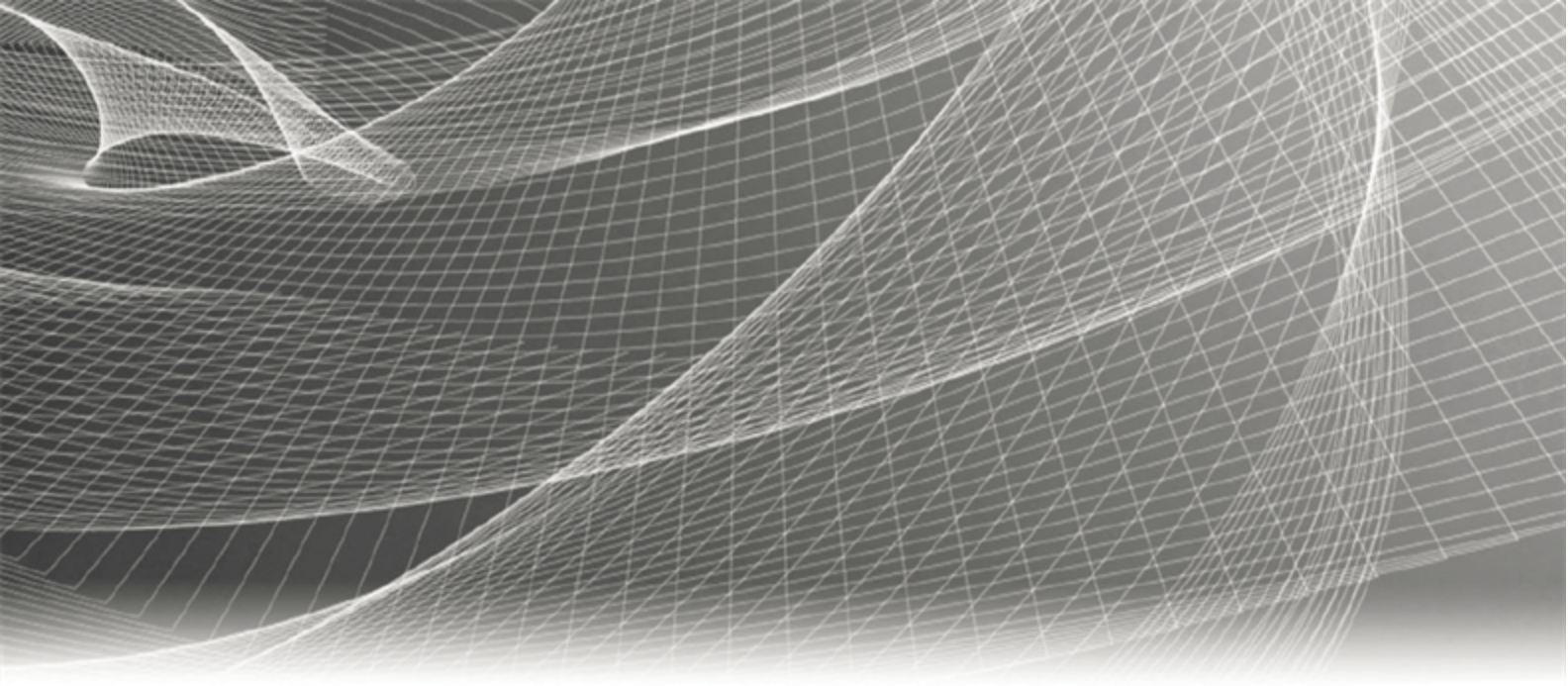

RSA SECURID® ACCESS

RSA® Agent d'authentification 8.1 pour PAM

Guide d’installation et de configuration pour SUSE

Informations de contact

RSA Link à l'adresse https://community.rsa.com 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.

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. D'autres marques éventuellement citées sont la propriété de leurs détenteurs respectifs. Pour obtenir la liste des marques commerciales de RSA, rendez-vous à l'adresse suivante : france.emc.com/legal/emc-corporation-trademarks.htm.

Contrat de licence

Ce logiciel et la documentation qui l'accompagne sont la propriété de Dell Inc. ou de ses filiales, et considérés comme confidentiels. Délivrés sous licence, ils ne peuvent être utilisés et copiés que conformément aux modalités de ladite licence et moyennant l'inclusion de la note de copyright ci-dessous. Ce logiciel et sa documentation, y compris toute copie éventuelle, ne peuvent pas être remis ou mis de quelque façon que ce soit à la disposition d'un tiers.

Aucun droit ou titre de propriété sur le logiciel ou sa documentation ni aucun droit de propriété intellectuelle ne vous est cédé par la présente. Toute utilisation ou reproduction non autorisée de ce logiciel et de sa documentation peut faire l'objet de poursuites civiles et/ou pénales.

Ce logiciel est modifiable sans préavis et ne doit nullement être interprété comme un engagement de la part de Dell Inc.

Licences tierces

Ce produit peut inclure des logiciels développés par d'autres entreprises que RSA. Le texte des contrats de licence applicables aux logiciels tiers présents dans ce produit peut être consulté sur la page de la documentation produit du site RSA Link. En faisant usage de ce produit, l'utilisateur convient qu'il est pleinement lié par les conditions des contrats de licence.

Remarque sur les technologies de chiffrement

Ce produit peut intégrer une technologie de chiffrement. Étant donné que de nombreux pays interdisent ou limitent l'utilisation, l'importation ou l'exportation des technologies de chiffrement, il convient de respecter les réglementations en vigueur lors de l'utilisation, de l'importation ou de l'exportation de ce produit.

Distribution

L'utilisation, la copie et la diffusion de tout logiciel Dell décrit dans cette publication nécessitent une licence logicielle en cours de validité.

Dell Inc. estime que les informations figurant dans ce document sont exactes à la date de publication. Ces informations sont modifiables sans préavis.

LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION SONT FOURNIES « EN L'ÉTAT ». DELL INC. NE FOURNIT AUCUNE DÉCLARATION OU GARANTIE D'AUCUNE SORTE CONCERNANT LES INFORMATIONS CONTENUES DANS CETTE PUBLICATION ET REJETTE PLUS SPÉCIALEMENT TOUTE GARANTIE IMPLICITE DE QUALITÉ COMMERCIALE OU D'ADÉQUATION À UNE UTILISATION PARTICULIÈRE..

Octobre 2018

Sommaire

Préface **7**
Audience 7
Support et service 7
Programme de partenariat RSA Ready 7
Chapitre 1: Installation de PAM Agent **9**
Présentation de RSA Authentication Agent 8.1 for PAM 10
Modes d'authentification 11
Workflow de PAM Agent 11
Configuration logicielle requise 12
Systèmes d'exploitation requis 12
Version prise en charge RSA Authentication Manager 12
Version prise en charge Service d'authentification cloud 13
Conditions de certification 13
Outils pris en charge 13
Prise en charge de OpenSSH (facultatif) 14
Planification de l'installation de PAM Agent 14
Installation de RSA Authentication Agent 8.1 for PAM 17
Spécification de l'adresse IP d'Agent pour le mode UDP 17
Configurer OpenSSH 18
Installer PAM Agent 18
Installation de PAM Agent sur une seule machine 19
Installation en masse de PAM Agent en mode silencieux 20
Mise à niveau vers RSA Authentication Agent 8.1 for PAM 22
Vérification des paramètres AppArmor 23
Configuration des outils 23
Configuration de telnet 23
Configurer la connexion 24
Configuration de rlogin 24
Configuration de su 24
Configuration de ssh et des outils connexes 24
Configuration de sudo 25

Configurer ftp 25
Configurer gdm 25
Configurer xdm 26
Chapitre 2: Configurer les fonctions **27**
Configuration des fonctions Agent et UNIX 28
Activation du reporting d'agent pour RSA SecurID Authentication Agent 8.1 for PAM 28
Activation de la sortie de débogage 28
Activer la consignation de trace SecurID pour le mode UDP 29
Configuration des modules empilables 29
Utilisation de mots de passe de réserve 30
Activation de l'authentification SecurID sélective 31
Activer l'authentification SecurID sélective pour les groupes UNIX 31
Activer l'authentification SecurID sélective pour les utilisateurs UNIX 32
Configurer l'intervalle exponentiel 32
Remplacer le certificat d'autorité de certification racine de confiance du serveur 33
Modification du mode d'authentification PAM Agent 34
Passer du protocole UDP au protocole REST 34
Passer du protocole REST au protocole UDP 36
Basculer entre RSA Authentication Manager et Service d'authentification cloud 37
Annexe A : Résolution des problèmes **39**
Problèmes connus liés à la configuration 40
Problèmes liés aux outils pris en charge 40
Problèmes de mise à niveau et de désinstallation 41
Utilitaires d'authentification pour le Mode UDP 41
Exécuter l'utilitaire acetest 41
Exécuter l'utilitaire acestatus 42
Utilitaire de conversion pour le mode UDP 43
Secrets de nœud pour le mode UDP 43
Effacer le secret de nœud dans RSA SecurID Authentication Agent 8.1 for PAM 43
Effacer le secret de nœud sur l'ordinateur PAM Agent 44
Générer un nouveau secret de nœud 44
Consignation pour PAM Agent 44
Messages log d'authentification de PAM Agent 45

Consignation pour le mode REST 45
Configuration du délai d'expiration et du nombre de nouvelles tentatives pour l'authentification REST .. 46
Désinstallation de RSA Authentication Agent 8.1 for PAM 47
Désinstaller PAM Agent sur un seul ordinateur 48
Désinstallation en masse de PAM Agent en mode silencieux 48
Annexe B : Fichiers de configuration critiques 49
Fichiers de configuration critiques 50

Préface

Audience

Ce guide est destiné aux administrateurs système et réseau qui installent, mettent à niveau et résolvent les problèmes de RSA SecurID® Authentication Agent for PAM (module d’authentification enfichable).

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.

Programme de partenariat RSA Ready

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.

Chapitre 1: Installation de PAM Agent

Présentation de RSA Authentication Agent 8.1 for PAM 10
Configuration logicielle requise 12
Planification de l'installation de PAM Agent 14
Installation de RSA Authentication Agent 8.1 for PAM 17
Mise à niveau vers RSA Authentication Agent 8.1 for PAM 22
Vérification des paramètres AppArmor 23
Configuration des outils 23

Présentation de RSA Authentication Agent 8.1 for PAM

RSA Authentication Agent 8.1 for PAM (module d'authentification enfichable) prend en charge l'authentification sur les systèmes UNIX avec outils de connexion standard ou OpenSSH. PAM agent utilise les bibliothèques partagées et personnalisées RSA, et prend en charge l'accès aux stations de travail et serveurs UNIX avec les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Vous pouvez choisir si PAM agent s'authentifie au Service d'authentification cloud ou à Authentication Manager. Les licences RSA SecurID Access Enterprise Edition et Premium Edition incluent ces deux composants de RSA SecurID Access. Authentication Manager n'est pas nécessaire pour utiliser PAM agent.

