de Directory Server. Sin embargo, no es necesario eliminar esos cambios manualmente porque no afectarán a la funcionalidad ni a la facilidad de uso de Access Manager una vez eliminada la revisión.

Compatibilidad con valores de tiempo de espera inactivo de sesión de aplicaciones específicas

La revisión 5 permite que distintas aplicaciones tengan valores de tiempo de espera inactivo de diferentes sesiones. En una empresa, puede que algunas aplicaciones necesiten valores de tiempo de espera inactivo de sesión inferiores al tiempo de espera inactivo de sesión especificado en el servicio de sesión. Por ejemplo, suponga que ha establecido el valor de tiempo de espera de inactividad de sesión en el servicio de sesión en 30 minutos, pero una aplicación de RR.HH. debe agotar el tiempo de espera si un usuario ha estado inactivo durante más de 10 minutos.

Los requisitos para utilizar esta función son:

- Los agentes que protegen la aplicación deben configurarse de tal manera que cumplan las decisiones de la directiva URL de Access Manager.
- Deben configurarse los agentes para ejecutarse en modo de caché de decisiones de directiva automática. Consulte las siguientes propiedades:
  - Para agentes web: `com.sun.am.policy.am.fetch_from_root_resource`
  - Para agentes de J2EE: `com.sun.identity.policy.client.cacheMode`
- El archivo `AMConfig.properties` de Access Manager debe especificar un orden de evaluación de componentes de directiva tal que esa condición se evalúe al final. Consulte la siguiente propiedad:

  `com.sun.identity.policy.Policy.policy_evaluation_weights`
- El acceso a la aplicación permitido por el agente basado en una decisión almacenada en caché local será desconocido para la condición sobre Access Manager. Por tanto, el tiempo de espera inactivo de la aplicación actual estará entre el tiempo de espera inactivo de la aplicación y el tiempo de espera inactivo de la aplicación menos la duración de la caché del agente.

Para usar esta función:

- Agregue una condición de esquema de autenticación a las directivas que protegen la aplicación que necesita el tiempo de espera inactivo de sesión específico de la aplicación.
- Especifique el nombre de la aplicación y el valor de tiempo de espera en la condición de esquema de autenticación.
- Utilice el mismo nombre de la aplicación y valor de tiempo de espera en todas las directivas aplicables a los recursos de la aplicación.
- Especifique el valor de tiempo de espera en minutos. Si el valor es 0 o superior al valor de tiempo de espera inactivo de la sesión especificado en el servicio de sesión, se ignorará el valor y se aplicará el tiempo de espera del servicio de sesión.

Por ejemplo, considere una directiva `http://host.sample.com/hr/*`, con esta condición de esquema de autenticación:

- Esquema de autenticación: LDAP

- Nombre de aplicación: RR.HH.
- Valor de tiempo de espera: 10

Si hay varias directivas definidas para proteger los recursos de la aplicación de RR.HH., debe agregar la condición a todas ellas.

Si un usuario intenta acceder, en una sesión distinta, a la aplicación de RR.HH. protegida por el agente de Access Manager, se le solicitará su autenticación para el esquema LDAP (si aún no se ha autenticado).

Si ya se ha autenticado para el esquema LDAP, podrá acceder sólo si el tiempo es inferior a 10 minutos desde la última autenticación o si el tiempo es inferior a 10 minutos desde el último acceso del usuario a la aplicación de RR.HH. De lo contrario, el usuario debe autenticarse de nuevo para el esquema LDAP para acceder a la aplicación.

CDC Servlet puede implementarse en un servidor de la IU de autenticación distribuida

CDC Servlet puede coexistir con un servidor de la IU de autenticación distribuida en DMZ para habilitar el inicio de sesión único de dominio cruzado (CDSSO). El servidor de Access Manager puede implementarse detrás de un servidor de seguridad, y CDC Servlet se encarga de todo el acceso a Access Manager para habilitar CDSSO en el servidor de la IU de autenticación distribuida. Para habilitar CDSSO, consulte la documentación del agente de directivas específica y realice los siguientes pasos adicionales:

- Modifique el archivo `AMAgent.properties` del agente para que señale a CDC Servlet en la autenticación distribuida (cliente). Por ejemplo, para agentes web, cambie la siguiente propiedad:

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- Defina las directivas como le convenga en Access Manager para los recursos que el agente deba proteger. Por ejemplo, si el agente está en `host.example.com:80` , defina una directiva para el recurso como `http://host.example.com:80/*` .

Se puede especificar un dominio cuando el servlet de CDC redirige a la URL de inicio de sesión de Access Manager

Ahora puede especificar un nombre de dominio en el servlet de CDC para que, cuando se produzca el redireccionamiento a la URL de inicio de sesión de Access Manager, el nombre de dominio esté incluido y el usuario pueda iniciar una sesión en el dominio específico. Por ejemplo:

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

El certificado de autenticación puede utilizar un valor UPN para asignar un perfil de usuario.

Previamente, el certificado de autenticación utilizó sólo el componente `dn` en `subjectDN` para asignar un perfil de usuario. Access Manager ahora permite el valor de nombre principal de usuario (UPN) en `SubjectAltNameExt` para la asignación de perfiles.

El proceso de cierre de la sesión posterior a la autenticación se produce en un entorno de varios servidores.

Este proceso ahora se produce cuando un usuario finaliza una sesión en un servidor distinto de aquel en el que inició la sesión originalmente en un entorno de varios servidores, con o sin la opción de migración tras error de sesión configurada.

SAML es compatible con una nueva SPI de identificador de nombres.

SAML ahora es compatible con una nueva interfaz de proveedor de servicios (SPI) de identificador de nombres, para que un sitio pueda personalizar el identificador de nombres en la afirmación SAML. Un sitio puede implementar la nueva interfaz `NameIdentifierMapper` para asignar una cuenta de usuario a un identificador de nombres en el asunto de una afirmación SAML.

Nuevas propiedades de configuración para la supervisión de sitios

La función de supervisión de sitios de Access Manager incluye las siguientes nuevas propiedades que permiten especificar el comportamiento de la comprobación de estado del sitio.

Propiedad	Descripción
`com.sun.identity.urlchecker.invalidate.interval`	Intervalo de tiempo en milisegundos para reconocer un sitio que no responde o está inactivo. Valor predeterminado: 70.000 milisegundos (70 segundos).
`com.sun.identity.urlchecker.sleep.interval`	Intervalo de tiempo en milisegundos que debería permanecer suspendida la comprobación de estado del sitio. Valor predeterminado: 30.000 milisegundos (30 segundos).

`com.sun.identity.urlchecker.targeturl`	Distintas URL de destino para la comprobación del estado del proceso de Access Manager. Valor predeterminado: `"/amserver/namingservice"`.

La revisión no agrega estas propiedades al archivo `AMConfig.properties` . Para utilizar las nuevas propiedades con valores diferentes a los predeterminados:

1. Agregue las propiedades y sus valores al archivo `AMConfig.properties` . Si utiliza agentes de directivas, agregue estas propiedades al archivo `AMAgents.properties`.
2. Reinicie el contenedor web de Access Manager para que se apliquen los valores.

El usuario ya no tiene que autenticarse dos veces en la cadena de autenticación.

Considere el siguiente escenario. Un sitio configura una cadena de autenticación con tres módulos LDAP. Todos los módulos se configuran en `SUFFICIENT` y las opciones `iplanet-am-auth-shared-state-enabled` y `iplanet-am-auth-store-shared-state-enabled` se configuran en `true`. Por ejemplo:

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

La revisión 5 agrega la nueva opción `iplanet-am-auth-shared-state-behavior-pattern` a las opciones de módulo con dos valores posibles: `tryFirstPass` (default) and `useFirstPass`.

Para evitar que un usuario tenga que introducir dos veces el Id. de usuario y la contraseña para autenticarse (tal como se describe en el escenario anterior), configure la nueva opción en `useFirstPass` para todos los módulos de la cadena. Anteriormente, se le solicitó a un usuario que existía sólo en la tercera instancia LDAP que introdujera un Id. de usuario y contraseña dos veces para autenticarse.

Cambios en las secuencias de comandos de ajuste del rendimiento

La revisión 5 incluye estos cambios en las secuencias de comandos de ajuste del rendimiento:

- "Las secuencias de comandos de ajuste son compatibles con un archivo de contraseñas" en la página 37

- "La secuencia de comandos de ajuste elimina los ACI innecesarios de Directory Server" en la página 37
- "Las secuencias de comandos de ajuste pueden ajustar el contenedor web del servidor de la IU de autenticación distribuida" en la página 38
- "La secuencia de comandos única `amtune-os` ajusta los SO Solaris y Linux" en la página 39
- "Las secuencias de comandos de ajuste se ejecutan hasta su finalización en una zona local de Solaris 10" en la página 39
- "Las secuencias de comandos de ajuste están disponibles para sistemas Windows" en la página 39
- "Consideraciones de ajuste para servidores Sun Fire T1000 y T2000" en la página 40

Consulte también "CR# 6527663: el valor predeterminado de la propiedad `com.sun.identity.log.resolveHostName` debe ser `false` en lugar de `true`" en la página 41.

Las secuencias de comandos de ajuste son compatibles con un archivo de contraseñas

La revisión 5 permite especificar contraseñas para las secuencias de comandos de ajuste en un archivo de texto. Anteriormente, podía introducir contraseñas sólo como argumento de la línea de comandos, opción que podía producir problemas de seguridad. Para utilizar un archivo de contraseñas, configure las variables siguientes como desee en el archivo:

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

Por ejemplo, para ajustar Application Server 8:

```
# ./amtune-as8 password-file
```

donde *password-file* contiene `AS_ADMIN_PASSWORD` definido en la contraseña de administrador de Application Server 8.

Las secuencias de comandos de ajuste utilizan la opción `-j` *password-file* cuando llaman a las utilidades `ldapmodify`, `ldapsearch`, `db2index` y `dsconf` de Directory Server.

La secuencia de comandos de ajuste elimina los ACI innecesarios de Directory Server

Si Access Manager 7 2005Q4 está instalado en modo de dominio, se utilizan privilegios de delegación para determinar los permisos de acceso y, por tanto, no son necesarios algunos ACI de Directory Server. La revisión 5 de Access Manager 7 2005Q4 permite eliminar los ACI innecesarios ejecutando la secuencia de comandos `amtune-prepareDSTuner.` Esta secuencia de comandos lee una lista de ACI del archivo `remacis.ldif` y, a continuación, llama a la utilidad `ldapmodify` para eliminarlos.

Puede ejecutar la secuencia de comandos `amtune-prepareDSTuner` para eliminar los ACI innecesarios de los sistemas Solaris, Linux, HP-UX y Windows. Para obtener más información, incluido cómo ejecutar la secuencia de comandos, consulte la *Technical Note: Sun Java System Access Manager ACI Guide* .

Las secuencias de comandos de ajuste pueden ajustar el contenedor web del servidor de la IU de autenticación distribuida

Después de implementar el servidor de la IU de autenticación distribuida en un contenedor web, puede ajustar el contenedor web ejecutando las secuencias de comandos de ajuste de Access Manager. Las siguientes secuencias de comandos de ajuste definen la máquina virtual de Java (Java Virtual Machine) y otras opciones de ajuste para el contenedor web correspondiente:

TABLA 2 Secuencias de comandos de ajuste del contenedor web de Access Manager

Contenedor web	Secuencia de comandos de ajuste
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

Para ajustar un contenedor web para un servidor de la IU de autenticación distribuida:

1. Como el servidor de Access Manager no está instalado en el sistema en el que está implementado el servidor de la IU de autenticación distribuida, copie la secuencia de comandos de ajuste del contenedor web adecuado (mostrada en la tabla anterior), el archivo de configuración `amtune-env` y la secuencia de comandos `amtune-utils` de una instalación de servidor de Access Manager. Si desea ajustar el sistema operativo Solaris o Linux, copie también la secuencia de comandos `amtune-os`.
2. Edite los parámetros en el archivo de configuración `amtune-env` para especificar el contenedor web y las opciones de ajuste. Para ejecutar la secuencia de comandos en modo REVIEW, defina `AMTUNE_MODE=REVIEW` en el archivo `amtune-env` .
3. Ejecute la secuencia de comandos de ajuste del contenedor web en modo REVIEW. En modo REVIEW, la secuencia de comandos sugiere cambios de ajuste basados en los valores del archivo `amtune-env` pero no realiza ningún cambio en la implementación.
4. Revise las recomendaciones de ajuste en el archivo de registro de depuración. Si es necesario, haga cambios en el archivo `amtune-env` basados en esta ejecución.
5. Para hacer cambios de ajuste, defina `AMTUNE_MODE=CHANGE` en el archivo `amtune-env`.
6. Ejecute la secuencia de comandos de ajuste en modo CHANGE para realizar los cambios de ajuste en la implementación.

Para obtener más información acerca de la ejecución de la secuencia de comandos de ajuste para ajustar un contenedor web de Access Manager, consulte el Capítulo 2, "Access Manager Tuning Scripts" de *Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide*.

La secuencia de comandos única `amtune-os` ajusta los SO Solaris y Linux

La revisión 5 incluye una secuencia de comandos única `amtune-os` para ajustar ambos SO. La secuencia de comandos determina el tipo de SO del comando `uname -s`. Anteriormente, Access Manager proporcionaba secuencias de comandos `amtune-os` individuales para ajustar cada SO.

Las secuencias de comandos de ajuste se ejecutan hasta su finalización en una zona local de Solaris 10

Si Access Manager está instalado en una zona local de Solaris 10, todas las secuencias de comandos de ajuste excepto `amtune-os` pueden ejecutarse en la zona local. En una zona local, la secuencia de comandos `amtune-os` muestra un mensaje de advertencia pero no ajusta el SO. La secuencia de comandos continúa ejecutando otras secuencias de comandos de ajuste que usted haya solicitado. Anteriormente, en una zona local, la secuencia de comandos `amtune-os` se cancelaría, además de no ejecutarse las posteriores secuencias de comandos de ajuste solicitadas.

En una zona global de Solaris 10, la secuencia de comandos `amtune` llama a `amtune-os` para ajustar el SO además de otras secuencias de comandos que haya solicitado.

Las secuencias de comandos de ajuste están disponibles para sistemas Windows

La revisión 5 incluye secuencias de comandos de ajuste para sistemas Windows. La ejecución de secuencias de comandos de ajuste en un sistema Windows es similar a la ejecución de las secuencias de comandos en un sistema Solaris o Linux, con estas diferencias:

- Las secuencias de comandos de Windows se escriben en Perl y necesitan Active Perl 5.8 para ejecutarse.
- Si desea ajustar Directory Server, tras ejecutar la secuencia de comandos `amtune-prepareDSTuner.pl` , debe copiar los archivos `amtune-utils.pl`, `amtune-directory.pl`, `remacis.ldif` y `amtune-samplepassordfile` en el sistema de Directory Server, ya que la secuencia de comandos no puede comprimir estos archivos.
- No se encuentra disponible ninguna secuencia de comandos para ajustar el sistema operativo Windows.
- No se proporciona compatibilidad para zonas.
- Antes de ejecutar una secuencia de comandos, debe definir el parámetro `$BASEDIR` en el directorio de instalación de Access Manager en el archivo `amtune-env.pl`.

Consideraciones de ajuste para servidores Sun Fire T1000 y T2000

Si Access Manager está instalado en un servidor Sun Fire T1000 o T2000, las secuencias de comandos de ajuste de la revisión 5 para Web Server 6.1 y Application Server 8 definen el parámetro `JVM GC ParallelGCThreads` en 8:

```
-XX:ParallelGCThreads=8
```

Este parámetro reduce el número de subprocesos de liberación de recursos, que podría ser innecesariamente elevado en un sistema compatible con 32 subprocesos. Sin embargo, puede incrementar el valor a 16 o incluso 20 para una CPU virtual de 32 como, por ejemplo, un servidor Sun Fire T1000 o T2000, si minimiza todas las actividades de liberación de recursos.

Además, para los sistemas Solaris SPARC con un procesador CMT con tecnología CoolThreads, se recomienda que agregue la siguiente propiedad al final del archivo `/etc/opt/SUNWam/config/AMConfig.properties`:

```
com.sun.am.concurrencyRate=value
```

El *value* predeterminado es 16, pero puede definir esta propiedad en un valor inferior, dependiendo del número de núcleos del servidor Sun Fire T1000 o T2000.

Autenticación básica en el agente de directivas de IIS 6.0

Para habilitar la autenticación básica en Microsoft Internet Information Services (IIS) 6.0, el agente de directivas debe obtener el nombre de usuario y la contraseña. La revisión 5 incluye las siguientes nuevas clases que habilitan esta funcionalidad utilizando cifrado DES de la contraseña del usuario.

- `DESGenKey.java` genera una clave exclusiva utilizada para cifrar y descifrar la contraseña del usuario.
- `ReplayPasswd.java` lee el valor de clave de cifrado de la propiedad `com.sun.am.replaypasswd.key` en el archivo `AMConfig.properties`, cifra la contraseña y la asigna a la propiedad de la sesión `sunIdentityUserPassword`.

Para utilizar la autenticación básica en IIS 6.0, debe realizar estos pasos tanto en el servidor de Access Manager como en el agente de directivas de IIS 6.0.

