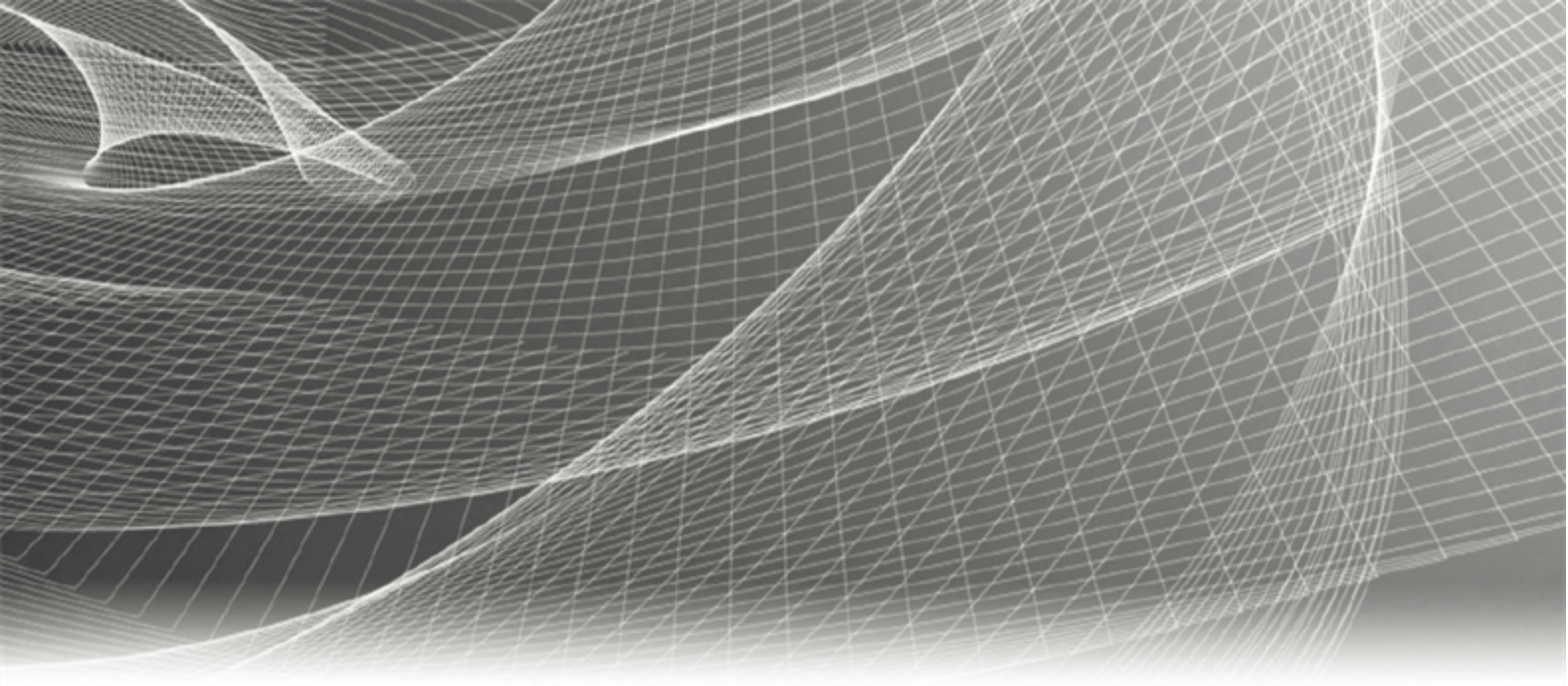

RSA SECURID® ACCESS

RSA® Agente de autenticación 8.1 para PAM

Guía de instalación y configuración de Oracle y RHEL

Información de contacto

RSA Link en https://community.rsa.com contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones para problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Marcas comerciales

Dell, RSA, el logotipo de RSA, EMC y otras marcas comerciales pertenecen a Dell Inc. o sus filiales. Las demás marcas comerciales pueden ser marcas comerciales de sus respectivos dueños. Para obtener una lista de las marcas comerciales de RSA, visite mexico.emc.com/legal/emc-corporation-trademarks.htm.

Acuerdo de licencia

Este software y la documentación asociada son propiedad e información confidencial de Dell Inc. o sus filiales, se suministran bajo licencia y pueden utilizarse y copiarse solamente de acuerdo con los términos de dicha licencia y con la inclusión del aviso de copyright mencionado a continuación. No se puede suministrar a ninguna persona, ni poner a su disposición de cualquier otra manera, este software ni la documentación, o cualquier copia de estos elementos.

Este documento no constituye ninguna transferencia de titularidad ni propiedad del software, la documentación o cualquier derecho de propiedad intelectual. Cualquier uso o reproducción sin autorización de este software y de la documentación pueden estar sujetos a responsabilidad civil o penal.

Este software está sujeto a cambios sin aviso y no debe considerarse un compromiso asumido por Dell Inc.

Licencias de otros fabricantes

Este producto puede incluir software que ha sido desarrollado por otros fabricantes. El texto de los acuerdos de licencia que se aplican al software de otros fabricantes en este producto puede encontrarse en la página de documentación del producto en RSA Link. Al usar este producto, el usuario acepta regirse totalmente por los términos de los acuerdos de licencia.

Nota sobre tecnologías de cifrado

Es posible que este producto contenga tecnologías de cifrado. Muchos países prohíben o limitan el uso, la importación o la exportación de las tecnologías de cifrado, y las regulaciones actuales de uso, importación y exportación deben cumplirse cuando se use, importe o exporte este producto.

Distribución

El uso, la copia y la distribución de cualquier software de Dell descrito en esta publicación requieren una licencia de software correspondiente.

Dell Inc. considera que la información de esta publicación es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA "TAL CUAL". Dell Inc. NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y ESPECÍFICAMENTE RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO.

Octubre de 2018

Contenido

Prefacio

Público al que va dirigido

Esta guía está dirigida a los administradores de red y del sistema que instalan, actualizan y solucionan problemas de RSA® Authentication Agent for PAM (módulo de autenticación con capacidad para conectarse).

Soporte y servicio

Puede acceder a la comunidad y a información de soporte en RSA Link en https://community.rsa.com. RSA Link contiene una base de conocimientos que responde a las preguntas comunes y brinda soluciones a problemas conocidos, documentación de productos, análisis de la comunidad y administración de casos.

Programa para partners RSA Ready

El sitio web del programa para partners RSA Ready en www.rsaready.com proporciona información sobre productos de hardware y software de otros fabricantes cuyo funcionamiento con productos de RSA se ha certificado. El sitio web incluye guías de implementación con instrucciones paso por paso y otra información acerca del funcionamiento de los productos de RSA con productos de otros fabricantes.

Capítulo 1: Instalación de PAM Agent

Descripción general de RSA Authentication Agent 8.1 for PAM

RSA Authentication Agent 8.1 for PAM (módulo de autenticación con capacidad para conectarse) admite la autenticación en sistemas UNIX con herramientas de conexión estándar o de OpenSSH. PAM Agent utiliza las bibliotecas compartidas personalizadas de RSA y admite el acceso a estaciones de trabajo y servidores UNIX con los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Puede elegir si PAM Agent se autentica en Cloud Authentication Service o Authentication Manager. La licencia de RSA SecurID Access Enterprise Edition y de Premium Edition incluyen estos componentes de RSA SecurID Access. No se requiere Authentication Manager para utilizar PAM Agent.

La versión 8.1 de PAM Agent ofrece los siguientes beneficios nuevos:

- Compatibilidad con Cloud Authentication Service. Cloud Authentication Service utiliza métodos de autenticación de múltiples factores, como Aprobar (notificación automática optimizada para los dispositivos móviles), Código de token de Authenticate, biometría de dispositivos, código de token de SMS, código de token de voz y tokens de RSA SecurID para permitir el acceso seguro a software como servicio (SaaS) y a las aplicaciones web en las instalaciones para los usuarios.
- Capacidad de acceder a Authentication Manager con el protocolo REST, en lugar del protocolo UDP.
- Soporte continuo para el protocolo UDP utilizado por las versiones anteriores de PAM Agent.
- Authentication Manager cuenta con informes de agentes que le ayudan a administrar los PAM Agent del protocolo REST instalados. En el modo REST, PAM Agent puede enviar información adicional al servidor de Authentication Manager, como un número de ID de software único para cada PAM Agent instalado e información sobre el sistema operativo utilizado por el agente.

El uso de PAM Agent en el modo REST ofrece ventajas adicionales frente al uso del protocolo UDP:

- Facilita la integración de la implementación de Authentication Manager a Cloud Authentication Service.
- Puede agregar y mantener un registro de agente de autenticación en Authentication Manager y usarlo para representar varios agentes instalados.
- Puede ejecutar varios agentes de autenticación en el mismo hardware de manera más fácil que a través del protocolo UDP.
- Utiliza el protocolo TCP para las implementaciones que requieren agentes de autenticación a fin de usar la configuración de red IPv4 o el protocolo IPv4.
- En los modos de autenticación del protocolo REST, la versión 8.1 de PAM Agent utiliza el módulo de biblioteca criptográfica que cumple con FIPS ,**fips-2.0.16**, con la versión 1.0.2l de OpenSSL. Para obtener más información, consulte la *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* en https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.
- Requiere menos actualizaciones de agentes de autenticación para nuevas funciones y mejoras que los agentes de autenticación que no utilizan el protocolo de REST. Los agentes de autenticación que usan el protocolo REST tienen más probabilidades de beneficiarse con los cambios en Authentication Manager, lo que reduce la cantidad de las actualizaciones necesarias en varios agentes.

Modos de autenticación

Puede instalar PAM Agent en uno de los tres modos de autenticación. Todos los modos proporcionan autenticación de RSA SecurID. Puede cambiar el modo después de la instalación según sea necesario. Para obtener instrucciones, consulte Cambio del modo de autenticación de PAM Agent En la página 36.

Modo de autenticación	Descripción
RSA Authentication Manager con el protocolo UDP	Los autenticadores de hardware y software de RSA SecurID generan códigos de token de RSA SecurID. El agente comprueba que los datos introducidos por el usuario coincidan con los datos almacenados en Authentication Manager y permite o deniega el acceso basado en el resultado. De forma predeterminada, la actualización de PAM Agent configura el agente para que use el protocolo UDP. Puede cambiar fácilmente a un modo de autenticación diferente que use el protocolo REST.
RSA Authentication Manager con el protocolo REST	Compatibilidad con todos los tipos de autenticación admitidos por Authentication Manager mediante el protocolo REST, como los tokens de software y hardware de RSA SecurID, y Código de token de Authenticate a través de una integración con el componente de Cloud Authentication Service.
Cloud Authentication Service con el protocolo REST	Admite Aprobar (notificación automática optimizada para los dispositivos móviles), Código de token de Authenticate, biometría de dispositivos, código de token de SMS, código de token de voz y tokens de RSA SecurID. Los tokens FIDO y las condiciones de autenticación que requieren combinaciones de métodos (como Aprobar Y el token de RSA SecurID) no son compatibles.

RSA Authentication Agent 8.1 for PAM es compatible con los dominios de confianza de RSA Authentication Manager. No se admite la autenticación basada en riesgo (RBA) de Authentication Manager.

Flujo de trabajo de PAM Agent

PAM Agent está instalado en un servidor UNIX. Actúa como un intermediario entre la autenticación de usuarios y el servidor de RSA Authentication Manager o Cloud Authentication Service.