La version 8.1 de PAM agent offre les nouveaux avantages suivants :

- Prise en charge du Service d'authentification cloud. Le Service d'authentification cloud utilise des méthodes d'authentification à plusieurs facteurs, par exemple Approve (notification push optimisée pour les mobiles), Authenticate Tokencode, données biométriques de périphérique, code de token SMS, code de token vocal 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.
- Possibilité d'accéder à Authentication Manager avec le protocole REST, plutôt que le protocole UDP.
- Prise en charge continue pour le protocole UDP utilisé par les versions antérieures de PAM agent.
- Authentication Manager inclut des rapports d'agent qui vous aident à gérer vos instances PAM agent de protocole REST installées. En mode REST, PAM agent peut envoyer des informations supplémentaires au serveur Authentication Manager, comme un numéro d'identification logicielle unique pour chaque instance PAM agent installée et des informations sur le système d'exploitation utilisé par l'agent.

L'utilisation de PAM agent en mode REST offre des avantages supplémentaires par rapport à l'utilisation du protocole UDP :

- Facilite l'intégration du Service d'authentification cloud pour votre déploiement Authentication Manager.
- 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 8.1 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.

Modes d'authentification

Vous pouvez installer PAM agent dans l'un des trois modes d'authentification. Tous les modes assurent une authentification RSA SecurID. Vous pouvez modifier le mode après l'installation en fonction des besoins. Pour savoir comment procéder, consultez la section Modification du mode d'authentification PAM Agent Page 34.

Mode d'authentification	Description
RSA Authentication Manager avec le protocole UDP	Les authentificateurs matériels et logiciels RSA SecurID génèrent des codes de token RSA SecurID. L'agent vérifie que les données saisies par l'utilisateur correspondent à celles stockées dans Authentication Manager et autorise ou refuse l'accès en fonction du résultat. Par défaut, la mise à niveau de PAM agent configure l'agent pour utiliser le protocole UDP. Vous pouvez facilement passer à un mode d'authentification différent qui utilise le protocole REST.
RSA Authentication Manager avec le protocole REST	Prise en charge de tous les types d'authentification pris en charge par Authentication Manager via le protocole REST, comme les tokens matériels et logiciels RSA SecurID et Authenticate Tokencode grâce à une intégration avec le composant Service d'authentification cloud.
Service d'authentification cloud avec le protocole REST	Prend en charge Approve (notification push optimisée pour les mobiles), Authenticate Tokencode, les données biométriques, le code de token SMS, le code de token vocal et les tokens RSA SecurID. Les jetons FIDO et les conditions d'authentification nécessitant des combinaisons de méthodes (par exemple, Approve et le token RSA SecurID) ne sont pas pris en charge.

RSA Authentication Agent 8.1 for PAM prend en charge les domaines de confiance RSA Authentication Manager. L'authentification basée sur le risque (RBA) Authentication Manager n'est pas prise en charge.

Workflow de PAM Agent

PAM agent est installé sur un serveur UNIX. Il joue le rôle d'intermédiaire entre les utilisateur s'authentifiant et le serveur RSA Authentication Manager ou le Service d'authentification cloud.

PAM agent prend en charge les fonctions de sécurité de Authentication Manager. Par exemple, si Authentication Manager détermine que l'utilisateur associé à un token spécifique requiert un nouveau code PIN, l'agent demande le code PIN, qui possède les caractéristiques définies dans Authentication Manager, et envoie les informations à Authentication Manager. Si Authentication Manager demande le code suivant indiqué sur le token de l'utilisateur, PAM agent invite l'utilisateur. Si le code de token correct suivant n'est pas envoyé à Authentication Manager, l'authentification échoue.

Les étapes suivantes décrivent le flux d'authentification pour PAM agent, dans les trois modes d'authentification :

1. Un utilisateur tente d'accéder à une machine protégée par PAM agent, en local, par connexion ou à distance, avec des outils tels que rlogin, telnet, SSH et FTP.

   L'utilisateur doit exister localement sur la machine sur laquelle PAM agent est installé.

2. L'infrastructure de module d'authentification enfichable (PAM, pluggable authentication module) UNIX intercepte toutes les demandes d'ouverture de session et utilise les fichiers de configuration PAM pour accéder au module RSA PAM :

- Si un utilisateur n'est pas configuré pour l'authentification RSA SecurID, le module PAM de RSA valide la demande.
- Si l'utilisateur demandant l'accès est invité par RSA SecurID, PAM agent poursuit l'authentification à l'étape 3.

3. En fonction du mode d'authentification PAM agent, l'agent contacte Authentication Manager ou le Service d'authentification cloud.

   Pour Authentication Manager avec une connexion UDP ou le protocole REST, les étapes suivantes se produisent :

   a. L'agent invite l'utilisateur à saisir le nom d'utilisateur, puis le code d'accès.
   b. L'agent envoie en toute sécurité le nom d'utilisateur et le code d'accès à Authentication Manager :
      - Si Authentication Manager approuve la demande, l'agent accorde l'accès à l'utilisateur.
      - Si Authentication Manager n'approuve pas la demande, l'agent refuse l'accès.

   Pour le Service d'authentification cloud, les étapes suivantes se produisent :

   a. L'agent invite l'utilisateur à saisir un nom d'utilisateur et envoie les informations au Service d'authentification cloud.
   b. Le Service d'authentification cloud fournit à l'agent les méthodes d'authentification configurées pour l'utilisateur dans le niveau d'assurance de la Service d'authentification cloudpolitique d'accès.
   c. L'agent invite l'utilisateur à s'authentifier.
   d. L'utilisateur choisit une méthode d'authentification disponible et s'authentifie :
      - Si le Service d'authentification cloud approuve la demande, l'agent accorde l'accès à l'utilisateur.
      - Si une méthode d'authentification a échoué, le Service d'authentification cloud invite l'utilisateur à utiliser la méthode d'authentification suivante.
      - Si le Service d'authentification cloud n'approuve pas la demande, l'agent refuse l'accès.

Configuration logicielle requise

Cette section décrit les versions minimales du logiciel prises en charge par PAM agent.

Systèmes d'exploitation requis

PAM agent requiert l'un des systèmes d'exploitation suivants :

- SUSE Linux Enterprise Server version 11 SP4 (32 bits et 64 bits)
- SUSE Linux Enterprise Server version 12 SP3 (64 bits)
- SUSE Linux Enterprise Server version 15 (64 bits)

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

Version prise en charge RSA Authentication Manager

RSA SecurID Authentication Agent 8.1 for PAM prend en charge l'API d'authentification RSA SecurID version 1.1, qui est la version actuelle des API REST.

Le tableau suivant répertorie les versions RSA Authentication Manager requises pour prendre en charge des fonctions spécifiques.

Version RSA Authentication Manager obligatoire	Fonction prise en charge
8.2 SP1 ou version supérieure	PAM agent requiert RSA Authentication Manager 8.2 SP1 ou version supérieure.
8.2 SP1 Patch 5 ou version supérieure	Si l'indicateur de reporting d'agent est activé sur PAM agent, RSA Authentication Manager 8.2 SP1 Patch 5 ou version supérieure est requis pour éviter les échecs d'authentification en mode REST.
8.3 ou versions supérieures	RSA Authentication Manager 8.3 et les versions supérieures incluent des rapports d'agent qui vous aident à gérer vos agents PAM de protocole REST installés. Ces rapports incluent des informations supplémentaires que PAM agent peut envoyer à Authentication Manager.

Version prise en charge Service d'authentification cloud

RSA SecurID Authentication Agent 8.1 for PAM prend en charge l'API d'authentification RSA SecurID version 1.1, qui est la version actuelle des API REST.

Conditions de certification

PAM agent utilise des certificats TLS 1.2 pour le protocole REST. Service d'authentification cloud et RSA Authentication Manager 8.2 ou version supérieure peuvent accepter ces certificats. Les déploiements qui n'utilisent pas des certificats TLS 1.2 doivent utiliser le mode d'authentification qui prend en charge Authentication Manager avec le protocole UDP.

Dans les modes d'authentification du protocole REST, 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.

Outils pris en charge

PAM agent prend en charge les outils suivants :

- telnet
- connexion
- rlogin
- su
- ssh (ssh, sftp et scp)
- sudo

  Téléchargez et installez la version sudo prise en charge à partir de https://www.sudo.ws.

- ftp (limité à une seule transaction)

- gdm
- xdm (limité à une seule transaction)

Prise en charge de OpenSSH (facultatif)

PAM agent prend en charge OpenSSH 6.0 P1. Si vous utilisez OpenSSH, vérifiez que vous utilisez la version compatible d'OpenSSH correspondant à votre plate-forme. OpenSSH n'est pas nécessaire.

Les outils OpenSSH en option suivants sont prises en charge :

- ssh
- sftp
- scp

Installez OpenSSH sur la machine de l'agent. Pour OpenSSH, y compris les conditions préalables et les logiciels supplémentaires requis pour compiler le code source, reportez-vous à la section https://www.openssh.com.

Planification de l'installation de PAM Agent

Avant de commencer l'installation de PAM agent, procédez comme suit :

- Sur la machine sur laquelle vous allez installer PAM agent :
  1. Obtenez les autorisations au niveau racine.
  2. Créez un répertoire **/var/ace** pour les fichiers de configuration de PAM agent, s'il n'existe pas déjà, et créez un répertoire d'installation.
  3. Obtenir le certificat d'autorité de certification racine de confiance de serveur à partir de RSA Authentication Manager ou du Service d'authentification cloud. (Pour obtenir des instructions, consultez l'article de la base de connaissances How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate). Ensuite, procédez comme suit :
     a. Vérifiez que le certificat n'a pas expiré.
     b. Stockez le certificat au format PEM. S'il existe plusieurs certificats d'autorité de certification, ils doivent être concaténés dans un seul fichier au format PEM.
     c. Copiez ***filename*.pem** dans le répertoire **/var/ace/**.
     d. Protégez le répertoire **/var/ace/** contenant les certificats disposant des privilèges appropriés.
- Pour vous authentifier avec RSA Authentication Manager, créez un enregistrement d'agent d'authentification pour PAM agent dans la base de données interne. Pour plus d'informations, contactez votre super administrateur Authentication Manager ou reportez-vous à l'aide Authentication Manager sur RSA Link.
- Pour vous authentifier via le protocole UDP, vous devez générer le fichier de configuration Authentication Manager, **sdconf.rec**, ou vous procurer ce fichier à partir de votre super administrateur Authentication Manager. Ce fichier n'est pas nécessaire pour l'authentification avec le protocole REST.

  Le fichier **sdconf.rec** spécifie la manière dont l'agent communique avec l'instance principale et les instances de réplica Authentication Manager par l'adresse IP. Effectuez ce qui suit :

  - Assurez-vous que la dernière version du fichier **sdconf.rec** se trouve dans un répertoire accessible sur la machine de l'agent, comme le répertoire **/var/ace** par défaut.

    - Vous devez disposer des autorisations en écriture sur le répertoire dans lequel le fichier **sdconf.rec** est stocké.
- Dans le mode d'authentification qui utilise le Service d'authentification cloud avec le protocole REST, PAM agent s'appuie sur le Service d'authentification cloud pour l'équilibrage de charge et le basculement.
- Dans le mode d'authentification qui utilise le RSA Authentication Manager avec le protocole REST, PAM agent ne prend pas en charge l'équilibrage de charge. PAM agent prend en charge le basculement pour un maximum de 15 instances de réplica Authentication Manager.
- Collectez les informations que vous fournirez pendant l'installation de PAM agent.

  Authentication Manager avec le protocole UDP. Vous pouvez conserver les valeurs par défaut ou spécifier de nouveaux répertoires.

Description	**Votre plan**
Répertoire dans lequel **sdconf.rec** se trouve. La valeur par défaut est **/var/ace/**.	
Chemin racine pour le répertoire PAM agent. La valeur par défaut est **/opt**.	