En el servidor de Access Manager:

1. Ejecute `DESGenKey.java` para generar una clave de cifrado exclusiva para el cifrado y el descifrado de la contraseña. En los sistemas Solaris, el archivo `DESGenKey.java` se ubica en el directorio `com/sun/identity/common` , incluido en `am_sdk.jar` en el directorio `/opt/SUNWam/lib.` Por ejemplo, el siguiente comando genera una clave de cifrado:

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```

2. Asigne un valor de clave de cifrado del Paso 1 a la propiedad `com.sun.am.replaypasswd.key` del archivo `AMConfig.properties`.
3. Implemente `ReplayPasswd.java` como un complemento posterior a la autenticación. Utilice el nombre de clase completo cuando configure el complemento: `com.sun.identity.authentication.spi.ReplayPasswd` .

En el agente de directivas de IIS 6.0:

1. Asigne el valor de clave de cifrado del servidor a la propiedad `com.sun.am.replaypasswd.key` del archivo `AMAgent.properties` . Tanto el servidor de Access Manager como el agente de directivas de IIS 6.0 deben utilizar la misma clave de cifrado.
2. Habilite la autenticación básica en IIS 6.0 Manager.

El agente de directivas de IIS 6.0 lee la contraseña cifrada de la respuesta de sesión, descifra la contraseña de la propiedad `com.sun.am.replaypasswd.key` y configura los encabezados de autenticación para que la autenticación básica comience a funcionar.

Para obtener más información acerca del agente de directivas de IIS 6.0, consulte *Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0* .

CR# 6567746: en los sistemas HP-UX, la revisión 5 de Access Manager informa de un valor incorrecto de "errorCode" si se supera el recuento de reintentos de introducción de la contraseña

Cuando se bloquea una cuenta de usuario, la revisión 5 de Access Manager 7 2005Q4 en los sistemas HP-UX informa de `errorCode = null` en lugar de `errorCode = 107` si se supera el recuento de reintentos de introducción de la contraseña.

Solución. Ninguna.

CR# 6527663: el valor predeterminado de la propiedad `com.sun.identity.log.resolveHostName` debe ser `false` en lugar de `true`

Antes de ejecutar la secuencia de comandos de ajuste `amtune-identity`, se recomienda que agregue la siguiente propiedad definida en `false` al archivo `AMConfig.properties`:

```
com.sun.identity.log.resolveHostName=false
```

Un valor `false` minimiza el impacto de resolver nombres de host y, por tanto, puede mejorar el rendimiento. Sin embargo, si desea que el nombre de sistema anfitrión del equipo cliente se imprima en el registro `amAuthentication.access`, establezca el valor en `true`.

CR# 6527528: la eliminación de la revisión deja los archivos XML con la contraseña `amldapuser` en texto sin formato

Si elimina la revisión 5 de una instalación de servidor completo de Access Manager, los archivos `amAuthLDAP.xml` y `amPolicyConfig.xml` contienen la contraseña `amldapuser` en texto sin formato. Estos archivos se encuentran en el siguiente directorio, dependiendo de la plataforma:

- Sistemas Solaris: `/etc/opt/SUNWam/config/xml`
- Sistemas Linux y HP-UX: `/etc/opt/sun/identity/config/xml`

Solución: Edite los archivos `amAuthLDAP.xml` y `amPolicyConfig.xml` y elimine la contraseña de texto sin formato.

CR# 6527516: el servidor completo en WebLogic necesita archivos JAR JAX-RPC 1.0 para comunicarse con el SDK de cliente

En las revisiones de Access Manager 7 2005Q4, la secuencia de comandos de configuración de Access Manager para BEA WebLogic Server (`amwl81config`) agrega los archivos JAR JAX-RPC 1.1 a la `classpath` de la instancia WebLogic. Aunque esta modificación es beneficiosa para productos como Sun Java System Portal Server, una instalación de servidor completo (`DEPLOY_LEVEL=1`) implementado en WebLogic Server no puede comunicarse con una instalación de SDK de cliente y, posteriormente, se producirán excepciones.

Si el servidor de Access Manager 7 2005Q4 está instalado en BEA WebLogic Server, la `CLASSPATH` de la secuencia de comandos `startWebLogic.sh` debe configurarse en la ubicación de los archivos JAR JAX-RPC 1.0 para comunicarse con el SDK de cliente de Access Manager.

Solución: antes de aplicar la revisión de Access Manager, establezca la ruta de clase, `CLASSPATH`, en la secuencia de comandos `startWebLogic.sh` para que la instancia de WebLogic Server utilice los archivos JAR de JAX-RPC 1.0 en lugar de los archivos JAR de JAX-RPC 1.1:

1. En el servidor de Access Manager, inicie una sesión como superusuario o conviértase en uno (`root`).
2. Edite la secuencia de comandos `startWebLogic.sh` y sustituya la `CLASSPATH` para utilizar los archivos JAR JAX-RPC 1.0. Por ejemplo:

Valor actual:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

Valor nuevo:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

donde *AccessManager-base* es el directorio base de instalación. El valor predeterminado es `/opt` en los sistemas Solaris y `/opt/sun` en los sistemas Linux y HP-UX. *AccessManager-package-dir* es el directorio de paquetes de Access Manager.

5. Reinicie la instancia de WebLogic Server.

CR # 6523499: el archivo `amsilent` de la revisión 5 puede ser leído por todos los usuarios en los sistemas Linux

En los sistemas Linux. la secuencia de comandos `postpatch` crea el archivo `/opt/sun/identity/amsilent` con los permisos 644, opción que permite que todos los usuarios tengan acceso de lectura.

Solución: Una vez ejecutada la secuencia de comandos `installpatch`, cambie los permisos del archivo `amsilent` para que sólo el propietario tenga acceso de lectura y escritura. Por ejemplo:

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326: la aplicación de la revisión 5 a una segunda instancia de Access Manager en un servidor sobrescribe `serverconfig.xml` en la primera instancia

En este escenario de implementación, dos instancias de Access Manager se instalan en el mismo servidor del sistema anfitrión, con cada instancia en una instancia de contenedor web distinto. A continuación siga estos pasos:

1. Aplique la revisión 5.
2. Modifique el archivo `amsilent` y vuelva a implementar la primera instancia de Access Manager.
3. Modifique el archivo `amsilent` de nuevo para la segunda instancia de Access Manager y, a continuación, vuelva a implementar esa instancia.

Si `NEW_INSTANCE=false` en el archivo `amsilent`, el archivo `serverconfig.xml` de la primera instancia de Access Manager se sobrescribe con la información de la segunda instancia de Access Manager. Falla un reinicio posterior de la primera instancia de Access Manager. El archivo `serverconfig.xml` se encuentra en el siguiente directorio dependiendo de su plataforma:

- Sistemas Solaris: `/etc/opt/SUNWam/config`
- Sistemas Linux: `/etc/opt/sun/identity/config`

Solución: Si implementa la segunda instancia de Access Manager, establezca `NEW_INSTANCE=true` en el archivo `amsilent`. El archivo `serverconfig.xml` de la segunda instancia de Access Manager se actualiza con la información correcta, y el archivo `serverconfig.xml` de la primera instancia de Access Manager no se sobrescribe.

CR# 6520016: la instalación sólo de SDK de la revisión 5 sobrescribe los archivos MAKE de ejemplos

La aplicación de la revisión 5 a un equipo sólo de SDK sobrescribe los archivos MAKE de ejemplos.

Solución: La aplicación de la revisión 5 a un equipo sólo de SDK no necesita una reconfiguración; sin embargo, si desea utilizar los archivos MAKE de ejemplos, siga estos pasos para actualizar los archivos LDIF y de propiedades (es decir, realice un intercambio de etiquetas) de los archivos MAKE de ejemplos:

1. Ejecute la secuencia de comandos `amconfig` con `DEPLOY_LEVEL=14` para desinstalar SDK y desconfigurar el contenedor web.
2. Ejecute la secuencia de comandos `amconfig` con `DEPLOY_LEVEL=4` para reinstalar SDK y volver a configurar el contenedor web.

CR#6515502: el complemento de depósito LDAPv3 no siempre administra correctamente el atributo de búsqueda de alias

Para la mayoría de las búsquedas, este problema se ha solucionado. Sin embargo, tenga cuidado cuando configure el atributo de búsqueda de alias. El valor de los atributos de búsqueda de alias debe ser exclusivo en una organización. Si se configura más de un atributo de búsqueda de alias, es posible que una entrada del almacén de datos coincida con un atributo y que otra entrada coincida con el otro atributo. En esta situación, el servidor de Access Manager emite el siguiente error:

```
An internal authentication error has occurred. Contact your system administrator.
```

Solución: Ninguna

CR# 6515383: la autenticación distribuida y el agente J2EE no funcionan en el mismo contenedor web

Un servidor de la IU de autenticación distribuida y un agente de directivas J2EE no funcionan si están instalados en el mismo contenedor web.

Solución: Cree una instancia de un segundo contenedor web e implemente el servidor de la IU de autenticación distribuida y el agente de directivas J2EE en distintas instancias del contenedor.

CR# 6508103: la ayuda en línea devuelve un error de aplicación con Application Server en los sistemas Windows

Si implementa Access Manager en Sun Java System Application Server en un sistema Windows, al hacer clic en la Ayuda del panel izquierdo de la pantalla de ayuda de la consola en modo de dominio aparece un error de aplicación.

Solución: copie el archivo *javaes-install-dir*`\share\lib\jhall.jar` en el directorio `JAVA_HOME\jre\lib\ext` y, a continuación, reinicie Application Server.

CR# 6507383 and CR# 6507377: la autenticación distribuida necesita el parámetro de URL `goto` explícito

Si no se especifica un parámetro de URL `goto` específico, un servidor de la IU de autenticación distribuida intenta redirigir al parámetro `goto` en una URL satisfactoria especificada en Access Manager. Este redireccionamiento puede fallar por estos motivos:

- La URL es relativa y no se encuentra disponible ninguna página correspondiente en el servidor de la IU de autenticación distribuida
- La URL es absoluta y el navegador no puede alcanzar la URL.

Solución: Especifique siempre un parámetro de URL `goto` explícito para un servidor de la IU de autenticación distribuida.

CR# 6402167: LDAP JDK 4.18 causa problemas en el cliente LDAP/Directory Server

Access Manager 7 2005Q4 fue lanzado con LDAP JDK 4.18 como parte de la revisión de Java ES 2005Q4, que causó una serie de problemas de conexión de Access Manager y Directory Server.

Solución: Aplique una de las siguientes revisiones de Java Development Kit de Sun Java System LDAP:

- SO Solaris, SPARC y plataformas x86: 119725-04
- SO Linux: 120834-02

Las revisiones están disponibles en SunSolve Online: `http://sunsolve.sun.com`.

CR# 6352135: los archivos del servidor de la IU de autenticación distribuida se instalan en una ubicación incorrecta

En los sistemas Solaris, el programa de instalación de Java ES instala el servidor de la IU de autenticación distribuida `Makefile.distAuthUI`, `README.distAuthUI` y los archivos `amauthdistui.war` en una ubicación incorrecta: `/opt/SUNComm/SUNWam`.

Solución: Copie estos archivos en la ubicación correcta: `/opt/SUNWam`.

Nota: cualquier problema de servidor de la IU de autenticación distribuida solucionado en una revisión se reflejará en el archivo `/opt/SUNComm/SUNWam/amauthdistui.war` , así que siempre que aplique una revisión en el servidor de Access Manager y, a continuación, genere de nuevo e implemente el archivo WAR, también debe copiar estos archivos en el directorio `/opt/SUNWam`.

CR# 6522720: la búsqueda en la ayuda en línea de la consola no funciona con caracteres de varios bytes en los sistemas Windows y HP-UX

Si se instala Access Manager en un idioma que utilice caracteres de varios bytes (como, por ejemplo, japonés) en un sistema Windows o HP-UX, no funcionará la búsqueda en la ayuda en línea de la consola con palabras clave introducidas utilizando caracteres de varios bytes.

Solución: Ninguna

Actualización de la revisión 6: la revisión 6 de Access Manager 7 2005Q4 soluciona este problema en los sistemas Windows. Sin embargo, el problema aún persiste en los sistemas HP-UX.

CR# 6524251: los caracteres de varios bytes en los mensajes de salida están distorsionados durante la configuración de Access Manager en los sistemas Windows

Si se instala Access Manager en un idioma que utilice caracteres de varios bytes (como, por ejemplo, japonés o chino) en un sistema Windows, durante la configuración de Access Manager, las palabras se distorsionan en los mensajes de salida en la ventana de terminal.

Solución: Ninguna, pero este problema no afecta a la configuración.

CR# 6526940: las claves de propiedad aparecen en lugar del texto del mensaje durante la instalación de la revisión 5 en idiomas diferentes del inglés en los sistemas Windows

Si instala la revisión 5 (124296-05) en un idioma distinto del inglés en un sistema Windows, algunas cadenas de los paneles de instalación aparecen como claves de propiedad en lugar del texto del mensaje. Ejemplos de claves de propiedad son `PRODUCT_NAME`, `JES_Patch_FinishPanel_Text1` y `JES_Patch_FinishPanel_Text2`.

Solución: Ninguna

CR# 6513653: problema con la configuración de la propiedad com.iplanet.am.session.purgedelay

La secuencia de comandos `amtune` de Access Manager configura la propiedad `com.iplanet.am.session.purgedelay` en 1, para permitir el mayor número posible de sesiones de Access Manager. Esta propiedad especifica el número de minutos de retraso de la operación de sesión de purga. Sin embargo, para clientes como, por ejemplo, Sun Java System Portal Server, no es suficiente un valor de 1.

Solución: Restablezca la propiedad `com.iplanet.am.session.purgedelay` una vez ejecutada la secuencia de comandos `amtune`:

1. En el archivo `AMConfig.properties`, defina la propiedad en el nuevo valor. Por ejemplo:

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. Reinicie el contenedor web de Access Manager para que se aplique el nuevo valor.

Revisión 4 de Access Manager 7 2005Q4

La revisión 4 de Access Manager 7 2005Q4 (versión 04) soluciona los siguientes problemas:

- CR# 6463796: la deshabilitación del servicio `iPlanetAMClientDetection` para `genericHTML` evita el acceso a cualquier página HTML de Access Manager
- CR# 6463779: la autenticación distribuida `amProfile_Client` y el servidor de Access Manager `amProfile_Server` incluyen una gran cantidad de excepciones inofensivas
- CR# 6463730: la vulnerabilidad de secuencias de comandos en varios sitios (XSS) existe con los parámetros `goto` y `gx-charset`
- CR# 6435889: el método `Session.getSession` falla porque `RestrictedTokenContext` no está configurado

Problemas conocidos y limitaciones de la revisión 4

- "CR# 6470055: mejora del rendimiento del servidor de la IU de autenticación distribuida" en la página 47
- "CR# 6455079: el servicio de restablecimiento de contraseña informa de errores de notificación cuando se modifica una contraseña" en la página 48

CR# 6470055: mejora del rendimiento del servidor de la IU de autenticación distribuida

Para mejorar el rendimiento en la lectura, búsqueda y comparación de atributos de usuario para un usuario de servidor de la IU de autenticación distribuida, siga estos pasos:

1. En el archivo `Makefile.distAuthUI`, cambie el nombre de usuario de la aplicación de `anonymous` a otro usuario. Por ejemplo:

```
APPLICATION_USERNAME=user1
```

2. En Directory Server, agregue el nuevo usuario (`user1` en el ejemplo) y ACI para permitir la lectura, búsqueda y comparación de atributos de usuario. El siguiente ejemplo agrega el nuevo ACI:

```
dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
changetype:modify add:aci
aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
(targetattr = *")(version 3.0;
acl "SunAM client data access to a Distributed Auth App User";
allow (read, search, compare)
userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
```

CR# 6455079: el servicio de restablecimiento de contraseña informa de errores de notificación cuando se modifica una contraseña

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`. Por 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 dirección del remitente para que incluya el nombre de dominio completo del servidor host en el archivo `amPasswordResetModuleMsgs.properties` :

1. cambie la etiqueta de dirección del remitente. Por ejemplo:

```
fromAddress.label=<Identity-Server@amhost.example.com>
```

2. Cambie la propiedad `lockOutEmailFrom` para garantizar que las notificaciones de bloqueo utilicen la dirección del remitente correcta. Por ejemplo:

```
lockOutEmailFrom=<Identity-Server@amhost.example.com>
```

   El archivo `amPasswordResetModuleMsgs.properties` está en el directorio *AccessManager-base*`/SUNWam/locale` en los sistemas Solaris y en el directorio *AccessManager-base*`/identity/locale` en los sistemas Linux.

   AccessManager-base es el directorio base de instalación. El directorio base de instalación predeterminado es `/opt` en los sistemas Solaris y `/opt/sun` en los sistemas Linux.

