Notes de mise à jour

RSA® Authentication Agent 2.0 for Citrix StoreFront

Mars 2019

Introduction

Lisez ce document avant d'installer le logiciel. Il fournit des informations sur RSA Authentication Agent for Citrix StoreFront, ainsi que les procédures de contournement des problèmes connus et 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/**.**

Présentation du produit

RSA Authentication Agent for Citrix StoreFront (l'Agent for Citrix StoreFront) est le logiciel d'authentification qui fournit à Citrix StoreFront des méthodes supplémentaires pour authentifier les utilisateurs à l'intérieur ou l'extérieur du pare-feu d'entreprise. Lorsque les utilisateurs tentent d'accéder à un magasin StoreFront, ils indiquent leurs noms d'utilisateur et leurs mots de passe pour l'authentification principale. L'Agent for Citrix StoreFront les invite alors à effectuer une ou plusieurs méthodes d'authentification supplémentaires, selon le mode d'authentification configuré.

Cet agent prend en charge les modes d'authentification suivants :

- **Service d'authentification Cloud (CAS) RSA.** L'agent se connecte à votre déploiement existant du service d'authentification Cloud, qui prend en charge les méthodes d'authentification suivantes :
  - Approuver
  - Authenticate Tokencode
  - Données biométriques
  - Code de token SMS
  - Code de token vocal
  - RSA SecurID Token (nécessite l'intégration entre le service d'authentification Cloud et RSA Authentication Manager)
- **RSA Authentication Manager avec le protocole REST (AM REST).** L'agent se connecte à votre déploiement RSA Authentication Manager existant à l'aide du protocole REST, qui prend en charge les méthodes d'authentification suivantes :
  - RSA SecurID Token
  - Authenticate Tokencode (nécessite l'intégration entre le service d'authentification Cloud et RSA Authentication Manager)

- **RSA Authentication Manager avec le protocole UDP (AM UDP).** L'agent se connecte à votre déploiement RSA Authentication Manager existant à l'aide du protocole UDP, qui prend en charge les méthodes d'authentification suivantes :
    - RSA SecurID Token
    - Authentification basée sur le risque (RBA)

Pour tout mode d'authentification, si vous souhaitez étendre l'authentification aux utilisateurs situés à l'extérieur du pare-feu de l'entreprise, vous devez utiliser l'agent parallèlement à Citrix NetScaler Gateway™ et Citrix Delegated Forms Authentication (DFA).

Nouveautés de cette version

Cette section décrit les fonctions majeures et les modifications principales ajoutées à cette version. Pour plus d'informations sur chaque fonction, consultez le *Guide d'administration de RSA Authentification Agent 2.0 for Citrix StoreFront*.

Modes d'authentification

L'agent prend en charge trois modes d'authentification :

- Service d'authentification Cloud (CAS) RSA.
- RSA Authentication Manager avec le protocole REST (AM REST).
- RSA Authentication Manager avec le protocole UDP (AM UDP).

Reporting d'agent

En mode AM REST, l'agent envoie des informations telles que le nom d'hôte, la version de l'agent et la version du système d'exploitation à Authentication Manager pour vous aider à gérer vos agents de protocole REST qui sont installés. Vous pouvez exécuter des rapports incluant les détails suivants à l'aide d'Authentication Manager 8.4 ou une version supérieure.

Prise en charge du protocole TLS 1.2

L'agent utilise le protocole de chiffrement TLS 1.2 pour les communications sécurisées.

Prise en charge de l'environnement de système d'exploitation compatible FIPS

Vous pouvez configurer le système d'exploitation pour qu'il fonctionne avec l'agent en mode FIPS (Federal Information Processing Standard). FIPS est une norme de sécurité informatique de l'administration des États-Unis qui est utilisée pour approuver les modules cryptographiques.

Collecte des risques pour le service d'authentification Cloud

L'agent prend en charge la collecte des données d'empreintes digitales des périphériques et d'autres informations lors de l'authentification. Le service d'authentification Cloud peut utiliser ces informations pour établir le niveau de fiabilité d'identité d'un utilisateur. Les règles d'accès peuvent utiliser l'attribut de fiabilité d'identité pour permettre aux utilisateurs disposant d'une haute fiabilité d'identité de s'authentifier plus facilement.

Personnalisation de la séquence d'invite de mot de passe Windows

Dans le cas d'un déploiement en mode CAS, vous pouvez choisir si l'agent invite les utilisateurs à saisir leurs mots de passe Windows au début du processus d'authentification ou après avoir effectué toutes les autres méthodes d'authentification requises.