  Authentication Manager avec le protocole REST. Demandez au super administrateur Authentication Manager les informations suivantes :

Description	**Votre plan**
URL du serveur REST pour la communication entre l'agent d'authentification et l'instance principale de Authentication Manager. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans la première instance, utilisez la valeur *HOSTNAME* du champ **Nom de domaine complet** sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.	
Nombre d'instances de réplica Authentication Manager qui peuvent être utilisées pour le basculement.	
URL du serveur REST pour chaque instance de réplica. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans l'instance de réplica, utilisez la valeur *HOSTNAME* du champ **Nom de domaine**	

Description	Votre plan
complet sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.	
Clé d'accès (clé client) pour transmettre en toute sécurité les demandes d'authentification à Authentication Manager. Cette valeur est générée dans la console de sécurité sur l'instance Authentication Manager principale. Pour obtenir des instructions sur l'obtention de la clé d'accès, consultez la rubrique suivante sur RSA Link : Configurer l'API d'authentification de RSA SecurID pour les agents d'authentification.	
Indiquez le répertoire et le nom du fichier correspondant au certificat de confiance du serveur sur l'agent d'authentification. La valeur par défaut est **/var/ace/cert.pem**.	
Nom de l'agent d'authentification (ID Client) qui a été créé pour PAM agent dans Authentication Manager.	
Chemin racine pour le répertoire PAM agent. La valeur par défaut est **/opt**.	

Service d'authentification cloud avec le protocole REST. Demandez au super administrateur Service d'authentification cloud les informations suivantes :

Description	Votre plan
URL du serveur REST pour la communication entre l'agent et le Service d'authentification cloud. Utilisez le format suivant : `https://HOSTNAME:PORT/mfa/v1_1/authn` Pour le Service d'authentification cloud, utilisez la valeur *HOSTNAME* du champ **Domaine du service d'authentification** sous l'onglet **Inscription** de la page de paramétrage du routeur d'identité figurant dans la Cloud Administration Console. Le *PORT* par défaut est 443.	
Clé API d'authentification (clé client) créée dans Cloud Administration Console pour transférer en toute sécurité les demandes	

Description	Votre plan
d'authentification utilisateur au Service d'authentification cloud. Pour obtenir des instructions sur l'obtention de la clé API d'authentification, consultez la rubrique suivante sur RSA Link : Add an RSA SecurID Authentication API Key. (Ajouter une clé API d'authentification RSA SecurID)	
Répertoire et nom du fichier pour le certificat de confiance du serveur sur l'agent d'authentification. La valeur par défaut est **/var/ace/cert.pem**.	
ID de tenant pour le Service d'authentification cloud. PAM agent peut fournir l'ID de tenant dans les demandes d'authentification, mais l'agent ne valide pas les données. Ce paramètre n'est actuellement pas pris en charge par le Service d'authentification cloud.	
Nom de stratégie d'accès pour le Service d'authentification cloud. Cette règle est définie dans Cloud Administration Console.	
Nom de l'agent d'authentification CLIENT_ID à afficher dans les notifications mobiles. Vous pouvez saisir n'importe quelle valeur. Par exemple, PAM_Agent.	
Chemin racine pour le répertoire PAM agent. La valeur par défaut est **/opt**.	

Installation de RSA Authentication Agent 8.1 for PAM

Pour installer PAM agent, effectuez les tâches suivantes :

1. Spécification de l'adresse IP d'Agent pour le mode UDP bas
2. Configurer OpenSSH Page suivante
3. Installer PAM Agent Page suivante
4. Pour le mode UDP, effectuez un test d'authentification. Pour plus d'informations, consultez la section Utilitaires d'authentification pour le Mode UDP Page 41.

   Pour un mode Protocole REST, testez la connexion en accédant à l'URL du serveur REST avec un navigateur ou un client http. Par exemple, saisissez https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Comme vous n'êtes pas en train de vous authentifier, votre navigateur ou votre client http doit afficher une réponse HTTP « Interdit » ou « Non autorisé ».

Spécification de l'adresse IP d'Agent pour le mode UDP

Pour le mode UDP, vous devez créer le fichier **sdopts.rec** dans le même répertoire que celui qui est utilisé par le

fichier **sdconf.rec**. Cette procédure ne s'applique pas au mode REST.

Fichier	Description
sdopts.rec	Répertorie l'adresse IP de l'ordinateur sur lequel vous avez installé l'agent. L'agent utilise l'adresse IP figurant dans le fichier **sdopts.rec** afin de communiquer avec RSA Authentication Manager.
sdconf.rec	Spécifie les adresses IP qui sont utilisées par Authentication Manager.

Procédure

1. Sur l'ordinateur agent, utilisez un éditeur de texte pour créer un fichier **sdopts.rec** dans le chemin d'accès où le fichier **sdconf.rec** est enregistré.
2. Dans le fichier, saisissez :

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

   où *x.x.x.x* est l'adresse IP de l'hôte d'agent.

   Remarque : Utilisez uniquement des lettres majuscules et n'insérez pas d'espaces.
3. Enregistrez le fichier.

Configurer OpenSSH

Si vous utilisez OpenSSH, la suite d'utilitaires réseau liés à la sécurité basés sur le protocole Secure Shell (SSH), vous devez configurer ce logiciel pour qu'il fonctionne avec PAM agent et affiche des messages d'authentification de code d'accès pour les utilisateurs.

Avant de commencer

Installez OpenSSH sur la machine de l'agent. Pour OpenSSH, y compris les conditions préalables et les logiciels supplémentaires requis pour compiler le code source, reportez-vous à la section https://www.openssh.com.

Procédure

1. Sur la machine de l'agent, ouvrez le fichier **sshd_config**.
2. Définissez les paramètres suivants et enregistrez les modifications :

Paramètre	Paramètre
UsePAM	Oui
PasswordAuthentication	Non
ChallengeResponseAuthentication	Oui

   La définition du paramètre PasswordAuthentication sur no désactive l'invite de mot de passe OpenSSH. PAM agent est utilisé à la place. Par conséquent, l'utilisateur est invité à procéder à l'authentification SecurID uniquement.
3. Redémarrez le service sshd. Saisissez :

   ```
   service sshd restart
   ```

Installer PAM Agent

Vous pouvez installer manuellement PAM agent sur les différentes machines, ou vous pouvez choisir d'utiliser une installation silencieuse pour automatiser le processus de déploiement de plusieurs copies de PAM agent.

Installation de PAM Agent sur une seule machine

Effectuez cette tâche pour installer une seule instance de PAM agent. Pour installer PAM agent sur plusieurs machines, consultez Installation en masse de PAM Agent en mode silencieux Page suivante.

Procédure

1. Sur l'ordinateur agent, accédez au répertoire du programme d'installation de PAM agent.
2. Décompressez le fichier en saisissant :

   ```
   tar -xvf nom du fichier.tar
   ```

3. Pour exécuter le script d'installation, saisissez

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

4. Exécutez ensuite les invites. Appuyez sur ENTRÉE pour accepter la valeur par défaut, ou entrez la valeur appropriée.

   Pour le mode UDP RSA Authentication Manager, procédez comme suit :

   - Acceptez la licence pour le logiciel RSA.
   - Saisissez 0 pour sélectionner RSA Authentication Manager avec le mode d'authentification Protocole UDP.
   - Indiquez le répertoire dans lequel se trouve **sdconf.rec**.
   - Indiquez le répertoire d'installation de PAM agent.

   Pour le mode REST RSA Authentication Manager, procédez comme suit :

   - Acceptez la licence pour le logiciel RSA.
   - Saisissez 1 pour sélectionner l'instance RSA Authentication Manager avec le mode d'authentification Protocole REST.
   - Indiquez l'URL du serveur REST pour la communication entre l'agent d'authentification et l'instance principale.
   - Saisissez y s'il y a des instances de réplica Authentication Manager pour le basculement.
   - Spécifiez le nombre d'instances de réplica.
   - Indiquez l'URL du serveur REST pour chaque instance de réplica.
   - Indiquez la clé client (clé d'accès) pour transmettre en toute sécurité les demandes d'authentification à Authentication Manager.
   - Indiquez le répertoire et le nom du fichier correspondant au certificat de confiance du serveur sur l'agent d'authentification.
   - Indiquez l'ID de client qui correspond au nom de l'agent d'authentification dans Authentication Manager.
   - Indiquez le répertoire d'installation de PAM agent.

   Pour le mode REST Service d'authentification cloud, procédez comme suit :

   - Acceptez la licence pour le logiciel RSA.
   - Saisissez 2 pour sélectionner l'instance Service d'authentification cloud avec le mode d'authentification Protocole REST.

- Indiquez l'URL du serveur REST pour la communication entre l'agent d'authentification et le Service d'authentification cloud.
- Indiquez la clé client (clé API d'authentification) pour transmettre en toute sécurité les demandes d'authentification au Service d'authentification cloud.
- Indiquez le répertoire et le nom du fichier correspondant au certificat de confiance du serveur sur l'agent d'authentification.
- Indiquez l'ID de tenant du Service d'authentification cloud.
- Indiquez le nom de la règle d'accès du Service d'authentification cloud.
- Indiquez le nom de l'agent d'authentification CLIENT_ID à afficher dans les notifications mobiles.
- Indiquez le répertoire d'installation de PAM agent.

5. Pour le mode UDP uniquement, vérifiez que VAR_ACE dans le fichier **/etc/sd_pam.conf** pointe vers l'emplacement correct du fichier **dconf.rec**. Il s'agit du chemin d'accès des fichiers de configuration. L'ensemble du chemin doit disposer de l'autorisation racine -rw-------.

Après avoir terminé

- Vous pouvez vérifier l'installation en consultant le fichier **installer.log** dans le répertoire qui contient le programme d'installation de PAM agent.
- Pour le mode UDP, effectuez un test d'authentification. Pour plus d'informations, consultez la section Utilitaires d'authentification pour le Mode UDP Page 41.
- Pour un mode Protocole REST, testez la connexion en accédant à l'URL du serveur REST avec un navigateur ou un client http. Par exemple, saisissez https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn. Étant donné que vous n'êtes pas en train de vous authentifier, votre navigateur ou votre client http doit afficher une réponse HTTP « Interdit » ou « Non autorisé ».

Installation en masse de PAM Agent en mode silencieux

Effectuez cette tâche pour déployer un grand nombre d'instances PAM agent avec des informations de configuration identiques. Par exemple, effectuez cette tâche si vous avez besoin d'installer un grand nombre d'agents pour assurer la communication avec les mêmes serveurs RSA Authentication Manager ou le même Service d'authentification cloud.

Avant de commencer

Installez PAM agent manuellement et notez les invites. Pour savoir comment procéder, consultez la section Installation de PAM Agent sur une seule machine Page précédente.

Procédure

1. Créez un fichier de configuration de type texte dans lequel vous indiquerez les options de configuration pour le script d'installation de PAM agent. Vous pouvez choisir un nom pour le fichier de configuration, par exemple **installoptions.conf**.
2. Ouvrez le fichier et répertoriez chaque option de configuration que vous souhaitez sélectionner sur une ligne distincte, dans l'ordre dans lequel les invites sont présentées lors d'une installation manuelle de PAM agent.