Revisión 3 de Access Manager 7 2005Q4

La revisión 3 de Access Manager 7 (versión 03) soluciona diversos problemas, como se indica en el archivo README (LÉAME) incluido con la revisión. Además, incluye también las siguientes nuevas funciones y problemas conocidos:

Nuevas funciones de la revisión 3

- "Nuevas propiedades de configuración para la supervisión de sitios" en la página 50
- "Compatibilidad con Liberty Identity Web Services Framework (ID-WSF) 1.1" en la página 51

Problemas conocidos y limitaciones de la revisión 3

- "CR# 6463779: el registro `amProfile_Client` de autenticación distribuida y el registro `amProfile_Server` del servidor de Access Manager incluyen una gran cantidad de excepciones inofensivas." en la página 52
- "CR# 6460974: el usuario predeterminado de la aplicación de autenticación distribuida no debe ser `amadmin`." en la página 52
- "CR# 6460576: no hay ningún vínculo para el Servicio de usuario en Rol filtrado en la ayuda en línea de la consola." en la página 53
- "CR# 6460085: el servidor de WebSphere no está accesible después de ejecutar `reinstallRTM` y reimplementar las aplicaciones Web." en la página 53
- "CR# 6455757: el marcador `sunISManagerOrganization` debe agregarse a una organización antes de realizar una actualización." en la página 54
- "CR# 6454489: la actualización de la revisión 2 de Access Manager 7 2005Q4 provoca un error en la ficha Sesiones actuales de la consola." en la página 54
- "CR# 6452320: se generan excepciones al utilizar el sondeo con el SDK de cliente." en la página 55
- "CR# 6442905: el `SSOToken` del usuario autenticado puede mostrarse de forma accidental en sitios poco fiables." en la página 55
- "CR# 6441918: propiedades de tiempo de espera e intervalo de supervisión de sitios. " en la página 56
- "CR# 6440697: la autenticación distribuida debe ejecutarse con un usuario que no sea amadmin." en la página 56
- "CR# 6440695: servidores de la IU de autenticación distribuida con equilibrador de carga." en la página 56
- "CR# 6440651: la repetición de las cookies requiere la propiedad `com.sun.identity.session.resetLBCookie`" en la página 57
- "CR# 6440648: la propiedad `com.iplanet.am.lbcookie.name` asume el valor predeterminado `amlbcookie`." en la página 57
- "CR# 6440641: la propiedad `com.iplanet.am.lbcookie.value` se ha dejado de utilizar." en la página 57
- "CR# 6429610: no se puede crear el token SSO al utilizar ID-FF SSO." en la página 57

- "CR# 6389564: se producen consultas sucesivas recurrentes sobre los miembros del rol del usuario en el almacén de datos LDAP v3 durante el inicio de sesión de Access Manager." en la página 58
- "CR# 6385185: el módulo de autenticación debe poder anular la URL "goto" y especificar una URL diferente." en la página 58
- "CR# 6385184: redirección desde un módulo de autenticación personalizado cuando el token SSO no presenta aún un estado válido. " en la página 58
- "CR# 6324056: la federación falla al utilizar un perfil de artefacto." en la página 59

Nuevas propiedades de configuración para la supervisión de sitios

La función de supervisión de sitios de Access Manager incluye las siguientes nuevas propiedades:

Propiedad	Descripción
`com.sun.identity.sitemonitor.interval`	Intervalo de tiempo en milisegundos para la supervisión de sitios. La función de supervisión de sitios comprueba la disponibilidad de cada sitio en el intervalo de tiempo especificado. Valor predeterminado: 60.000 milisegundos (1 minuto).
`com.sun.identity.sitemonitor.timeout`	Tiempo de espera en milisegundos para la comprobación de disponibilidad del sitio. La función de supervisión de sitios espera durante el valor de tiempo de espera especificado la recepción de una respuesta del sitio. Valor predeterminado: 5.000 milisegundos (5 segundos).

La revisión no agrega estas propiedades al archivo `AMConfig.properties` . Para utilizar las nuevas propiedades con valores diferentes a los predeterminados:

1. Agregue las propiedades y sus valores al archivo `AMConfig.properties` en el siguiente directorio en función de su plataforma:
   - Sistemas Solaris: `/etc/opt/SUNWam/config`
   - Sistemas Linux: `/etc/opt/sun/identity/config`

   Si utiliza agentes de directivas, agregue estas propiedades al archivo `AMAgents.properties`.
2. Reinicie el contenedor Web de Access Manager para que se apliquen los valores.

Implementación personalizada. Además, la clase `com.sun.identity.sitemonitor.SiteStatusCheck` le permite personalizar su propia implementación para la comprobación de la disponibilidad del sitio mediante la siguiente interfaz:

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

Cada clase de implementación debe utilizar el método `doCheckSiteStatus`.

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Compatibilidad con Liberty Identity Web Services Framework (ID-WSF) 1.1

La versión predeterminada de ID-WSF de la revisión 3 de Access Manager 7 es WSF1.1. No es necesario realizar ninguna configuración independiente para activar ID-WSF, aunque las muestras deben utilizar los nuevos mecanismos de seguridad. Los nuevos mecanismos de seguridad de ID-WSF1.1 son:

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Nueva propiedad para la compatibilidad con Liberty ID-WSF

La propiedad `com.sun.identity.liberty.wsf.version` determina la estructura de Liberty ID-WSF cuando ésta no puede determinar a partir del mensaje entrante o la oferta de recursos si Access Manager está actuando como WSC. Los valores pueden ser 1.0 ó 1.1. El valor predeterminado es 1.1.

Nota: la instalación de la revisión no agrega la propiedad `com.sun.identity.liberty.wsf.version` al archivo `AMConfig.properties` (CR# 6458184). Para utilizar esta nueva propiedad, agréguela al archivo `AMConfig.properties` con el valor adecuado después de instalar la revisión y, a continuación, reinicie el contenedor Web de Access Manager.

Una vez instalada la revisión 3 de Access Manager 7, ejecute el siguiente comando para cargar los cambios de esquema, el cual aparece con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

Al efectuar el registro, la función de detección de ID-WSF podrá utilizar estos nuevos mecanismos de seguridad. Además, los WSC detectarán automáticamente la versión que se

utilizará al establecer comunicación con los WSP. Al realizar la configuración para ID-WSF1.1, consulte los archivos Readme (Léame) para obtener la muestra1 de Liberty ID-FF y las muestras de ID-WSF incluidas con el producto.

CR# 6463779: el registro `amProfile_Client` de autenticación distribuida y el registro `amProfile_Server` del servidor de Access Manager incluyen una gran cantidad de excepciones inofensivas.

Las solicitudes al servidor de Access Manager mediante la IU de autenticación distribuida genera excepciones en el registro `distAuth/amProfile_Client` y en el registro `debug/amProfile_Server` del servidor de Access Manager. Tras numerosas sesiones, el tamaño del registro `amProfile_Client` y del registro `amProfile_Server` del servidor de Access Manager puede aumentar hasta varios gigabytes. Estas excepciones en los registros no provocan ninguna pérdida de funcionalidad, pero pueden causar una falsa alarma a los usuarios además de que los registros pueden ocupar potencialmente una gran parte del espacio del disco duro.

Solución. Ejecute los trabajos `cron` que convertirán el contenido de los archivos de registro en nulo. Por ejemplo:

- En un equipo cliente de la IU de autenticación distribuida, ejecute "`cat /dev/null > distAuth/amProfile_Client`" cada varias horas en función del volumen de tráfico.
- En el servidor de Access Manager, ejecute "`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`" cada varios días en lugar de cada varias horas.

CR# 6460974: el usuario predeterminado de la aplicación de autenticación distribuida no debe ser `amadmin`.

Si va a implementar un servidor de la IU de autenticación distribuida, el administrador de autenticación distribuida no debe ser `amadmin`. El usuario predeterminado de la aplicación de autenticación distribuida es `amadmin` en el archivo `Makefile.distAuthUI` y, posteriormente, en el archivo `AMConfig.properties` una vez implementado el archivo `distAuth.war` en el cliente. El usuario `amadmin` tiene un `AppSSOToken` que caduca una vez agotado el tiempo de sesión de `amadmin`, lo que puede provocar un ERROR GRAVE en el archivo de registro `amSecurity` (ubicado de forma predeterminada en el directorio `/tmp/distAuth`).

Solución. Especifique `UrlAccessAgent` como usuario de la aplicación de autenticación distribuida. Por ejemplo:

Antes de implementar el archivo `distAuth.war` en el contenedor Web, cambie los siguientes parámetros en el archivo `Makefile.distAuthUI` :

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password or amldapuser-password
```

o

Después de implementar el archivo `distAuth.war` en el contenedor Web, cambie las siguientes propiedades en el archivo `AMConfig.properties` para cada servidor de Access Manager:

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password or amldapuser-password
```

Consulte también "CR# 6440697: la autenticación distribuida debe ejecutarse con un usuario que no sea amadmin." en la página 56.

CR# 6460576: no hay ningún vínculo para el Servicio de usuario en Rol filtrado en la ayuda en línea de la consola.

La ayuda en línea de la consola de Access Manager no incluye ningún vínculo para el Servicio de usuario en Rol filtrado. En la ayuda en línea, vaya a Contenido, Rol filtrado y "Para crear un rol filtrado". Desplácese a la siguiente página y, en función del tipo de identidad seleccionado, aparecerá una lista de servicios, pero no estará disponible ningún vínculo de Servicio de usuario.

Solución. Ninguna.

CR# 6460085: el servidor de WebSphere no está accesible después de ejecutar `reinstallRTM` y reimplementar las aplicaciones Web.

Después de aplicar la revisión 3 de Access Manager 7 para una implementación `DEPLOY_LEVEL=1` en IBM WebSphere Application Server 5.1.1.6 en Red Hat Linux AS 3.0 Update 4, la secuencia de comandos `reinstallRTM` se ejecuta para restablecer los RPM de RTM. A continuación, se reimplementan las aplicaciones Web después de editar el archivo `amsilent` generado por la secuencia de comandos `reinstallRTM`. WebSphere se reinicia mediante las secuencias de comandos `stopServer.sh` y `startServer.sh`. Sin embargo, al acceder a la página de inicio de sesión, WebSphere muestra un error 500, relacionado con el filtro `amlcontroller`.

Este problema se produce debido a que el nuevo archivo `server.xml` generado por la secuencia de comandos `reinstallRTM` está dañado.

Solución. El archivo `server.xml` del que la secuencia de comandos `amconfig` ha realizado una copia de seguridad aún es válido. Utilice esta copia anterior de la siguiente forma:

1. Pare el servidor.
2. Sustituya el archivo `server.xml` dañado por la copia de seguridad realizada por la secuencia de comandos `amconfig`.

   El archivo `server.xml` del que la secuencia de comandos `amconfig` ha realizado una copia de seguridad presenta el nombre `server.xml-orig-` *pid*, donde *pid* es el Id. de proceso de la secuencia de comandos `amwas51config`. El archivo se encuentra en el siguiente directorio:

WebSphere-home-directory/config/cells/*WebSphere-cell*/nodes/*WebSphere-node*/servers/*server-name*

3. Reinicie el servidor.

CR# 6455757: el marcador sunISManagerOrganization debe agregarse a una organización antes de realizar una actualización.

Es posible que una organización de un DIT de Access Manager creada con una versión anterior a Access Manager 7 no presente la clase de objeto `sunISManagerOrganization`. Además, una organización creada con un producto diferente a Access Manager no incluirá la clase de objeto `sunISManagerOrganization` en su definición.

Solución. Antes de actualizar a Access Manager 7 2005Q4, asegúrese de que todas las organizaciones del DIT incluyan la clase de objeto `sunISManagerOrganization` en su definición. Si es necesario, agregue manualmente esta clase de objeto antes de realizar la actualización.

CR# 6454489: la actualización de la revisión 2 de Access Manager 7 2005Q4 provoca un error en la ficha Sesiones actuales de la consola.

Una actualización ha provocado el siguiente error en la ficha Sesiones actuales de la consola de Access Manager:

```
Failed to get valid Sessions from the Specified server
```

Este problema hace referencia a las implementaciones que se actualizan desde las versiones de Access Manager 6 que tienen un sufijo root con el formato `o=orgname`.

Solución. Después de instalar Manager 7 2005Q4, aplique la revisión 3 de Access Manager 7 y, a continuación, ejecute la secuencia de comandos `amupgrade` para migrar los datos de la siguiente forma:

1. Realice una copia de seguridad del DIT de Access Manager 6.
2. Ejecute la secuencia de comandos `ampre70upgrade`.
3. Instale Access Manager 7 2005Q4 con la opción Configurar más tarde.
4. Anule la implementación de las aplicaciones Web de Access Manager.
5. Implemente las aplicaciones Web de Access Manager.
6. Aplique la revisión 3 de Access Manager 7, pero no aplique los cambios de XML/LDIF. Estos cambios deben aplicarse después de ejecutar la secuencia de comandos `amupgrade` en el siguiente paso.
7. Ejecute la secuencia de comandos `amupgrade`.
8. Reimplemente las aplicaciones Web de Access Manager debido a los cambios efectuados por la revisión 3 de Access Manager 7.

9. Acceda a la consola de Access Manager.

CR# 6452320: se generan excepciones al utilizar el sondeo con el SDK de cliente.

Al implementar el SDK de cliente de Access Manager (`amclientsdk.jar`) y habilitar la función de sondeo, pueden producirse errores como los siguientes:

```
ERROR: Send Polling Error:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller thread pool's task queue is full.
```

Estos errores pueden producirse después de implementar un servidor de la IU de autenticación distribuida, los agentes de J2EE o en cualquier situación en la que se implemente el SDK de cliente de Access Manager en un equipo cliente.

Solución. Si sólo tiene varias centenas de sesiones concurrentes, agregue las siguientes propiedades y valores al archivo `AMConfig.properties` o `AMAgents.properties`:

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

Si tiene varios miles o decenas de miles de sesiones, deben establecerse los mismos valores que los de la notificación en el archivo `AMConfig.properties` de Access Manager después de ejecutar la secuencia de comandos `amtune-identity`. Por ejemplo, en un equipo con 4 GB de RAM, la secuencia de comandos `amtune-identity` de Access Manager establece los siguientes valores:

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

Establezca valores parecidos en el archivo `AMAgent.properties` o `AMConfig.properties` del cliente al implementar el servidor de la IU de autenticación distribuida o el SDK de cliente de Access Manager en un equipo cliente con 4 GB de RAM.

CR# 6442905: el `SSOToken` del usuario autenticado puede mostrarse de forma accidental en sitios poco fiables.

Un usuario autenticado de Access Manager puede mostrar de forma accidental el `SSOToken` en un sitio poco fiable haciendo clic en una URL de dicho sitio.

Solución. Cree siempre un perfil de usuario de agente exclusivo en Access Manager para todos los agentes de directivas que participen para asegurarse de que el sitio sea fiable. Además, compruebe que ninguno de los usuarios de agente exclusivos utilice la misma contraseña que la contraseña secreta compartida o la contraseña de `amldapuser`. Los agentes de directivas se autentican de forma predeterminada en el módulo de autenticación de la aplicación Access Manager como usuario `UrlAccessAgent`.

Para obtener más información sobre cómo crear un agente mediante la consola de administración de Access Manager, consulte "Agents" de *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

CR# 6441918: propiedades de tiempo de espera e intervalo de supervisión de sitios.

La función de conmutación por error de sitios de Access Manager incluye las siguientes nuevas propiedades:

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

Para obtener más información, consulte "Nuevas propiedades de configuración para la supervisión de sitios" en la página 50.

CR# 6440697: la autenticación distribuida debe ejecutarse con un usuario que no sea amadmin.

Para crear un administrador de autenticación distribuida que no sea el usuario administrativo predeterminado (`amadmin`) para la autenticación de la aplicación de autenticación distribuida, siga el siguiente procedimiento:

1. Cree un usuario LDAP para el administrador de autenticación distribuida. Por ejemplo:

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. Agregue el administrador de autenticación distribuida a la lista de usuarios especiales. Por ejemplo:

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   Agregue esta propiedad al archivo `AMConfig.properties` de todos los servidores de Access Manager para que el `AppSSOToken` del administrador de autenticación distribuida no caduque al finalizar la sesión.

CR# 6440695: servidores de la IU de autenticación distribuida con equilibrador de carga.

Si la implementación incluye un equilibrador de carga frente a varios servidores de la IU de autenticación distribuida, establezca las siguientes propiedades en el archivo `AMConfig.properties` después de implementar el archivo WAR.

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651: la repetición de las cookies requiere la propiedad com.sun.identity.session.resetLBCookie

Para que la repetición de las cookies funcione correctamente para una migración tras error de sesión de Access Manager, agregue la propiedad `com.sun.identity.session.resetLBCookie` con un valor `true` tanto para el agente de directivas como para el servidor de Access Manager. Por ejemplo:

```
com.sun.identity.session.resetLBCookie='true'
```

- Para el agente de directivas, agregue la propiedad al archivo `AMAgent.properties` .
- Para el servidor de Access Manager, agregue la propiedad al archivo `AMConfig.properties`.

Nota: esta propiedad es necesaria sólo si se ha implementado la migración tras error de sesión de Access Manager.

CR# 6440648: la propiedad com.iplanet.am.lbcookie.name asume el valor predeterminado amlbcookie.

De forma predeterminada, un agente de directivas y los servidores de Access Manager asumen el nombre de cookie de equilibrador de carga `amlbcookie`. Si cambia el nombre de la cookie en el servidor de servicios de fondo, debe utilizar el mismo nombre en el archivo `AMAgent.properties` del agente de directivas. Además, si utiliza el SDK de cliente de Access Manager, debe usar el mismo nombre de cookie utilizado por el servidor de servicios de fondo.

CR# 6440641: la propiedad com.iplanet.am.lbcookie.value se ha dejado de utilizar.

