Versionshinweise
RSA SecurID Authentication Agent 8.0 for PAM

12. Dezember 2017

Einführung

In diesem Dokument sind die Neuerungen und Änderungen in RSA Authentication Agent 8.0 for PAM sowie bekannte Probleme und Workarounds aufgeführt. Lesen Sie das Dokument, bevor Sie die Software installieren. Dieses Dokument enthält folgende Abschnitte:

Diese *Versionshinweise* werden möglicherweise aktualisiert. Die neueste Version finden Sie auf RSA Link unter **https://community.rsa.com/**.

Neuheiten in dieser Version

In diesem Abschnitt werden die Hauptänderungen ab dieser Version beschrieben. Detaillierte Informationen zu den einzelnen Änderungen finden Sie im entsprechenden *RSA SecurID Authentication Agent 8.0 for PAM – Installations- und Konfigurationsleitfaden*.

Optionale Authentifizierung beim Cloud Authentication Service oder bei RSA Authentication Manager. Sie können auswählen, ob sich PAM Agent beim Cloud Authentication Service oder bei Authentication Manager authentifiziert. Die RSA SecurID Access Enterprise Edition-Lizenz und die Premium Edition-Lizenz enthalten beide Komponenten von RSA SecurID Access. Authentication Manager muss nicht PAM Agent verwenden.

Unterstützung für das Cloud Authentication Service-REST-Protokoll. Mit Version 8.0 von PAM Agent können sich Ihre Benutzer beim Cloud Authentication Service authentifizieren. Der Cloud Authentication Service verwendet Multifaktor-Authentifizierungsmethoden wie Approve (für Mobilgeräte optimierte Push-Benachrichtigung), Authenticate Tokencodes, Gerätebiometrie und RSA SecurID-Token, um einen sicheren Zugriff auf Software as a Service (SaaS) und lokale Webanwendungen für Benutzer bereitzustellen. Version 8.0 von PAM Agent bietet keine Unterstützung für FIDO-Token, SMS-Tokencodes und Voice Tokencodes.

Unterstützung für das RSA Authentication Manager-REST-Protokoll oder das UDP-Protokoll. PAM Agent kann mit dem REST-Protokoll statt dem UDP-Protokoll auf RSA Authentication Manager zugreifen. Aktualisierte PAM Agent-Instanzen können weiterhin das UDP-Protokoll verwenden.

Agent-Reporting. RSA Authentication Manager 8.3 enthält Agent-Berichte, mit denen Sie Ihre installierten REST-Protokoll-Agents verwalten können. Im REST-Modus kann PAM Agent zusätzliche Informationen an den Authentication Manager-Server senden, z. B. eine eindeutige Software-ID-Nummer für jede installierte PAM Agent-Instanz, die Versionsnummer des Agent, den Hostnamen für den Computer, auf dem der Agent installiert ist, sowie Informationen zu dem vom Agent verwendeten Betriebssystem. Wenn das Agent-Reporting in PAM Agent aktiviert ist, ist RSA Authentication Manager 8.2 SP1 Patch 5 oder höher erforderlich, um Authentifizierungsfehler im REST-Modus zu vermeiden.

Unterstützung für das REST-Protokoll. Die Verwendung von PAM Agent mit dem REST-Protokoll bietet im Vergleich zum UDP-Protokoll einige Vorteile:

- Sie sorgt dafür, dass der Cloud Authentication Service einfacher in Ihre Authentication Manager-Bereitstellung integriert werden kann.
- Sie können einen Authentifizierungs-Agent-Datensatz in Authentication Manager hinzufügen und diesen verwenden, um mehrere installierten Agents darzustellen.
- Sie können mehrere Authentifizierungs-Agents einfacher auf derselben Hardware ausführen als mit dem UDP-Protokoll.
- Für Bereitstellungen, bei denen der Authentifizierungs-Agent IPv4-Netzwerkeinstellungen oder das IPv4-Protokoll verwenden muss, wird das TCP-Protokoll verwendet.