   L'exemple suivant décrit l'invite correspondant à chaque option spécifiée dans la configuration UDP :

Exemple de valeur	Option
y	Continuer l'installation en mode silencieux ? (y) Cette invite est toujours indiquée en premier.
Accepter	Accepter les conditions générales? (Accepter)
0	Mode d'authentification ? (valeur numérique pour le mode désiré) 0 : RSA Authentication Manager avec le protocole UDP 1 : RSA Authentication Manager avec le protocole REST 2 : Service d'authentification Cloud avec le protocole REST
/var/ace	Répertoire contenant le fichier sdconf.rec ? (chemin d'accès du répertoire)
/opt	Chemin d'installation du répertoire de PAM agent ? (chemin d'accès du répertoire)
y	Mettre à niveau/remplacer l'installation existante ? (y/n)

Dans ce cas, le fichier de configuration de type texte contient :

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

Autre exemple : pour le mode REST Authentication Manager, le fichier de configuration peut contenir des données similaires aux données suivantes :

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

Remarque : Le nombre et l'ordre des invites d'installation varient en fonction du mode de PAM agent et de la plate-forme sur laquelle vous effectuez l'installation.

3. Accédez au répertoire d'installation de PAM agent.
4. Décompressez le fichier en saisissant :

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

5. Pour exécuter le script d'installation, saisissez

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

   où ***installoptions.conf*** est le fichier de configuration que vous avez créé à l'étape 1. Si le fichier de configuration se trouve à un emplacement autre que celui du répertoire actif, spécifiez le chemin d'accès complet du fichier ***installoptions.conf***.

Mise à niveau vers RSA Authentication Agent 8.1 for PAM

Vous pouvez mettre à niveau vers RSA Authentication Agent 8.1 for PAM à partir de la version 7.1 Patch 2 (7.1.0.2) ou de la version 8.0.

Lors d'une mise à niveau à partir de la version 7.1.0.2, l'agent mis à niveau utilise RSA Authentication Manager et le protocole UDP pour l'authentification. Vous pouvez modifier le mode d'authentification pour tirer parti de Service d'authentification cloud ou d'Authentication Manager et du protocole REST. Pour savoir comment procéder, consultez la section Modification du mode d'authentification PAM Agent Page 34.

Lors de la mise à niveau à partir de la version 8,0, l'agent mis à niveau conserve le même mode d'authentification configuré pour la version précédente.

Avant de commencer

- Vous devez disposer d'autorisations racines sur l'hôte d'agent et de l'autorisation d'écriture sur le répertoire dans lequel le fichier **sdconf.rec** est stocké. Ce fichier est habituellement stocké dans le répertoire **/var/ace** par défaut.
- Sauvegardez les fichiers de configuration avant de les remplacer afin d'enregistrer les paramètres de configuration. Pour plus d'informations, consultez la section Fichiers de configuration critiques Page 50.
- Configurez les outils protégés RSA SecurID pour utiliser le module PAM standard fourni avec votre système d'exploitation, et non pas le module RSA PAM. Les sessions actives utilisant les modules RSA PAM doivent être fermées avant de poursuivre la mise à niveau.

Procédure

1. Sur l'ordinateur agent, accédez au répertoire du programme d'installation de PAM agent.
2. Décompressez le fichier en saisissant :

   `tar -xvf` ***nom du fichier.tar***

3. Pour exécuter le script d'installation, saisissez :

   /<nom du fichier>/install_pam.sh

4. Remplacez les fichiers d'installation existants. Saisissez **y** lorsque le programme d'installation vous invite à remplacer l'installation actuelle.
5. Obtenez le numéro de version de l'agent pour déterminer si la mise à niveau a réussi. Saisissez :

   strings pam_securid.so | grep "Agent"

   Cette commande affiche le numéro de version de l'agent installé.

Vérification des paramètres AppArmor

AppArmor est un module de sécurité du noyau Linux qui permet aux administrateurs de limiter les applications. Cette section présente les étapes de vérification des paramètres du module AppArmor.

Procédure

1. Exécutez la commande suivante pour vérifier si AppArmor est activé. Saisissez :

   /boot/grub/menu.lst

2. Exécutez la commande suivante pour vérifier les stratégies prises en charge par AppArmor. Saisissez :

   /usr/sbin/apparmor_status

Configuration des outils

Vous devez configurer les outils pris en charge pour inviter les utilisateurs à utiliser les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Remarque : Le nombre de paramètres d'utilisateurs simultanés autorisés sur le serveur Unix doit être configuré pour chaque outil, le système d'exploitation utilisé, ainsi que les ouvertures de session simultanées attendues sur le serveur, surtout lorsque vous utilisez le Service d'authentification cloud.

Configuration de telnet bas

Configurer la connexion Page suivante

Configuration de rlogin Page suivante

Configuration de su Page suivante

Configuration de ssh et des outils connexes Page suivante

Configuration de sudo Page 25

Configurer ftp Page 25

Configurer gdm Page 25

Configurer xdm Page 26

Configuration de telnet

Configurez telnet pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **remote**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

   ```
   auth required pam_securid.so
   ```

Configurer la connexion

Configurez la commande de connexion pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **login**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configuration de rlogin

Configurez l'utilitaire rlogin pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Avant de commencer

Si les connexions rlogin sont fermées, suivez la procédure décrite dans Problèmes connus liés à la configuration Page 40.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **rlogin**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configuration de su

Configurez la commande su pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **su**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configuration de ssh et des outils connexes

Vous pouvez configurer SSH et les outils connexes, tels que scp et sftp pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **sshd**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configuration de sudo

Si vous avez besoin de sudo, vous devez configurer la commande sudo pour demander aux utilisateurs les méthodes d'authentification prises en charge par le Service d'authentification cloud et RSA Authentication Manager.

Avant de commencer

Téléchargez et installez la version sudo prise en charge à partir de https://www.sudo.ws.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **sudo**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configurer ftp

Configurer le protocole ftp pour demander aux utilisateurs les méthodes d'authentification prises en charge par RSA Authentication Manager.

Vous ne pouvez pas utiliser le Service d'authentification cloud pour protéger le ftp ; toutefois, vous pouvez utiliser le sftp. Pour savoir comment procéder, reportez-vous à la section Configuration de ssh et des outils connexes Page précédente.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **vsftpd**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

```
auth required pam_securid.so
```

Configurer gdm

Vous pouvez configurer gdm pour demander aux utilisateurs les méthodes d'authentification prises en charge par Service d'authentification cloud et RSA Authentication Manager.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Modifiez les fichiers **gdm**,**gdm-password** et **gdm-autologin** comme suit :
   a. Ouvrez chaque fichier gdm.
   b. Mettez en commentaire toutes les lignes qui commencent par `auth`.
   c. Ajoutez la ligne :

      ```
      auth required pam_securid.so
      ```

Configurer xdm

Vous pouvez configurer xdm pour demander aux utilisateurs les méthodes d'authentification prises en charge par Service d'authentification cloud et RSA Authentication Manager.

Procédure

1. Accédez au répertoire **/etc/pam.d**.
2. Ouvrez le fichier **xdm**.
3. Mettez en commentaire toutes les lignes qui commencent par `auth`.
4. Ajoutez la ligne :

   ```
   auth required pam_securid.so
   ```

Chapitre 2: Configurer les fonctions

Configuration des fonctions Agent et UNIX 28
Modification du mode d’authentification PAM Agent 34

Configuration des fonctions Agent et UNIX

Vous pouvez personnaliser la configuration PAM agent pour utiliser l'agent facultatif et les fonctions UNIX.

Remarque : Avant de personnaliser l'agent, effectuez des copies de sauvegarde des fichiers de configuration d'origine.

Plusieurs fichiers de configuration se trouvent dans le répertoire **/etc/pam.d**. Chaque fichier utilise le nom de l'outil de connexion.

Pour personnaliser l'agent, reportez-vous à la section :

Activation du reporting d'agent pour RSA SecurID Authentication Agent 8.1 for PAM bas

Activation de la sortie de débogage bas

Activer la consignation de trace SecurID pour le mode UDP Page opposée

Configuration des modules empilables Page opposée

Utilisation de mots de passe de réserve Page 30

Activation de l'authentification SecurID sélective Page 31

Configurer l'intervalle exponentiel Page 32

Activation du reporting d'agent pour RSA SecurID Authentication Agent 8.1 for PAM

Vous pouvez configurer le paramètre ENABLE_AGENT_REPORTING dans le fichier **mfa_api.properties** pour envoyer les informations sur l'agent, tels que le nom d'hôte, la version de l'agent et la version du système d'exploitation, à RSA Authentication Manager. Vous pouvez utiliser RSA Authentication Manager 8.3 ou les versions supérieures pour exécuter des rapports qui incluent ces informations.

Avant de commencer

Vous devez disposer d'autorisations racines sur l'ordinateur sur lequel l'agent est installé et d'une autorisation en écriture sur le répertoire dans lequel le fichier **mfa_api.properties** est stocké. Par défaut, ce fichier est stocké dans **/var/ace/conf**.

Procédure

1. Accédez au répertoire dans lequel se trouve **mfa_api.properties**. Par défaut, il s'agit du répertoire **/var/ace/conf**.
2. Ouvrez **mfa_api.properties**.
3. Remplacez la valeur du paramètre ENABLE_AGENT_REPORTING par 1, ce qui permet le reporting d'agent. La valeur par défaut est 0.
4. Enregistrez le fichier.

   Les informations sur l'instance PAM agent et l'ordinateur sur laquelle elle est installée sont incluses dans les informations sur PAM agent qui sont envoyées à Authentication Manager.

Activation de la sortie de débogage

Pour le dépannage, vous pouvez activer la sortie de débogage pour les outils spécifiques utilisés par PAM agent.

Vous pouvez également configurer le log système pour enregistrer tous les messages logs afin d'enregistrer

tous les messages de log d'authentification de PAM agent. Pour obtenir des informations, reportez-vous à la section Consignation pour PAM Agent Page 44.

Procédure

1. Accédez au répertoire **/etc/** et ouvrez le fichier **pam.d**.
2. Modifiez le fichier approprié en ajoutant un argument de débogage pour le module pam_securid.so. Saisissez :

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

Activer la consignation de trace SecurID pour le mode UDP

Vous pouvez activer la consignation de trace SecurID détaillée pour PAM agent et les utilitaires d'authentification acetest et acestatus. Par défaut, lorsque vous installez PAM agent, la consignation de trace SecurID est désactivée.

Procédure

1. Accédez au répertoire **/etc** et ouvrez le fichier **sd_pam.conf**.
2. Pour activer la consignation d'agent détaillée et définir le niveau de consignation, définissez la variable suivante :

   `RSATRACELEVEL=`*`valeur`*

   Où *`valeur`* est définie dans le tableau suivant.

Valeur	Description
0	Désactive la consignation (par défaut)
1	Consigne les messages normaux
2	Consigne les points d'entrée de fonction
4	Consigne les points de sortie de fonction
8	Tous les contrôles de flux logique utilisent cela (ifs)

   Pour les combinaisons, ajoutez les valeurs correspondantes. Par exemple, pour consigner des messages normaux et les points d'entrée de fonction, définissez la valeur sur 3.

3. Spécifiez le chemin du fichier dans lequel les logs sont réacheminés. Définissez la variable suivante :

   `RSATRACEDEST=`*`filepath`*

   Où *`filepath`* est le chemin d'accès du fichier.