PAM Agent admite las funciones de seguridad de Authentication Manager. Por ejemplo, si Authentication Manager determina que el usuario asociado con un token específico requiere un PIN nuevo, entonces el agente solicitará el PIN, que cuenta con características definidas en Authentication Manager, y enviará la información a Authentication Manager. Si Authentication Manager requiere el código de token siguiente que aparece en el token del usuario, entonces PAM Agent se lo solicitará al usuario. Si no se envía el código de token siguiente correcto a Authentication Manager, se producirá un error de autenticación.

Estos pasos describen el flujo de autenticación para PAM Agent en los tres modos de autenticación:

1. Un usuario intenta acceder a una máquina protegida por PAM Agent, ya sea de manera local con inicio de sesión o de forma remota con herramientas como rlogin, telnet, SSH y FTP.

   El usuario debe existir localmente en la máquina donde PAM Agent está instalado.

2. La infraestructura de módulo de autenticación con capacidad para conectarse (PAM) de UNIX intercepta todas las solicitudes de inicio de sesión y utiliza los archivos de configuración de PAM para tener acceso el módulo PAM de RSA:
   - Si un usuario no está configurado para la autenticación de RSA SecurID, el módulo PAM de RSA permite que la solicitud tenga éxito.
   - Si al usuario que solicita acceso se le pide la contraseña de RSA SecurID, PAM Agent continúa la autenticación con el paso 3.

3. Según el modo de autenticación de PAM Agent, el agente se contacta con Authentication Manager o Cloud Authentication Service.

   Para Authentication Manager con una conexión UDP o el protocolo REST, se llevan a cabo los siguientes pasos:

   a. El agente le solicita al usuario el nombre de usuario y el código de acceso.
   b. El agente envía de forma segura el nombre de usuario y el código de acceso a Authentication Manager:
      - Si Authentication Manager aprueba la solicitud, el agente otorga acceso al usuario.
      - Si Authentication Manager no aprueba la solicitud, el agente deniega el acceso.

   Para Cloud Authentication Service, se llevan a cabo los siguientes pasos:

   a. El agente le solicita al usuario un nombre de usuario y envía la información a Cloud Authentication Service.
   b. Cloud Authentication Service proporciona al agente los métodos de autenticación configurados para el usuario en el nivel de seguridad de la política de acceso de Cloud Authentication Service.
   c. El agente le solicita al usuario la contraseña para autenticarse.
   d. El usuario elige un método de autenticación disponible y autentica:
      - Si Cloud Authentication Service aprueba la solicitud, el agente otorga acceso al usuario.
      - Si un método de autenticación no se realiza correctamente, Cloud Authentication Service le solicita al usuario el siguiente método de autenticación.
      - Si Cloud Authentication Service no aprueba la solicitud, el agente deniega el acceso.

Requisitos de software

Esta sección describe las versiones de software mínimas admitidas por PAM Agent.

Sistema operativo requerido

PAM Agent requiere uno de los siguientes sistemas operativos:

- RHEL 6.10: (32 bits y 64 bits)
- RHEL 7.5 (64 bits)
- CentOS Linux 7.5 (64 bits)
- Oracle Linux 6.10 (64 bits)
- Oracle Linux 7.5 (64 bits)

La versión de 32 bits o 64 bits correspondiente de **libuuid.so** (biblioteca de UUID) debe estar instalada en la máquina de PAM Agent.

Requisitos de SELinux

Si SELinux se encuentra habilitado en algún sistema RHEL u Oracle Linux, debe instalar los siguientes paquetes antes de instalar RSA SecurID Authentication Agent 8.1 for PAM:

selinux-policy-devel*.noarch.rpm
policycoreutils-devel*.rpm

Si SELinux se encuentra habilitado en RHEL 6.10 de 32 bits y 64 bits, o en Oracle Linux 6.10 de 64 bits, debe instalar los siguientes paquetes antes de instalar RSA SecurID Authentication Agent 8.1 for PAM:

setools-libs-3.3.7-4.el6.x86_64.rpm
setools-libs-python-3.3.7-4.el6.x86_64.rpm
audit-libs-python-2.4.5-3.el6.x86_64.rpm
libsemanage-python-2.0.43-5.1.el6.x86_64.rpm
policycoreutils-python-2.0.83-29.0.1.el6.x86_64
setroubleshoot-plugins-3.0.40-2.0.1.el6.noarch
setroubleshoot-server-3.0.47-11.0.1.el6.x86_64

Compatibilidad con versiones de RSA Authentication Manager

RSA SecurID Authentication Agent 8.1 for PAM es compatible con la API de autenticación de RSA SecurID versión 1.1, que es la versión actual de las API REST.

En la siguiente tabla se enumeran las versiones de RSA Authentication Manager que se requieren para admitir funciones específicas.

Versión requerida de RSA Authentication Manager	Función compatible
8.2 SP1 o superior	PAM Agent requiere RSA Authentication Manager 8.2 SP1 o superior.
8.2 SP1 parche 5 o superior	Si el indicador de creación de informes de agentes está habilitado en PAM Agent, se requiere RSA Authentication Manager 8.2 SP1 parche 5 o superior para evitar las autenticaciones fallidas en el modo REST.
8.3 o superior	RSA Authentication Manager 8.3 y versiones superiores incluyen informes de agentes con los que puede administrar las instancias de PAM Agent de protocolo REST instaladas. Estos informes incluyen la información adicional que PAM Agent puede enviar a Authentication Manager.

Compatibilidad con versiones de Cloud Authentication Service

RSA SecurID Authentication Agent 8.1 for PAM es compatible con la API de autenticación de RSA SecurID versión 1.1, que es la versión actual de las API REST.

Requisitos de los certificados

PAM Agent utiliza certificados de protocolo TLS 1.2 para el protocolo REST. Cloud Authentication Service y RSA Authentication Manager 8.2 o superior pueden aceptar estos certificados. Las implementaciones que no utilizan certificados de protocolo TLS 1.2 deben usar el modo de autenticación que admite Authentication Manager con el protocolo UDP.

En los modos de autenticación del protocolo REST, PAM Agent usa el módulo de biblioteca criptográfica conforme a la norma FIPS ,**fips-2.0.16**, con OpenSSL version 1.0.2l. Para obtener más información, consulte la *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* en https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.

Herramientas compatibles

PAM Agent es compatible con las siguientes herramientas:

- telnet
- login
- rlogin
- su
- ssh (ssh, sftp y scp)
- sudo

  Descargue e instale la versión compatible de sudo desde https://www.sudo.ws.

- ftp (limitado a una única transacción)
- gdm

Compatibilidad con OpenSSH (opcional)

PAM Agent admite OpenSSH 6.0 P1. Si está utilizando OpenSSH, verifique que esté usando la versión compatible de OpenSSH correspondiente a su plataforma. No se requiere OpenSSH.

Se admiten las siguientes herramientas OpenSSH opcionales:

- ssh
- sftp
- scp

Instale OpenSSH en la máquina del agente. Para OpenSSH, incluidos los requisitos previos y el software adicional necesario para compilar el código fuente, consulte https://www.openssh.com.

Planificación para instalar PAM Agent

Antes de instalar PAM Agent, realice lo siguiente:

- En la máquina donde está instalando PAM Agent:
  1. Obtenga los permisos de raíz.
  2. Cree un directorio **/var/ace** para los archivos de configuración de PAM Agent, si aún no existe ninguno, y cree un directorio de instalación.
  3. Obtenga el certificado de CA raíz de confianza del servidor de RSA Authentication Manager o Cloud Authentication Service. (Para obtener instrucciones, consulte el artículo de la base de conocimientos How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate). A continuación, realice lo siguiente:
     a. Verifique que el certificado no esté caducado.
     b. Almacene los certificados en el formato PEM. Si hay varios certificados de CA, deben estar concatenados en un único archivo en formato PEM.
     c. Copia ***filename*.pem** en el directorio **/var/ace/**.
     d. Proteja el directorio **/var/ace/** que contiene los certificados con los privilegios adecuados.

- Para autenticar con RSA Authentication Manager, cree un registro del agente de autenticación para PAM Agent en la base de datos interna. Para obtener más información, póngase en contacto con su superadministrador de Authentication Manager o consulte la ayuda de Authentication Manager en RSA Link.
- Para autenticar con el protocolo UDP, debe generar el archivo de configuración de Authentication Manager, **sdconf.rec**, u obtener este archivo de su superadministrador de Authentication Manager. Este archivo no se necesita para la autenticación con el protocolo REST.

  El archivo **sdconf.rec** especifica la forma en que el agente se comunica con la instancia primaria y las instancias de réplica de Authentication Manager mediante la dirección IP. Realice lo siguiente:

  - Asegúrese de que la versión más reciente del archivo **sdconf.rec** se encuentre en un directorio accesible en la máquina del agente, como el directorio predeterminado **/var/ace**.
  - Debe tener permisos de escritura en el directorio donde se almacena el archivo **sdconf.rec**.
- En el modo de autenticación que utiliza Cloud Authentication Service con el protocolo REST, PAM Agent se basa en Cloud Authentication Service para el balanceo de carga y la conmutación por error.
- En el modo de autenticación que utiliza RSA Authentication Manager con el protocolo REST, PAM Agent no es compatible con el balanceo de carga. PAM Agent admite la conmutación por error con un máximo de 15 instancias de réplica de Authentication Manager.
- Recopile la información que proporcionará durante la instalación de PAM Agent.

  Authentication Manager con el protocolo UDP. Puede conservar los valores predeterminados o especificar nuevos directorios.

Descripción	**Su plan**
Directorio donde se ubica **sdconf.rec**. El valor predeterminado es **/var/ace/**.	
Ruta raíz del directorio de PAM Agent. El valor predeterminado es **/opt**.	

  Authentication Manager con el protocolo REST. Solicite la siguiente información a su superadministrador de Authentication Manager:

Descripción	**Su plan**
Dirección URL del servidor REST para la comunicación entre el agente de autenticación y la instancia primaria de Authentication Manager. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia primaria, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El	

Descripción	Su plan
valor predeterminado de *PORT* es 5555.	
Cantidad de instancias de réplica de Authentication Manager que pueden usarse para la conmutación por error.	
Dirección URL del servidor REST para cada instancia de réplica. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia de réplica, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El valor predeterminado de *PORT* es 5555.	
Clave de acceso (clave del cliente) para transmitir de manera segura las solicitudes de autenticación de usuarios a Authentication Manager. Este valor se genera en la Consola de seguridad de la instancia primaria de Authentication Manager. Para obtener instrucciones sobre cómo conseguir la clave de acceso, consulte el siguiente tema en RSA Link: Configurar la API de autenticación de RSA SecurID para los agentes de autenticación.	
Ingrese el directorio y el nombre de archivo para el certificado de confianza del servidor en el agente de autenticación. El valor predeterminado es **/var/ace/cert.pem**.	
Nombre del agente de autenticación (ID del cliente) que se creó para PAM Agent en Authentication Manager.	
Ruta raíz del directorio de PAM Agent. El valor predeterminado es **/opt**.	