Access Manager ya no admite la propiedad `com.iplanet.am.lbcookie.value` en los servidores para personalizar la cookie del equilibrador de carga. En su lugar, Access Manager utiliza ahora el Id. de servidor, que se configura como parte del proceso de configuración de sesión, para el valor de la cookie y para el nombre que va a repetir el agente.

CR# 6429610: no se puede crear el token SSO al utilizar ID-FF SSO.

Después de configurar la muestra 1 de Liberty Identity Federation Framework (ID-FF), la federación se realiza con éxito, pero se producen errores en SSO.

Solución. Agregue el `uuid` de `dsameuser` a la propiedad `com.sun.identity.authentication.special.users` del archivo `AMConfig.properties`. En la autenticación de aplicaciones, `dsameuser` necesita un token SSO que no caduque para el servidor de Access Manager.

CR# 6389564: se producen consultas sucesivas recurrentes sobre los miembros del rol del usuario en el almacén de datos LDAP v3 durante el inicio de sesión de Access Manager.

Cuando un usuario inicia una sesión en Access Manager, se realizan varias búsquedas de LDAP recurrentes en el atributo `nsRoleDN` del usuario.

Solución. Una vez instalada la revisión 3 de Access Manager 7, ejecute el siguiente comando que aparece con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185: el módulo de autenticación debe poder anular la URL "goto" y especificar una URL diferente.

Un módulo de autenticación puede anular la URL "goto" y solicitar la redirección a una URL diferente de un sitio Web externo para obtener la validación del estado del usuario.

Para anular la URL "goto" una vez completada la autenticación, establezca la propiedad que aparece en el siguiente ejemplo en el `SSOToken`. Debe establecer esta propiedad mediante el método `onLoginSuccess` de la clase `PostProcess` que implementa `AMPostAuthProcessInterface`. Por ejemplo, *OverridingURL* es la URL que anula la URL "goto":

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184: redirección desde un módulo de autenticación personalizado cuando el token SSO no presenta aún un estado válido.

La nueva función `RedirectCallback` del módulo de autenticación personalizado permite la redirección a un sitio Web externo mediante la IU de administración para conseguir la validación de un usuario. Si la autenticación se realiza con éxito, el usuario se redirige de nuevo a la URL original del servidor de Access Manager. Entre los archivos de muestra, se incluyen:

- `LoginModuleSample.java`

- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

Para implementar esta función:

1. Cree un módulo de autenticación personalizado utilizando el archivo de muestra `LoginModuleSample.java`.
2. Cargue el módulo en el servidor de Access Manager.
3. Cree la función `RedirectCallback` en el archivo XML mediante el archivo de muestra `LoginModuleSample.xml`.
4. Para probar el módulo, utilice el archivo de muestra `testExtWebSite.jsp` del sitio Web externo.
5. Inicie sesión mediante esta URL:

   ```
   http://example.com/amserver/UI/Login?module=LoginModuleSample
   ```

El nombre de usuario y la contraseña se redirigen al sitio Web externo para la validación. Si el nombre y la contraseña son válidos, la autenticación se realiza con éxito y el usuario se redirige de nuevo a la URL original del servidor de Access Manager.

Por ejemplo, imagine una situación en la que la implementación utiliza un módulo de autenticación personalizado para acceder a un sitio de suministro/tarjetas de crédito.

1. El usuario ejecuta el proceso de autenticación o la página de inicio de sesión para el módulo de autenticación personalizado.
2. El usuario introduce las credenciales (el nombre de usuario y la contraseña) y envía una solicitud al módulo de autenticación personalizado.
3. El módulo de autenticación personalizado redirecciona al usuario a un sitio de suministro/tarjetas de créditos externo con la información de usuario necesaria junto con la solicitud.
4. Este sitio externo comprueba el estado del usuario y devuelve la solicitud con una respuesta de éxito o fallo, que se establece como parte de la solicitud devuelta.
5. El módulo de autenticación valida el usuario en función del estado devuelto en el paso 4 y devuelve el correspondiente estado al servicio de autenticación.
6. El proceso de autenticación del usuario se completa de forma satisfactoria o, por el contrario, con errores.

CR# 6324056: la federación falla al utilizar un perfil de artefacto.

Solución: Para solucionar este problema, aplique la versión más reciente de la revisión "Core Mobile Access" en función de la plataforma que utilice:

- SO Solaris en sistemas basados en SPARC: 119527
- SO Solaris en plataformas x86: 119528

- Sistemas Linux: 119529

Una vez aplicada la revisión, reinicie el contenedor Web.

Revisión 2 de Access Manager 7 2005Q4

La revisión 2 de Access Manager 7 (versión 02) soluciona diversos problemas, como se indica en el archivo README (LÉAME) incluido con la revisión. Además, incluye también las siguientes nuevas funciones y problemas conocidos:

New Features in Patch 2

- "Nuevas propiedades de las cachés de administración de usuarios, repositorio de identidades y administración de servicios" en la página 60
- "Nueva propiedad para el proveedor de servicios de federación" en la página 62
- "Compatibilidad con la condición de filtro LDAP " en la página 62

Problemas conocidos y limitaciones de la revisión 2

- "CR# 6283582: el número de fallos de inicio de sesión no se comparte entre las instancias de Access Manager." en la página 63
- "CR# 6293673: es necesario conservar la información de sesión original al enviar la notificación de tiempo de espera de sesión agotado." en la página 63
- "CR# 6244578: Access Manager debería avisar al usuario de que la compatibilidad con las cookies del explorador se ha deshabilitado o no está disponible." en la página 64
- "CR# 6236892: se muestra un marcador de imagen/texto mientras CDCServlet procesa AuthNResponse tras el inicio de sesión." en la página 64
- "CR# 6363157: la nueva propiedad deshabilita las búsquedas persistentes si son absolutamente necesarias" en la página 64
- "CR# 6385696: los IDP y SP nuevos y existentes no están visibles." en la página 65

Nuevas propiedades de las cachés de administración de usuarios, repositorio de identidades y administración de servicios

La revisión 2 incluye las siguientes nuevas propiedades para las cachés de administración de usuarios, el repositorio de identidades (IdRepo) y la administración de usuarios (SDK de Access Manager). Estas propiedades permiten habilitar y deshabilitar de forma independiente las diferentes cachés en función de los requisitos de implementación, y establecer el periodo de vida (TTL, Time To Live) de las entradas de la caché.

TABLA 3 Nuevas propiedades de las cachés de administración de usuarios, repositorio de identidades y administración de servicios

Propiedad	Descripción

TABLA 3 Nuevas propiedades de las cachés de administración de usuarios, repositorio de identidades y administración de servicios *(Continuación)*

Nuevas propiedades para habilitar y deshabilitar las cachés	
`com.iplanet.am.sdk.caching.enabled`	Propiedad global que habilita (true) o deshabilita (false) las cachés del repositorio de identidades (IdRepo), la administración de usuarios y la administración de servicios. Si se establecer como true (verdadero), o si la propiedad no está presente en el archivo `AMConfig.properties`, se habilitan las tres cachés.
Nota Las siguientes tres propiedades para habilitar o deshabilitar las cachés específicas sólo se aplican si la propiedad global anterior se establece en false (falso).	
`com.sun.identity.amsdk.cache.enabled`	Habilita (true) o deshabilita (false) únicamente la caché de administración de usuarios (Access Manager SDK).
`com.sun.identity.idm.cache.enabled`	Habilita (true) o deshabilita (false) sólo la caché del repositorio de identidades (IdRepo).
`com.sun.identity.sm.cache.enabled`	Habilita (true) o deshabilita (false) sólo la caché de administración de servicios.
Nuevas propiedades de la caché de administración de usuarios para TTL	
`com.iplanet.am.` `sdk.cache.entry.expire.enabled`	Habilita (true) o deshabilita (false) la caducidad (tal y como se define en las dos propiedades siguientes) para la caché de administración de usuarios.
`com.iplanet.am.` `sdk.cache.entry.user.expire.time`	Especifica el tiempo en minutos que las entradas de usuario de la caché de administración de usuarios seguirán siendo válidas desde su última modificación. Es decir, una vez transcurrido el periodo de tiempo especificado (después de la última modificación o lectura desde el directorio), los datos de la entrada almacenada en la caché caducarán. Las solicitudes de datos de dichas entradas deberán leerse desde el directorio.
`com.iplanet.am.` `sdk.cache.entry.default.expire.time`	Especifica el tiempo en minutos que las entradas de la caché de administración de usuarios que no son de usuario seguirán siendo válidas desde su última modificación. Es decir, una vez transcurrido el periodo de tiempo especificado (después de la última modificación o lectura desde el directorio), los datos de la entrada almacenada en la caché caducarán. Las solicitudes de datos de dichas entradas deberán leerse desde el directorio. Nuevas propiedades de la caché del repositorio de identidades para TTL

TABLA 3 Nuevas propiedades de las cachés de administración de usuarios, repositorio de identidades y administración de servicios *(Continuación)*

`com.sun.identity.idm.cache.entry.expire.enabled`	Habilita (true) o deshabilita (false) la caducidad (como se define en la siguiente propiedad) para la caché de IdRepo.
`com.sun.identity.idm.cache.entry.default.expire.time`	Especifica el tiempo en minutos que las entradas de la caché de IdRepo que no son de usuario seguirán siendo válidas desde su última modificación. Es decir, una vez transcurrido el periodo de tiempo especificado (después de la última modificación o lectura desde el repositorio), los datos de la entrada almacenada en la caché caducarán. Las nuevas solicitudes de datos de dichas entradas deberán leerse desde el repositorio.

Using the New Caching Properties

Las revisiones de Access Manager 7 2005Q4 no actualizan automáticamente las nuevas propiedades de caché en el archivo `AMConfig.properties`.

Para utilizar las nuevas propiedades de caché:

1. Con un editor de textos, agregue las propiedades y sus valores al archivo `AMConfig.properties` en el siguiente directorio en función de su plataforma:
   - Sistemas Solaris: `/etc/opt/SUNWam/config`
   - Sistemas Linux: `/etc/opt/sun/identity/config`
2. Reinicie el contenedor Web de Access Manager para que se apliquen los valores.

Nueva propiedad para el proveedor de servicios de federación

La nueva propiedad `com.sun.identity.federation.spadapter` define la clase de implementación para `com.sun.identity.federation.plugins.FederationSPAdapter` , que se utiliza para agregar el procesamiento específico de la aplicación durante el procesamiento de la federación en el proveedor de servicios.

Consulte también "CR# 6385696: los IDP y SP nuevos y existentes no están visibles." en la página 65.

Compatibilidad con la condición de filtro LDAP

Se ha agregado la compatibilidad con la condición de filtro LDAP en la revisión 2. Un administrador de directivas puede ahora especificar un filtro LDAP en la condición al definir una directiva. La directiva sólo se aplica al usuario si la entrada LDAP del usuario satisface el filtro LDAP especificado en la condición. La entrada LDAP del usuario se consulta desde el directorio especificado en el servicio de configuración de directivas.

Para registrar y utilizar la condición de filtro LDAP, ejecute los siguientes comandos una vez instalada la revisión 2 de Access Manager 7 que aparece con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

Nota sobre la revisión 5 si agregó la revisión 5 de Access Manager 7 2005Q4 y ejecutó la secuencia de comandos `updateschema.sh`, no es necesario cargar estos archivos utilizando `amadmin`. Para obtener más información consulte "Nueva secuencia de comandos `updateschema.sh` para cargar archivos LDIF y XML" en la página 32.

CR# 6283582: el número de fallos de inicio de sesión no se comparte entre las instancias de Access Manager.

Una vez instalada la revisión 2 de Access Manager 7, ejecute los siguientes comandos que aparecen con Access Manager instalado en el directorio predeterminado en los sistemas Solaris:

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

El valor predeterminado de *DirectoryServer-base* es `/var/opt/mps/serverroot` en los sistemas Solaris y `/var/opt/sun/directory-server` en los sistemas Linux.

Nota sobre la revisión 5 si agregó la revisión 5 de Access Manager 7 2005Q4 y ejecutó la secuencia de comandos `updateschema.sh`, no es necesario cargar estos archivos utilizando `amadmin`. Para obtener más información consulte "Nueva secuencia de comandos `updateschema.sh` para cargar archivos LDIF y XML" en la página 32.

CR# 6293673: es necesario conservar la información de sesión original al enviar la notificación de tiempo de espera de sesión agotado.

La nueva propiedad `com.sun.identity.session.property.doNotTrimList` del archivo `AMConfig.properties` puede contener una lista de nombres de propiedades de sesión separados por comas. Una vez agotado el tiempo de espera de una sesión, las propiedades definidas en esta lista no se recortarán, para que se pueda acceder a ellas antes de que se purgue la sesión. Por ejemplo:

`com.sun.identity.session.property.doNotTrimList=`*UserId*`,`*HostName*

CR# 6244578: Access Manager debería avisar al usuario de que la compatibilidad con las cookies del explorador se ha deshabilitado o no está disponible.

La nueva propiedad `com.sun.identity.am.cookie.check` del archivo `AMConfig.properties` indica si el servidor debe comprobar si existe compatibilidad con las cookies o si las cookies están habilitadas en el explorador. El valor `true` (verdadero) provoca que el servidor compruebe la compatibilidad con las cookies o si éstas están habilitadas en el explorador, y genera una página de error en caso de que no exista compatibilidad o no estén habilitadas. Este valor debería establecerse como "false" (falso), que es el valor predeterminado, si se espera que el servidor admita el modo sin cookies para la función de autenticación.

CR# 6236892: se muestra un marcador de imagen/texto mientras CDCServlet procesa AuthNResponse tras el inicio de sesión.

CDCServlet agrega las siguientes propiedades a `AMConfig.properties` y las lee:

- Si se ha establecido como "true" (verdadero); `com.iplanet.services.cdc.WaitImage.display` provoca que se muestre una imagen en el explorador mientras un usuario espera la página protegida, en caso de utilizar CDSSO. El valor predeterminado es false.
- `com.iplanet.services.cdc.WaitImage.name` especifica el nombre de la imagen. El valor predeterminado es `waitImage.gif`. Esta imagen se copia del directorio de `login_images`.
- `com.iplanet.services.cdc.WaitImage.width` especifica el ancho de la imagen. El valor predeterminado es 420.
- `com.iplanet.services.cdc.WaitImage.height` especifica el alto de la imagen. El valor predeterminado es 120.

CR# 6363157: la nueva propiedad deshabilita las búsquedas persistentes si son absolutamente necesarias

La nueva propiedad `com.sun.am.event.connection.disable.list` del archivo `AMConfig.properties` especifica la conexión que puede deshabilitarse. Los valores (no se distingue entre mayúsculas y minúsculas) pueden ser:

`aci` - Cambios del atributo `aci` con la búsqueda utilizando el filtro LDAP (`aci=*`)

`sm` - Cambios en el árbol de información de Access Manager (o nodo de administración de servicios), que incluye objetos con la clase de objeto de marcador `sunService` o `sunServiceComponent`. Por ejemplo, puede crear una directiva que defina privilegios de acceso a un recurso protegido o puede modificar las reglas, temas, condiciones o proveedores de respuesta de una directiva existente.

`um` - Cambios en el directorio de usuario (o nodo de administración de usuarios). Por ejemplo, puede cambiar el nombre o la dirección del usuario.

Por ejemplo, para deshabilitar las búsquedas persistentes de cambios en el árbol de información de Access Manager (o nodo de administración de servicios):

```
com.sun.am.event.connection.disable.list=sm
```

Para especificar varios valores, separe cada valor con una coma.

Precaución – Las búsquedas persistentes causan una sobrecarga en el rendimiento en Directory Server. Si cree que el hecho de eliminar parte de esta sobrecarga en el rendimiento es muy importante en un entorno de producción, puede deshabilitar una o más búsquedas persistentes utilizando la propiedad `com.sun.am.event.connection.disable.list`.

Sin embargo, antes de deshabilitar una búsqueda persistente, debe comprender las limitaciones descritas anteriormente. Se recomienda que no se modifique esta propiedad a menos que sea absolutamente necesario. Esta propiedad fue introducida principalmente para evitar la sobrecarga en Directory Server cuando se utilizan varios agentes J2EE 2.1, porque cada uno de estos agentes establece estas búsquedas persistentes. Los agentes J2EE 2.2 ya no establecen estas búsquedas persistentes, así que puede que no sea necesario utilizar esta propiedad.

Para obtener más información, consulte "Información acerca de la deshabilitación de búsquedas persistentes (6486927)" en la página 104.

CR# 6385696: los IDP y SP nuevos y existentes no están visibles.

La nueva propiedad `com.sun.identity.federation.spadapter` del archivo `AMConfig.properties` especifica la implementación predeterminada del adaptador del proveedor de servicios de federación en el que la aplicación puede obtener la información de aserciones y de respuesta. Por ejemplo:

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Revisión 1 de Access Manager 7 2005Q4

La revisión 1 de Access Manager 7 (versión 01) soluciona diversos problemas, como se indica en el archivo README (LÉAME) incluido con la revisión. Además, incluye también las siguientes nuevas funciones y problemas conocidos:

- "Creación de archivos de depuración" en la página 66
- "Compatibilidad con los roles y los roles filtrados en el complemento LDAPv3" en la página 66
- "CR# 6320475: la propiedad `com.iplanet.am.session.client.polling.enable` del servidor no debe ser "true" (verdadera)." en la página 66

- "CR# 6358751: la aplicación de la revisión 1 de Access Manager 7 falla si hay espacios incrustados en la clave de cifrado." en la página 66

Creación de archivos de depuración

Los archivos de depuración de Access Manager se crean de forma predeterminada en el directorio de depuración, incluso aunque la propiedad `com.iplanet.services.debug.level` del archivo `AMConfig.properties` se haya establecido en error. Antes del lanzamiento de la revisión 1 de Access Manager 7, sólo se creaba un archivo de depuración al registrar el primer mensaje de depuración en el archivo.