   Par défaut, cette variable est vide. Si vous ne définissez pas cette variable, les logs affichent une erreur standard pour les utilitaires d'authentification acetest et acestatus, et aucun log n'est généré pour les outils d'authentification même si la valeur `RSATRACELEVEL` a été spécifiée.

4. Enregistrez vos modifications.

Configuration des modules empilables

Dans une configuration empilée, vous utilisez l'agent pour intégrer le module d'authentification RSA SecurID PAM avec les autres modules d'authentification PAM de votre environnement. Le mot de passe ou le code secret est transmis du module d'authentification au module d'authentification suivant. Vous pouvez configurer la

priorité des demandes d'authentification en modifiant le fichier de configuration approprié **/etc/pam.d/*nom de l'outil***.

Remarque : Les arguments use_first_pass et try_first_pass ne sont pas pris en charge lorsqu'une configuration empilée est utilisée avec le Service d'authentification cloud.

L'agent travaille avec ces arguments :

- **use_first_pass.** L'agent utilise uniquement le mot de passe ou le code secret transmis depuis le module précédent, et interdit l'accès si les informations d'identification ne correspondent pas. L'utilisateur n'est pas invité à s'authentifier à nouveau.
- **try_first_pass.** L'agent utilise le mot de passe ou le code secret transmis depuis le module précédent. Si les informations d'identification ne correspondent pas, l'utilisateur est invité à s'authentifier.
- **not_set_pass.** L'agent n'envoie pas le mot de passe ou le code d'accès au module de mot de passe empilé.

Remarque : Lorsque les utilisateurs exclus de l'authentification SecurID réalisent des tentatives de connexion qui échouent pour accéder au module RSA PAM, la fonctionnalité d'interruption exponentielle garantit que le module RSA PAM conserve le contrôle jusqu'à ce que la connexion soit établie ou que la session d'authentification se termine. Pour plus d'informations sur la configuration d'un délai d'interruption exponentielle, consultez la section Configurer l'intervalle exponentiel Page 32.

La section suivante comporte un exemple qui illustre la manière de configurer un outil de connexion (outil login) dans un environnement empilé.

Procédure

1. Accédez à **/etc/pam.d** et ouvrez le fichier **login**.
   Les lignes suivantes s'affichent :
   ```
   auth required pam_securetty.so
   auth include common-auth
   auth required pam_nologin.so
   account include common-account
   password include common-password
   session include common-session
   session required pam_lastlog.so nowtmp
   session required pam_resmgr.so
   session optional pam_mail.so standard
   session required pam_limits.so
   ```
2. Mettez en commentaire les lignes suivantes :
   ```
   auth required pam_securetty.so
   auth include common-auth
   auth required pam_nologin.so
   ```
3. Ajoutez les lignes suivantes. Saisissez :
   ```
   auth required pam_securid.so
   ```

Utilisation de mots de passe de réserve

La fonctionnalité de mots de passe de réserve est une méthode d'accès d'urgence qui vous permet, en tant qu'administrateur, de vous authentifier auprès de l'ordinateur protégé sur lequel l'agent est installé, sans indiquer de code secret RSA SecurID. PAM agent n'autorise que les administrateurs principaux à utiliser des mots de passe de réserve lors de circonstances imprévues, par exemple la perte de communication entre l'agent

et RSA SecurID Authentication Agent 8.1 for PAM. Dans ces circonstances, les administrateurs peuvent désactiver provisoirement l'agent si les utilisateurs ont besoin d'accéder immédiatement aux ressources hébergées.

Remarque : Le mot de passe UNIX est le mot de passe de réserve.

Procédure

1. Ouvrez le fichier approprié dans **/etc/pam.d.**
2. Ajoutez un argument de réserve au module pam_securid.so. Saisissez :

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

Activation de l'authentification SecurID sélective

Vous pouvez configurer l'agent pour qu'il demande toujours ou jamais une authentification SecurID de façon sélective pour les utilisateurs ou groupes UNIX spécifiques.

Activer l'authentification SecurID sélective pour les groupes UNIX bas

Activer l'authentification SecurID sélective pour les utilisateurs UNIX Page suivante

Remarque : Lorsque la prise en charge sélective des groupes et la prise en charge sélective des utilisateurs sont toutes deux activées, seule la prise en charge sélective des utilisateurs est activée. La prise en charge sélective des groupes est ignorée.

Le tableau suivant répertorie les valeurs possibles qui peuvent être définies dans le fichier **sd_pam.conf**.

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	Résultat
0	0	Aucune fonction n'est activée. Chaque utilisateur et groupe d'utilisateurs est remis en question.
0	1	La prise en charge des utilisateurs sélectionnés est activée. PAM agent invite toujours les utilisateurs UNIX spécifiques à s'authentifier avec SecurID, ou n'invite jamais les utilisateurs spécifiques à s'authentifier avec SecurID.
1	0	La prise en charge des groupes sélectionnés est activée. PAM agent invite toujours les groupes UNIX spécifiques à s'authentifier avec RSA SecurID, ou n'invite jamais les groupes spécifiques à s'authentifier avec SecurID.
1	1	La prise en charge des utilisateurs sélectionnés est activée. PAM agent invite toujours les utilisateurs UNIX spécifiques à s'authentifier avec SecurID, ou n'invite jamais les utilisateurs spécifiques à s'authentifier avec SecurID.

Activer l'authentification SecurID sélective pour les groupes UNIX

Vous pouvez configurer PAM agent pour qu'il invite toujours ou jamais les groupes UNIX spécifiques à s'authentifier avec RSA SecurID. Lorsque PAM agent est installé, cette fonction n'est pas activée.

Les membres du groupe exclus de l'authentification SecurID peuvent s'authentifier avec les informations d'identification UNIX ou via un autre module PAM de la pile. Pour cela, configurez le paramètre PAM_IGNORE_SUPPORT.

Remarque : Ne spécifiez pas de groupes RSA Authentication Manager. Cette fonction est réservée aux groupes UNIX.

Procédure

1. Accédez au répertoire **/etc** et ouvrez le fichier **sd_pam.conf**.
2. Définissez le paramètre ENABLE_GROUP_SUPPORT sur 1. La valeur par défaut est 0.
3. Renseignez le paramètre LIST_OF_GROUPS.
4. Définissez la valeur du paramètre INCL_EXCL_GROUPS.
   Les valeurs autorisées sont les suivantes :
   0 : Désactiver l'authentification SecurID pour les groupes répertoriés (par défaut).
   1 : N'activer l'authentification SecurID que pour les groupes répertoriés.
5. (Facultatif) Définissez le paramètre PAM_IGNORE_SUPPORT.
   Les valeurs autorisées sont les suivantes :
   0 : Activer l'authentification par mot de passe UNIX (par défaut).
   1 : Désactiver l'authentification par mot de passe UNIX.
   Ce paramètre ne s'applique qu'aux groupes exclus de l'authentification SecurID.
6. Enregistrez le fichier.

Activer l'authentification SecurID sélective pour les utilisateurs UNIX

Vous pouvez configurer PAM agent pour qu'il invite toujours ou jamais les utilisateurs UNIX spécifiques à s'authentifier avec SecurID. Lorsque PAM agent est installé, cette fonction n'est pas activée.

Les utilisateurs exclus de l'authentification SecurID peuvent s'authentifier avec les informations d'identification UNIX ou via un autre module PAM de la pile. Pour cela, configurez le paramètre PAM_IGNORE_SUPPORT_FOR_USERS.

Procédure

1. Accédez au répertoire **/etc** et ouvrez le fichier **sd_pam.conf**.
2. Définissez le paramètre ENABLE_USERS_SUPPORT sur 1. La valeur par défaut est 0.
3. Renseignez le paramètre LIST_OF_USERS.
4. Définissez la valeur du paramètre INCL_EXCL_USERS.
   Les valeurs autorisées sont les suivantes :
   0 : Désactiver l'authentification SecurID pour les utilisateurs répertoriés (par défaut).
   1 : N'activer l'authentification SecurID que pour les utilisateurs répertoriés.
5. (Facultatif) Définissez le paramètre PAM_IGNORE_SUPPORT_FOR_USERS.
   Les valeurs autorisées sont les suivantes :
   0 : Activer l'authentification par mot de passe UNIX (par défaut).
   1 : Désactiver l'authentification par mot de passe UNIX.
   Ce paramètre ne s'applique qu'aux utilisateurs exclus de l'authentification SecurID.
6. Enregistrez le fichier.

Configurer l'intervalle exponentiel

Vous pouvez configurer la durée pendant laquelle un utilisateur exclu de l'authentification RSA SecurID doit

patienter avant de pouvoir s'authentifier après chaque échec de tentative de connexion. Par défaut, les utilisateurs peuvent réessayer l'authentification UNIX après un échec de tentative de connexion avec un délai de pow(4, failattempts) secondes. Par exemple, trois échecs de tentative de connexion résultent en un délai de 64 secondes (4 puissance 3, ou 4 X 4 X 4 = 64).

Remarque : Le protocole ftp ne gère pas l'intervalle exponentiel.

Procédure

1. Accédez au répertoire **/etc** et ouvrez le fichier **sd_pam.conf**.
2. Définissez le paramètre BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS sur *N*, comme suit :

N	**Comportement de l'authentification**
0	Désactivez la nouvelle tentative d'authentification UNIX après un échec de tentative de connexion. Il n'existe aucun délai d'authentification pour les tentatives de connexion qui suivent un échec de tentative de connexion.
1,2,3	Activez la nouvelle tentative d'authentification UNIX après un échec de tentative de connexion avec un délai de pow(3, failattempts) secondes.
4	Activez la nouvelle tentative d'authentification UNIX après un échec de tentative de connexion avec un délai de pow(4, failattempts) secondes.
5/Plus	Activez la nouvelle tentative d'authentification UNIX après un échec de tentative de connexion avec un délai de pow(5/Above, failattempts) secondes.

Remplacer le certificat d'autorité de certification racine de confiance du serveur

Vous devrez peut-être remplacer le certificat d'autorité de certification racine de confiance du serveur, par exemple, si le certificat actuel de RSA Authentication Manager ou Service d'authentification cloud est mis à jour.

Pour obtenir des instructions concernant l'obtention de ce certificat, consultez l'article de la base de connaissances How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate.

Avant de commencer

- Vous devez disposer des autorisations au niveau racine vers le répertoire **/var/ace** sur la machine sur laquelle PAM agent est installé.
- Confirmez que le nouveau certificat est au format PEM. S'il existe plusieurs certificats d'autorité de certification, ils doivent être concaténés dans un seul fichier au format PEM.

  Le format de fichier doit être comme suit :

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

  Thawte (BASE64)

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

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

Entrust (BASE64)

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

Procédure

1. Renommez le nouveau certificat racine de sorte qu'il porte le même nom que le certificat que vous remplacez.
2. Sur l'ordinateur sur lequel PAM agent est installé, copiez et remplacez ***new_cert_file*.pem** dans le répertoire **/var/ace/**.

Modification du mode d'authentification PAM Agent

Vous pouvez modifier le mode d'authentification pour PAM agent. Par exemple, vous pouvez modifier le mode si vous souhaitez utiliser les options d'authentification avancées fournies par Service d'authentification cloud. Par défaut, PAM agent mis à niveau utilise RSA Authentication Manager avec le protocole UDP.

Passer du protocole UDP au protocole REST

Vous pouvez passer du mode d'authentification par protocole UDP au protocole REST pour RSA SecurID Authentication Agent 8.1 for PAM ou Service d'authentification cloud.

