Notes de mise à jour de RSA SecurID Authentication Agent 8.0 for PAM

12 décembre 2017

Introduction

Ce document présente les nouveautés et modifications introduites dans RSA SecurID Authentication Agent 8.0 for PAM, ainsi que les problèmes connus et les procédures de contournement associées. Lisez ce document avant d'installer le logiciel. Ce document contient les sections suivantes :

Ces *Notes de mise à jour* peuvent faire l'objet d'une actualisation. La version la plus récente est disponible sur RSA link à l'adresse **https://community.rsa.com/**.

Nouveautés de cette version

Cette section décrit les principaux changements apportés à cette version. Pour obtenir des informations détaillées sur chacun d'eux, consultez le document *RSA SecurID Authentication Agent 8.0 for PAM Installation and Configuration Guide*.

Capacité à s'authentifier auprès du Service d'authentification cloud ou de RSA Authentication Manager. Vous pouvez choisir si PAM Agent s'authentifie auprès du Service d'authentification cloud ou d'Authentication Manager. La licence RSA SecurID Access Enterprise Edition et la licence Premium Edition comprennent ces deux composants de RSA SecurID Access. Il n'est pas nécessaire qu'Authentication Manager utilise PAM Agent.

Prise en charge du protocole REST du Service d'authentification cloud. Avec la version 8.0 de PAM Agent, vos utilisateurs peuvent s'authentifier auprès du Service d'authentification cloud. Le Service d'authentification cloud utilise des méthodes d'authentification à plusieurs facteurs, par exemple Approuver (notification push optimisée pour les mobiles), codes de token Authenticate, données biométriques de périphérique et tokens RSA SecurID afin d'aider à sécuriser l'accès au logiciel en tant que service (SaaS) et aux applications Web sur site pour les utilisateurs. La version 8.0 de PAM Agent ne prend pas en charge les Tokens FIDO, les codes de token SMS et les codes de token Voice.

Prise en charge du protocole REST ou UDP de RSA Authentication Manager. PAM Agent peut accéder à RSA Authentication Manager avec le protocole REST au lieu du protocole UDP. Les instances PAM Agent mises à niveau peuvent continuer à utiliser le protocole UDP.

Reporting de l'agent. RSA Authentication Manager 8.3 inclut des rapports d'agent qui vous aident à gérer vos agents de protocole REST installés. En mode REST, PAM Agent peut envoyer des informations supplémentaires au serveur Authentication Manager, par exemple un numéro d'ID de logiciel spécifique pour chaque instance PAM Agent installée, le numéro de version de l'agent, le nom d'hôte de la machine sur laquelle l'agent est installé, ainsi que des informations sur le système d'exploitation utilisé par l'agent. Si le reporting de l'agent est activé sur PAM Agent, RSA Authentication Manager 8.2 SP1 Patch 5 ou une version supérieure est requis pour éviter les erreurs d'authentification en mode REST.

Prise en charge du protocole REST. Il est plus avantageux d'utiliser PAM Agent avec le protocole REST qu'avec le protocole UDP :

- Simplifie l'intégration du déploiement d'Authentication Manager avec le Service d'authentification cloud.
- Vous pouvez ajouter et mettre à jour un enregistrement de l'agent d'authentification dans Authentication Manager, puis l'utiliser pour représenter plusieurs agents installés.
- Le protocole UDP vous permet d'exécuter plus facilement plusieurs agents d'authentification sur le même matériel.
- Utilise le protocole TCP pour les déploiements qui nécessitent que les agents d'authentification utilisent les paramètres réseau IPv4 ou le protocole IPv4.

- Dans les modes d'authentification du protocole REST, la version 8.0 de PAM Agent utilise le module de bibliothèque cryptographique compatible FIPS-2.0.16 avec la version OpenSSL 1.0.2l. Pour plus d'informations, consultez la section *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* à l'adresse **https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf**.
- Nécessite moins de mises à jour de l'agent d'authentification pour les nouvelles fonctionnalités et améliorations que les agents d'authentification qui n'utilisent pas le protocole REST. Les agents d'authentification qui utilisent le protocole REST sont plus susceptibles de tirer parti des modifications introduites dans Authentication Manager, ce qui réduit le nombre de mises à jour requises sur plusieurs agents.

Fichiers log du programme d'installation et du programme de désinstallation. Vous pouvez vérifier une installation en consultant le fichier **installer.log** dans le répertoire qui contient le programme d'installation de PAM Agent. Pour vérifier que PAM Agent a bien été supprimé, consultez le fichier **/var/pam_uninstaller/uninstaller.log**.

Consignation supplémentaire pour le mode REST. Le mode REST prend en charge la consignation supplémentaire mise en œuvre avec la bibliothèque **log4cxx**. La consignation de mode REST prend en charge la rotation des journaux basée sur la taille de journal et la consignation locale et distante dans le syslog. Les messages d'authentification de PAM Agent et la consignation pour le mode UDP restent identiques à ceux présents dans les versions précédentes de PAM Agent.