Cloud Authentication Service con el protocolo REST. Solicite la siguiente información al super-radministrador de Cloud Authentication Service:

Descripción	Su plan
Dirección URL del servidor REST para la comunicación entre el agente y Cloud Authentication Service. Utiliza el siguiente formato:	

Descripción	Su plan
`https://HOSTNAME:PORT/mfa/v1_1/authn` Para Cloud Authentication Service, obtenga el valor *HOSTNAME* del campo **Dominio del servicio de autenticación** en la pestaña **Registro** de la página de configuración para cualquier enrutador de identidad en Consola de administración de nube. El valor predeterminado de *PORT* es 443.	
Clave de la API de autenticación (clave del cliente) creada en Consola de administración de nube para pasar de manera segura las solicitudes de autenticación a Cloud Authentication Service. Para obtener instrucciones sobre cómo conseguir la clave de la API de autenticación, consulte el siguiente tema en RSA Link: Agregar una clave de la API de autenticación de RSA SecurID.	
Directorio y nombre de archivo del certificado de confianza del servidor en el agente de autenticación. El valor predeterminado es **/var/ace/cert.pem**.	
ID de grupo de usuarios para Cloud Authentication Service. PAM Agent puede proporcionar el ID de grupo de usuarios en las solicitudes de autenticación, pero el agente no valida los datos. Actualmente, este parámetro no es compatible con Cloud Authentication Service.	
Nombre de la política de acceso para Cloud Authentication Service. Esta política se define en Consola de administración de nube.	
Nombre del agente de autenticación CLIENT_ID que se mostrará en las notificaciones móviles. Puede ingresar el valor que desee. Por ejemplo, PAM_Agent.	
Ruta raíz del directorio de PAM Agent. El valor predeterminado es **/opt**.	

Instalación de RSA Authentication Agent 8.1 for PAM

Complete las siguientes tareas para instalar PAM Agent:

1. Especificar la dirección IP del agente para el modo UDP abajo
2. Configurar OpenSSH abajo
3. Instalar PAM Agent En la página opuesta
4. Para el modo UDP, realice una autenticación de prueba. Para obtener más información, consulte Utilidades de autenticación para el modo UDP En la página 43.

   Para un modo de protocolo REST, pruebe la conexión mediante el acceso a la URL del servidor REST con cualquier navegador o cliente http. Por ejemplo, ingrese https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Debido a que no está autenticando actualmente, el navegador o cliente http debe mostrar una respuesta de HTTP "prohibido" o "no autorizado".

5. Habilitar SELinux En la página 22 (si es necesario).

Especificar la dirección IP del agente para el modo UDP

Para el modo UDP, debe crear el archivo **sdopts.rec** en el mismo directorio que utiliza el archivo **sdconf.rec**. Este procedimiento no se aplica al modo REST.

Archivo	Descripción
sdopts.rec	Indica la dirección IP de la máquina donde está instalado el agente. El agente utiliza la dirección IP en el archivo **sdopts.rec** para comunicarse con RSA Authentication Manager.
sdconf.rec	Especifica las direcciones IP que son utilizadas por Authentication Manager.

Procedimiento

1. En la máquina del agente, utilice un editor de texto para crear un archivo **sdopts.rec** en la ruta donde se guardó el archivo **sdconf.rec**.
2. En el archivo, escriba:

   ```
   CLIENT_IP=x.x.x.x
   ```

   donde *x.x.x.x* es la dirección IP del host del agente.

   Nota: Utilice solamente letras mayúsculas y no incluya espacios.

3. Guarde el archivo.

Configurar OpenSSH

Si está usando OpenSSH, la suite de utilidades de red relacionadas con la seguridad basada en el protocolo Secure Shell (SSH), debe configurar este software para que funcione con PAM Agent y para mostrar los mensajes de autenticación del código de acceso a los usuarios.

Antes de comenzar

Instale OpenSSH en la máquina del agente. Para OpenSSH, incluidos los requisitos previos y el software adicional necesario para compilar el código fuente, consulte https://www.openssh.com.

Procedimiento

1. En la máquina del agente, abra el archivo **sshd_config**.
2. Configure los siguientes parámetros y guarde los cambios:

Parámetro	Configuración
UsePAM	yes
PasswordAuthentication	No
ChallengeResponseAuthentication	yes

   Si se configura el parámetro PasswordAuthentication en no, se inhabilita el indicador de contraseña de OpenSSH. En su lugar, se utiliza PAM Agent. Como resultado, al usuario se le solicita únicamente la autenticación de SecurID.

3. Reinicie sshd. Escriba:

```
service sshd restart
```

Instalar PAM Agent

Puede instalar manualmente PAM Agent en máquinas individuales, o puede elegir la instalación silenciosa para automatizar el proceso de implementación de múltiples copias del PAM Agent.

Instalar PAM Agent en una máquina

Realice esta tarea para instalar un PAM Agent. Para instalar PAM Agent en más de una máquina, consulte Instalar masivamente PAM Agent con la instalación silenciosa En la página siguiente.

Procedimiento

1. En la máquina del agente, vaya al directorio del instalador de PAM Agent.
2. Descomprima el archivo escribiendo lo siguiente:

```
tar -xvf filename.tar
```

3. Para ejecutar el script de instalación, escriba:

```
/filename/install_pam.sh
```

4. Siga los indicadores. Presione INTRO para aceptar el valor predeterminado o escriba el valor correcto.

   Para el modo UDP de RSA Authentication Manager, realice lo siguiente:

   - Acepte la licencia del software RSA.
   - Escriba 0 para seleccionar RSA Authentication Manager con el modo de autenticación del protocolo UDP.
   - Ingrese el directorio donde se encuentra **sdconf.rec**.
   - Ingrese el directorio de instalación de PAM Agent.

   Para el modo REST de RSA Authentication Manager, realice lo siguiente:

   - Acepte la licencia del software RSA.
   - Escriba 1 para seleccionar RSA Authentication Manager con el modo de autenticación del protocolo REST.

- Ingrese la URL del servidor REST para la comunicación entre el agente de autenticación y la instancia primaria.
- Escriba y si hay instancias de réplica de Authentication Manager para la conmutación por error.
- Especifique la cantidad de instancias de réplica.
- Ingrese la URL del servidor REST para cada instancia de réplica.
- Ingrese la clave del cliente (clave de acceso) para pasar de manera segura las solicitudes de autenticación a Authentication Manager.
- Ingrese el directorio y el nombre de archivo para el certificado de confianza del servidor en el agente de autenticación.
- Ingrese el ID de cliente, que es el nombre del agente de autenticación en Authentication Manager.
- Ingrese el directorio de instalación de PAM Agent.

Para el modo REST de Cloud Authentication Service, realice lo siguiente:

- Acepte la licencia del software RSA.
- Escriba 2 para seleccionar Cloud Authentication Service con el modo de autenticación del protocolo REST.
- Ingrese la URL del servidor REST para la comunicación entre el agente de autenticación y Cloud Authentication Service.
- Ingrese la clave del cliente (clave de la API de autenticación) para pasar de manera segura las solicitudes de autenticación a Cloud Authentication Service.
- Ingrese el directorio y el nombre de archivo para el certificado de confianza del servidor en el agente de autenticación.
- Ingrese el ID de grupo de usuarios para Cloud Authentication Service.
- Ingrese el nombre de la política de acceso para Cloud Authentication Service.
- Ingrese el nombre del agente de autenticación CLIENT_ID para que aparezca en las notificaciones móviles.
- Ingrese el directorio de instalación de PAM Agent.

5. Solo para el modo UDP, verifique que VAR_ACE en el archivo **/etc/sd_pam.conf**señale la ubicación correcta del archivo **sdconf.rec**. Esta es la ruta a los archivos de configuración. La ruta completa debe tener el permiso -rw------- root.

Después de finalizar

- Puede verificar la instalación mediante la comprobación del archivo **installer.log** en el directorio del instalador de PAM Agent.
- Para el modo UDP, realice una autenticación de prueba. Para obtener más información, consulte Utilidades de autenticación para el modo UDP En la página 43.
- Para un modo de protocolo REST, pruebe la conexión mediante el acceso a la URL del servidor REST con cualquier navegador o cliente http. Por ejemplo, ingrese https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Debido a que no está autenticando actualmente, el navegador o cliente http debe mostrar una respuesta de HTTP "prohibido" o "no autorizado".

Instalar masivamente PAM Agent con la instalación silenciosa

Realice esta tarea para implementar una gran cantidad de PAM Agent con información de configuración idéntica.

Por ejemplo, realice esta tarea si es necesario instalar una gran cantidad de agentes que se comunican con los mismos servidores RSA Authentication Manager o el mismo Cloud Authentication Service.

Antes de comenzar

Instale PAM Agent manualmente y registre las indicaciones. Para obtener instrucciones, consulte Instalar PAM Agent en una máquina En la página 19.

Procedimiento

1. Cree un archivo de configuración basado en texto donde especificará las opciones de configuración para el script de instalación de PAM Agent. Puede elegir cualquier nombre para el archivo de configuración, como **installoptions.conf**.
2. Abra el archivo y enumere cada opción de configuración que desea seleccionar en una línea aparte, en el mismo orden que se presentan los indicadores durante la instalación manual de PAM Agent.

   El siguiente ejemplo describe el indicador correspondiente para cada opción especificada en la configuración de UDP:

Valor de ejemplo	Opción
y	¿Desea continuar con la instalación silenciosa? (y) Este indicador siempre se incluye en primer lugar.
Accept	¿Acepta los términos y condiciones de la licencia? (Accept)
0	¿Modo de autenticación? (valor numérico para el modo deseado) 0: RSA Authentication Manager con el protocolo UDP 1: RSA Authentication Manager con el protocolo REST 2: Servicio de autenticación de nube con el protocolo REST
/var/ace	¿Cuál es el directorio que contiene sdconf.rec? (ruta del directorio)
/opt	¿Cuál es la ruta de instalación del directorio de PAM Agent? (ruta del directorio)
y	¿Desea actualizar/sobrescribir la instalación existente? (y/n)

   En este caso, el archivo de configuración basado en texto debería contener lo siguiente:

```
y
Accept
0
/var/ace
/opt
y
```

   Como otro ejemplo, para el modo REST de Authentication Manager, el archivo de configuración puede contener datos similares a lo siguiente:

```
y
Accept
```

```
1
https://am821.example.com:5555/mfa_v1_1/authn
0i78x21rih887gb48126ufxh4g63orh3a3rt28k5416a2b3jxh05h86i7gntjfh3
/var/ace/cert.pem
sp7-dp33.network.com
/opt
y
```

Nota: La cantidad y el orden de los indicadores de instalación varían en función del modo y la plataforma de PAM Agent que está instalando.

3. Vaya al directorio del instalador de PAM Agent.
4. Descomprima el archivo escribiendo lo siguiente:

   ```
   tar -xvf filename.tar
   ```

5. Para ejecutar el script de instalación, escriba:

   ```
   /filename/install_pam.sh -s < installoptions.conf
   ```

   donde ***installoptions.conf*** es el archivo de configuración que creó en el paso 1. Si el archivo de configuración está en una ubicación diferente que el directorio actual, especifique la ruta de acceso completa del archivo ***installoptions.conf***.

Habilitar SELinux

Después de instalar PAM Agent, puede habilitar SELinux (Security-Enhanced Linux).

Antes de comenzar

- En la máquina del agente, verifique que PAM Agent esté funcionando correctamente.

  Por ejemplo, realice una autenticación de prueba en el modo UDP o intente hacer ping a un servidor de Authentication Manager o a Cloud Authentication Service en el modo REST. Para obtener más información sobre las pruebas del modo UDP, consulte Utilidades de autenticación para el modo UDP En la página 43.

- Cree un respaldo de los directorios **/etc/sd_pam.conf** y **/var/ace**.
- Para evitar que se bloquee el acceso a la máquina de PAM Agent, configure las herramientas protegidas por RSA SecurID para que usen el módulo PAM estándar proporcionado con el sistema operativo y no el módulo PAM de RSA. Revierta la configuración de la herramienta para trabajar sin RSA Authentication Agent 8.1 for PAM.

  Cierre las sesiones activas mediante los módulos PAM de RSA.

Nota: Si desinstala el módulo RSA mientras existen referencias al módulo RSA en el directorio **/etc/pam.d**, se bloqueará el acceso al sistema.