Avant de commencer

- Vous devez disposer des autorisations au niveau racine sur la machine sur laquelle l'agent est installé.
- Vous devez disposer des autorisations en écriture sur le répertoire dans lequel le fichier **sdconf.rec** est stocké. Par défaut, ce fichier est stocké dans **/etc**.
- Vous devez disposer des autorisations en écriture sur le répertoire dans lequel le fichier **mfa_api.properties** est stocké. Par défaut, ce fichier est stocké dans **/var/ace/conf**.
- Collectez les informations nécessaires.

  Pour l'authentification Authentication Manager à l'aide du protocole REST, demandez les informations suivantes à votre super administrateur Authentication Manager.

Paramètre	Description
REST_URL	URL du serveur REST pour la communication entre l'agent d'authentification et l'instance principale de Authentication Manager. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans la première instance, utilisez la valeur *HOSTNAME* du champ **Nom de domaine complet** sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.
REPLICA_*number* où *number* est un nombre compris entre 1 et 15.	Une URL de serveur REST pour chaque instance de réplica pouvant être utilisée pour le basculement. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans l'instance de réplica, utilisez la valeur *HOSTNAME* du champ **Nom de**

Paramètre	Description
	domaine complet sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.
CLIENT_KEY	Clé d'accès (clé de client) pour transmettre en toute sécurité les demandes d'authentification utilisateur à Authentication Manager. Cette valeur est générée dans la Console de sécurité sur l'instance principale Authentication Manager. Pour obtenir des instructions sur l'obtention de la clé d'accès, consultez la rubrique suivante sur RSA Link : Configurer l'API d'authentification de RSA SecurID pour les agents d'authentification.
CA_CERT_FILE_ PATH	Répertoire et nom du fichier pour le certificat de confiance du serveur sur l'agent d'authentification. La valeur par défaut est **/var/ace/cert.pem**.
CLIENT_ID	Nom de l'agent d'authentification (ID Client) qui a été créé pour PAM agent dans Authentication Manager.

Pour l'authentification à l'aide de Service d'authentification cloud, demandez les informations suivantes à votre super administrateur Service d'authentification cloud.

Paramètre	Description
REST_URL	URL du serveur REST pour la communication entre l'agent et le Service d'authentification cloud. Utilisez le format suivant : `https://HOSTNAME:PORT/mfa/v1_1/authn` Pour le Service d'authentification cloud, utilisez la valeur *HOSTNAME* du champ **Domaine du service d'authentification** sous l'onglet **Inscription** de la page de paramétrage du routeur d'identité figurant dans la Cloud Administration Console. Le *PORT* par défaut est 443.
CLIENT_KEY	Clé API d'authentification (clé client) créée dans Cloud Administration Console pour transférer en toute sécurité les demandes d'authentification utilisateur au Service d'authentification cloud. Pour obtenir des instructions sur l'obtention de la clé API d'authentification, consultez la rubrique suivante sur RSA Link : Add an RSA SecurID Authentication API Key. (Ajouter une clé API d'authentification RSA SecurID)
CA_CERT_FILE_ PATH	Indiquez le répertoire et le nom du fichier correspondant au certificat de confiance du serveur sur l'agent d'authentification. La valeur par défaut est **/var/ace/cert.pem**.
TENANT_ID	ID de tenant pour le Service d'authentification cloud. PAM agent peut fournir l'ID de tenant dans les demandes d'authentification, mais l'agent ne valide pas les données. Ce paramètre n'est actuellement pas pris en charge par Service d'authentification cloud.
ASSURANCE_ POLICY_ID	Nom de stratégie d'accès pour le Service d'authentification cloud.
CLIENT_ID	Nom de l'agent d'authentification à afficher dans les notifications mobiles. Vous pouvez saisir n'importe quelle valeur. Par exemple, PAM_Agent.

Procédure

1. Accédez au répertoire dans lequel se trouve **sd_pam.conf**. L'emplacement par défaut est **/etc**.
2. Ouvrez **sd_pam.conf**.
3. Modifiez le paramètre OPERATION_MODE :
   - Pour Authentication Manager avec le protocole REST, entrez 1.
   - Pour Service d'authentification cloud avec le protocole REST, entrez 2.

   Si le paramètre OPERATION_MODE est 0, non spécifié ou mis en commentaire, PAM agent utilise le mode UDP par défaut.
4. Accédez au répertoire **/var/ace/conf**. Vous devez mettre à jour le fichier **mfa_api.properties**.
5. Ouvrez **mfa_api.properties**.
6. Supprimez les commentaires pour activer les paramètres requis.
7. Entrez une valeur pour chaque paramètre requis.
8. Enregistrez le fichier.

   Vous pouvez désormais utiliser le protocole REST.

Passer du protocole REST au protocole UDP

Après avoir installé PAM agent pour utiliser le protocole REST, vous pouvez modifier le mode d'authentification pour utiliser RSA SecurID Authentication Agent 8.1 for PAM avec le protocole UDP.

Une fois le mode d'authentification modifié pour utiliser le protocole UDP, les paramètres de configuration du protocole REST dans le fichier **mfa_api.properties** ne sont plus applicables.

Avant de commencer

- Le fichier de configuration Authentication Manager, **sdconf.rec**, est requis. Vous pouvez générer ce fichier dans Authentication Manager ou le demander à votre super administrateur Authentication Manager. Pour plus d'informations, reportez-vous à la section Planification de l'installation de PAM Agent Page 14.
- Vous devez disposer d'autorisations racines sur la machine sur laquelle l'agent est installé et d'autorisations en écriture dans le répertoire dans lequel le fichier **sd_pam.conf** est stocké. Par défaut, ce fichier est stocké dans le répertoire **/etc**.

Procédure

1. Accédez au répertoire dans lequel se trouve **sd_pam.conf**. L'emplacement par défaut est **/etc**.
2. Ouvrez **sd_pam.conf**.
3. Définissez le paramètre OPERATION_MODE sur 0 pour le protocole UDP :

   ```
   OPERATION_MODE=0
   ```

   Si le paramètre OPERATION_MODE est 0, non spécifié ou mis en commentaire, PAM agent utilise le mode UDP par défaut.
4. Copiez **sdconf.rec** dans le répertoire **/var/ace**.

   Vous pouvez désormais utiliser le protocole UDP.

Basculer entre RSA Authentication Manager et Service d'authentification cloud

Vous pouvez modifier si PAM agent utilise le protocole REST avec Authentication Manager ou Service d'authentification cloud.

Avant de commencer

- Vous devez disposer des autorisations au niveau racine sur la machine sur laquelle l'agent est installé.
- Vous devez disposer des autorisations en écriture sur le répertoire dans lequel le fichier **sdconf.rec** est stocké. Par défaut, ce fichier est stocké dans **/var/ace**.
- Vous devez disposer des autorisations en écriture sur le répertoire dans lequel le fichier **mfa_api.properties** est stocké. Par défaut, ce fichier est stocké dans **/var/ace/conf**.
- Le paramètre CA_CERT_FILE_PATH pour le certificat de confiance du serveur peut rester le même. Pour les autres paramètres, collectez les informations requises :
  Pour l'authentification Authentication Manager à l'aide du protocole REST, demandez les informations suivantes à votre super administrateur Authentication Manager :

Paramètre	Description
REST_URL	URL du serveur REST pour la communication entre l'agent d'authentification et l'instance principale de Authentication Manager. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans la première instance, utilisez la valeur *HOSTNAME* du champ **Nom de domaine complet** sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.
REPLICA_*number* où *number* est un nombre compris entre 1 et 15.	Une URL de serveur REST pour chaque instance de réplica pouvant être utilisée pour le basculement. Utilisez le format suivant : `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` Dans l'instance de réplica, utilisez la valeur *HOSTNAME* du champ **Nom de domaine complet** sur la page **Administration > Réseau > Paramètres réseau de l'appliance** de la Console des opérations. Le *PORT* par défaut est 5555.
CLIENT_KEY	Clé d'accès (clé de client) pour transmettre en toute sécurité les demandes d'authentification utilisateur à Authentication Manager. Cette valeur est générée dans la Console de sécurité sur l'instance principale Authentication Manager. Pour obtenir des instructions sur l'obtention de la clé d'accès, consultez la rubrique suivante sur RSA Link : Configurer l'API d'authentification de RSA SecurID pour les agents d'authentification.
CLIENT_ID	Nom de l'agent d'authentification (ID Client) qui a été créé pour PAM agent dans Authentication Manager.

Pour l'authentification à l'aide de Service d'authentification cloud, demandez les informations suivantes à votre super administrateur Service d'authentification cloud :

Paramètre	Description
REST_URL	URL du serveur REST pour la communication entre l'agent et le Service d'authentification cloud. Utilisez le format suivant :

Paramètre	Description
	`https://`*`HOSTNAME`*`:`*`PORT`*`/mfa/v1_1/authn` Pour le Service d'authentification cloud, utilisez la valeur *`HOSTNAME`* du champ **Domaine du service d'authentification** sous l'onglet **Inscription** de la page de paramétrage du routeur d'identité figurant dans la Cloud Administration Console. Le *`PORT`* par défaut est 443.
CLIENT_KEY	Clé API d'authentification (clé client) créée dans Cloud Administration Console pour transférer en toute sécurité les demandes d'authentification utilisateur au Service d'authentification cloud. Pour obtenir des instructions sur l'obtention de la clé API d'authentification, consultez la rubrique suivante sur RSA Link : Add an RSA SecurID Authentication API Key. (Ajouter une clé API d'authentification RSA SecurID)
TENANT_ID	ID de tenant pour le Service d'authentification cloud. PAM agent peut fournir l'ID de tenant dans les demandes d'authentification, mais l'agent ne valide pas les données. Ce paramètre n'est actuellement pas pris en charge par Service d'authentification cloud.
ASSURANCE_POLICY_ID	Nom de stratégie d'accès pour le Service d'authentification cloud.
CLIENT_ID	Nom de l'agent d'authentification à afficher dans les notifications mobiles. Vous pouvez saisir n'importe quelle valeur. Par exemple, PAM_Agent.

Procédure

1. Accédez au répertoire dans lequel se trouve **sd_pam.conf**. L'emplacement par défaut est **/etc**.
2. Ouvrez **sd_pam.conf**.
3. Modifiez le paramètre OPERATION_MODE :
   - Pour Authentication Manager avec le protocole REST, entrez 1.
   - Pour Service d'authentification cloud avec le protocole REST, entrez 2.

   Si le paramètre OPERATION_MODE est 0, non spécifié ou mis en commentaire, PAM agent utilise le mode UDP par défaut.
4. Accédez au répertoire **/var/ace/conf**. Vous devez mettre à jour les valeurs requises pour les paramètres dans le fichier **mfa_api.properties**.
5. Ouvrez **mfa_api.properties**.
6. Supprimez les commentaires pour activer les paramètres requis et commentez les paramètres qui ne sont plus nécessaires.
7. Entrez une valeur pour chaque paramètre requis.
8. Enregistrez le fichier.

   Vous pouvez désormais utiliser le protocole REST avec le nouveau mode d'authentification.