- In den REST-Protokollauthentifizierungsmodi wird in Version 8.0 von PAM Agent das FIPS-vorgabenkonforme kryptografische Bibliotheksmodul fips-2.0.16 mit der OpenSSL-Version 1.0.2l verwendet. Weitere Informationen finden Sie in *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* unter **https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf**.
- Es sind weniger Aktualisierungen des Authentifizierungs-Agent für neue Funktionen und Verbesserungen erforderlich als bei Authentifizierungs-Agents, die das REST-Protokoll nicht verwenden. Authentifizierungs-Agents, die das REST-Protokoll verwenden, nutzen mit höherer Wahrscheinlichkeit Änderungen in Authentication Manager und reduzieren damit die Anzahl der erforderlichen Aktualisierungen für mehrere Agents.

Protokolle des Installations- und Deinstallationsprogramms. Sie können eine Installation überprüfen, indem Sie die Datei **installer.log** im Verzeichnis mit dem PAM Agent-Installationsprogramm prüfen. Zum Überprüfen, ob PAM Agent erfolgreich entfernt wurde, prüfen Sie die Datei **/var/pam_uninstaller/uninstaller.log**.

Zusätzliche Protokollierung für den REST-Modus. Der REST-Modus unterstützt die zusätzliche Protokollierung, die mit der **log4cxx**-Bibliothek implementiert wird. Die REST-Modusprotokollierung unterstützt eine größenbasierte Protokollrotation sowie die lokale und Remoteprotokollierung an syslog. PAM Agent-Authentifizierungsmeldungen und die Protokollierung für den UDP-Modus sind mit früheren Versionen von PAM Agent identisch.

Unterstützung für RSA SecurID Authentication Agent 7.1 for PAM-Funktionen. Version 8.0 beinhaltet Funktionen von Version 7.1.x, z. B. die Unterstützung für SELinux, die Unterstützung für exponentielles Backoff und eine Option für eine automatische, unbeaufsichtigte Installation.

Einstellung des Supports für AIX-Betriebssysteme zum Ende der Lebensdauer. PAM Agent bietet keine Unterstützung mehr für AIX 5.3 (32-Bit und 64-Bit) und AIX 6.1 (64-Bit). RSA empfiehlt, ein Upgrade auf eine unterstützte Version von AIX durchzuführen.

Einstellung des Supports für HP-UX. PAM Agent bietet keine Unterstützung mehr für die HP-UX-Versionen 11i v2 und 11i v3 Itanium (64-Bit). RSA empfiehlt die Verwendung eines der unten aufgeführten unterstützten Betriebssysteme.

Unterstützung für AIX. Die folgenden AIX-Betriebssysteme werden von dieser Version unterstützt:

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

Unterstützung für RHEL. Die folgenden RHEL-Betriebssysteme werden von dieser Version unterstützt:

- RHEL 6.8: 32-Bit und 64-Bit
- RHEL 7.1: 64-Bit
- RHEL 7.3: 64-Bit

Unterstützung für Oracle Linux. Die folgenden Oracle Linux-Betriebssysteme werden von dieser Version unterstützt:

- Oracle Linux 6.8 64-Bit
- Oracle Linux 7.3 64-Bit

Unterstützung für Solaris. Die folgenden Solaris-Betriebssysteme werden von dieser Version unterstützt:

- Solaris SPARC 10 (32-Bit und 64-Bit). RSA empfiehlt Update 8 oder höher.
- Solaris SPARC 10.5 (32-Bit und 64-Bit) mit Zonen
- Solaris SPARC 11.2 (32-Bit und 64-Bit)
- Solaris x86 10.5 Update 11 (32-Bit)
- Solaris x86 11.2 (32-Bit)

Unterstützung für SUSE Enterprise Linux. Die folgenden SUSE Enterprise Linux-Betriebssysteme werden von dieser Version unterstützt:

- SUSE Enterprise Linux Server Version 11 SP3 oder höher (32-Bit und 64-Bit)
- SUSE Enterprise Linux Server Version 12 (64-Bit)

Hinweis: Die entsprechende 32-Bit- oder 64-Bit-Version von **libuuid.so** (UUID-Bibliothek) muss auf dem PAM Agent-Computer installiert sein.