Procedimiento

1. En la máquina del agente, habilite SELinux.
2. Reinstale PAM Agent a fin de crear políticas de SELinux para todas las herramientas:
   a. Para ejecutar el script de instalación, escriba:

      ```
      /<filename>/install_pam.sh
      ```

b. Escriba **y** cuando el instalador le pregunte si desea sobrescribir la instalación actual.
c. Sobrescriba la política de SELinux existente. Cuando se le solicite, escriba **y** o presione INTRO para seleccionar el valor predeterminado **yes**.

Después de finalizar

- Habilite `auth required pam_securid.so` para cualquier herramienta configurada y pruebe la autenticación.
- Si SELinux se encuentra habilitado y el archivo **cert.pem** está instalado en un directorio personalizado, en lugar del directorio **/var/ace/** predeterminado, debe habilitar la política de SELinux en el directorio personalizado.

  Ejecute los siguientes comandos, donde *cust_cert* es el directorio del certificado personalizado:

  ```
  semanage fcontext -a -t var_t '/cust_cert/cert.pem'
  ```

  ```
  restorecon -v '/cust_cert/cert.pem'
  ```

Actualizar a RSA Authentication Agent 8.1 for PAM

Puede actualizar a RSA Authentication Agent 8.1 for PAM desde la versión 7.1 parche 2 (7.1.0.2) o desde la versión 8.0.

Cuando se actualiza de 7.1.0.2, el agente actualizado utiliza RSA Authentication Manager y el protocolo UDP para la autenticación. Puede cambiar el modo de autenticación para sacar provecho de Cloud Authentication Service o Authentication Manager, y del protocolo REST. Para obtener instrucciones, consulte Cambio del modo de autenticación de PAM Agent En la página 36.

Cuando se actualiza de 8.0, el agente actualizado conserva el mismo modo de autenticación configurado para la versión anterior.

Antes de comenzar

- Debe tener permisos de raíz en el host del agente y el permiso de escritura en el directorio donde se almacena el archivo **sdconf.rec**. Este archivo se suele almacenar en el directorio predeterminado **/var/ace**.
- Respalde los archivos de configuración antes de la sobrescritura para guardar los ajustes de configuración. Para obtener más información, consulte Archivos de configuración críticos En la página 54.
- Configure las herramientas protegidas por RSA SecurID para que usen el módulo PAM estándar proporcionado con el sistema operativo y no el módulo PAM de RSA. Todas las sesiones activas que utilizan módulos PAM de RSA deben cerrarse antes de continuar con la actualización.

Procedimiento

1. En la máquina del agente, vaya al directorio del instalador de PAM Agent.
2. Descomprima el archivo escribiendo lo siguiente:

   ```
   tar -xvf filename.tar
   ```

3. Para ejecutar el script de instalación, escriba:

```
/<filename>/install_pam.sh
```

4. Sobrescriba los archivos de instalación existentes. Escriba **y** cuando el instalador le pregunte si desea sobrescribir la instalación actual.
5. Si SELinux está habilitado y planea usar el protocolo REST para la autenticación, debe sobrescribir la política de SELinux existente. Cuando se le solicite, escriba **y** o presione INTRO para seleccionar el valor predeterminado **yes**.

   Si escribe **n**, algunas herramientas no podrán autenticarse con el protocolo REST. Sin embargo, puede sobrescribir la política de SELinux existente si vuelve a ejecutar el script de instalación. Los archivos que ya se actualizaron no se verán afectados.

6. Obtenga el número de versión del agente para determinar si la actualización se realizó correctamente. Escriba:

   strings pam_securid.so | grep "Agent"

   Esto muestra el número de versión del agente instalado.

Configuración de herramientas

Debe configurar las herramientas compatibles para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Nota: La cantidad de configuraciones de usuarios simultáneos permitidos en el servidor de Unix debe configurarse para cada herramienta, el sistema operativo utilizado y los inicios de sesión simultáneos esperados para el servidor, en especial cuando se usa Cloud Authentication Service. Por ejemplo, establezca la configuración de "MaxStartups" en el archivo **/etc /ssh/sshd_config** para el protocolo SSH y la configuración de "Instancias" en el archivo **/etc/xinetd.d/telnet** para telnet.

Configurar telnet abajo

Configurar login En la página opuesta

Configurar rlogin En la página opuesta

Configurar su En la página opuesta

Configurar ssh y las herramientas relacionadas En la página 26

Configurar sudo En la página 26

Configurar ftp En la página 26

Configurar gdm En la página 26

Configurar telnet

Configure telnet para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Procedimiento

Nota: PAM Agent 8.1 no es compatible con kerberos telnet.

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **remote**.

3. Comente las líneas que empiezan con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

5. Solo para Oracle Linux 6.8 (64 bits), repita estos pasos para el archivo **/etc/pam.d/login**.

   Para todas las otras versiones de RHEL y Oracle Linux, el procedimiento está completado.

Configurar login

Configure el comando login para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **login**.
3. Comente las líneas que empiezan con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar rlogin

Configure la utilidad rlogin para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Antes de comenzar

Si no está funcionando rlogin en RHEL 6.8 u Oracle Linux 6.8, siga los procedimientos descritos en Problemas de configuración conocidos En la página 42.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **rlogin**.
3. Comente las líneas que empiezan con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar su

Configure el comando su para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **sshd**.
3. Comente todas las líneas que comiencen con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar ssh y las herramientas relacionadas

Puede configurar el protocolo SSH y las herramientas relacionadas, como scp y sftp, para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **sshd**.
3. Comente las líneas que empiezan con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar sudo

Si necesita sudo, debe configurar el comando sudo para solicitarles a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Antes de comenzar

Descargue e instale la versión compatible de sudo desde https://www.sudo.ws.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **sudo**.
3. Comente todas las líneas que comiencen con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar ftp

Configure el protocolo ftp para solicitarles a los usuarios los métodos de autenticación compatibles con RSA Authentication Manager.

No se puede usar Cloud Authentication Service para proteger ftp; sin embargo, se puede usar sftp. Para obtener instrucciones, consulte Configurar ssh y las herramientas relacionadas arriba.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Abra el archivo **vsftpd**.
3. Comente las líneas que empiezan con `auth`.
4. Agregue la línea:

```
auth required pam_securid.so
```

Configurar gdm

Puede configurar gdm para solicitar a los usuarios los métodos de autenticación compatibles con Cloud Authentication Service y RSA Authentication Manager.

Procedimiento

1. Vaya al directorio **/etc/pam.d**.
2. Modifique los archivos **gdm**,**gdm-password** y **gdm-autologin**como se indica a continuación:
   a. Abra cada archivo gdm.
   b. Comente todas las líneas que comiencen con `auth`.
   c. Agregue la línea:

      ```
      auth required pam_securid.so
      ```

Capítulo 2: Configuración de funciones

Configuración del agente y las funciones de UNIX

Puede personalizar la configuración de PAM Agent para utilizar funciones opciones de UNIX y del agente.

Nota: Antes de personalizar el agente, realice copias de respaldo de los archivos de configuración originales.

Hay múltiples archivos de configuración en el directorio **/etc/pam.d**. Cada archivo usa el nombre de la herramienta de conexión.

Para personalizar al agente, consulte lo siguiente:

Habilitar la creación de informes relacionados con el agente para RSA SecurID Authentication Agent 8.1 for PAM abajo

Habilitar la salida de depuración abajo

Habilitar el registro de seguimiento de SecurID para el modo UDP En la página opuesta

Configurar módulos apilables En la página opuesta

Utilizar contraseñas de reserva En la página 32

Habilitar la autenticación selectiva de SecurID En la página 33

Configurar el tiempo de retroceso exponencial En la página 34

Habilitar la creación de informes relacionados con el agente para RSA SecurID Authentication Agent 8.1 for PAM

Puede configurar el parámetro ENABLE_AGENT_REPORTING en el archivo **mfa_api.properties** para que se envíen los detalles del agente, como el nombre de host, la versión del agente y la versión del SO, a RSA Authentication Manager. Puede usar RSA Authentication Manager 8.3 o superior para ejecutar informes que incluyan estos detalles.

Antes de comenzar

Debe tener permisos de raíz en el equipo donde está instalado el agente y el permiso de escritura en el directorio donde se encuentra almacenado el archivo **mfa_api.properties**. De forma predeterminada, este archivo se almacena en **/var/ace/conf**.

Procedimiento

1. Vaya al directorio donde se encuentra **mfa_api.properties**. De forma predeterminada, el directorio es **/var/ace/conf**.
2. Abra **mfa_api.properties**.
3. Cambie el parámetro ENABLE_AGENT_REPORTING a 1, lo que permite la creación de informes relacionados con el agente. El valor predeterminado es 0.
4. Guarde el archivo.

   Los detalles de PAM Agent y de la máquina en la que se encuentra instalado se incluyen en los detalles de la creación de informes de PAM Agent que se envían a Authentication Manager.

Habilitar la salida de depuración

Para la solución de problemas, puede habilitar la salida de depuración para las herramientas específicas que utiliza PAM Agent.

También puede configurar el registro del sistema para que registre todos los mensajes de registro de autenticación de PAM Agent. Para obtener más información, consulte Registro para PAM Agent En la página 47.

Procedimiento

1. Vaya al directorio **/etc/** y abra el archivo **pam.d**.
2. Edite el archivo adecuado mediante la adición de un argumento de depuración para el módulo pam_securid.so. Escriba:

   ```
   auth required pam_securid.so debug
   ```

Habilitar el registro de seguimiento de SecurID para el modo UDP

Puede habilitar el registro de seguimiento de SecurID para PAM Agent y para las utilidades de autenticación acetest y acestatus. De forma predeterminada, cuando se instala PAM Agent, el registro de seguimiento de SecurID está deshabilitado.

Procedimiento

1. Vaya al directorio **/etc** y abra el archivo **sd_pam.conf**.
2. Para habilitar el registro de agente detallado y establecer el nivel de registro, configure la siguiente variable:

   `RSATRACELEVEL=value`

   Donde *value* es un ajuste de la siguiente tabla.

Valor	Descripción
0	Deshabilita el registro (valor predeterminado)
1	Registra mensajes regulares
2	Registra puntos de entrada de la función
4	Registra puntos de salida de la función
8	Todos los controles de flujo lógico utilizan este (ifs)

   Para las combinaciones, agregue los valores correspondientes. Por ejemplo, para registrar mensajes regulares y puntos de entrada de la función, establezca el valor en 3.

3. Especifique la ruta de archivo hacia donde se redirigen los registros. Establezca la variable siguiente:

   `RSATRACEDEST=filepath`

   Donde *filepath* es la ruta de archivo.

   De forma predeterminada, este valor está en blanco. Si no establece esta variable, los registros informarán un error estándar para las utilidades de autenticación acetest y acestatus, y no se generarán registros para las herramientas de autenticación, aunque se haya especificado el valor de `RSATRACELEVEL`.

4. Guarde los cambios.

Configurar módulos apilables

En una configuración apilada, use el agente para integrar el módulo de autenticación PAM de RSA SecurID con otros módulos de autenticación PAM en su ambiente. La contraseña o el código de acceso se envía de un módulo

de autenticación al siguiente. Puede configurar la prioridad de los retos de autenticación mediante la edición del archivo de configuración **/etc/pam.d/*tool name*** correspondiente.

Nota: Los argumentos use_first_pass y try_first_pass no son compatibles cuando se utiliza una configuración apilada con Cloud Authentication Service.

El agente funciona con estos argumentos:

- **use_first_pass.** El agente utiliza solamente la contraseña o el código de acceso que se transmiten desde el módulo anterior y niega el acceso si las credenciales no coinciden. Al usuario no se le vuelve a pedir la autenticación.
- **try_first_pass.** El agente utiliza la contraseña o el código de acceso que se transmiten desde el módulo anterior. Si las credenciales no coinciden, se le solicita la autenticación al usuario.
- **not_set_pass.** El agente no envía la contraseña ni el código de acceso al módulo de contraseña apilado.