Annexe A : Résolution des problèmes

Problèmes connus liés à la configuration 40
Utilitaires d'authentification pour le Mode UDP 41
Utilitaire de conversion pour le mode UDP 43
Secrets de nœud pour le mode UDP 43
Consignation pour PAM Agent 44
Consignation pour le mode REST 45
Configuration du délai d'expiration et du nombre de nouvelles tentatives pour l'authentification REST 46
Désinstallation de RSA Authentication Agent 8.1 for PAM 47

Problèmes connus liés à la configuration

Cette section décrit les problèmes connus.

Problèmes liés aux outils pris en charge

Outil	Problème connu
dtlogin	**Problème** : Les restrictions d'affichage peuvent engendrer deux problèmes pour les utilisateurs : • Les utilisateurs s'authentifiant ne peuvent pas voir l'intégralité du message à propos des méthodes d'authentification disponibles. • Les utilisateurs de mot de passe de réserve peuvent afficher un champ de saisie de texte partiel sur les écrans, là où cela n'est pas nécessaire. **Solution :** Les utilisateurs s'authentifiant peuvent appuyer sur ENTRÉE, comme indiqué sur l'écran, pour voir le message dans son intégralité. Les utilisateurs de mot de passe de réserver peuvent ignorer le champ inutile.
ftp	• **Problème :** Lorsque vous utilisez SecurID pour protéger le ftp, les invites d'authentification SecurID et les messages d'erreur ne s'affichent pas pour les utilisateurs. Seuls les invites et messages d'erreur du système d'exploitation standard s'affichent. **Solution :** Demandez aux utilisateurs de saisir leur nom d'utilisateur à l'invite de nom d'utilisateur du système d'exploitation, et leur code secret SecurID à l'invite de mot de passe du système d'exploitation. Si un utilisateur ne connaît pas l'état de token (par exemple, si le token est en mode Code de token suivant, ou en mode Nouveau code PIN), l'utilisateur doit s'authentifier avec un autre outil de connexion, comme rlogin pour vérifier que le code PIN ou le code de token est toujours valide. • Le FTP ne gère pas l'intervalle exponentiel. • Vous ne pouvez pas utiliser le Service d'authentification cloud pour protéger le ftp ; toutefois, ce dernier est pris en charge.
ssh	**Problème :** Une fois que l'utilisateur effectue trois tentatives d'authentification SecurID en une seule session, la connexion est interrompue. **Solution :** L'utilisateur peut mettre fin à la session et démarrer une autre session.
rlogin	**Problème :** Avant de configurer rlogin pour qu'il fonctionne avec PAM agent, les connexions rlogin sont fermées. **Solution :** Assurez-vous que rlogin fonctionne avant de configurer PAM agent. Procédez comme suit : 1. Ouvrez le fichier **/etc/xinet, d/rlogin**. 2. Ajoutez **nice = 5** à la fin de la configuration rlogin. 3. Redémarrez les services xinetd : `service xinetd restart`
rlogin	**Problème :** En cas d'échec de la première tentative de traitement d'une demande rlogin, la session est transmise au processus de connexion. **Solution :** Si vous configurez Linux pour utiliser rlogin, vous devez configurer le fichier de connexion à distance dans **/etc/pam.d**.

Outil	Problème connu
rlogin	**Problème :** Lorsqu'un utilisateur tente d'accéder au système via l'outil rlogin et saisit les informations d'identification incorrectes, le système redirige le processus d'authentification vers l'outil telnet et peut inviter à saisir le mot de passe ou le code secret conformément à la configuration telnet. **Solution :** Lorsque rlogin est protégé par SecurID, telnet doit également être protégé par SecurID et vice versa.
rlogin	**Problème :** Si PAM agent est le seul module d'authentification utilisé pour protéger rlogin (en d'autres termes, rlogin est utilisé dans une configuration non empilée) et si le mot de passe incorrect est saisi, le système invite l'utilisateur à saisir le mot de passe UNIX et permet l'accès s'il est entré correctement. **Solution :** Utilisez une configuration empilée.

Problèmes de mise à niveau et de désinstallation

Problème : Si vous décidez de mettre à niveau ou de désinstaller PAM agent sans désactiver le module RSA PAM, vous pouvez recevoir le message d'erreur : « pam_securid.so is busy, not able to remove/replace ».
Solution : Pour résoudre ce problème, vous devez vous connecter avec des outils autres que ssh et supprimer pam_securid.so manuellement.

Utilitaires d'authentification pour le Mode UDP

Les utilitaires d'authentification se trouvent dans les répertoires suivants :

- Système d'exploitation 32 bits : ***répertoire d'installation pam agent*/bin/32bit**
- Système d'exploitation 64 bits : ***répertoire d'installation pam agent*/bin/64bit**

Utilisez ces utilitaires pour :

- Procéder à un test d'authentification. Pour plus d'informations, reportez-vous à la section Exécuter l'utilitaire acetest bas.
- Vérifier la communication entre PAM agent et RSA Authentication Manager. Pour plus d'informations, reportez-vous à la section Exécuter l'utilitaire acestatus Page suivante

Vous pouvez activer la consignation de ces utilitaires. Pour plus d'informations, reportez-vous à la section Activer la consignation de trace SecurID pour le mode UDP Page 29

Exécuter l'utilitaire acetest

Cet utilitaire vérifie que l'agent fonctionne correctement en effectuant un test d'authentification.

Procédure

1. Accédez au répertoire des utilitaires d'authentification PAM agent :
   - Système d'exploitation 32 bits : ***répertoire d'installation pam agent*/bin/32bit**
   - Système d'exploitation 64 bits : ***répertoire d'installation pam agent*/bin/64bit**
2. Saisissez :

   ```
   ./acetest
   ```

3. Saisissez un nom d'utilisateur et un code secret valides.

Si l'accès vous est refusé à plusieurs reprises, testez la connectivité au serveur Authentication Manager avec l'utilitaire Exécuter l'utilitaire acestatus bas ou contactez votre administrateur Authentication Manager.

Exécuter l'utilitaire acestatus

Cet utilitaire vérifie l'état de chaque Authentication Manager où PAM agent est enregistré en tant qu'hôte d'agent. Si vous avez des questions concernant les informations affichées, contactez votre administrateur Authentication Manager.

Procédure

1. Accédez au répertoire des utilitaires PAM agent.
2. Saisissez :

```
./acestatus
```

Le tableau suivant répertorie les informations affichées dans la section Authentication Manager.

Informations renvoyées	Description
Version de configuration	Version du fichier **sdconf.rec** en cours d'utilisation. Pour RSA Authentication Manager 8.0 ou versions ultérieures, ce nombre est de 14.
DES activé	Si votre environnement de configuration prend en charge des protocoles existants, OUI est affiché.
Client Retries	Nombre de fois où PAM agent envoie des données d'authentification à Authentication Manager avant l'expiration du délai.
Expiration du délai client	Durée (en secondes) pendant laquelle PAM agent attend avant de renvoyer les données d'authentification à Authentication Manager.
Version du serveur	Numéro de version de Authentication Manager.
Communication	Version du protocole utilisée par Authentication Manager et PAM agent.

Le tableau suivant répertorie les informations d'état affichées dans la section Authentication Manager.

Informations d'état	Description
Adresse du serveur active	Adresse IP que PAM agent utilise pour communiquer avec le serveur. Cette adresse peut être l'adresse IP réelle du serveur que vous avez sélectionné, ou une adresse IP d'alias attribuée au serveur. L'adresse IP 0.0.0.0 indique que l'agent n'a pas encore reçu la communication du serveur.

Le tableau suivant répertorie les informations d'état de serveur affichées dans la section Authentication Manager.

État du serveur	Description
Available for Authentications	Ce serveur est disponible pour gérer les demandes d'authentification.
Non utilisé	Le serveur n'a pas encore reçu une demande d'authentification.
Pour basculement uniquement	Le serveur est réservé à des fins de basculement uniquement.
Serveur par défaut pendant les requêtes initiales	Seul ce serveur est disponible pour gérer les demandes pour l'instant.

Utilitaire de conversion pour le mode UDP

L'utilitaire de conversion est utilisé lorsqu'un agent PAM basé sur UDP coexiste avec d'autres agents SecurID.

L'utilitaire de conversion ns_conv_util se trouve dans les répertoires suivants :

- Système d'exploitation 32 bits : ***pam agent home*/bin/32bit**
- Système d'exploitation 64 bits : ***pam agent home*/bin/64bit**

Procédure

1. Accédez au répertoire des utilitaires de PAM Agent.
2. Saisissez :

   `./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>`

   où *<chemin_fichier_Securid_existant>* est le chemin où se trouve le fichier SecurID actif,

   et *<nouveau_chemin_rép_Securid>* est le répertoire dans lequel le fichier SecurID récemment généré doit être stocké.

   Par exemple :

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

3. Si le nouvel emplacement de destination n'est pas identique à l'emplacement spécifié par VAR_ACE, copiez le nouveau fichier SecurID à cet emplacement.

Secrets de nœud pour le mode UDP

Le secret de nœud est une clé de chiffrement symétrique qui est utilisée par RSA Authentication Manager et PAM agent pour chiffrer et déchiffrer les paquets de données circulant sur le réseau. Les secrets de nœud sont requis pour les agents qui utilisent le protocole UDP. Le secret de nœud partagé est stocké à la fois dans la base de données Authentication Manager et dans un fichier présent sur l'ordinateur sur lequel PAM agent est installé. Pour les agents qui utilisent le protocole REST, aucun fichier de secret de nœud n'est utilisé. Au lieu d'un secret de nœud, une clé négociée de manière dynamique est utilisée pour chiffrer le canal, ainsi qu'un algorithme de chiffrement fort.

Pour les agents de type UDP, si le secret de nœud est manquant sur le serveur Authentication Manager ou l'ordinateur sur lequel PAM agent est installé, effacez le secret de nœud dans l'autre emplacement. Si les fichiers de secret de nœud présents dans l'instance Authentication Manager et l'ordinateur PAM agent ne concordent pas, effacez le secret de nœud dans les deux emplacements. Après avoir effacé le secret de nœud, vous devez générer un nouveau secret de nœud.

Effacer le secret de nœud dans RSA SecurID Authentication Agent 8.1 for PAM

Si le secret de nœud n'est pas identique dans l'instance RSA SecurID Authentication Agent 8.1 for PAM et l'ordinateur sur lequel PAM agent est installé, ou que le secret de nœud est absent de l'ordinateur PAM agent, vous devez effacer le secret de noeud dans Authentication Manager. Par exemple, si vous réinstallez PAM agent, le secret de nœud est absent de l'ordinateur PAM agent.

Procédure

1. Dans la console de sécurité Authentication Manager, cliquez sur **Accès > Agents d'authentification > Gérer l'existant**.
2. Recherchez l'ordinateur agent concerné et sélectionnez **Gérer le secret de nœud** dans le menu déroulant.
3. Cochez la case **Effacer le secret de nœud**, puis cliquez sur **Enregistrer**.

Après avoir terminé

- Si l'ordinateur PAM agent contient un secret de nœud, consultez la section Effacer le secret de nœud sur l'ordinateur PAM Agent bas.
- Si l'ordinateur PAM agent ne contient pas de secret de nœud, suivez la procédure Générer un nouveau secret de nœud bas.

Effacer le secret de nœud sur l'ordinateur PAM Agent

Si le secret de nœud n'est pas identique dans l'instance RSA Authentication Manager et l'ordinateur PAM agent ou que le secret de nœud est absent de l'instance Authentication Manager, vous devez effacer le secret de noeud sur l'ordinateur PAM agent. Par exemple, si vous installez une nouvelle instance Authentication Manager et que vous ajoutez une instance PAM agent existante, le secret de nœud est absent dans Authentication Manager.

