Notas de la versión
RSA SecurID Authentication Agent 8.0 for PAM

12 de diciembre de 2017

Introducción

Este documento detalla las novedades y los cambios de RSA Authentication Manager 8.0 for PAM, así como soluciones alternativas a problemas conocidos. Lea este documento antes de instalar el software. El documento incluye las siguientes secciones:

Estas *notas de la versión* pueden ser actualizadas. Puede encontrar la versión más reciente en RSA Link que se ubica en **https://community.rsa.com/**.

Novedades de esta versión

Esta sección describe los cambios más importantes que se incorporaron en esta versión. Para obtener información detallada sobre cada uno de ellos, consulte la *Guía de instalación y configuración de RSA SecurID Authentication Agent 8.0 for PAM* pertinente.

Capacidad de autenticarse en Cloud Authentication Service o 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.

Compatibilidad con el protocolo REST de Cloud Authentication Service. Con la versión 8.0 de PAM Agent, sus usuarios pueden autenticarse en el servicio de autenticación de nube. Cloud Authentication Service utiliza métodos de autenticación de varios factores, como Approve (notificación automática optimizada para dispositivos móviles), Authenticate Tokencodes, Device Biometrics y los 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. La versión 8.0 de PAM Agent no es compatible con los tokens de FIDO, los códigos de token de SMS y los códigos de token de voz.

Compatibilidad con el protocolo REST o UDP de RSA Authentication Manager. PAM Agent puede acceder a RSA Authentication Manager con el protocolo REST, en lugar del protocolo UDP. Los PAM Agents actualizados pueden continuar utilizando el protocolo UDP.

Informe de agentes. RSA Authentication Manager 8.3 incluye informes de agentes que lo ayudan a administrar sus agentes de protocolo REST instalados. En el modo REST, PAM Agent puede enviar información adicional al servidor de Authentication Manager, como un ID de software único para cada PAM Agent instalado, el número de versión del agente, el nombre de host para la máquina en el que está instalado el agente y la información sobre el sistema operativo utilizado por el agente. Si está habilitado el agente de creación de informes en PAM Agent, se requiere RSA Authentication Manager 8.2 SP1 parche 5 o superior para evitar errores de autenticación en el modo REST.

Compatibilidad con protocolos REST. El uso de PAM Agent con el protocolo REST ofrece ventajas en comparación con el uso del protocolo UDP:

- Permite que la implementación de Authentication Manager se integre fácilmente 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 8.0 de PAM Agent utiliza el módulo de biblioteca criptográfica que cumple con la norma 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 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 actualizaciones necesarias en varios agentes.

Registros del instalador y el desinstalador. Puede verificar la instalación mediante la comprobación del archivo **installer.log** en el directorio del instalador de PAM Agent. Para verificar que PAM Agent se haya eliminado correctamente, compruebe el archivo **/var/pam_uninstaller/uninstaller.log**.

Registro adicional para el modo REST. El modo REST admite el registro adicional implementado con la biblioteca **log4cxx**. El registro del modo REST admite la rotación de registros basada en el tamaño y el registro local y remoto en syslog. Los registros y mensajes de autenticación de PAM Agent para el modo UDP permanecen igual que en las versiones anteriores de PAM Agent.

Compatibilidad con las funciones RSA SecurID Authentication Agent 7.1 for PAM. La versión 8.0 incluye funciones de la versión 7.1.x, como la compatibilidad con SELinux y con el retroceso exponencial, y una opción para una instalación silenciosa y sin supervisión.

Finalización de la compatibilidad con sistemas operativos AIX durante su vida útil. PAM Agent ya no es compatible con AIX 5.3 (32 bits y 64 bits) ni con AIX 6.1 (64 bits). RSA recomienda actualizar a una versión compatible de AIX.

Finalización de la compatibilidad con HP-UX. PAM Agent ya no es compatible con las versiones 11i v2 y 11i v3 Itanium de HP-UX (64 bits). RSA recomienda usar uno de los sistemas operativos compatibles que se enumeran continuación.