Nota: Cuando los usuarios excluidos de la autenticación de SecurID realizan intentos de inicio de sesión fallidos para acceder el módulo PAM de RSA, la función de crecimiento exponencial garantiza que el módulo PAM de RSA conserve control hasta un inicio de sesión exitoso o hasta que finalice la sesión de autenticación. Para obtener más información sobre cómo configurar el tiempo de retroceso exponencial, consulte Configurar el tiempo de retroceso exponencial En la página 34.

La siguiente sección proporciona un ejemplo de cómo configurar una herramienta de conexión (inicio de sesión) en un ambiente apilado.

Procedimiento

1. Vaya a **/etc/pam.d** y abra el archivo **login**.

   Se muestra el siguiente texto:

```
#%PAM-1.0
auth required pam_securetty.so
auth required pam_stack.so service=system-auth
auth required pam_nologin.so
account required pam_stack.so service=system-auth
password required pam_stack.so service=system-auth
# pam_selinux.so close should be the first session rule
session required pam_selinux.so close
session required pam_stack.so service=system-auth
session required pam_loginuid.so
session optional pam_console.so
# pam_selinux.so open should be the last session rule
session required pam_selinux.so open
```

2. Comente las siguientes líneas:

```
auth required pam_securetty.so
auth required pam_stack.so service=system-auth
auth required pam_nologin.so
```

3. Agregue las siguientes líneas. Escriba:

```
auth required pam_securid.so
```

Utilizar contraseñas de reserva

La función de contraseña de reserva es un método de acceso de emergencia que le permite a usted, el

administrador, autenticarse en la máquina protegida donde está instalado el agente sin ingresar un código de acceso de RSA SecurID. PAM Agent permite que solo los administradores raíz utilicen contraseñas de reserva durante circunstancias imprevistas, como la pérdida de comunicación entre el agente y RSA SecurID Authentication Agent 8.1 for PAM. En estas situaciones, los administradores pueden deshabilitar temporalmente el agente si los usuarios requieren acceso inmediato a los recursos alojados.

Nota: La contraseña de UNIX es la contraseña de reserva.

Procedimiento

1. Abra el archivo apropiado en **/etc/pam.d.**
2. Agregue un argumento de reserva al módulo pam_securid.so. Escriba:

```
auth required pam_securid.so reserve
```

Habilitar la autenticación selectiva de SecurID

Puede configurar al agente para que solicite siempre o nunca la autenticación de SecurID a usuarios o grupos de UNIX específicos de manera selectiva:

Habilitar la autenticación selectiva de SecurID para los grupos de UNIX abajo

Habilitar la autenticación selectiva de SecurID para los usuarios de UNIX En la página siguiente

Nota: Cuando se encuentra habilitada la compatibilidad selectiva de grupos y la compatibilidad selectiva de usuarios, solo se habilita la compatibilidad selectiva de usuarios y se ignora la compatibilidad selectiva de grupos.

La siguiente tabla enumera los valores posibles que se pueden configurar en el archivo **sd_pam.conf**.

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	Resultado
0	0	Ninguna función está habilitada. Se solicita la autenticación de cada usuario y grupo de usuarios.
0	1	La compatibilidad selectiva de usuarios está habilitada. PAM Agent siempre les solicita a usuarios específicos de UNIX que se autentiquen con SecurID, o nunca les solicita autenticarse con SecurID.
1	0	La compatibilidad selectiva de grupos está habilitada. PAM Agent siempre les solicita a grupos específicos de UNIX que se autentiquen con RSA SecurID, o nunca les solicita autenticarse con SecurID.
1	1	La compatibilidad selectiva de usuarios está habilitada. PAM Agent siempre les solicita a usuarios específicos de UNIX que se autentiquen con SecurID, o nunca les solicita autenticarse con SecurID.

Habilitar la autenticación selectiva de SecurID para los grupos de UNIX

Puede configurar PAM Agent para que siempre o nunca solicite a grupos específicos de UNIX que se autentiquen con RSA SecurID. Cuando PAM Agent está instalado, esta función no se encuentra habilitada.

Los miembros de grupos que se excluyen de la autenticación de SecurID se pueden autenticar con credenciales de UNIX o a través de otro módulo PAM en la pila. Para ello, configure el parámetro PAM_IGNORE_SUPPORT.

Nota: No se especifique grupos de RSA Authentication Manager. Esta función es para los grupos de UNIX solamente.

Procedimiento

1. Vaya al directorio **/etc** y abra el archivo **sd_pam.conf**.
2. Establezca el parámetro ENABLE_GROUP_SUPPORT en 1. El valor predeterminado es 0.
3. Complete el parámetro LIST_OF_GROUPS.
4. Establezca el valor para el parámetro INCL_EXCL_GROUPS.
   Los valores válidos son:
   0—Disable SecurID authentication for the listed groups (opción predeterminada).
   1—Enable SecurID authentication only for the listed groups.
5. (Opcional) Establezca el parámetro PAM_IGNORE_SUPPORT.
   Los valores válidos son:
   0—Enable UNIX password authentication (opción predeterminada).
   1—Disable UNIX password authentication.
   Este parámetro se aplica solamente a los grupos que se excluyen de la autenticación de SecurID.
6. Guarde el archivo.

Habilitar la autenticación selectiva de SecurID para los usuarios de UNIX

Puede configurar PAM Agent para que siempre o nunca solicite a usuarios específicos de UNIX que se autentiquen con SecurID. Cuando PAM Agent está instalado, esta función no se encuentra habilitada.

Los usuarios que se excluyen de la autenticación de SecurID se pueden autenticar con credenciales de UNIX o a través de otro módulo PAM en la pila. Para ello, configure el parámetro PAM_IGNORE_SUPPORT_FOR_USERS.

Procedimiento

1. Vaya al directorio **/etc** y abra el archivo **sd_pam.conf**.
2. Establezca el parámetro ENABLE_USERS_SUPPORT en 1. El valor predeterminado es 0.
3. Complete el parámetro LIST_OF_USERS.
4. Establezca el valor para el parámetro INCL_EXCL_USERS.
   Los valores válidos son:
   0—Disable SecurID authentication for the listed user (opción predeterminada).
   1—Enable SecurID authentication only for the listed users.
5. (Opcional) Establezca el parámetro PAM_IGNORE_SUPPORT_FOR_USERS.
   Los valores válidos son:
   0—Enable UNIX password authentication (opción predeterminada).
   1—Disable UNIX password authentication.
   Este parámetro se aplica solamente a los usuarios que se excluyen de la autenticación de SecurID.
6. Guarde el archivo.

Configurar el tiempo de retroceso exponencial

Puede configurar el tiempo que un usuario excluido de la autenticación de RSA SecurID debe esperar antes de autenticarse después de cada intento de inicio de sesión fallido consecutivo. De forma predeterminada, los usuarios pueden reintentar la autenticación de UNIX después de un intento de inicio de sesión fallido con una demora de pow(4, failattempts) segundos. Por ejemplo, tres intentos de inicio de sesión fallidos dan como resultado una demora de 64 segundos (cuatro a la potencia de tres o 4 x 4 x 4 = 64).

Nota: El protocolo ftp no es compatible con la demora de retroceso exponencial.

Procedimiento

1. Vaya al directorio **/etc** y abra el archivo **sd_pam.conf**.
2. Establezca el parámetro BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS en *N*, como se indica a continuación:

N	**Comportamiento de la autenticación**
0	Deshabilita el reintento de autenticación de UNIX tras un intento de inicio de sesión fallido. No hay ninguna demora de autenticación para los intentos de inicio de sesión que siguen a un intento de inicio de sesión fallido.
1,2,3	Habilita el reintento de autenticación de UNIX después de un intento de inicio de sesión fallido con una demora de pow(3, failattempts) segundos.
4	Habilita el reintento de autenticación de UNIX después de un intento de inicio de sesión fallido con una demora de pow(4, failattempts) segundos.
5 o más	Habilita el reintento de autenticación de UNIX después de un intento de inicio de sesión fallido con una demora de pow(5 o más, failattempts) segundos.

Reemplazar el certificado de CA raíz de confianza del servidor

Es posible que deba reemplazar el certificado de CA raíz de confianza del servidor, por ejemplo, si se actualiza el certificado actual de RSA Authentication Manager o Cloud Authentication Service.

Para obtener instrucciones sobre cómo conseguir este certificado, consulte el artículo de la base de conocimientos How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.

Antes de comenzar

- Debe tener permisos raíz para el directorio **/var/ace** en la máquina donde está instalado PAM Agent.
- Confirme que el nuevo certificado esté en formato PEM. Si hay varios certificados de CA, deben estar concatenados en un único archivo en formato PEM.

  El formato de archivo debe ser similar a lo siguiente:

  -----BEGIN CERTIFICATE-----

  Thawte (BASE64)

  -----END CERTIFICATE-----

  -----BEGIN CERTIFICATE-----

  Entrust (BASE64)

  -----END CERTIFICATE-----

Procedimiento

1. Cambie el nombre del nuevo certificado raíz de modo que tenga el mismo nombre que el certificado que está reemplazando.
2. En la máquina donde está instalado PAM Agent, copie y reemplace ***new_cert_file*.pem** en el directorio **/var/ace/**.

Cambio del modo de autenticación de PAM Agent

Puede cambiar el modo de autenticación de PAM Agent. Por ejemplo, puede cambiar el modo si desea utilizar las opciones de autenticación expandida que se obtienen con Cloud Authentication Service. De forma predeterminada, un PAM Agent actualizado utiliza RSA Authentication Manager con el protocolo UDP.

Cambio del protocolo UDP al protocolo REST

Puede cambiar el modo de autenticación del protocolo UDP al protocolo REST para RSA SecurID Authentication Agent 8.1 for PAM o Cloud Authentication Service.

Antes de comenzar

- Debe tener permisos raíz en la máquina donde está instalado el agente.
- Debe tener permisos de escritura en el directorio donde se almacena el archivo **sdconf.rec**. De forma predeterminada, este archivo se almacena en **/etc**.
- Debe tener permisos de escritura en el directorio donde se almacena el archivo **mfa_api.properties**. De forma predeterminada, este archivo se almacena en **/var/ace/conf**.
- Recopile la información necesaria.

  Para la autenticación de Authentication Manager con el protocolo REST, solicite a su superadministrador de Authentication Manager la siguiente información.

Parámetro	Descripción
REST_URL	Dirección URL del servidor REST para la comunicación entre el agente de autenticación y la instancia primaria de Authentication Manager. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia primaria, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El valor predeterminado de *PORT* es 5555.
REPLICA_*number* Donde *number* es un número del 1 al 15.	Una URL de servidor REST para cada instancia de réplica que puede usarse para la conmutación por error. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia de réplica, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El valor predeterminado de *PORT* es 5555.

Parámetro	Descripción
CLIENT_KEY	Clave de acceso (clave del cliente) para pasar de manera segura las solicitudes de autenticación de usuarios a Authentication Manager. Este valor se genera en la consola de seguridad de la instancia primaria de Authentication Manager. Para obtener instrucciones sobre cómo conseguir la clave de acceso, consulte el siguiente tema en RSA Link: Configurar la API de autenticación de RSA SecurID para los agentes de autenticación.
CA_CERT_FILE_PATH	Directorio y nombre de archivo del certificado de confianza del servidor en el agente de autenticación. El valor predeterminado es **/var/ace/cert.pem**.
CLIENT_ID	Nombre del agente de autenticación (ID del cliente) que se creó para PAM Agent en Authentication Manager.