Compatibilidad con los roles y los roles filtrados en el complemento LDAPv3

La revisión 1 de Access Manager proporciona compatibilidad con los roles y los roles filtrados en el complemento LDAPv3 si los datos se han almacenado en Sun Java System Directory Server. Para obtener más información, consulte "Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3 (6365196)" en la página 109.

CR# 6320475: la propiedad `com.iplanet.am.session.client.polling.enable` del servidor no debe ser "true" (verdadera).

La propiedad `com.iplanet.am.session.client.polling.enable` del archivo `AMConfig.properties` del servidor se establece como "false" (falsa) de forma predeterminada y nunca debe restaurarse a "true" (verdadera).

CR# 6358751: la aplicación de la revisión 1 de Access Manager 7 falla si hay espacios incrustados en la clave de cifrado.

Si la clave de cifrado de la contraseña contiene espacios, no se podrá aplicar la revisión.

Solución. Utilice una nueva clave de cifrado que no incluya espacios. Para obtener los pasos detallados para cambiar la clave de cifrado, consulte: Apéndice B, "Changing the Password Encryption Key" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Novedades de esta versión

Para obtener una lista de las nuevas funciones de las revisiones de Access Manager, consulte "Versiones de las revisiones de Access Manager 7 2005Q4" en la página 10. La revisión inicial de Access Manager 7 2005Q4 incluía las siguientes nuevas funciones:

- "Modos de Access Manager" en la página 67
- "Nueva consola de Access Manager" en la página 67

- "Repositorio de identidades" en la página 68
- "Árbol de información de Access Manager" en la página 68
- "Cambios en la conmutación por error de la sesión" en la página 68
- "Notificación de cambio de propiedad de sesión" en la página 69
- "Restricciones de cuota de sesión" en la página 69
- "Autenticación distribuida" en la página 70
- "Compatibilidad con varias instancias del módulo de autenticación" en la página 70
- "Espacio de nombre de "cadena" o "configuración con nombre" de autenticación" en la página 70
- "Mejoras del módulo de directivas" en la página 71
- "Configuración del sitio" en la página 72
- "Federación en masa" en la página 72
- "Mejoras del registro" en la página 72

Modos de Access Manager

Access Manager 7 2005Q4 incluye los modos tradicional y de dominio. Ambos modos admiten:

- Las nuevas funciones de Access Manager 7 2005Q4
- Las funciones de Access Manager 6 2005Q1, excepto las siguientes limitaciones:
  - Al crear los dominios, no se crean las organizaciones correspondientes en Sun Java System Directory Server.
  - La nueva consola de Access Manager 7 2005Q4 no puede establecer una prioridad de plantilla de Clase de servicio (CoS). Consulte "La nueva consola de Access Manager no puede establecer las prioridades de plantilla de CoS (6309262)" en la página 90.
- Repositorios de identidades en Sun Java System Directory Server y otros almacenes de datos

El modo tradicional es necesario para:

- Sun Java System Portal Server
- Los servidores de Sun Java System Communications Services, incluidos Messaging Server, Calendar Server, Instant Messaging o Delegated Administrator
- La coexistencia de implementaciones cuando Access Manager 6 2005Q1 y Access Manager 7 2005Q4 acceden al mismo Directory Server

Nueva consola de Access Manager

Se ha rediseñado la consola de Access Manager para esta versión. Sin embargo, si Access Manager se implementa con Portal Server, Messaging Server, Calendar Server, Instant Messaging o Delegated Administrator, deberá instalar Access Manager en el modo tradicional y utilizar la consola de Access Manager 6 2005Q1:

Para obtener más información, consulte "Problemas de compatibilidad" en la página 75.

Repositorio de identidades

Un repositorio de identidades de Access Manager contiene información relativa a las identidades como, por ejemplo, los usuarios, grupos y roles. Puede crear y mantener un repositorio de identidades mediante Access Manager u otro producto de configuración como Sun Java System Identity Manager.

En la versión actual, el repositorio de identidades puede residir en Sun Java System Directory Server o Microsoft Active Directory. Access Manager puede tener acceso de lectura y escritura, o de sólo lectura al repositorio de identidades.

Árbol de información de Access Manager

El árbol de información de Access Manager contiene información sobre el acceso al sistema. Cada instancia de Access Manager crea y mantiene un árbol de información independiente en Sun Java System Directory Server. A estos árboles se les puede asignar cualquier nombre (sufijo). El árbol de información de Access Manager incluye dominios (y subdominios, si es necesario), como se describe en la siguiente sección.

Dominios de Access Manager

Un dominio y sus subdominios forman parte del árbol de información de Access Manager y pueden contener información de configuración para definir un conjunto de usuarios o grupos, la forma en que se autentican los usuarios, los recursos a los que pueden acceder y la información disponible para las aplicaciones una vez que los usuarios obtienen acceso a los recursos. También pueden contener otro tipo de información de configuración, incluidas la configuración de globalización, restablecimiento de contraseña, sesión y consola, y las preferencias del usuario. Un dominio o subdominio también puede estar vacío.

Puede crear un dominio mediante la consola de Access Manager o la utilidad de CLI `amadmin`. Para obtener más información, consulte la ayuda en línea de la consola o el Capítulo 14, "The amadmin Command Line Tool" de *Sun Java System Access Manager 7 2005Q4 Administration Guide*.

Cambios en la conmutación por error de la sesión

Access Manager proporciona una implementación independiente del servicio de conmutación por error de sesión del contenedor web utilizando Sun Java System Message Queue (Message Queue) como agente de comunicaciones y Berkeley DB de Sleepycat Software, Inc. como base de datos de almacenamiento de sesiones. Entre las mejoras de Access Manager 7 2005Q4 se incluyen la secuencia de comandos `amsfoconfig`, que permite configurar el entorno de conmutación por error de sesión, y la secuencia de comandos `amsfo`, que permite iniciar y detener el agente de Message Queue y el cliente de Berkeley DB.

Para obtener más información, consulte "Implementing Access Manager Session Failover" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Notificación de cambio de propiedad de sesión

La función de notificación de cambio de propiedad de sesión permite a Access Manager enviar una notificación a las escuchas específicas cuando se produce un cambio en una determinada propiedad de sesión. Esta función se aplica al activar el atributo "Activar notificaciones de cambio de propiedad" (Enable Property Change Notifications) en la consola de administrador de Access Manager. Por ejemplo, en un entorno de inicio de sesión único (SSO), varias aplicaciones pueden compartir una sesión de Access Manager. Cuando se produce un cambio en una propiedad de sesión específica definida en la lista de propiedades de notificación, Access Manager envía una notificación a todas las escuchas registradas.

Para obtener más información, consulte "Enabling Session Property Change Notifications" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Restricciones de cuota de sesión

La función de restricciones de cuota de sesión permite al administrador de Access Manager (`amadmin`) establecer el atributo "Activar sesiones de usuario" (Active User Sessions) para limitar el número máximo de sesiones simultáneas permitidas para un usuario. El administrador puede establecer una restricción de cuota de sesión en un nivel global para todos los usuarios o para una entidad como, por ejemplo, una organización, un dominio, un rol o un usuario, que se aplique sólo a uno o varios usuarios específicos.

Las restricciones de cuota de sesión están desactivadas (OFF) de forma predeterminada, pero el administrador puede habilitarlas estableciendo el atributo "Habilitar restricciones de cuota" (Enable Quota Constraints) en la consola de administrador de Access Manager.

El administrador también puede configurar el comportamiento cuando se agote la cuota de sesión de la restricción. Para ello, debe establecer el atributo "Comportamiento resultante si se agota la cuota de la sesión" (Resulting Behavior If Session Quota Exhausted):

- DENY_ACCESS. Access Manager rechaza la solicitud de inicio de una nueva sesión.
- DESTROY_OLD_SESSION. Access Manager destruye la sesión existente que va a caducar para el mismo usuario y permite que se realice una nueva solicitud de inicio de sesión.

El atributo "Exención de los administradores de nivel superior de la comprobación de restricción" (Exempt Top-Level Admins From Constraint Checking) especifica si deben aplicarse las cuotas de sesión de la restricción a los usuarios con un rol de administración de nivel superior.

Para obtener más información, consulte "Setting Session Quota Constraints" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*

Autenticación distribuida

Access Manager 7 2005Q4 incluye la IU de autenticación distribuida, que es el componente de la IU de autenticación remota que proporciona una autenticación segura y distribuida entre dos servidores de seguridad en una implementación. Sin el componente de la IU de autenticación distribuida, las URL de los servicios de Access Manager quedarían expuestas a los usuarios finales. Para evitar esta exposición, puede utilizarse un servidor proxy. Sin embargo, en muchas implementaciones, el servidor proxy no es necesariamente una solución adecuada.

El componente de la IU de autenticación distribuida se instala en uno o varios servidores en el nivel no seguro (DMZ) de la implementación de Access Manager. El servidor de la IU de autenticación distribuida no ejecuta Access Manager; simplemente proporciona la interfaz de autenticación para los usuarios finales mediante un explorador web.

El usuario final envía una solicitud HTTP a la IU de autenticación distribuida que, a su vez, presenta una página de inicio de sesión al usuario. El componente de autenticación distribuida envía a continuación la solicitud del usuario, a través de un segundo servidor de seguridad, al servidor de Access Manager, lo que suprime la necesidad de abrir agujeros en los servidores de seguridad entre los usuarios finales y el servidor de Access Manager.

Para obtener más información, consulte *Technical Note: Using Access Manager Distributed Authentication* .

Compatibilidad con varias instancias del módulo de autenticación

Se han ampliado todos los módulos de autenticación para que admitan el subesquema con compatibilidad para la IU de la consola. Se pueden crear varias instancias del módulo de autenticación para cada tipo de módulo (clase de módulo cargada). Por ejemplo, en el caso de instancias de un tipo de módulo LDAP con los nombres `ldap1` y `ldap2`, cada instancia puede señalar a un servidor de directorios LDAP diferente. Se admiten instancias del módulo con nombres iguales a los de sus tipos para obtener compatibilidad con versiones anteriores. Se debe llamar a:

server_deploy_uri`/UI/Login?module=`*module-instance-name*

Espacio de nombre de "cadena" o "configuración con nombre" de autenticación

Se crea un espacio de nombre diferente en una organización/dominio, es decir, una cadena de instancias del módulo de autenticación. Esta misma cadena puede utilizarse de nuevo y asignarse a una organización/dominio, rol o usuario. La instancia del servicio de autenticación es igual a la cadena de autenticación. Se debe llamar a:

server_deploy_uri/UI/Login?service=*authentication-chain-name*

Mejoras del módulo de directivas

Atributos de personalización

Además de reglas, asuntos y condiciones, las directivas pueden tener ahora atributos de personalización (IDResponseProvider). La decisión de directiva enviada al cliente desde el servicio de evaluación de directivas incluye ahora atributos de personalización de respuestas basados en directivas en las directivas pertinentes. Se admiten dos tipos de atributos de personalización:

- Atributos estáticos. Puede definir el nombre y el valor del atributo en la directiva.
- Atributos dinámicos. Puede mostrar los nombres de atributos en las directivas, mientras que los valores se obtienen de los almacenes de datos del repositorio de identidades durante la evaluación de las directivas.

Los puntos de aplicación de directivas (o agentes) reenvían normalmente los valores de estos atributos en forma de atributos de solicitud, cookies o encabezados HTTP a la aplicación protegida.

Access Manager 7 2005Q4 no permite que los clientes utilicen implementaciones personalizadas de la interfaz del proveedor de respuesta.

Condición de propiedad de sesión

La implementación de la condición de propiedad de sesión (SessionPropertyCondition) decide si se debe aplicar una directiva a la solicitud en función de los valores de propiedades establecidos en la sesión de Access Manager del usuario. Durante la evaluación de directivas, la condición devuelve "true" sólo si se han definido todos los valores de propiedades de la condición en la sesión de Access Manager del usuario. En las propiedades definidas con varios valores en la condición, sólo es necesario que la sesión de usuario presente, como mínimo, un valor de la propiedad en la condición.

Asunto de directiva

La implementación del asunto de directiva (asunto de identidad de Access Manager) permite utilizar las entradas del repositorio de identidades configurado como valores de asunto de directiva.

Exportación de directivas

Puede exportar directivas en formato XML con el comando amadmin. Los nuevos elementos GetPolices y RealmGetPolicies del archivo amAdmin.dtd admiten esta función.

Estado de la directiva

Ahora, la directiva incluye un atributo de estado, que puede establecerse como activo o inactivo. Se omitirán todas las directivas inactivas durante la evaluación de directivas.

Configuración del sitio

Access Manager 7 2005Q4 presenta el "concepto de sitio", que permite una administración centralizada de la configuración para la implementación de Access Manager. Al configurar Access Manager como sitio, las solicitudes de cliente se transfieren siempre al equilibrador de carga, que simplifica la implementación y soluciona determinados problemas, como el servidor de seguridad entre el cliente y los servidores de servicios de fondo de Access Manager.

Para obtener más información, consulte "Configuring an Access Manager Deployment as a Site" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Federación en masa

Access Manager 7 2005Q4 proporciona un servicio de federación en masa de cuentas de usuario para las aplicaciones que se derivan a socios empresariales. Anteriormente, para llevar a cabo la federación de cuentas entre un proveedor de servicios (SP) y un proveedor de identidades (IDP), era necesario que cada usuario accediera tanto a los sitios del SP como del IDP, creara las cuentas (si aún no existían) y realizase el proceso de federación de las dos cuentas mediante un vínculo web. Este proceso requería mucho tiempo y no siempre era el más adecuado para una implementación con cuentas existentes o un sitio que funcionase como proveedor de identidades, o utilizase uno de sus asociados como proveedor de autenticación.

Para obtener más información, consulte *Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide* .

Mejoras del registro

Se han mejorado algunos aspectos del registro en Access Manager 7 2005Q4:

- Nuevos campos (o columnas): el campo `MessageID` contiene el identificador de mensaje del evento registrado. El campo `ContextID` contiene el identificador de contexto, que es análogo al identificador de sesión y se aplica a todos los eventos de un determinado inicio de sesión del usuario. Para cada inicio de sesión específico del usuario, el valor de `ContextID` será el mismo en todos los archivos de registro de los eventos registrados.
- API de registro. La API de registro incluye funciones adicionales para la lectura de los registros, incluso desde una base de datos (BD), cuando se haya configurado el servicio de registro en DB. Consulte `LogReaderSample.java` en el directorio `/opt/SUNWam/samples/logging`, que muestra los resultados recuperados de los registros desde un archivo sin formato o un repositorio de tabla de base de datos.

Precaución – El tamaño de las tablas de base de datos suele ser mayor que los registros de archivo sin formato. Por tanto, en una solicitud específica, no recupere todos los registros de la base de datos, ya que la cantidad de datos puede consumir todos los recursos del servidor de Access Manager.

Requisitos de hardware y software

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

TABLA 4 Requisitos de hardware y software

Componente	Requisito
Sistema operativo (SO)	SO Solaris en sistemas basados en SPARC™, versiones 8, 9 y 10, incluida compatibilidad con zonas locales root completas en Solaris 10
	SO Solaris en plataformas x86, versiones 9 y 10, incluida compatibilidad con zonas locales root completas en Solaris 10.
	SO Solaris en plataformas AMD64, versión 10, incluida compatibilidad con zonas locales root completas
	Red Hat™ Linux, WS/AS/ES 2.1 Update 6 o superior
	Red Hat Linux, WS/AS/ES 3.0
	Red Hat Linux, WS/AS/ES 3.0 Updates 1, 2, 3, y 4
	SO HP-UX. Consulte la recopilación de documentos de Sun Java Enterprise System 2005Q4 para HP-UX: `http://docs.sun.com/coll/1258.2`
	SO Windows. Consulte la recopilación de documentos de Sun Java Enterprise System 2005Q4 para Microsoft Windows: `http://docs.sun.com/coll/1259.2`
Java 2 Standard Edition (J2SE)	J2SE platform 1.5.0_04, 1.5_01, 1.5 y 1.4.2
Directory Server	Árbol de información de Access Manager: Sun Java System Directory Server 5 2005Q4
	Depósito de identidades de Access Manager: Sun Java System Directory Server 5 2005Q4 o Microsoft Active Directory

TABLA 4 Requisitos de hardware y software *(Continuación)*

Componente	Requisito
Contenedores web	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 y 5.1.1 (y revisiones acumuladas asociadas)
RAM	Prueba básica: 512 Mbytes
	Implementación real: 1 Gbyte para los subprocesos, Access Manager SDK, el servidor HTTP y otros componentes internos
Espacio en 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.

Exploradores compatibles

La siguiente tabla muestra los exploradores compatibles con la versión Sun Java Enterprise System 2005Q4.