Prise en charge de RSA SecurID Authentication Agent 7.1 pour les fonctions de PAM. La version 8.0 inclut des fonctions de la version 7.1.x, par exemple la prise en charge de SELinux, celle d'Exponential Backoff, ainsi qu'une option d'installation sans assistance et en mode silencieux.

Fin de la prise en charge des systèmes d'exploitation AIX en fin de vie. PAM Agent n'est plus compatible avec AIX 5.3 (32 bits et 64 bits) et AIX 6.1 (64 bits). RSA vous recommande de mettre à niveau vers une version d'AIX prise en charge.

Fin de la prise en charge de HP-UX. PAM Agent n'est plus compatible avec HP-UX versions 11i v2 et 11i v3 Itanium (64 bits). RSA vous recommande d'utiliser l'un des systèmes d'exploitation pris en charge répertoriés ci-dessous.

Prise en charge d'AIX. Les systèmes d'exploitation AIX suivants sont pris en charge par cette version :

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

Prise en charge de Red Hat Enterprise Linux. Les systèmes d'exploitation Red Hat Enterprise Linux suivants sont pris en charge par cette version :

- Red Hat Enterprise Linux 6.8 : 32 bits et 64 bits
- Red Hat Enterprise Linux 7.1 : 64 bits
- Red Hat Enterprise Linux 7.3 : 64 bits

Prise en charge d'Oracle Linux. Les systèmes d'exploitation Oracle Linux sont pris en charge par cette version :

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

Prise en charge de Solaris. Les systèmes d'exploitation Solaris suivants sont pris en charge par cette version :

- Solaris SPARC 10 (32 bits et 64 bits). RSA recommande Update 8 ou une version supérieure.
- Solaris SPARC 10.5 (32 bits et 64 bits) avec Zones
- Solaris SPARC 11.2 (32 bits et 64 bits)
- Solaris x86 10.5 Mise à jour 11 (32 bits)
- Solaris x86 11.2 (32 bits)

Prise en charge de SUSE Enterprise Linux. Les systèmes d'exploitation SUSE Enterprise Linux suivants sont pris en charge par cette version :

- SUSE Enterprise Linux Server version 11 SP3 ou une version supérieure (32 bits et 64 bits)
- SUSE Enterprise Linux Server version 12 (64 bits)

Remarque : La version 32 bits ou 64 bits correspondante de **libuuid.so** (bibliothèque UUID) doit être installée sur la machine de PAM Agent.

Si SELinux est activé sur RHEL 6.8 32 bits, RHEL 64 bits ou Oracle Linux 6.8 64 bits, vous devez installer les packages requis supplémentaires avant d'installer RSA SecurID Authentication Agent 8.0 for PAM. Pour plus d'informations, consultez la section Configuration SELINUX requise dans le document *Guide d'installation et de configuration de RSA SecurID Authentication Agent 8.0 for PAM pour Oracle et Red Hat Enterprise Linux*.

Documentation publiée sur RSA Link. Au lieu d'inclure la documentation dans les kits logiciels, la documentation la plus récente est disponible sur RSA Link à l'adresse **https://community.rsa.com/community/products/securid/authentication-agent-pam**.

Problème connu

Cette section décrit un problème non résolu dans cette version.

La version 7.1 Patch 2 (7.1.0.2) ne peut être mise à niveau que depuis le répertoire d'installation /opt par défaut

Numéro de suivi : AAPAM-677

Problème : Si la version 7.1.0.2 est installée dans un répertoire personnalisé, le programme d'installation de la version 8.0 vous invite à installer une nouvelle version 8.0. La mise à niveau n'est prise en charge que si la version 7.1.0.2 se trouve dans le répertoire d'installation ***/* opt** par défaut.

Contournement : Désinstallez la version 7.1.0.2 et installez la version 8.0. Pour savoir comment procéder, consultez le document approprié *Guide d'installation et de configuration de RSA SecurID Authentication Agent 8.0 for PAM*.

Support et service

Vous pouvez accéder à la communauté et aux informations de support sur RSA Link à l'adresse **https://community.rsa.com**. RSA Link contient une base de connaissances qui répond aux questions courantes et fournit des solutions aux problèmes connus, de la documentation produit, des discussions communautaires et la gestion de dossiers.

Le site Web du programme Partenaires technologiques RSA Ready, accessible à l'adresse **www.rsaready.com**, fournit des informations concernant des produits matériels et logiciels tiers certifiés pour fonctionner avec les produits RSA. Ce site Web met à disposition des guides d'implémentation contenant des instructions détaillées et d'autres informations sur l'interopérabilité des produits RSA avec ces produits tiers.

Marques commerciales

Clause de propriété intellectuelle

Licence Open Source