Wenn SELinux unter RHEL 6.8 32-Bit, RHEL 64-Bit oder Oracle Linux 6.8 64-Bit aktiviert ist, müssen Sie vor der Installation von RSA SecurID Authentication Agent 8.0 for PAM zusätzlich erforderliche Pakete installieren. Weitere Informationen finden Sie unter „Anforderungen für SELINUX“ im *RSA SecurID Authentication Agent 8.0 for PAM – Installations- und Konfigurationsleitfaden für Oracle und RHEL*.

Auf RSA Link veröffentlichte Dokumentation. Statt die Dokumentation in die Softwarekits einzufügen, steht die neueste Dokumentation auf RSA Link unter **https://community.rsa.com/community/products/securid/authentication-agent-pam** zur Verfügung.

Bekanntes Problem

In diesem Abschnitt wird ein Problem beschrieben, das in dieser Version fortbesteht.

Ein Upgrade von Version 7.1 Patch 2 (7.1.0.2) kann nur vom Standardinstallationsverzeichnis /opt durchgeführt werden.

Rückverfolgungsnummer: AAPAM-677

Problem: Wenn Version 7.1.0.2 in einem benutzerdefinierten Verzeichnis installiert ist, fordert das Installationsprogramm von Version 8.0 Sie auf, eine neue Version von 8.0 zu installieren. Ein Upgrade wird nur unterstützt, wenn sich Version 7.1.0.2 im Standardinstallationsverzeichnis **/opt** befindet.

Workaround: Deinstallieren Sie Version 7.1.0.2 und installieren Sie Version 8.0. Anweisungen finden Sie im entsprechenden *RSA SecurID Authentication Agent 8.0 for PAM – Installations- und Konfigurationsleitfaden*.

Support und Service

Sie können auf die Community- und Supportinformationen auf RSA Link unter **https://Community.RSA.com** zugreifen. RSA Link enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme sowie Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Die Website **www.rsaready.com** des RSA Ready-Partnerprogramms enthält Informationen über Hardware- und Softwareprodukte von Drittanbietern, die für den Einsatz mit RSA-Produkten zertifiziert sind. Auf der Website werden Leitfäden für die Implementierung mit detaillierten Anweisungen sowie weitere Informationen zur Interoperabilität von RSA- und Drittanbieterprodukten bereitgestellt.

Marken

Dell, RSA, das RSA-Logo, EMC und andere Marken sind Marken von Dell Inc. oder ihren Tochtergesellschaften. Alle anderen Marken können Marken ihrer jeweiligen Inhaber sein. Eine Liste der RSA-Marken finden Sie unter **www.germany.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

Geistiges Eigentum

Diese Software enthält das geistige Eigentum von Dell Inc. oder wurde von Drittanbietern an Dell Inc. lizenziert. Die Nutzung dieser Software und des darin enthaltenen geistigen Eigentums ist ausdrücklich auf die Bedingungen der Lizenzvereinbarung beschränkt, in deren Rahmen sie durch oder im Namen von Dell Inc. oder ihrer Tochtergesellschaften bereitgestellt wird.

Open-Source-Lizenz

Dieses Produkt kann mit Open-Source-Code bereitgestellt und unter Einhaltung der anwendbaren Open-Source-Lizenzbestimmungen lizenziert werden. Wenn Sie eine Kopie des Quellcodes benötigen, stellt Ihnen Dell Inc. oder ihre Tochtergesellschaften eine Kopie des Quellcodes, der zur Verfügung gestellt werden muss, in Übereinstimmung mit den Open-Source-Lizenzbestimmungen bereit. Dell Inc. oder ihre Tochtergesellschaften kann eine für die Bereitstellung angemessene Versand- und Bearbeitungsgebühr verlangen. Bitte senden Sie eine schriftliche Anfrage an: Dell Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.