TABLA 5 Exploradores compatibles

Explorador	Plataforma
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	SO Solaris, versiones 9 y 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

TABLA 5 Exploradores compatibles *(Continuación)*

Explorador	Plataforma
Netscape™ 7.0	SO Solaris, versiones 9 y 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

Compatibilidad con la virtualización de sistemas

La virtualización de sistemas es una tecnología que permite ejecutar de forma independiente varias instancias del sistema operativo (SO) en el hardware compartido. Funcionalmente, un software implementado en un sistema operativo alojado en un entorno virtualizado no detecta en general que la plataforma subyacente se haya virtualizado. Sun realiza pruebas de sus productos de Sun Java System en combinaciones seleccionadas de sistemas de virtualización y sistemas operativos para ayudar a confirmar que los productos de Sun Java System siguen funcionando en entornos virtualizados, configurados y dimensionados correctamente, como lo hacen en sistemas no virtualizados. Para obtener información acerca de la compatibilidad de Sun con los productos de Sun Java System en entornos virtualizados, consulte http://docs.sun.com/doc/820-4651.

Problemas de compatibilidad

- "Modo tradicional de Access Manager" en la página 75
- "Agentes de directivas de Access Manager" en la página 77

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 76
- "Opción de instalación "Configurar ahora" (Configure Now) en el modo gráfico" en la página 76

- "Opción de instalación "Configurar ahora" (Configure Now) en el modo basado en texto" en la página 76
- "Opción de instalación "Configure más tarde" (Configure Later)" en la página 77

Para determinar el modo de la instalación de Access Manager 7 2005Q4, consulte "Determinar el modo de Access Manager" en la página 77.

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, "Instalación en el modo silencioso" de *Guía de instalación de Sun Java Enterprise System 2005Q4 para 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
...
```

En sistemas Windows, el archivo de configuración es *AccessManager-base* `\setup\AMConfigurator.properties`.

Para obtener más información sobre cómo configurar Access Manager con la ejecución de la secuencia de comandos `amconfig`, consulte la *Sun Java System Access Manager 7 2005Q4 Administration Guide* .

Determinar el modo de Access Manager

Para determinar si la instalación de Access Manager 7 2005Q4 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 2005Q4.

TABLA 6 Compatibilidad de los agentes de directivas con los modos de Access Manager 7 2005Q4

Agente y versión	Modo compatible
Agentes web y J2EE , versión 2.2	Modos tradicional y de dominio
Agentes web, versión 2.1	Modos tradicional y de dominio
Agentes J2EE, versión 2.1	Sólo en modo tradicional

Notas sobre la instalación

Las notas sobre la instalación de Access Manager incluyen la siguiente información:

- "Modo tradicional de Access Manager" en la página 75
- "Problemas de instalación" en la página 80

Limitaciones y problemas conocidos

Esta sección describe los siguientes problemas conocidos y sus soluciones (si las hay) en el momento de la publicación.

- "Problemas de compatibilidad" en la página 78
- "Problemas de instalación" en la página 80
- "Problemas de actualización" en la página 83
- "Problemas de configuración" en la página 85
- "Problemas de la consola de Access Manager" en la página 89
- "Problemas de SDK y de cliente" en la página 92
- "Problemas de las utilidades de línea de comandos" en la página 93
- "Problemas de autenticación" en la página 94
- "Problemas de sesión y SSO" en la página 95
- "Problemas de directivas" en la página 98
- "Problemas de inicio del servidor" en la página 98
- "Problemas relacionados con el SO Linux" en la página 99
- "Problemas de federación y SAML" en la página 99
- "Problemas de internacionalización (g11n) " en la página 101
- "Problemas de documentación" en la página 103

Problemas de compatibilidad

- "Incompatibilidad entre los servidores de Java ES 2004Q2 e IM en Java ES 2005Q4 (6309082)" en la página 79
- "Existen incompatibilidades en el módulo de autenticación principal para el modo tradicional (6305840)" en la página 79
- "El agente no puede iniciar sesión porque el perfil no se encuentra en la organización (6295074)" en la página 79
- "La utilidad `commadmin` de Delegated Administrator no crea un usuario (6294603)" en la página 80
- "La utilidad `commadmin` de Delegated Administrator no crea una organización (6292104)" en la página 80

Incompatibilidad entre los servidores de Java ES 2004Q2 e IM en Java ES 2005Q4 (6309082)

La siguiente implementación ha provocado este problema:

- servidor-1: Java ES 2004Q2: Directory Server
- servidor-2: Java ES 2004Q2: Application Server, Access Manager y Portal Server
- servidor-3: Java ES 2004Q2: Calendar Server y Messaging Server
- servidor-4: Java ES 2005Q4: Application Server, Instant Messaging y Access Manager SDK

Al ejecutar la utilidad `imconfig` para configurar Instant Messaging en el servidor-4, la configuración no se pudo realizar con éxito. Access Manager 7 2005Q4 SDK, utilizado por Instant Messaging (IM) en el servidor-4, no es compatible con la versión Java ES 2004Q2.

Solución: es recomendable que el servidor de Access Manager y Access Manager SDK tengan la misma versión. Para obtener más información, consulte *Guía de actualización de Sun Java Enterprise System 2005Q4*.

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

El modo tradicional de Access Manager 7 2005Q4 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 2005Q4, la lista desplegable muestra la opción `ldapService` seleccionada de forma predeterminada. 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.

El agente no puede iniciar sesión porque el perfil no se encuentra en la organización (6295074)

En la consola de Access Manager, puede crear un agente en el modo de dominio. Si cierra la sesión y, a continuación, vuelve a iniciarla con el mismo nombre de agente, Access Manager devuelve un mensaje de error debido a que el agente no cuenta con los privilegios suficientes para acceder al dominio.

Solución: modifique los permisos para brindar acceso de lectura y escritura al agente.

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 2005Q4 sin actualizar Delegated Administrator. Para obtener información sobre la actualización de Delegated Administrator, consulte la *Guía de actualización de Sun Java Enterprise System 2005Q4*.

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 instalación

- "Después de aplicar la revisión 1, el archivo `/tmp/amsilent` concede acceso de lectura a todos los usuarios (6370691)" en la página 81
- "En la instalación de SDK con la configuración del contenedor, la dirección URL de notificación no es correcta (6327845)" en la página 81
- " `classpath` de Access Manager hace referencia a un paquete de JCE 1.2.1 caducado (6297949)" en la página 81
- "Para instalar Access Manager en un DIT existente, es necesario volver a crear los índices de Directory Server (6268096)" en la página 81

- "Permisos de directorios de registro y depuración incorrectos para los usuarios que no son root (6257161)" en la página 82
- "El servicio de autenticación no se inicializa si se instala Access Manager y Directory Server en distintos equipos (6229897)" en la página 82
- "El programa de instalación no agrega la entrada de plataforma para la instalación de Directory Server existente (6202902)" en la página 82

Después de aplicar la revisión 1, el archivo `/tmp/amsilent` concede acceso de lectura a todos los usuarios (6370691)

Después de aplicar la revisión 1, el archivo `/tmp/amsilent` concede acceso de lectura a todos los usuarios.

Solución: Una vez aplicada la revisión, restablezca los permisos del archivo para conceder sólo acceso de lectura al administrador de Access Manager.

En la instalación de SDK con la configuración del contenedor, la dirección URL de notificación no es correcta (6327845)

Si realiza una instalación de SDK con la configuración del contenedor (DEPLOY_LEVEL=4), la dirección URL de notificación no se mostrará correctamente.

Solución:

1. establezca la siguiente propiedad en el archivo `AMConfig.properties`:

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. Reinicie Access Manager para que se aplique el nuevo valor.

`classpath` de Access Manager hace referencia a un paquete de JCE 1.2.1 caducado (6297949)

La variable `classpath` de Access Manager hace referencia a un paquete de Java Cryptography Extension (JCE) 1.2.1 (Certificado de firma) que caducó el 27 de julio de 2005.

Solución: Ninguna. Aunque la referencia del paquete se encuentra en `classpath`, Access Manager no utiliza este paquete.

Para instalar Access Manager en un DIT existente, es necesario volver a crear los índices de Directory Server (6268096)

Directory Server dispone de nuevos índices para mejorar el rendimiento de la búsqueda.

Solución: después de instalar Access Manager con un Árbol de información de directorios (DIT, Directory Information Tree) existente, vuelva a crear los índices de Directory Server ejecutando la secuencia de comandos `db2index.pl`. Por ejemplo:

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

La secuencia de comandos `db2index.pl` está disponible en el directorio *DS-install-directory/slapd-hostname/*.

Permisos de directorios de registro y depuración incorrectos para los usuarios que no son root (6257161)

Cuando se especifica un usuario que no es root en el archivo de configuración de la instalación silenciosa, los permisos de los directorios de depuración, registro e inicio no se establecen adecuadamente.

Solución: cambie los permisos de estos directorios para permitir el acceso a un usuario no root.

El servicio de autenticación no se inicializa si se instala Access Manager y Directory Server en distintos equipos (6229897)

Aunque se actualicen `classpath` y otras variables de entorno del contenedor web de Access Manager durante la instalación, el proceso de instalación no reinicia el contenedor web. Si se intenta iniciar la sesión en Access Manager después de la instalación y antes de que se reinicie el contenedor web, se devolverá el siguiente error:

```
Authentication Service is not initialized.
Contact your system administrator.
```

Solución: reinicie el contenedor web antes de iniciar la sesión en Access Manager. Directory Server debe estar ejecutándose también antes de iniciar la sesión.

El programa de instalación no agrega la entrada de plataforma para la instalación de Directory Server existente (6202902)

El programa de instalación de Java ES no agrega ninguna entrada de plataforma para una instalación de Directory Server existente (DIRECTORY_MODE=2).

Solución: agregue manualmente los alias de dominio/DNS y las entradas de la lista de servidores de plataforma. Para ver los pasos, consulte "Adding Additional Instances to the Platform Server List and Realm/DNS Aliases" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Problemas de actualización

- "La secuencia de comandos `ampre70upgrade` de Access Manager no elimina los paquetes traducidos (6378444)" en la página 83
- "El archivo `AMConfig.properties` incluye una versión antigua del contenedor web (6316833)" en la página 83
- "El archivo `server.policy` del agente del nodo no se ha actualizado durante el proceso de actualización de Access Manager (6313416)" en la página 84
- "Una vez realizada la actualización, falta la condición de propiedad de sesión en la lista de condiciones (6309785)" en la página 84
- "Una vez realizada la actualización, falta el tipo de asunto de identidad en la lista de asuntos de la directiva (6304617)" en la página 84
- "Error en la actualización de Access Manager debido a que no se ha migrado `classpath` (6284595)" en la página 84
- "Una vez realizada la actualización, el comando `amadmin` muestra una versión incorrecta (6283758)" en la página 85
- "Adición del atributo `ContainerDefaultTemplateRole` después de la migración de datos (4677779)" en la página 85

La secuencia de comandos `ampre70upgrade` de Access Manager no elimina los paquetes traducidos (6378444)

Si actualiza Access Manager a la versión Access Manager 7 2005Q4, la secuencia de comandos `ampre70upgrade` no elimina ninguno de los paquetes traducidos de Access Manager presentes en el sistema.

Solución: antes de actualizar a Access Manager 7 2005Q4, utilice el comando `pkgrm` para eliminar manualmente los paquetes traducidos de Access Manager instalados en el sistema.

El archivo `AMConfig.properties` incluye una versión antigua del contenedor web (6316833)

Una vez actualizados Access Manager y Application Server a la versión Java ES 2005Q4, el archivo `AMConfig.properties` de Access Manager incluye una versión antigua de Application Server.

Solución: antes de ejecutar el programa de configuración de Delegated Administrator (`config-commda`), cambie la siguiente propiedad en el archivo `AMConfig.properties`:

```
com.sun.identity.webcontainer=IAS8.1
```

El archivo `server.policy` del agente del nodo no se ha actualizado durante el proceso de actualización de Access Manager (6313416)

El archivo `server.policy` del agente del nodo no se actualiza después de actualizar Access Manager.

Solución: sustituya el archivo `server.policy` del agente del nodo por el siguiente archivo:

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

Una vez realizada la actualización, falta la condición de propiedad de sesión en la lista de condiciones (6309785)

Después de actualizar Access Manager de la versión 2005Q1 a la 2005Q4, la condición de propiedad de sesión no se muestra como una opción en la lista de condiciones de la directiva al intentar agregar una condición a una directiva.

Solución: seleccione el tipo de condición de propiedad de sesión en la plantilla de servicio de configuración de directivas del dominio correspondiente.

Una vez realizada la actualización, falta el tipo de asunto de identidad en la lista de asuntos de la directiva (6304617)

Después de actualizar Access Manager de la versión 2005Q1 a la 2005Q4, el asunto de identidad, un tipo de asunto de directiva recién agregado, no se muestra como opción en la lista de asuntos de la directiva.

Solución: seleccione el tipo de asunto de identidad como tipo de asunto predeterminado en la plantilla de servicio de configuración de directivas.

Error en la actualización de Access Manager debido a que no se ha migrado `classpath` (6284595)

Durante la actualización de Access Manager de Java ES 2004Q2 a Java ES 2005Q4, ha fallado la actualización de Java ES 2004Q2 a Java ES 2005Q1. Access Manager se estaba implementando en Application Server, que también se estaba actualizando de Java ES 2004Q2 a Java ES 2005Q4. La secuencia de comandos `classpath` en el archivo `domain.xml` no disponía de rutas a los archivos JAR de Access Manager.

Solución: Siga estos pasos:

1. Antes de ejecutar la secuencia de comandos `amupgrade`, deberá volver a indexar Directory Server debido a un problema con la secuencia de comandos `comm_dssetup.pl`.
2. Agregue entradas de Access Manager al archivo `server.policy` del agente del nodo. Basta con una copia de `server.policy` desde la política del servidor predeterminado(`/var/opt/SUNWappserver/domains/domain1/config/server.policy`).

3. Actualice `classpath` en el archivo `domain.xml` del agente del nodo de la siguiente forma. Copie el sufijo `classpath-suffix` y la ruta `classpath` pertinentes de los atributos `server-classpath` del elemento `java-config` del archivo `server.xml` en los atributos correspondientes del elemento `java-config` de `domain.xml`. El elemento `java-config` se encuentra bajo el elemento `config` de `domain.xml`.

Una vez realizada la actualización, el comando `amadmin` muestra una versión incorrecta (6283758)

Después de actualizar Access Manager de la versión 6 2005Q1 a la versión 7 2005Q4, el comando `amadmin --version` devuelve una versión incorrecta: Sun Java System Access Manager versión 2005Q1.

Solución: después de actualizar Access Manager, ejecute la secuencia de comandos `amconfig` para configurar esta aplicación. Al ejecutar `amconfig`, especifique la ruta completa al archivo de configuración (`amsamplesilent`). Por ejemplo, en un sistema Solaris:

```
# ./amconfig -s ./config-file
```

o

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

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

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.

Problemas de configuración

- "El archivo `server.policy` de Application Server 8.1 debe editarse al utilizar valores de URI no predeterminados (6309759)" en la página 86

- "No se actualizan la lista de servidores de plataforma ni el atributo de alias FQDN (6309259, 6308649)" en la página 87
- "Validación de datos para los atributos necesarios en los servicios (6308653)" en la página 87
- "Solución para la implementación en una instancia de WebLogic 8.1 segura (6295863)" en la página 87
- "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 88
- "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 88
- "Error en la firma de URL en IBM WebSphere al utilizar la clave RSA (6271087)" en la página 88

El archivo `server.policy` de Application Server 8.1 debe editarse al utilizar valores de URI no predeterminados (6309759)

Si implementa Access Manager 7 2005Q4 en Application Server 8.1 y utiliza URI no predeterminados para los servicios, la consola y las aplicaciones web de contraseña, que presentan valores de URI predeterminados en `amserver`, `amconsole` y `ampassword` respectivamente, debe editar el archivo `server.policy` del dominio de Application Server antes de intentar acceder a Access Manager mediante un explorador web.

Solución: edite el archivo `server.policy` de la siguiente forma:

1. Detenga la instancia de Application Server en la que se ha implementado Access Manager.
2. Vaya al directorio `/config`. Por ejemplo:

   ```
   cd /var/opt/SUNWappserver/domains/domain1/config
   ```

3. Realice una copia de seguridad del archivo `server.policy`. Por ejemplo:

   ```
   cp server.policy server.policy.orig
   ```

4. En el archivo `server.policy`, busque las siguientes directivas:

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amserver/-" { ...
   };
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amconsole/-" { ...
   };
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/ampassword/-" { ...
   };
   ```

5. Sustituya `amserver` por el valor de URI no predeterminado que se utiliza para la aplicación web de servicios en la siguiente línea:

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" {
```

6. En las instalaciones con el modo tradicional, sustituya `amconsole` por el valor de URI no predeterminado que se utiliza para la aplicación web de la consola en la siguiente línea:

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/amconsole/-" {
   ```

7. Sustituya `ampassword` por el valor de URI no predeterminado que se utiliza para la aplicación web de contraseña en la siguiente línea:

   ```
   grant codeBase "file:\${com.sun.aas.instanceRoot}/
   applications/j2ee-modules/ampassword/-" {
   ```

8. Inicie la instancia de Application Server en la que se ha implementado Access Manager.

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 2005Q4 Deployment Planning Guide*.