Para la autenticación con Cloud Authentication Service, solicite a su superadministrador de Cloud Authentication Service la siguiente información.

Parámetro	Descripción
REST_URL	Dirección URL del servidor REST para la comunicación entre el agente y Cloud Authentication Service. Utiliza el siguiente formato: `https://HOSTNAME:PORT/mfa/v1_1/authn` Para Cloud Authentication Service, obtenga el valor *HOSTNAME* del campo **Dominio del servicio de autenticación** en la pestaña **Registro** de la página de configuración para cualquier enrutador de identidad en Consola de administración de nube. El valor predeterminado de *PORT* es 443.
CLIENT_KEY	Clave de la API de autenticación (clave del cliente) creada en Consola de administración de nube para pasar de manera segura las solicitudes de autenticación a Cloud Authentication Service. Para obtener instrucciones sobre cómo conseguir la clave de la API de autenticación, consulte el siguiente tema en RSA Link: Agregar una clave de la API de autenticación de RSA SecurID.
CA_CERT_FILE_PATH	Ingrese el directorio y el nombre de archivo para el certificado de confianza del servidor en el agente de autenticación. El valor predeterminado es **/var/ace/cert.pem**.
TENANT_ID	ID de grupo de usuarios para Cloud Authentication Service. PAM Agent puede proporcionar el ID de grupo de usuarios en las solicitudes de autenticación, pero el agente no valida los datos. Actualmente, este parámetro no es compatible con Cloud Authentication Service.
ASSURANCE_POLICY_ID	Nombre de la política de acceso para Cloud Authentication Service.
CLIENT_ID	Nombre del agente de autenticación que aparecerá en las notificaciones móviles. Puede ingresar el valor que desee. Por ejemplo, PAM_Agent.

Procedimiento

1. Vaya al directorio donde se encuentra **sd_pam.conf**. La ubicación predeterminada es **/etc**.
2. Abra **sd_pam.conf**.

3. Cambie el parámetro OPERATION_MODE:
   - Para Authentication Manager con el protocolo REST, ingrese 1.
   - Para Cloud Authentication Service con el protocolo REST, ingrese 2.

   Si el parámetro OPERATION_MODE es 0, no especificado o comentado, PAM Agent vuelve al modo UDP.
4. Vaya al directorio **/var/ace/conf**. Debe actualizar el archivo **mfa_api.properties**.
5. Abra **mfa_api.properties**.
6. Elimine los comentarios para habilitar los parámetros requeridos.
7. Ingrese un valor para cada parámetro requerido.
8. Guarde el archivo.

   Ahora puede usar el protocolo REST.

Después de finalizar

Si SELinux se encuentra habilitado, debe ejecutar el siguiente comando, donde *REST_port_number* es el puerto utilizado para la autenticación de REST (el puerto predeterminado es 5555):

```
semanage port -a -t dns_port_t -p tcp REST_port_number
```

Cambio del protocolo REST al protocolo UDP

Después de instalar PAM Agent para usar el protocolo REST, puede cambiar el modo de autenticación para usar RSA SecurID Authentication Agent 8.1 for PAM con el protocolo UDP.

Después de cambiar el modo de autenticación para usar el protocolo UDP, los ajustes de configuración del protocolo REST en el archivo **mfa_api.properties** dejarán de aplicarse.

Antes de comenzar

- Se requiere el archivo de configuración de Authentication Manager, **sdconf.rec**. Puede generar este archivo en Authentication Manager u obtener este archivo a través de su superadministrador de Authentication Manager. Para obtener más información, consulte Planificación para instalar PAM Agent En la página 14.
- Debe tener permisos de raíz en la máquina donde está instalado el agente y el permiso de escritura en el directorio donde se encuentra almacenado el archivo **sd_pam.conf**. De forma predeterminada, este archivo se almacena en el directorio **/etc**.

Procedimiento

1. Vaya al directorio donde se encuentra **sd_pam.conf**. La ubicación predeterminada es **/etc**.
2. Abra **sd_pam.conf**.
3. Cambie el parámetro OPERATION_MODE a 0 para el protocolo UDP:

   ```
   OPERATION_MODE=0
   ```

   Si el parámetro OPERATION_MODE es 0, no especificado o comentado, PAM Agent vuelve al modo UDP.
4. Copie **sdconf.rec** en el directorio **/var/ace**.

   Ahora puede usar el protocolo UDP.

Cambio entre RSA Authentication Manager y Cloud Authentication Service

Puede cambiar si desea que PAM Agent utilice el protocolo REST con Authentication Manager o con Cloud Authentication Service.

Antes de comenzar

- Debe tener permisos de raíz en la máquina donde está instalado el agente.
- Debe tener permisos de escritura en el directorio donde se almacena el archivo **sdconf.rec**. De forma predeterminada, este archivo se almacena en **/var/ace**.
- Debe tener permisos de escritura en el directorio donde se almacena el archivo **mfa_api.properties**. De forma predeterminada, este archivo se almacena en **/var/ace/conf**.
- El parámetro CA_CERT_FILE_PATH para el certificado de confianza del servidor puede permanecer tal cual. Para los demás parámetros, recopile la información necesaria:
  Para la autenticación de Authentication Manager con el protocolo REST, solicite a su superadministrador de Authentication Manager la siguiente información.

Parámetro	**Descripción**
REST_URL	Dirección URL del servidor REST para la comunicación entre el agente de autenticación y la instancia primaria de Authentication Manager. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia primaria, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El valor predeterminado de *PORT* es 5555.
REPLICA_*number* Donde *number* es un número del 1 al 15.	Una URL de servidor REST para cada instancia de réplica que puede usarse para la conmutación por error. Utiliza el siguiente formato: `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` En la instancia de réplica, obtenga el valor *HOSTNAME* del campo **Nombre de dominio calificado** en la página **Administración > Red > Configuración de red de dispositivo** de la Consola de operaciones. El valor predeterminado de *PORT* es 5555.
CLIENT_KEY	Clave de acceso (clave del cliente) para pasar de manera segura las solicitudes de autenticación de usuarios a Authentication Manager. Este valor se genera en la consola de seguridad de la instancia primaria de Authentication Manager. Para obtener instrucciones sobre cómo conseguir la clave de acceso, consulte el siguiente tema en RSA Link: Configurar la API de autenticación de RSA SecurID para los agentes de autenticación.
CLIENT_ID	Nombre del agente de autenticación (ID del cliente) que se creó para PAM Agent en Authentication Manager.

Para la autenticación con Cloud Authentication Service, solicite a su superadministrador de Cloud Authentication Service la siguiente información:

Parámetro	**Descripción**
REST_URL	Dirección URL del servidor REST para la comunicación entre el agente y Cloud Authentication Service. Utiliza el siguiente formato:

Parámetro	Descripción
	`https://HOSTNAME:PORT/mfa/v1_1/authn` Para Cloud Authentication Service, obtenga el valor *HOSTNAME* del campo **Dominio del servicio de autenticación** en la pestaña **Registro** de la página de configuración para cualquier enrutador de identidad en Consola de administración de nube. El valor predeterminado de *PORT* es 443.
CLIENT_KEY	Clave de la API de autenticación (clave del cliente) creada en Consola de administración de nube para pasar de manera segura las solicitudes de autenticación a Cloud Authentication Service. Para obtener instrucciones sobre cómo conseguir la clave de la API de autenticación, consulte el siguiente tema en RSA Link: Agregar una clave de la API de autenticación de RSA SecurID.
TENANT_ID	ID de grupo de usuarios para Cloud Authentication Service. PAM Agent puede proporcionar el ID de grupo de usuarios en las solicitudes de autenticación, pero el agente no valida los datos. Actualmente, este parámetro no es compatible con Cloud Authentication Service.
ASSURANCE_POLICY_ID	Nombre de la política de acceso para Cloud Authentication Service.
CLIENT_ID	Nombre del agente de autenticación que aparecerá en las notificaciones móviles. Puede ingresar el valor que desee. Por ejemplo, PAM_Agent.

Procedimiento

1. Vaya al directorio donde se encuentra **sd_pam.conf**. La ubicación predeterminada es **/etc**.
2. Abra **sd_pam.conf**.
3. Cambie el parámetro OPERATION_MODE:
   - Para Authentication Manager con el protocolo REST, ingrese 1.
   - Para Cloud Authentication Service con el protocolo REST, ingrese 2.

   Si el parámetro OPERATION_MODE es 0, no especificado o comentado, PAM Agent vuelve al modo UDP.
4. Vaya al directorio **/var/ace/conf**. Debe actualizar los valores requeridos para los parámetros en el archivo **mfa_api.properties**.
5. Abra **mfa_api.properties**.
6. Elimine los comentarios para habilitar los parámetros requeridos y comente cualquier parámetro que ya no sea necesario.
7. Ingrese un valor para cada parámetro requerido.
8. Guarde el archivo.

   Ahora puede usar el protocolo de REST con el nuevo modo de autenticación.

Apéndice A: Solución de problemas

Problemas de configuración conocidos

Esta sección describe los problemas conocidos.

Problemas con herramientas compatibles

Herramienta	Problema conocido
dtlogin	**Problema:** Las limitaciones de visualización pueden significar dos problemas para los usuarios: • Los usuarios que se autentican no pueden visualizar el mensaje completo acerca de los métodos de autenticación disponibles. • Los usuarios de contraseñas de reserva pueden ver un campo de entrada de texto parcial en las pantallas donde no se requiere. **Solución:** Los usuarios que se autentican puede presionar INTRO, como se indica en la pantalla, para ver el mensaje completo. Los usuarios de contraseñas de reserva pueden ignorar el campo innecesario.
ftp	• **Problema:** Cuando utiliza SecurID a fin de proteger ftp, no se muestran los mensajes de error ni los indicadores de autenticación de SecurID a los usuarios. Solo se muestran los indicadores y mensajes de error estándares del sistema operativo (SO). **Solución:** Indique a los usuarios que ingresen sus nombres de usuario en el indicador de nombre de usuario del SO y sus códigos de acceso de SecurID en el indicador de contraseña del SO. Si un usuario no conoce el estado del token (por ejemplo, si el token está en el modo de código de token siguiente o en el modo de nuevo PIN), el usuario debe autenticarse con otra herramienta de conexión, como rlogin, para verificar que el PIN o el código de token continúen siendo válidos. • FTP no es compatible con la demora del retroceso exponencial. • No se puede usar Cloud Authentication Service para proteger ftp; sin embargo, se admite sftp.
ssh	**Problema:** Después de que un usuario realiza tres intentos fallidos de autenticación de SecurID en una sola sesión, la conexión se cierra. **Solución:** El usuario puede finalizar la sesión e iniciar otra.
ftp con SELinux	**Problema:**Cuando SELinux se encuentra habilitado, los usuarios de la herramienta ftp ven el mensaje "500 OOPS: cannot change directory:/home/tzfFjG_9su". **Solución:** En la máquina del agente, ejecute el comando "setsebool -P ftp_*home_dir* on", donde *home_dir* es el directorio principal del usuario.
gdm	**Problema:** Es probable que los mensajes de PAM Agent se trunquen. **Solución:**El tema gdm puede configurarse adecuadamente para evitar este problema.
rlogin	**Problema:** En RHEL 6.8, antes de que rlogin se configure para trabajar con el PAM Agent, se cierran las conexiones de rlogin. **Solución:** Asegúrese de que rlogin funcione antes de configurar PAM Agent. Siga estos pasos: 1. Abra el archivo **/etc/xinet,d/rlogin**. 2. Agregue **nice = 5** al final de la configuración de rlogin. 3. Reinicie los servicios de xinetd:

Herramienta	Problema conocido
	`service xinetd restart`
rlogin	**Problema:** En Oracle Linux 6.8, rlogin no funciona. **Solución:** Baje de categoría a los siguientes rpm: **util-linux-ng-2.17.2-12.18.el6.x86_64.rpm** **libblkid-2.17.2-12.18.el6.x86_64.rpm** **libuuid-2.17.2-12.18.el6.x86_64.rpm**
rlogin	**Problema:** Si falla el primer intento para procesar una solicitud de rlogin, la sesión se traslada al demonio de inicio de sesión. **Solución:** Si configura Linux para utilizar rlogin, debe configurar el archivo de inicio de sesión remoto en **/etc/pam.d**.
rlogin	**Problema:** Rlogin solicita una contraseña en lugar de un código de acceso cuando hay entradas ambiguas en el archivo **/etc/hosts**. **Solución:** Si aparece un nombre de máquina junto a la dirección IP de loopback y la dirección real del equipo, quite el nombre de máquina junto a la dirección IP de loopback, tras lo cual rlogin se comportará según lo esperado.
rlogin	**Problema:** Cuando un usuario intenta acceder al sistema mediante la herramienta rlogin e ingresa las credenciales incorrectas, el sistema redirige el proceso de autenticación a la herramienta telnet, y el sistema podría solicitar la contraseña o el código de acceso según la configuración de telnet. **Solución:** Cuando rlogin está protegido con SecurID, telnet también se debe proteger con SecurID y viceversa.