Toutes les options de configuration de l'Agent intégrées à la console de gestion Citrix StoreFront

RSA Control Center est obsolète pour cette version de l'agent. Toutes les fonctions existantes de RSA Control Center et les nouvelles options de configuration de l'agent sont désormais intégrées avec la console de gestion Citrix StoreFront.

Coexistence avec RSA Authentication Agent 7.4.2 for Microsoft Windows

Vous pouvez installer l'Agent for Citrix StoreFront sur un serveur qui est également protégé par l'Agent for Microsoft Windows 7.4.2.

Prise en charge de la mise à niveau de l'Agent for Citrix StoreFront version 1.5

Si l'Agent for Citrix StoreFront version 1.5 est déjà installé sur votre serveur Citrix StoreFront, le programme d'installation version 2.0 conserve les paramètres précédents, met à niveau l'agent et configure automatiquement le mode UDP.

Options d'équilibrage de charge pour le mode AM REST

Lorsque l'agent est installé en mode AM REST, il prend en charge les schémas d'équilibrage de charge suivants :

- **Weighted Round Robin (Permutation circulaire pondérée) (par défaut).** L'agent mesure régulièrement le temps nécessaire à chaque serveur pour traiter une demande d'authentification et distribue plus de demandes sur les serveurs rapides et moins de demandes sur les serveurs lents.
- **Round Robin (Permutation circulaire).** L'agent distribue les demandes à chaque serveur dans l'ordre dans lequel les serveurs ont été ajoutés par l'administrateur.

Utilisation du secret de nœud existant configuré pour l'Agent pour Microsoft Windows

Si l'Agent for Microsoft Windows est déjà installé et configuré avec un secret de nœud sur le serveur Citrix StoreFront, l'Agent for Citrix StoreFront inclut une option permettant d'utiliser le même secret de nœud pour activer la fonction WPI en mode AM REST.

Gestion de la fonction WPI au niveau de l'Agent pour le mode AM REST

La fonction WPI peut être activée ou désactivée au niveau de l'Agent dans la page Manage SecurID Options de la console de gestion Citrix StoreFront.

Conditions requises

RSA Authentication Agent for Citrix StoreFront nécessite les composants suivants :

Composants système

- Un des systèmes d'exploitation suivants
  - Windows Server 2016
  - Windows Server 2012 R2
  - Windows Server 2012
  - Windows Server 2008 R2

  Remarque : Le mode Windows Server Core n'est pas pris en charge.
- L'une des versions Citrix StoreFront suivantes :
  - 3.13 (compatible avec tous les systèmes d'exploitation Windows répertoriés ci-dessus)
  - 3.16 (fonctionne avec Windows Server 2012 R2 et 2016 uniquement)
- Microsoft PowerShell 3.0 ou une version ultérieure
- Microsoft .NET Framework 4.5 ou une version ultérieure

Outre la configuration matérielle imposée par les composants ci-dessus, l'agent requiert au moins 50 Mo d'espace disque disponible.

Navigateurs Web pris en charge

- Edge 41 sur Windows 10
- Internet Explorer 11
- Google Chrome 71
- Mozilla Firefox 64
- Safari sur OS X
- Navigateur Web Android sur Android 9
- Safari sur iOS 12.0.1

Remarque : JavaScript doit être activé dans le navigateur.

Contenu de l'emballage

RSA Authentication Agent for Citrix StoreFront est disponible dans les Téléchargements RSA Authentication Agent for Citrix StoreFront sur RSA Link.

Le dossier du produit de l'agent contient les dossiers suivants :

Dossier	Description
AuthenticationManagerRBAHelper	Contient le package du programme d'installation Windows pour l'installation de RSA Authentication Manager. Aide de l'authentification basée sur le risque (RBA) pour les ordinateurs 64 bits.

Documentation	Contient la documentation produit.
Licences	Contient le contrat de licence RSA (**shrinkwrap-license-combined.pdf**).
NodeSecretLoadUtility	Contient l'utilitaire de chargement du secret de nœud (**agent_nsload.exe**) pour ordinateurs 32 bits et 64 bits. Vous pouvez utiliser cet utilitaire pour copier en toute sécurité le secret de nœud à partir d'un serveur Authentication Manager vers un hôte d'agent avant d'utiliser l'authentification RSA SecurID. L'utilitaire de chargement du secret de nœud n'est pas nécessaire pour créer un secret de nœud. Pour plus d'informations, consultez le *Guide d'installation et d'administration*. Remarque : Vous devez utiliser l'utilitaire de chargement du secret de nœud lors de l'installation de l'Agent sur un groupe de serveurs Citrix StoreFront.
x64	Contient le package du programme d'installation Windows pour l'installation de RSA Authentication Agent for Citrix StoreFront sur les ordinateurs 64 bits.