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

En Access Manager 7 2005Q4, 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 2005Q4 en una instancia de BEA WebLogic 8.1 SP4 segura (con SSL activado), 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 2005Q4 Deployment Planning 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
```

Error en la firma de URL en IBM WebSphere al utilizar la clave RSA (6271087)

Al utilizar una clave RSA en IBM WebSphere, la firma de la cadena de URL falla con la siguiente excepción:

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

Solución: falta el proveedor "SunRsaSign" en el JDK incluido en WebSphere. Para solucionar este problema, edite el archivo *websphere_jdk_root*`/jre/lib/security/java.security` y agregue la siguiente línea para habilitar "SunRsaSign" como uno de los proveedores:

```
security.provider.6=com.sun.rsajca.Provider
```

Problemas de la consola de Access Manager

- "Errores de edición en la consola al duplicar un socio de confianza en SAML (6326634)" en la página 89
- "No funciona el registro remoto para `amConsole.access` y `amPasswordReset.access` (6311786)" en la página 90
- "La adición de más propiedades de `amadmin` en la consola cambia la contraseña de usuario `amadmin` (6309830)." en la página 90
- "La nueva consola de Access Manager no puede establecer las prioridades de plantilla de CoS (6309262)" en la página 90
- "Se produce una excepción al agregar un grupo a un usuario como usuario de administración de directivas (6299543)" en la página 90
- "En el modo tradicional, no se pueden eliminar todos los usuarios de un rol. (6293758)" en la página 90
- "No se pueden agregar, eliminar ni modificar las ofertas de recursos de Discovery Service (6273148)" en la página 91
- "Una contraseña de enlace LDAP incorrecta debería provocar un error en la búsqueda de asuntos (6241241)" en la página 91
- "Access Manager no puede crear una organización en un contenedor en el modo tradicional (6290720)" en la página 91
- "Aparece la antigua consola al agregar servicios relacionados con Portal Server (6293299)" en la página 91
- "La consola no devuelve el conjunto de resultados de Directory Server una vez alcanzado el límite de recursos (6239724)" en la página 91

Errores de edición en la consola al duplicar un socio de confianza en SAML (6326634)

En la consola de Access Manager, cree un socio de confianza de SAML en Federation (Federación) > ficha SAML. Si intenta duplicar el socio de confianza, se producirán errores.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

No funciona el registro remoto para `amConsole.access` y `amPasswordReset.access` (6311786)

Al configurar el registro remoto, todos los registros se escriben en la instancia remota de Access Manager, excepto la información de restablecimiento de contraseña de `amConsole.access` y `amPasswordReset.access` . El registro no se escribe en ninguna ubicación.

Solución: Ninguna.

La adición de más propiedades de `amadmin` en la consola cambia la contraseña de usuario `amadmin` (6309830).

La adición o edición de algunas de las propiedades del usuario `amadmin` en la consola de administración provoca que se modifique la contraseña de usuario `amadmin`.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

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

La nueva consola de Access Manager 7 2005Q4 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.

Se produce una excepción al agregar un grupo a un usuario como usuario de administración de directivas (6299543)

La consola de Access Manager devuelve una excepción al agregar un grupo a un usuario como usuario de administración de directivas.

Solución: Ninguna.

En el modo tradicional, no se pueden eliminar todos los usuarios de un rol. (6293758)

En el modo tradicional, al intentar eliminar todos los usuarios de un rol, siempre queda un usuario.

Solución: intente eliminar de nuevo el usuario del rol.

No se pueden agregar, eliminar ni modificar las ofertas de recursos de Discovery Service (6273148)

La consola de administración de Access Manager no permite la adición, eliminación ni modificación de las ofertas de recursos de un usuario, rol o dominio.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

Una contraseña de enlace LDAP incorrecta debería provocar un error en la búsqueda de asuntos (6241241)

La consola de administración de Access Manager no devuelve un error al utilizar una contraseña de enlace LDAP incorrecta.

Solución: Ninguna.

Access Manager no puede crear una organización en un contenedor en el modo tradicional (6290720)

Si se intenta crear un contenedor y, a continuación, una organización en el mismo, Access Manager devuelve un error de infracción de la unicidad.

Solución: Ninguna.

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 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 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 o 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.

Problemas de SDK y de cliente

- "No se puede eliminar la configuración del servicio de sesión para un subdominio (6318296)" en la página 92
- "El servlet CDC redirecciona a una página de inicio de sesión no válida al especificar la condición de directiva (6311985)" en la página 92
- "Los clientes no reciben notificaciones después de reiniciarse el servlet (6309161)" en la página 93
- "Los clientes de SDK deben reiniciarse después del cambio de esquema de servicio. (6292616)" en la página 93

No se puede eliminar la configuración del servicio de sesión para un subdominio (6318296)

Después de crear un subdominio en el dominio de nivel superior y agregarle el servicio de sesión, si se intenta eliminar la configuración del servicio de sesión, se devolverá un mensaje de error.

Solución: elimine el repositorio de Id. de nivel superior predeterminado (AMSDK1) y, a continuación, vuelva a agregarlo en la configuración.

Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

El servlet CDC redirecciona a una página de inicio de sesión no válida al especificar la condición de directiva (6311985)

Con el agente Apache 2.2 en el modo CDSSO, al acceder al recurso protegido del agente, el servlet CDC redirecciona al usuario a la página de autenticación anónima en lugar de a la página de inicio de sesión predeterminada.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

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. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

Problemas de las utilidades de línea de comandos

- "La búsqueda LDAP de atributos nulos devuelve un error cuando Access Manager señala a Directory Proxy (6357975)" en la página 93
- "Faltan los nuevos archivos de esquema en la secuencia de comandos `amserveradmin` (6255110)" en la página 94
- "No se pueden guardar los documentos XML con caracteres de escape en Internet Explorer 6.0 (4995100)" en la página 94

La búsqueda LDAP de atributos nulos devuelve un error cuando Access Manager señala a Directory Proxy (6357975)

Si está utilizando Sun Java System Directory Proxy Server, la búsqueda LDAP de atributos nulos devolverá un error. Por ejemplo:

```
# ldapsearch -b base-dn uid=user ""
```

Si Access Manager señala directamente al servidor de directorios LDAP, la misma búsqueda se realizará satisfactoriamente.

Solución: si utiliza Directory Proxy Server, habilite las búsquedas de atributos nulos o proporcione un nombre de atributo para la búsqueda.

Faltan los nuevos archivos de esquema en la secuencia de comandos `amserveradmin` (6255110)

Después de la instalación, al ejecutar la secuencia de comandos `amserveradmin` para cargar los servicios en Directory Server, no se encuentran los archivos de esquema `defaultDelegationPolicies.xml` e `idRepoDefaults.xml` en la secuencia de comandos.

Solución: cargue manualmente los archivos `defaultDelegationPolicies.xml` e `idRepoDefaults.xml` utilizando la herramienta de CLI `amadmin` con la opción `-t`.

No se pueden guardar los documentos XML con caracteres de escape en Internet Explorer 6.0 (4995100)

Si agrega un carácter especial (como, por ejemplo, "`amp;`" junto a "&") en un archivo XML, éste se guardará correctamente. Sin embargo, al recuperar el perfil XML más adelante con Internet Explorer 6.0, el archivo no se mostrará correctamente. Si, a continuación, intenta guardar el perfil de nuevo, se devolverá un error.

Solución: Ninguna.

Problemas de autenticación

- "El token SSO `UrlAccessAgent` está a punto de caducar. (6327691)" en la página 94
- "No se puede iniciar sesión en un subdominio con un perfil dinámico/de complemento LDAPV3 después de corregir la contraseña (6309097)" en la página 95
- "Incompatibilidad de la configuración predeterminada del servicio de estadísticas de Access Manager en el modo tradicional (compatible) (6286628)" en la página 95
- "La unicidad del atributo se ha interrumpido en las organizaciones de nivel superior para los atributos de nombre (6204537)" en la página 95

El token SSO `UrlAccessAgent` está a punto de caducar. (6327691)

El token SSO `UrlAccessAgent` puede caducar debido a que el módulo de la aplicación no devuelve el `DN` de usuario especial, lo que provoca la coincidencia de dicho `DN` y, por tanto, el error de un token que no caduque.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

No se puede iniciar sesión en un subdominio con un perfil dinámico/de complemento LDAPV3 después de corregir la contraseña (6309097)

En el modo de dominio, si se crea un almacén de datos ldapv3 en un dominio con una contraseña "incorrecta" y, a continuación, se cambia la contraseña como `amadmin`, al intentar iniciar sesión con la contraseña modificada, el inicio de sesión fallará debido a que no se encuentra ningún perfil.

Solución: Ninguna.

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

- "Las instancias de Access Manager en diferentes zonas horarias provocan que se agote el tiempo de espera de las otras sesiones de usuario (6323639)" en la página 96
- "La secuencia de comandos de conmutación por error de sesión (`amsfoconfig`) tiene permisos incorrectos en el sistema Linux 2.1 (6298433)" en la página 96
- "La secuencia de comandos de conmutación por error de sesión (`amsfoconfig`) presenta errores en el sistema Linux 2.1 (6298462)" en la página 96

- "El sistema crea un nombre de host de servicio no válido cuando el equilibrador de carga tiene una finalización SSL (6245660)" en la página 97
- "Uso de `HttpSession` con contenedores web de otros fabricantes (Sin número de CR)" en la página 97

Las instancias de Access Manager en diferentes zonas horarias provocan que se agote el tiempo de espera de las otras sesiones de usuario (6323639)

Las instancias de Access Manager instaladas en diferentes zonas horarias y en el mismo círculo de confianza provocan que se agote el tiempo de espera de las sesiones de usuario.

La secuencia de comandos de conmutación por error de sesión (`amsfoconfig`) tiene permisos incorrectos en el sistema Linux 2.1 (6298433)

La secuencia de comandos de conmutación por error de sesión (`/opt/sun/identity/bin/amsfoconfig`) incluye permisos incorrectos y no se puede ejecutar en el sistema Linux 2.1.

Solución: cambie los permisos para que la secuencia de comandos `amsfoconfig` sea ejecutable (por ejemplo, 755).

Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

La secuencia de comandos de conmutación por error de sesión (`amsfoconfig`) presenta errores en el sistema Linux 2.1 (6298462)

La secuencia de comandos de conmutación por error de sesión (`amsfoconfig`) presenta errores en el servidor Linux 2.1 debido a que el carácter de tabulación (`\t`) no se interpreta correctamente.

Solución: configure manualmente la conmutación por error de sesión. Para obtener información sobre los pasos de este proceso, consulte "Configuring Session Failover Manually" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

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 recibe las conexiones en el puerto 3030. El equilibrador de carga recibe las conexiones 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 posterior) 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"/>
```

Uso de `HttpSession` con contenedores web de otros fabricantes (Sin número de CR)

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 Invalid Dynamic property being set" (Error, se está estableciendo una propiedad dinámica no válida). 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)" en la página 98
- "Uso del servidor BEA WebLogic como contenedor web" en la página 98

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

Al iniciar Access Manager 7 2005Q4, 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. No tenga en cuenta estos mensajes.

Uso del servidor BEA WebLogic como contenedor web

Si se implementa Access Manager utilizando el servidor BEA WebLogic como contenedor web, es posible que no se pueda acceder a Access Manager.

Solución: reinicie de nuevo el servidor WebLogic para poder acceder a Access Manager.

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: defina 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 federación y SAML

- "La ejecución de los ejemplos de servicios web devuelve el mensaje "Oferta de recursos no encontrada" (6359900)" en la página 99
- "La federación presenta errores al utilizar el perfil de artefacto (6324056)" en la página 100
- "Los caracteres especiales (&) de las declaraciones SAML deberían codificarse (6321128)" en la página 100
- "Se produce una excepción al intentar agregar el servicio de disco a un rol (6313437)" en la página 100
- "Los atributos del contexto de autenticación no se pueden configurar hasta que se hayan configurado y guardado los demás atributos (6301338)" en la página 101
- "El ejemplo de EP no funciona si el sufijo root contiene el carácter " &" (6300163)" en la página 101
- "Error de cierre de sesión en la federación (6291744)" en la página 101

La ejecución de los ejemplos de servicios web devuelve el mensaje "Oferta de recursos no encontrada" (6359900)

Si Access Manager se ha configurado para acceder a ejemplos de servicios web en el directorio *AccessManager-base*`/SUNWam/samples/phase2/wsc` en los sistemas Solaris o en el directorio *AccessManager-base* `/identity/samples/phase2/wsc` en los sistemas Linux, la consulta de Discovery Service o la modificación de la oferta de recursos devuelve el mensaje de error: "Oferta de recursos no encontrada".

AccessManager-base es el directorio base de instalación. El directorio base de instalación predeterminado es `/opt` en los sistemas Solaris y `/opt/sun` en los sistemas Linux.

Solución:

1. Acceda al siguiente directorio de ejemplos: *AccessManager-base* `/SUNWam/samples/phase2/wsc`) en los sistemas Solaris o *AccessManager-base*`/identity/samples/phase2/wsc` en los sistemas Linux
2. En el archivo `index.jsp`, busque la siguiente cadena:

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```

3. Justo antes de la línea que contiene la cadena indicada en el paso anterior, inserte la siguiente nueva línea:

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```

4. Vuelva a ejecutar el ejemplo: (No es necesario que reinicie Access Manager.)

La federación presenta errores al utilizar el perfil de artefacto (6324056)

Si se configuran un proveedor de identidades (IDP, Identity Provider) y un proveedor de servicios (SP, Service Provider), se cambia el protocolo de comunicación para utilizar el perfil de artefacto del explorador y, a continuación, se intenta realizar la federación de usuarios entre el IDP y el SP, el proceso de federación fallará.

Solución: Ninguna.

Los caracteres especiales (&) de las declaraciones SAML deberían codificarse (6321128)

Si se establece Access Manager como el sitio de origen y destino, y se configura SSO, se producirá un error en el sitio de destino. Esto se debe a que el carácter especial (&) de las declaraciones SAML no se ha codificado, por lo que falla el análisis de la aserción.

Solución: Ninguna. Este problema se ha solucionado en la revisión 1. Consulte "Revisión 1 de Access Manager 7 2005Q4" en la página 65 para obtener información sobre la aplicación de la revisión en su plataforma específica.

Se produce una excepción al intentar agregar el servicio de disco a un rol (6313437)

En la consola de Access Manager, si se intenta agregar una oferta de recurso al servicio de disco, se produce una excepción desconocida.

Solución: Ninguna.

Los atributos del contexto de autenticación no se pueden configurar hasta que se hayan configurado y guardado los demás atributos (6301338)

Los atributos del contexto de autenticación no se pueden configurar hasta que se hayan configurado y guardado los demás atributos.

Solución: configure y guarde el perfil del proveedor antes de configurar los atributos del contexto de autenticación.

El ejemplo de EP no funciona si el sufijo root contiene el carácter " &" (6300163)

Si Directory Server tiene un sufijo root que contiene el carácter "& " y se intenta agregar una oferta de recurso del servicio de perfil de empleado, se producirá una excepción.

Solución: Ninguna.

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)

- "Las preferencias de configuración regional de usuario no se aplican en toda la consola de administración (6326734)" en la página 102
- "La ayuda en línea no está disponible completamente para los idiomas europeos cuando Access Manager se implementa en IBM WebSphere (6325024)" en la página 102
- "La información de versión aparece en blanco cuando Access Manager se implementa en IBM WebSphere (6319796)" en la página 102
- "No se puede eliminar UTF-8 en la sección de detección de cliente. (5028779)" en la página 102
- "Los caracteres de varios bytes se muestran en forma de signos de interrogación en los archivos de registro (5014120)" en la página 103

Las preferencias de configuración regional de usuario no se aplican en toda la consola de administración (6326734)

Parte de la consola de administración de Access Manager no sigue las preferencias de configuración regional del usuario, sino que utiliza los valores de configuración regional del explorador. Este problema afecta a los botones de ayuda en línea, versión y cierre de sesión, así como al contenido de la versión y la ayuda en línea.

Solución: cambie la configuración del explorador para que se ajuste a las preferencias de configuración regional del usuario.

La ayuda en línea no está disponible completamente para los idiomas europeos cuando Access Manager se implementa en IBM WebSphere (6325024)

La ayuda en línea no está accesible por completo para todas las configuraciones regionales europeas (español, alemán y francés) cuando Access Manager se implementa en una instancia de IBM WebSphere Application Server. La ayuda en línea muestra un error de aplicación en los siguientes marcos:

- En el marco superior, en el que deberían estar los botones Ayuda (Help) y Cerrar (Close).
- En el marco izquierdo, en el que deberían estar los botones Contenido (Contents), Índice (Index) y Buscar (Search).

Solución: establezca la configuración del explorador en inglés y actualice la página para acceder al marco izquierdo. No obstante, el marco superior seguirá mostrando el mensaje de error de aplicación.

La información de versión aparece en blanco cuando Access Manager se implementa en IBM WebSphere (6319796)

En cualquier configuración regional, cuando Access Manager se implementa en una instancia de IBM WebSphere Application Server, no se puede ver la versión del producto al hacer clic en el botón Versión (Version). En su lugar, aparece una página en blanco.

Solución: Ninguna.