Avant de commencer

S'il existe un secret de nœud dans l'instance Authentication Manager, consultez la section Effacer le secret de nœud dans RSA SecurID Authentication Agent 8.1 for PAM Page précédente.

Procédure

1. Connectez-vous à l'ordinateur sur lequel l'instance PAM agent est installée et recherchez le fichier de secret de nœud **securid**, dans le répertoire **/var/ace**.
2. Renommez ou supprimez le fichier de secret de nœud.
3. Le secret de nœud est également stocké dans le cache du serveur. Redémarrez l'ordinateur pour effacer le secret de noeud dans le cache.

Après avoir terminé

Générer un nouveau secret de nœud bas

Générer un nouveau secret de nœud

Procédure

1. Exécutez l'utilitaire acetest sur l'ordinateur PAM agent pour générer le fichier de secret de nœud. Pour plus d'informations, consultez la section Utilitaires d'authentification pour le Mode UDP Page 41.
2. Consultez vos logs d'authentification pour vous assurer qu'un nouveau secret de nœud a été envoyé.
3. Redémarrez votre ordinateur PAM agent pour que l'agent puisse lire le fichier de secret de nœud.

Consignation pour PAM Agent

Si la consignation est activée, par défaut, les messages d'authentification de PAM agent sont enregistrés dans le

log système. À des fins de suivi, vous pouvez configurer votre log système pour enregistrer les messages de lot d'authentification PAM agent pour des outils spécifiques. Reportez-vous à la section Activation de la sortie de débogage Page 28.

Pour plus d'informations sur l'apport de modifications à la consignation, consultez la documentation syslog-ng disponible avec le système d'exploitation SUSE 11 et SUSE 12.

Messages log d'authentification de PAM Agent

Le tableau suivant répertorie les messages log d'authentification.

Message	Description
Cannot locate **sd_pam.conf** file	Le fichier de configuration **sd_pam.conf** n'est pas dans le répertoire **/etc.** ; **/etc.** doit contenir le fichier de configuration correct afin que VAR_ACE puisse être défini correctement.
AceInitialize failed	AceInitialize est un appel de fonction d'API qui initialise les threads de travail et charge les paramètres de configuration à partir de **sdconf.rec**. Vérifiez que vous disposez de la dernière copie de **sdconf.rec** à partir de votre administrateur Authentication Manager et que VAR_ACE est défini correctement.
Cannot communicate with RSA ACE/Server	Soit les brokers Authentication Manager ne sont pas démarrés, soit il y a une panne réseau. Contactez votre administrateur Authentication Manager ou votre administrateur réseau.
Reserve password exceeds character limit	La limite de caractères maximale est de 256 caractères.
Invalid reserve password	Le mot de passe de réservation est identique au mot de passe du système pour l'hôte. Vous devez connaître ce mot de passe si Authentication Manager est incapable de traiter les demandes d'authentification.
User name exceeds character limit	Le nom d'utilisateur ne doit pas comporter plus de 31 caractères.
Reserve password not allowed. User is not root.	Vérifiez que vous êtes un utilisateur root. Seuls les utilisateurs root peuvent utiliser le mot de passe de réserve.

Consignation pour le mode REST

Le mode REST prend en charge la consignation mise en œuvre avec la bibliothèque **log4cxx**. La consignation de la couche REST est distincte des logs PAM agent. RollingFileAppender et SyslogAppender sont pris en charge. Par défaut, RollingFileAppender est activé. Logs : accéder à **/var/ace/log/mfa_rest.log** avec le niveau de log défini sur INFO. La rotation basée sur la taille est activée avec une taille de rotation de 10 Mo.

La rotation de log temporelle n'est pas prise en charge. Les outils pris en charge, comme ssh et su, chargent l'agent authentification pour chaque requête. PAM agent ne peut donc pas faire tourner les logs d'après la durée. PAM agent prend en charge la rotation de log d'après la taille.

Vous pouvez modifier les paramètres de log par défaut pour le mode REST.

Procédure

1. Accédez au répertoire **/var/ace/conf**.
2. Ouvrez le fichier **log.properties**.
3. Configurez les entrées suivantes pour la rotation d'après la taille :

```
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. Configurez les entrées suivantes pour prendre en charge la consignation locale et à distance dans le 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. Enregistrez vos modifications.
6. Redémarrez le processus syslog.

Configuration du délai d'expiration et du nombre de nouvelles tentatives pour l'authentification REST

Vous pouvez configurer le délai de connexion de PAM agent à RSA Authentication Manager ou au Service d'authentification cloud et le délai pendant lequel l'agent PAM agent attend une réponse. Vous pouvez également configurer le nombre de fois que l'agent PAM agent essaie de contacter une instance principale ou de réplica Authentication Manager ou le Service d'authentification cloud. Ces paramètres ne sont utilisés que par le protocole REST.

Veillez à tenir compte de la vitesse de votre réseau. Lorsque des valeurs de délai d'expiration élevées ont été définies sur un réseau lent, l'authentification aboutit.

Avant de commencer

Vous devez disposer d'autorisations racines sur la machine sur laquelle l'agent est installé et d'autorisations en écriture dans le répertoire dans lequel le fichier **mfa_api.properties** est stocké. Par défaut, ce fichier est stocké dans **/var/ace/conf**.

Procédure

1. Accédez au répertoire dans lequel se trouve **mfa_api.properties**. Par défaut, il s'agit du répertoire **/var/ace/conf**.
2. Ouvrez **mfa_api.properties**.
3. Vous pouvez modifier les paramètres suivants :
    - CONNECT_TIMEOUT. Nombre maximal de secondes autorisé à l'agent pour se connecter au serveur. La valeur par défaut est 60 secondes.
    - READ_TIMEOUT. Nombre maximal de secondes autorisé pour la connexion au serveur et la lecture de la réponse. La valeur READ_TIMEOUT doit être égale à la somme de la valeur CONNECT_TIMEOUT et du délai maximal autorisé pour la lecture de la réponse. La valeur par défaut est 120 secondes.
    - MAX_RETRIES. Nombre de fois que l'agent PAM agent tente de se connecter à Authentication Manager ou au Service d'authentification cloud. La valeur par défaut est 3.
    - Pour la phase d'initialisation de l'interface REST d'Authentication Manager, lorsque le PAM agent démarre une tentative d'authentification, le paramètre MAX_RETRIES correspond au nombre de fois que l'agent tente de contacter le même serveur avant le basculement vers un autre serveur. Pendant la phase de vérification, lorsque l'agent PAM agent fournit les informations d'authentification, le basculement n'est pas pris en charge et le paramètre MAX_RETRIES correspond au nombre de fois que l'agent tente de contacter le même serveur avant l'échec de l'authentification.
    - Le Service d'authentification cloud ne prend pas en charge le basculement. Pour les phases d'initialisation et de vérification, le paramètre MAX_RETRIES correspond au nombre de fois que l'agent tente de contacter le même serveur avant l'échec de l'authentification.
4. Enregistrez le fichier.

Désinstallation de RSA Authentication Agent 8.1 for PAM

Vous pouvez désinstaller manuellement PAM agent sur les différents ordinateurs, ou vous pouvez choisir de désinstaller en mode silencieux et automatique plusieurs copies de PAM agent.

Avant de commencer

- Configurez les outils protégés RSA SecurID pour utiliser le module PAM standard fourni avec votre système d'exploitation, et non pas le module RSA PAM. Les sessions actives utilisant les modules RSA PAM doivent être fermées avant de poursuivre la désinstallation. Vous devez annuler les procédures que vous avez suivies dans Configuration des outils Page 23.

Remarque : Si vous désinstallez le module RSA alors qu'il existe des références au module RSA dans le répertoire **/etc/pam.d**, votre accès à votre système sera verrouillé.

- Vérifiez que vous disposez d'autorisations racines sur l'hôte.

Désinstaller PAM Agent sur un seul ordinateur

Effectuez cette tâche pour désinstaller une seule instance de PAM agent.

Procédure

1. Accédez au répertoire personnel de PAM agent. Par exemple, **/opt/pam**.
2. Exécutez le script de désinstallation. Saisissez :

   ```
   ./uninstall_pam.sh
   ```

3. Vérifiez que le répertoire d'installation a été supprimé. Si le répertoire existe encore, vous devez le supprimer manuellement.
4. Pour vérifier que PAM agent a bien été supprimé, consultez le fichier **var/pam_uninstaller/uninstaller.log**.

Désinstallation en masse de PAM Agent en mode silencieux

Effectuez cette tâche pour désinstaller un grand nombre d'instances PAM agent.

Procédure

1. Créez un fichier de configuration de type texte portant le nom **unconfig**. Ce fichier doit contenir les informations suivantes :

   ```
   y
   y
   y
   ```

   Chaque « y » est la réponse à une invite :

   - 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. Accédez au répertoire personnel de PAM agent. Par exemple, **/opt/pam**.
3. Exécutez le script de désinstallation. Saisissez :

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

Annexe B : Fichiers de configuration critiques

Fichiers de configuration critiques 50

Fichiers de configuration critiques

Le répertoire d'installation PAM agent par défaut est **/opt/pam**, et peut être modifié lors de l'installation. Par défaut, le répertoire **/var/ace** comprend les bibliothèques et les fichiers REST. Cet emplacement de répertoire ne peut pas être modifié.

Outre les fichiers binaires (**pam_securid.so**, **acetest**, **acestatus**, et **ns_conv_util**), PAM agent conserve les fichiers de configuration critiques répertoriés dans le tableau suivant.

Fichier	Description
log.properties	Fichier de configuration de consignation PAM agent pour le protocole REST. PAM agent utilise la bibliothèque **log4cxx** pour la consignation en mode REST.
mfa_ api.properties	Contient les paramètres utilisés par le protocole REST pour l'authentification à Authentication Manager et au Service d'authentification cloud.
sdconf.rec	Ce fichier est généré par RSA Authentication Manager et contient des informations de configuration qui contrôlent le comportement de PAM Agent. Cette autorisation de fichier doit être -rw------- root root. Ce fichier est uniquement utilisé en mode UDP.
sdopts.rec	Ce fichier est utilisé pour l'équilibrage de charge manuel. Il contient une liste d'adresses IP pour les instances Authentication Manager. Cette autorisation de fichier doit être -rw------- root root. Ce fichier est uniquement utilisé en mode UDP.
sdstatus.12	Ce fichier est généré par l'API d'authentification PAM agent pour suivre le dernier état connu des serveurs Authentication Manager. Cette autorisation de fichier doit être -rw------- root root.
sd_pam.conf	Contient des paramètres de configuration qui contrôlent le comportement de PAM agent. Cette autorisation de fichier doit être -rw-r--r-- root root.
securid	Ce fichier contient une clé secrète partagée qui permet de protéger les communications du protocole UDP entre la machine locale et Authentication Manager. Le nom de ce fichier dérive du nom du protocole configuré du système local pour le port sur lequel l'agent communique avec Authentication Manager, généralement via le fichier « services ». Cette autorisation de fichier doit être -r-------- root root. Toutefois, elle dépend également du paramètre OS Umask. Le protocole UDP requiert ce fichier. Ce fichier est facultatif pour l'authentification avec le protocole REST.