Actualizar y desinstalar problemas

Problema: Si intenta actualizar o desinstalar PAM Agent sin deshabilitar el módulo PAM de RSA, puede recibir el mensaje de error: "pam_securid.so is busy, not able to remove/replace".
Solución: Para resolver este problema, debe iniciar sesión con herramientas distintas a ssh y quitar **pam_securid.so**.

Utilidades de autenticación para el modo UDP

Las utilidades de autenticación se encuentran en los siguientes directorios:

- sistema operativo de 32 bits: ***pam agent installation directory*/bin/32bit**
- sistema operativo de 64 bits: ***pam agent installation directory*/bin/64bit**

Utilice estas utilidades para:

- Realizar una autenticación de prueba. Para obtener más información, consulte Ejecutar la utilidad acetest abajo.
- Verifique la comunicación entre PAM Agent y RSA Authentication Manager. Para obtener más información, consulte Ejecutar la utilidad acestatus En la página siguiente

Puede habilitar el registro de estas utilidades. Para obtener más información, consulte Habilitar el registro de seguimiento de SecurID para el modo UDP En la página 31

Ejecutar la utilidad acetest

Esta utilidad comprueba que el agente esté funcionando correctamente mediante la ejecución de una

autenticación de prueba.

Procedimiento

1. Vaya al directorio de utilidades de autenticación del PAM Agent:
   - sistema operativo de 32 bits: ***pam agent installation directory*/bin/32bit**
   - sistema operativo de 64 bits: ***pam agent installation directory*/bin/64bit**
2. Escriba:

   ```
   ./acetest
   ```

3. Escriba un nombre de usuario y un código de acceso válidos.

Si repetidamente se le deniega el acceso, pruebe la conectividad con el servidor de Authentication Manager mediante la utilidad Ejecutar la utilidad acestatus abajo o comuníquese con su administrador de Authentication Manager.

Ejecutar la utilidad acestatus

Esta utilidad comprueba el estado de cada Authentication Manager, donde PAM Agent está registrado como un host de agente. Si tiene preguntas con respecto a la información que se muestra, póngase en contacto con su administrador de Authentication Manager.

Procedimiento

1. Vaya al directorio de utilidades de PAM Agent.
2. Escriba:

   ```
   ./acestatus
   ```

La siguiente tabla enumera la información que aparece en la sección de Authentication Manager.

Información requerida	**Descripción**
Configuration Version	Versión del archivo **sdconf.rec** que está en uso. Para RSA Authentication Manager 8.0 o superior, este número es 14.
DES Enabled	Si su ambiente de configuración es compatible con los protocolos existentes, se muestra YES.
Client Retries	Cantidad de veces que PAM Agent envía datos de autenticación a Authentication Manager antes de que se produzca un tiempo de espera.
Client Timeout	Tiempo (en segundos) que PAM Agent espera antes de volver a enviar los datos de autenticación a Authentication Manager.
Server Release	Número de versión de Authentication Manager.
Communication	Versión del protocolo utilizado por Authentication Manager y PAM Agent.

La siguiente tabla enumera la información de estado que aparece en la sección de Authentication Manager.

Información de estado	**Descripción**
Server Active Address	La dirección IP que PAM Agent utiliza para comunicarse con el servidor. Esta dirección podría ser la dirección IP real del servidor que haya seleccionado, o podría ser una dirección IP de alias asignada al servidor. Una dirección IP de 0.0.0.0 indica que el

Información de estado	Descripción
	agente aún no ha recibido la comunicación desde el servidor.

La siguiente tabla enumera la información de estado del servidor que aparece en la sección de Authentication Manager.

Estado del servidor	Descripción
Available for Authentications	Este servidor está disponible para manejar las solicitudes de autenticación.
Unused	El servidor aún no ha recibido una solicitud de autenticación.
For Failover only	El servidor está reservado para el uso exclusivo de la conmutación por error.
Default Server During initial requests	Solo este servidor está disponible para manejar las solicitudes en este momento.

Utilidad de conversión para el modo UDP

La utilidad de conversión se usa cuando un PAM Agent basado en UDP coexiste con otros agentes de SecurID.

La utilidad de conversión ns_conv_util se encuentra en los siguientes directorios:

- sistema operativo de 32 bits: ***pam agent home*/bin/32bit**
- sistema operativo de 64 bits: ***pam agent home*/bin/64bit**

Procedimiento

1. Cambie el directorio de utilidades de PAM Agent.
2. Escriba:

   `./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>`

   donde *<Existing_Securid_file_path>* es la ruta donde se encuentra el archivo de SecurID actual,

   y *<New_Securid_dir_path>* es el directorio donde se debe almacenar el archivo de SecurID recientemente generado.

   Por ejemplo:

   ```
   ./ns_conv_util /var/ace/securid /var/ace_pam/
   ```

3. Si la nueva ubicación de destino no es igual a la ubicación especificada por VAR_ACE, copie el nuevo archivo de SecurID a esta ubicación.

Señas secretas de nodo para el modo UDP

La seña secreta de nodo es un clave de cifrado simétrica que RSA Authentication Manager y PAM Agent utilizan para cifrar y descifrar paquetes de datos mientras viajan por la red. Las señas secretas de nodo se requieren para los agentes que usan el protocolo UDP. La seña secreta de nodo compartida se almacena en la base de datos de Authentication Manager y en un archivo en la máquina donde PAM Agent está instalado. Para los agentes que utilizan el protocolo REST, no se utiliza un archivo de seña secreta de nodo. En lugar de una seña

secreta de nodo, se utiliza una clave negociada dinámicamente para cifrar el canal, junto con un algoritmo de cifrado seguro.

Para los agentes basados en UDP, si la seña secreta de nodo no se encuentra en el servidor de Authentication Manager o en la máquina donde PAM Agent está instalado, borre la seña secreta de nodo en la otra ubicación. Si los archivos de la seña secreta de nodo en Authentication Manager y en la máquina de PAM Agent no coinciden, borre la seña secreta de nodo en ambas ubicaciones. Después de borrar la seña secreta de nodo, debe generar una nueva.

Borrar la seña secreta de nodo de RSA SecurID Authentication Agent 8.1 for PAM

Si la seña secreta de nodo no corresponde a RSA SecurID Authentication Agent 8.1 for PAM ni a la máquina donde PAM Agent está instalado, o si la seña secreta de nodo no se encuentra en la máquina de PAM Agent, debe borrar la seña secreta de nodo de Authentication Manager. Por ejemplo, si reinstala PAM Agent, la seña secreta de nodo no estará presente en la máquina de PAM Agent.

Procedimiento

1. En la consola de seguridad de Authentication Manager, haga clic en **Acceso > Agentes de autenticación > Administrar existentes**.
2. Ubique la máquina del agente afectada y seleccione **Administrar seña secreta de nodo** en el menú desplegable.
3. Seleccione la casilla de verificación **Borrar la seña secreta de nodo** y luego haga clic en **Guardar**.

Después de finalizar

- Si hay una seña secreta de nodo en la máquina de PAM Agent, consulte Borrar la seña secreta de nodo en la máquina de PAM Agent abajo.
- Si la máquina de PAM Agent no tiene una seña secreta de nodo, siga el procedimiento Generar una nueva seña secreta de nodo En la página opuesta.

Borrar la seña secreta de nodo en la máquina de PAM Agent

Si la seña secreta de nodo no corresponde a la instancia de RSA Authentication Manager ni a la máquina de PAM Agent, o si la seña secreta de nodo no se encuentra en Authentication Manager, debe borrar la seña secreta de nodo de la máquina de PAM Agent. Por ejemplo, si instala una nueva instancia de Authentication Manager y agrega un PAM Agent existente, la seña secreta de nodo no estará presente en Authentication Manager.

Antes de comenzar

Si hay una seña secreta de nodo en Authentication Manager, consulte Borrar la seña secreta de nodo de RSA SecurID Authentication Agent 8.1 for PAM arriba.

Procedimiento

1. Inicie sesión en la máquina donde PAM Agent está instalado y busque el archivo de seña secreta de nodo, **securid**, en el directorio **/var/ace**.
2. Cambiar el nombre o eliminar el archivo de seña secreta de nodo.
3. La seña secreta de nodo también se almacena en la caché del servidor. Reinicie la máquina para borrar la seña secreta de nodo de la caché.

Después de finalizar

Generar una nueva seña secreta de nodo abajo

Generar una nueva seña secreta de nodo

Procedimiento

1. Ejecute la utilidad acetest desde la máquina de PAM Agent para generar el archivo de seña secreta de nodo. Para obtener más información, consulte Utilidades de autenticación para el modo UDP En la página 43.
2. Compruebe los registros de autenticación y asegúrese de que se ha enviado una nueva seña secreta de nodo.
3. Reinicie su máquina de PAM Agent para que el agente pueda leer el archivo de seña secreta de nodo.

Registro para PAM Agent

Si está habilitado el registro, los mensajes de autenticación de PAM Agent se guardan en el registro de sistema de forma predeterminada. Para fines de rastreo, puede configurar su registro de sistema para guardar los mensajes de registro de autenticación de PAM Agent para herramientas específicas. Consulte Habilitar la salida de depuración En la página 30.

Configurar el registro de sistema

El siguiente procedimiento envía todos los mensajes de autenticación al registro de sistema.

Procedimiento

1. Vaya al directorio **/etc/**.
2. Abra el archivo **syslog.conf**.
3. Agregue el parámetro `auth.notice` a la línea que especifica el archivo de registro de su sistema.
4. Quite el parámetro `authpriv.none` si se especifica para el archivo de registro de sistema.
5. Si utiliza telnet o login, agregue el parámetro `authpriv.notice` a la línea que especifica el archivo de registro de sistema.
6. Guarde los cambios.
7. Reinicie el demonio de syslog.

Mensajes de registro de autenticación de PAM Agent

En la tabla siguiente, se enumeran los mensajes de registro de autenticación.