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 2005Q4 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 están codificados de forma nativa y no siempre en UTF-8. Cuando una instancia del contenedor web se inicia en una determinada configuración local, los archivos de registro presentarán la codificación nativa de esa configuración local. 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

- "Access Manager no puede pasar del modo tradicional al modo de dominio (6508473)" en la página 104
- "Información acerca de la deshabilitación de búsquedas persistentes (6486927)" en la página 104
- "Información sobre privilegios admitidos y no admitidos de Access Manager (2143066)" en la página 105
- "Información sobre encaminamiento de solicitudes persistentes basadas en cookies (6476922)" en la página 106
- "Información sobre configuración de inicio de sesión único (SSO) de Windows Desktop para Windows 2003 (6487361)" en la página 107
- "Información sobre los pasos para configurar las contraseñas del servidor de la IU de autenticación distribuida (6510859)" en la página 107
- "La ayuda en línea "To create new site name" ("Para crear un nuevo nombre de sitio") necesita más información (2144543)" en la página 108

- "El parámetro de configuración de contraseña de administrador es ADMIN_PASSWD en los sistemas Windows (6470793)" en la página 108
- "Las Notas de la versión presentan una solución incorrecta para un problema conocido. (6422907)" en la página 109
- "Documento com.iplanet.am.session.protectedPropertiesList en AMConfig.properties (6351192)" en la página 109
- "Información sobre la compatibilidad de los roles y los roles filtrados con el complemento LDAPv3 (6365196)" en la página 109
- "Información sobre las propiedades no utilizadas en el archivo AMConfig.properties (6344530)" en la página 109
- "La propiedad com.iplanet.am.session.client.polling.enable del servidor no puede ser "true" (verdadera) (6320475)" en la página 110
- "La dirección URL de éxito predeterminada es incorrecta en la ayuda en línea de la consola (6296751)" en la página 110
- "Información sobre cómo habilitar el cifrado XML (6275563)" en la página 110

Access Manager no puede pasar del modo tradicional al modo de dominio (6508473)

Si instala Access Manager 7 2005Q4 en modo de dominio, no puede volver al modo tradicional.

Sin embargo, si instala Access Manager 7 2005Q4 en modo tradicional, puede cambiar al modo de dominio utilizando el comando amadmin con la opción -M. Por ejemplo:

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password
-M dc=example,dc=com
```

Información acerca de la deshabilitación de búsquedas persistentes (6486927)

Access Manager utiliza búsquedas persistentes para recibir información acerca de las entradas de Sun Java Directory Server que cambian. De manera predeterminada, Access Manager crea las siguientes conexiones de búsquedas persistentes durante el inicio del servidor:

aci - Cambios del atributo aci, con la búsqueda utilizando el filtro LDAP (aci=*)

sm - Cambios en el árbol de información de Access Manager (o nodo de administración de servicios), que incluye objetos con la clase de objeto de marcador sunService o sunServiceComponent. Por ejemplo, puede crear una directiva que defina privilegios de acceso a un recurso protegido o puede modificar las reglas, temas, condiciones o proveedores de respuesta de una directiva existente.

um - Cambios en el directorio de usuario (o nodo de administración de usuarios). Por ejemplo, puede cambiar el nombre o la dirección del usuario.

Precaución – No es recomendable deshabilitar las búsquedas persistentes de ninguno de estos componentes, ya que un componente con una búsqueda persistente deshabilitada no recibe notificaciones de Directory Server. Consecuentemente, los cambios realizados en Directory Server en ese determinado componente no se notificarán a la caché del componente y ésta caduca.

Por ejemplo, si deshabilita las búsquedas persistentes de cambios en el directorio de usuarios(`um`), el servidor de Access Manager no recibirá notificaciones de Directory Server. Por tanto, un agente no recibirá notificaciones de Access Manager para que actualice su caché de usuario local con los nuevos valores de atributo de usuario. Si una aplicación solicita al agente los atributos de usuario, puede recibir el valor antiguo de ese atributo.

Utilice esta propiedad sólo en circunstancias especiales cuando sea absolutamente necesario. Por ejemplo, si sabe que los cambios de la configuración del servicio (referente a los valores cambiantes de alguno de los servicios como, por ejemplo, los servicios de autenticación y el servicio de sesiones) no se producirán en el entorno de producción, puede deshabilitarse la búsqueda persistente en el componente (`sm`) de administración de servicios. Sin embargo, si se produce un cambio en alguno de los servicios, es necesario el reinicio de un servidor. Esto es también aplicable a otras búsquedas persistentes, especificadas por los valores `aci` y `um`.

Para obtener más información, consulte "CR# 6363157: la nueva propiedad deshabilita las búsquedas persistentes si son absolutamente necesarias" en la página 64.

Información sobre privilegios admitidos y no admitidos de Access Manager (2143066)

Los privilegios definen los permisos de acceso de los administradores que son miembros de roles o grupos que existen dentro de un dominio. Access Manager permite configurar permisos para los siguientes tipos de administradores:

- Los administradores de dominios pueden realizar todas las tareas relacionadas con el dominio, incluidas la definición de depósitos de identidades (almacenes de datos), la configuración de autenticación y la definición de directivas.
- Los administradores de directivas pueden configurar directivas en dominios existentes.

Se admiten los siguientes privilegios:

- Acceso de lectura y escritura a todas las propiedades de directivas y dominio. Define los privilegios de acceso de lectura y escritura para los administradores de dominios.
- Acceso de lectura y escritura sólo a las propiedades de directivas. Define los privilegios de acceso de lectura y escritura para los administradores de directivas.
- Combinación de privilegios admitidos: Acceso de lectura y escritura sólo para propiedades de directivas y acceso de sólo lectura a almacenes de datos. No se admiten otras combinaciones de privilegios.

Información sobre encaminamiento de solicitudes persistentes basadas en cookies (6476922)

Si los servidores de Access Manager se implementan detrás de un equilibrador de carga, el encaminamiento de solicitudes persistentes basadas en cookies evita que la solicitud de un cliente sea mal enrutada a un servidor de Access Manager incorrecto (es decir, a un servidor que no aloje la sesión). Esta función se implementó en la revisión 3 de Access Manager 7 2005Q4.

Anteriormente, sin encaminamiento de solicitudes persistentes basadas en cookies, las solicitudes de clientes no basados en navegador (como, por ejemplo, agentes de directivas y clientes que utilizan el SDK de cliente de Access Manager remoto) se enrutaban mal en un servidor de Access Manager que no alojaba la sesión. Posteriormente, para enviar la solicitud al servidor correcto, el servidor de Access Manager tenía que validar la sesión utilizando comunicación alternativa, lo cual solía causar una degradación del rendimiento. El enrutamiento de solicitudes persistentes basadas en cookies evita la necesidad de esta comunicación alternativa y, por tanto, mejora el rendimiento de Access Manager.

Para implementar el encaminamiento de solicitudes persistentes basadas en cookies, debe configurarse la implementación de Access Manager como un sitio. Para obtener más información, consulte "Configuring an Access Manager Deployment as a Site" de *Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide*.

Para configurar el encaminamiento de solicitudes persistentes basadas en cookies:

1. Para especificar un nombre de cookie, establezca la propiedad `com.iplanet.am.lbcookie.name` en el archivo `AMConfig.properties`. Access Manager generará el valor de la cookie del equilibrador de carga utilizando el Id. de servidor de dos bytes (por ejemplo 01, 02 y 03). Si no especifica un nombre de cookie, Access Manager genera el valor de la cookie del equilibrador de carga utilizando el nombre predeterminado `amlbcookie` más el Id. de servidor de dos bytes.

   Si define el nombre de la cookie en el servidor de Access Manager, debe utilizar el mismo nombre en el archivo `AMAgent.properties` del agente de directivas. Además, si utiliza el SDK de cliente de Access Manager, debe usar el mismo nombre de cookie utilizado por el servidor de Access Manager.

   Nota: No establezca la propiedad `com.iplanet.am.lbcookie.value`, pues Access Manager establece el valor de la cookie utilizando el Id. de servidor de dos bytes.
2. Configure su equilibrador de carga con el nombre de la cookie del paso 1. Puede utilizar un equilibrador de carga de hardware o software con la implementación de Access Manager.
3. Si se implementa la migración tras error de sesión, habilite la propiedad `com.sun.identity.session.resetLBCookie` para los agentes de directivas y el servidor de Access Manager.
   - Para un agente de directivas, agregue y habilite la propiedad en el archivo `AMAgent.properties`.

- Para el servidor de Access Manager, agregue y habilite la propiedad en el archivo `AMConfig.properties`.

Por ejemplo:

```
com.sun.identity.session.resetLBCookie='true'
```

Si se produce una situación de migración tras error, se enruta la sesión a un servidor secundario de Access Manager y se establece el valor de la cookie del equilibrador de carga utilizando el Id. de servidor para el servidor secundario de Access Manager. Las solicitudes posteriores de la sesión se enrutarán al servidor secundario de Access Manager.

Información sobre configuración de inicio de sesión único (SSO) de Windows Desktop para Windows 2003 (6487361)

Para configurar el inicio de sesión único (SSO) de Windows Desktop en Windows 2003, tal como se describe en "Configuring Windows Desktop SSO" de *Sun Java System Access Manager 7 2005Q4 Administration Guide*, utilice el siguiente comando `ktpass`:

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

Por ejemplo:

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

Para obtener las definiciones de sintaxis, consulte el siguiente sitio:

```
http://technet2.microsoft.com/
WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true
```

Información sobre los pasos para configurar las contraseñas del servidor de la IU de autenticación distribuida (6510859)

El siguiente procedimiento describe cómo configurar las contraseñas cifradas para un servidor de la IU de autenticación distribuida que se comunica con un servidor de Access Manager.

Para configurar las contraseñas de un servidor de la IU de autenticación distribuida:

1. En el servidor de Access Manager:
   a. cifre la contraseña `amadmin` utilizando la utilidad `ampassword -e`. Por ejemplo, en sistemas Solaris:

```
# cd /opt/SUNWam/bin
# ./ampassword -e amadmin-password
AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
```

Guarde este valor cifrado.

b. Copie y guarde el valor de la propiedad `am.encryption.pwd` del archivo `AMConfig.properties` del servidor de Access Manager. Por ejemplo:

```
am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
```

2. En el servidor de la IU de autenticación distribuida, realice estos cambios en el archivo `AMConfig.properties`:
   a. Comente la propiedad `com.iplanet.am.service.password`.
   b. Establezca la propiedad `com.iplanet.am.service.secret` en la contraseña `amadmin` cifrada del Paso 1a.
   c. Agregue `am.encryption.pwd` y el valor cifrado que ha copiado en el paso 1b. Por ejemplo:

```
com.sun.identity.agents.app.username=username
#com.iplanet.am.service.password=password
com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
```

3. Reinicie el servidor de la IU de autenticación distribuida.

La ayuda en línea “To create new site name” ("Para crear un nuevo nombre de sitio") necesita más información (2144543)

Falta el paso Save (Guardar) en “To create new site name” ("Para crear un nuevo nombre de sitio") en la ayuda en línea de la consola de Access Manager que se ubica en Configuración>Propiedades del sistema>Plataforma. Si no hace clic en Save (Guardar) tras agregar un nuevo nombre de sitio e intenta agregar un nombre de instancia, el proceso fallará. Por tanto, haga siempre clic en Save (Guardar) tras agregar el nombre del sitio y, a continuación, agregue el nombre de la instancia.

El parámetro de configuración de contraseña de administrador es `ADMIN_PASSWD` en los sistemas Windows (6470793)

En los sistemas Solaris y Linux, el parámetro de configuración de contraseña de administrador de Access Manager (`amadmin`) en el archivo `amsamplesilent` es `ADMINPASSWD`. En los sistemas Windows, sin embargo, el parámetro en el archivo `AMConfigurator.properties` es `ADMIN_PASSWD` .

Si ejecuta `amconfig.bat` en los sistemas Windows, establezca la contraseña `amadmin` en el archivo `AMConfigurator.properties` utilizando el parámetro `ADMIN_PASSWORD` y no `ADMINPASSWD`.

Las Notas de la versión presentan una solución incorrecta para un problema conocido. (6422907)

Se ha corregido el paso 3 de la solución del problema "La ejecución de los ejemplos de servicios web devuelve el mensaje "Oferta de recursos no encontrada" (6359900)" en la página 99.

Documento `com.iplanet.am.session.protectedPropertiesList` en `AMConfig.properties` (6351192)

El parámetro `com.iplanet.am.session.protectedPropertiesList` permite proteger determinadas propiedades de sesión interna o central frente a actualizaciones remotas mediante el método `SetProperty` del servicio de sesión. Al establecer este parámetro clave de seguridad "oculto", puede personalizar los atributos de sesión para participar en la autorización, así como en otras funciones de Access Manager. Para utilizar este parámetro:

1. Con un editor de textos, agregue el parámetro al archivo `AMConfig.properties` .
2. Establezca el parámetro en las propiedades de sesión que desee proteger. Por ejemplo:

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1,PropertyName2,PropertyName3
   ```

3. Reinicie el contenedor Web de Access Manager para que se apliquen los valores.

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 problema CR 6349959). En la consola de administración de Access Manager 7 2005Q4, 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
```

La propiedad `com.iplanet.am.session.client.polling.enable` del servidor no puede ser "true" (verdadera) (6320475)

La propiedad `com.iplanet.am.session.client.polling.enable` del archivo `AMConfig.properties` no debe establecerse nunca como "true" (verdadera) en el servidor.

Solución: esta propiedad debe establecerse como "false" (falsa) y nunca como "true" (verdadera).

La dirección URL de éxito predeterminada es incorrecta en la ayuda en línea de la consola (6296751)

La dirección URL de éxito predeterminada aparece de forma incorrecta en el archivo de ayuda en línea de la consola, `service.scserviceprofile.iplanetamauthservice.html` . El campo de URL de éxito predeterminada acepta una lista de varios valores que especifican la dirección URL a la que se redirigen los usuarios tras realizarse con éxito la autenticación. El formato de este atributo es `clientType|URL`, aunque se puede especificar únicamente el valor de la dirección URL, por lo que se presupone que se trata de un tipo predeterminado de HTML.

El valor predeterminado "`/amconsole`" es incorrecto.

Solución: El valor predeterminado correcto es "`/amserver/console`".

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

- "Colección de documentos de Sun Java System Access Manager 7 2005Q4" en la página 111
- "Colección de documentos de Sun Java System Federation Manager 7.0 2005Q4" en la página 112
- "Colección de documentos de Sun Java System Access Manager Policy Agent 2.2" en la página 112

Colección de documentos de Sun Java System Access Manager 7 2005Q4

La siguiente tabla muestra los documentos nuevos y revisados de Access Manager 7 2005Q4 que se han publicado desde la versión inicial. Para acceder a estos documentos, consulte la colección de documentos de Access Manager 7 2005Q4:

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

TABLA 7 Historial de actualización de la documentación de Access Manager 7 2005Q4

Título	Fecha de publicación
Notas de la versión de Sun Java System Access Manager 7 2005Q4	Consulte la Tabla 1.
Sun Java System Access Manager 7 2005Q4 Administration Guide	Febrero de 2006
Sun Java System Access Manager 7 2005Q4 Developers Guide	Febrero de 2006
Sun Java System Access Manager Policy Agent 2.2 User's Guide	Febrero de 2006
Sun Java System Access Manager 7 2005Q4 C API Reference	Febrero de 2006
Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide	Febrero de 2006
Technical Note: Using Access Manager Distributed Authentication	Febrero de 2006
Technical Note: Installing Access Manager to Run as a Non-Root User	Febrero de 2006
Sun Java System SAML v2 Plug-in for Federation Services User's Guide	Febrero de 2006

TABLA 7 Historial de actualización de la documentación de Access Manager 7 2005Q4 *(Continuación)*

Título	Fecha de publicación
Sun Java System SAML v2 Plug-in for Federation Services Release Notes	Febrero de 2006
Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference	Febrero de 2006
Sun Java System Access Manager 7 2005Q4 Deployment Planning Guide	Enero de 2006
Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide	Diciembre de 2005
Sun Java System Access Manager 7 2005Q4 Technical Overview	Diciembre de 2005

Colección de documentos de Sun Java System Federation Manager 7.0 2005Q4

Para acceder a los documentos de la colección de Federation Manager 7.0 2005Q4, consulte:

`http://docs.sun.com/coll/1321.1`

Colección de documentos de Sun Java System Access Manager Policy Agent 2.2

La colección de documentos de Access Manager Policy Agent 2.2 se revisa de forma continuada para informar de los nuevos agentes. Para acceder a los documentos de esta colección, consulte:

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

Archivos redistribuibles

Sun Java System Access Manager 7 2005Q4 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:

- Puede encontrar los 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 que podamos ayudarle de forma óptima en la resolución de problemas, tenga a mano la siguiente información cuando se ponga en contacto con el servicio de asistencia técnica:

- 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, incluida cualquier revisión del producto y otro software que pudiera influir en el problema
- Pasos detallados de los métodos que haya usado para solucionar el problema
- Cualquier registro de error o volcado del núcleo

Sun valora sus comentarios

Sun tiene interés en mejorar su documentación y agradece sus comentarios y sugerencias. Diríjase `http://docs.sun.com/` y haga clic en 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 Notas de la versión de Access Manager es 819-2134-22.

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 encontrar 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

En este documento se mencionan direcciones URL de terceros que proporcionan información adicional relacionada.

Nota – Sun no se hace responsable de la disponibilidad de los sitios web de terceras partes mencionados 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.