Compatibilidad con AIX. Los siguientes sistemas operativos AIX son compatibles con esta versión:

- AIX 7.1 TL3 (SP5) Power 6: 32 bits y 64 bits
- AIX 7.2 TL1 (SP2) Power 8: 32 bits y 64 bits

Compatibilidad con RHEL. Los siguientes sistemas operativos RHEL son compatibles con esta versión:

- RHEL 6.8: 32 bits y 64 bits
- RHEL 7.1: 64 bits
- RHEL 7.3: 64 bits

Compatibilidad con Oracle Linux. Los siguientes sistemas operativos Oracle Linux son compatibles con esta versión:

- Oracle Linux 6.8 de 64 bits
- Oracle Linux 7.3 de 64 bits

Compatibilidad con Solaris. Los siguientes sistemas operativos Solaris son compatibles con esta versión:

- Solaris SPARC 10 (32 bits y 64 bits). RSA recomienda actualizar a la versión 8 o superior.
- Solaris SPARC 10.5 (32 bits y 64 bits) con Zones
- Solaris SPARC 11.2 (32 bits y 64 bits)
- Solaris x86 10.5 actualización 11 (32 bits)
- Solaris x86 11.2 (32 bits)

Compatibilidad con SUSE Enterprise Linux. Los siguientes sistemas operativos SUSE Enterprise Linux son compatibles con esta versión:

- SUSE Enterprise Linux Server versión 11 SP3 o superior (32 bits y 64 bits)
- SUSE Enterprise Linux Server versión 12 (64 bits)

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

Si SELinux está habilitado en RHEL 6.8 de 32 bits, RHEL de 64 bits u Oracle Linux 6.8 de 64 bits, debe instalar los paquetes requeridos adicionales antes de instalar RSA SecurID Authentication Agent 8.0 for PAM. Para obtener más información, consulte “Requisitos de SELINUX” en la *Guía de instalación y configuración de RSA SecurID Authentication Agent 8.0 for PAM para Oracle y RHEL*.

Documentación publicada en RSA Link. En lugar de incluir la documentación en los kits de software, la documentación más reciente está disponible en RSA Link ubicado en **https://community.rsa.com/community/products/securid/authentication-agent-pam**.

Problema conocido

En esta sección, se describen los problemas que permanecen pendientes en esta versión.

La versión 7.1 parche 2 (7.1.0.2) solo se puede actualizar desde el directorio de instalación /opt predeterminado

Número de rastreo: AAPAM-677

Problema: Si la versión 7.1.0.2 está instalada en un directorio personalizado, el instalador de la versión 8.0 le solicita que instale una nueva versión 8.0. Solo se admite una actualización si la versión 7.1.0.2 está en el directorio de instalación predeterminado **/opt**.

Solución alternativa: Desinstale la versión 7.1.0.2 e instale la versión 8.0. Para obtener instrucciones, consulte la *Guía de instalación y configuración de RSA SecurID Authentication Agent 8.0 for PAM*.

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.

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.

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 **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

Aviso de propiedad intelectual

Este software contiene la propiedad intelectual de Dell Inc. o se otorga a Dell Inc. bajo licencia de terceros. El uso de este software y de la propiedad intelectual incluida se limita expresamente a los términos y condiciones del acuerdo de licencia en virtud del cual se recibe de Dell Inc. o de un representante de Dell Inc. o sus filiales.

Licencia de código abierto

Este producto se puede distribuir con código abierto y su licencia se otorga de acuerdo con la licencia de código abierto pertinente. Si desea recibir una copia de cualquier código fuente, Dell Inc. o sus filiales le proporcionarán una copia del código fuente que debe estar disponible de acuerdo con la licencia de código abierto pertinente. Dell Inc. o sus filiales pueden cobrar cargos razonables por el envío y el manejo de dicha distribución. Las solicitudes se deben enviar por escrito a Dell Legal, 176 South St., Hopkinton, MA 01748, a la atención de: Open Source Program Office.