Mensaje	Descripción
Cannot locate **sd_pam.conf** file	El archivo de configuración **sd_pam.conf** no está en el directorio **/etc**; **/etc** debe contener el archivo de configuración correcto para establecer VAR_ACE correctamente.
AceInitialize failed	AceInitialize es una llamada de la función API que inicializa los subprocesos de trabajo y carga los ajustes de configuración desde **sdconf.rec**. Verifique que tenga la copia más reciente de **sdconf.rec** desde su administrador de Authentication Manager y que VAR_ACE esté configurado correctamente.
Cannot communicate	Puede que los intermediadores de Authentication Manager no se hayan iniciado o se haya producido un error de red. Comuníquese con su administrador de Authentication Manager o su

Mensaje	Descripción
with RSA ACE/Server	administrador de red.
Reserve password exceeds character limit	El límite máximo de caracteres es de 256.
Invalid reserve password	La contraseña de reserva es igual a la contraseña del sistema para el host. Debe conocer esta contraseña si Authentication Manager no puede procesar las solicitudes de autenticación.
User name exceeds character limit	El nombre de usuario no debe superar los 31 caracteres.
Reserve password not allowed. User is not root.	Verifique que posea permisos de usuario raíz. Solo los usuarios de raíz pueden usar la contraseña de reserva.

Registro para el modo REST

El modo REST admite el registro adicional implementado con la biblioteca **log4cxx**. El registro de la capa de REST es independiente de los registros de PAM Agent. RollingFileAppender y SyslogAppender son compatibles. De forma predeterminada, RollingFileAppender se encuentra habilitado. Los registros se dirigen a **/var/ace/log/mfa_rest.log** con el nivel de registro configurado en INFO. La rotación basada en el tamaño se habilita con un tamaño de rotación de 10 MB.

No se admite la rotación de registros basada en tiempo. Las herramientas compatibles, como ssh y su, cargan el agente de autenticación para todas las solicitudes, por lo que PAM Agent no puede rotar los registros basado en el tiempo. PAM Agent admite la rotación de registros basada en el tamaño.

Es posible cambiar la configuración de registro predeterminada para el modo REST.

Procedimiento

1. Vaya al directorio **/var/ace/conf**.
2. Abra el archivo **log.properties**.
3. Configure las siguientes entradas para la rotación basada en el tamaño:

```
log4j.rootLogger=INFO, RestLogger

log4j.appender.RestLogger=org.apache.log4j.RollingFileAppender

log4j.appender.RestLogger.File=/var/ace/log/mfa_rest.log

log4j.appender.RestLogger.MaxFileSize=10MB

log4j.appender.RestLogger.MaxBackupIndex=10

log4j.appender.RestLogger.layout=org.apache.log4j.PatternLayout
```

```
log4j.appender.RestLogger.layout.ConversionPattern=%d [%t] %-5p
(%F:%L) - %m%n

log4j.appender.RestLogger.Append=true

log4j.appender.RestLogger.ImmediateFlush=true
```

4. Configure las siguientes entradas para admitir el registro local y remoto en syslog:

```
log4j.rootLogger=INFO,Syslog

log4j.appender.Syslog=org.apache.log4j.net.SyslogAppender

log4j.appender.Syslog.syslogHost=localhost

log4j.appender.Syslog.Facility=DAEMON

log4j.appender.Syslog.layout=org.apache.log4j.PatternLayout

log4j.appender.Syslog.layout.ConversionPattern=%d{yyyy-MM-dd
HH:mm:ss:SSS}%p [%c] %m%n
```

5. Guarde los cambios.
6. Reinicie el demonio de syslog.

Solución de problemas de SELinux

En ocasiones, SELinux (Security-Enhanced Linux) requiere procedimientos adicionales según se especifica a continuación.

Uso del protocolo REST en un agente de actualización

Para usar el protocolo REST en la autenticación, debe sobrescribir la política de SELinux existente cuando se actualiza PAM Agent. De lo contrario, algunas herramientas no podrán autenticarse con el protocolo REST.

Para actualizar la política de SELinux, puede volver a ejecutar el script de instalación y sobrescribir la política existente. Los archivos que ya se actualizaron no se verán afectados.

Habilitar la configuración de las rutas personalizadas

Cuando se habilita SELinux, la configuración de las rutas personalizadas para VAR_ACE y RSATRACEDEST no funcionan de manera predeterminada.

Procedimiento

Para habilitar la configuración de rutas personalizadas, debe ingresar los siguientes comandos, donde *<custom_directory_path>* es la ruta del archivo del directorio predeterminado VAR_ACE o RSATRACEDEST que desea usar:

```
semanage fcontext -a -t var_t <custom_directory_path>

restorecon -R <custom_directory_path>
```

Configurar los valores de tiempo de espera agotado y de reintentos para la autenticación de REST

Puede configurar cuánto tiempo tarda PAM Agent para conectarse a RSA Authentication Manager o Cloud Authentication Service, y por cuánto tiempo PAM Agent espera una respuesta. También puede configurar la cantidad de veces que PAM Agent intenta contactarse con una instancia primaria o de réplica de Authentication Manager o con Cloud Authentication Service. Estos parámetros solo se usan con el protocolo de REST.

Asegúrese de tener en cuenta la velocidad de su red. La configuración de valores de tiempo de espera agotado altos en una red más lenta permite que la autenticación se realice correctamente.

Antes de comenzar

Debe tener permisos de raíz en la máquina donde está instalado el agente y el permiso de escritura en el directorio donde se encuentra almacenado el archivo **mfa_api.properties**. De forma predeterminada, este archivo se almacena en **/var/ace/conf**.

Procedimiento

1. Vaya al directorio donde se encuentra **mfa_api.properties**. De forma predeterminada, el directorio es **/var/ace/conf**.
2. Abra **mfa_api.properties**.
3. Se pueden cambiar los siguientes parámetros:
    - CONNECT_TIMEOUT. La cantidad máxima de segundos permitidos para que el agente se conecte al servidor. El valor predeterminado es 60 segundos.
    - READ_TIMEOUT. La cantidad máxima de segundos permitidos para conectarse al servidor y leer la respuesta. El valor READ_TIMEOUT debe ser igual a la suma del valor CONNECT_TIMEOUT y el tiempo máximo permitido para la lectura de la respuesta. El valor predeterminado es 120 segundos.
    - MAX_RETRIES. La cantidad de veces que PAM Agent intenta conectarse a Authentication Manager o Cloud Authentication Service. El valor predeterminado es 3.
    - Para la fase de inicialización de la interfaz de REST de Authentication Manager, cuando PAM Agent inicia un intento de autenticación, MAX_RETRIES representa la cantidad de veces que el agente intenta contactarse con el mismo servidor antes de la conmutación por error a otro servidor. Cuando PAM Agent proporciona las credenciales de autenticación durante la fase de verificación, no se admite la conmutación por error, y MAX_RETRIES representa la cantidad de veces que el agente intenta ponerse en contacto con el mismo servidor antes de que la autenticación falle.
    - Cloud Authentication Service no admite la conmutación por error. Para las fases de la inicialización y la verificación, MAX_RETRIES representa la cantidad de veces que el agente intenta contactarse con el mismo servidor antes de que la autenticación falle.
4. Guarde el archivo.

Desinstalar RSA Authentication Agent 8.1 for PAM

Puede desinstalar manualmente PAM Agent en máquinas individuales, o elegir una desinstalación silenciosa y

automática de varias copias de PAM Agent.

La desinstalación de RSA Authentication Agent 8.1 for PAM elimina las etiquetas de SELINUX configuradas para las bibliotecas de REST que se crearon durante la instalación de PAM Agent.

Antes de comenzar

- Configure las herramientas protegidas por RSA SecurID para que usen el módulo PAM estándar proporcionado con el sistema operativo y no el módulo PAM de RSA. Todas las sesiones activas que utilizan módulos PAM de RSA deben cerrarse antes de continuar con la desinstalación. Debe deshacer los procedimientos que siguió en la sección Configuración de herramientas En la página 24.

  Nota: Si desinstala el módulo RSA mientras existen referencias a dicho módulo en el directorio **/etc/pam.d**, se bloqueará el acceso al sistema.

- Verifique que tenga permisos de raíz en el host.

Desinstalar PAM Agent de una máquina

Realice esta tarea para desinstalar un PAM Agent.

Procedimiento

1. Vaya al directorio principal de PAM Agent. Por ejemplo, **/opt/pam**.
2. Ejecute el script de desinstalación. Escriba:

   ```
   ./uninstall_pam.sh
   ```

3. Verifique que el directorio de instalación se haya eliminado. Si todavía existe el directorio, se debe quitar manualmente.
4. Para verificar que PAM Agent se haya eliminado correctamente, compruebe el archivo **/var/pam_uninstaller/uninstaller.log**.

Desinstalar masivamente PAM Agent en modo silencioso

Realice esta tarea para desinstalar una gran cantidad de PAM Agent.

Procedimiento

1. Cree un archivo de configuración basado en texto con el nombre **unconfig**. El archivo debe contener la siguiente información:

   ```
   y
   y
   y
   ```

   Cada "y" es una respuesta a un indicador:

   - Are you sure that you would like to uninstall the RSA Authentication Agent 8.1.0 [101] for PAM?
   - The RSA Authentication Agent for PAM will be deleted from the <*install_path*> directory. Ok?
   - If you uninstall the RSA module while there are references to the RSA module in the PAM configuration file (file **pam.conf** or inside the directory **pam.d**), you will be locked out of your system. Proceed with uninstall? Ok?

2. Vaya al directorio principal de PAM Agent. Por ejemplo, **/opt/pam**.

3. Ejecute el script de desinstalación. Escriba:

```
./uninstall_pam.sh < unconfig
```

Apéndice B: Archivos de configuración críticos

Archivos de configuración críticos

El directorio de instalación predeterminado de PAM Agent es **/opt/pam**, y se puede cambiar durante la instalación. De forma predeterminada, el directorio **/var/ace** incluye archivos y bibliotecas relacionados con REST. No se puede cambiar la ubicación de este directorio.

Además de los archivos binarios (**pam_securid.so**, **acetest**, **acestatus** y **ns_conv_util**), PAM Agent mantiene los archivos de configuración críticos que se enumeran en la siguiente tabla.

Archivo	Descripción
log.properties	Archivo de configuración de registro de PAM Agent para el protocolo REST. PAM Agent utiliza el archivo **log4cxx** de la biblioteca para el registro en modo REST.
mfa_ api.properties	Contiene la configuración utilizada por el protocolo REST para la autenticación en Authentication Manager y Cloud Authentication Service.
sdconf.rec	Este archivo es generado por RSA Authentication Manager y contiene la información de configuración que controla el comportamiento de PAM Agent. El permiso de este archivo debe ser -rw------- root root. Este archivo solo se usa en el modo UDP.
sdopts.rec	Este archivo se usa para el balanceo de carga manual. Contiene una lista de direcciones IP para las instancias de Authentication Manager. El permiso de este archivo debe ser -rw------- root root. Este archivo solo se usa en el modo UDP.
sdstatus.12	Este archivo es generado por la API de autenticación de PAM Agent para rastrear el último estado conocido de los servidores de Authentication Manager. El permiso de este archivo debe ser -rw------- root root.
sd_pam.conf	Contiene los ajustes de configuración que controlan el comportamiento de PAM Agent. El permiso de este archivo debe ser -rw-r--r-- root root.
securid	Este archivo contiene una clave secreta compartida que se usa para proteger la comunicación mediante el protocolo UDP entre la máquina local y Authentication Manager. El nombre de este archivo se deriva del nombre de protocolo configurado del sistema local para el puerto en el cual el agente se comunica con Authentication Manager, por lo general, mediante el archivo de "servicios". El permiso de este archivo debe ser -r-------- root root. Sin embargo, también depende de la configuración de Umask del sistema operativo. El protocolo UDP requiere este archivo. Este archivo es opcional para la autenticación con el protocolo REST.