Documentation

La documentation produit est disponible sur RSA Authentication Agent for Citrix StoreFront sur RSA Link.

La documentation comprend les éléments suivants :

- *Notes de mise à jour*
- *Guide d'installation et d'administration*
- *Aide de RSA Authentication Agent for Citrix StoreFront* (installée avec le produit)

Problèmes connus

Cette section répertorie les problèmes connus et leurs solutions de contournement.

La règle « Envoyer le domaine et le nom d'utilisateur à Authentication Manager » ne peut pas prendre en charge les comptes utilisateur RSA Authentication Manager qui utilisent le format UPN pour le nom d'utilisateur

Numéro de suivi : AACTX-5

Problème : L'Agent for Citrix StoreFront inclut une règle « Envoyer le domaine et le nom d'utilisateur à Authentication Manager » qui peut être configurée via la console de gestion Citrix StoreFront. Lorsque cette règle est activée, l'Agent inclut le nom du domaine dans le nom d'utilisateur RSA SecurID qu'il envoie à RSA Authentication Manager. L'Agent envoie le nom au format domain_name\user_name. Il n'existe aucun moyen de configurer l'Agent pour qu'il envoie le nom d'utilisateur RSA SecurID au format UPN (user_name@domain_name).

Contournement : L'administrateur Authentication Manager peut créer des comptes utilisateur au format domain_name\user_name, puis configurer les alias de connexion au format UPN pour ces comptes utilisateur.

Lorsque la limite par défaut de 25 tentatives d'authentification simultanées est atteinte, les performances de l'authentification se dégradent et les tentatives d'authentification supplémentaires peuvent échouer.

Numéro de suivi : AACTX-6

Problème : L'Agent for Citrix StoreFront prend en charge jusqu'à 25 tentatives d'authentification simultanées par défaut. Lorsque cette limite est atteinte, les utilisateurs peuvent constater une dégradation des performances d'authentification ou l'échec de l'authentification.

Contournement : Pour remplacer la limite par défaut des tentatives d'authentification simultanées, procédez comme suit :

1. Dans le panneau de configuration Windows, cliquez sur **Système et sécurité > Paramètres système avancés**.
2. Cliquez sur **Variables d'environnement**…
3. Sous Variables système, cliquez sur **Nouvelle**...
4. Dans le champ **Nom de la variable**, indiquez `RSA_DA_API_THREAD_POOL`.
5. Dans le champ **Valeur de la variable**, indiquez le nombre de connexions simultanées que vous souhaitez autoriser.

   Remarque : RSA dispose d'un logiciel Agent for Citrix StoreFront qualifié avec jusqu'à 400 connexions simultanées.

Problèmes résolus

Authentication Agent for Citrix StoreFront contient des correctifs pour les problèmes suivants :

AACTX-2 : lorsque vous modifiez l'emplacement du fichier log de trace d'Agent for Citrix StoreFront dans la page Manage SecurID Options, le service d'authentification RSA SecurID est redémarré automatiquement et la modification de l'emplacement prend effet.

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 de partenariat 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

Dell, RSA, le logo RSA, EMC et les autres marques commerciales citées sont des marques commerciales de Dell Inc. ou de ses filiales. Toutes les autres marques commerciales éventuellement citées sont la propriété de leurs détenteurs respectifs. Pour obtenir la liste des marques commerciales de RSA, consultez la rubrique correspondante sur www.france.emc.com/legal/emc-corporation-trademarks.htm.

Clause de propriété intellectuelle

Ce logiciel contient la propriété intellectuelle de Dell Inc. ou est concédé sous licence à Dell Inc. par des tiers. L'utilisation de ce logiciel et la propriété intellectuelle incluse sont expressément limitées aux conditions du contrat de licence sous lequel le logiciel a été fourni par ou au nom de Dell Inc. ou de ses filiales.

Licence Open Source

Ce produit peut être distribué avec un code Open Source qui vous est octroyé sous licence conformément à la licence Open Source applicable. Si vous souhaitez obtenir une copie du code source, adressez-vous à Dell Inc. ou ses filiales, qui vous la fourniront selon les termes de la licence Open Source applicable. Dell Inc. ou ses filiales peuvent prélever les frais de gestion et d'expédition jugés raisonnables pour cette distribution. Envoyez les demandes par écrit à Dell Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office