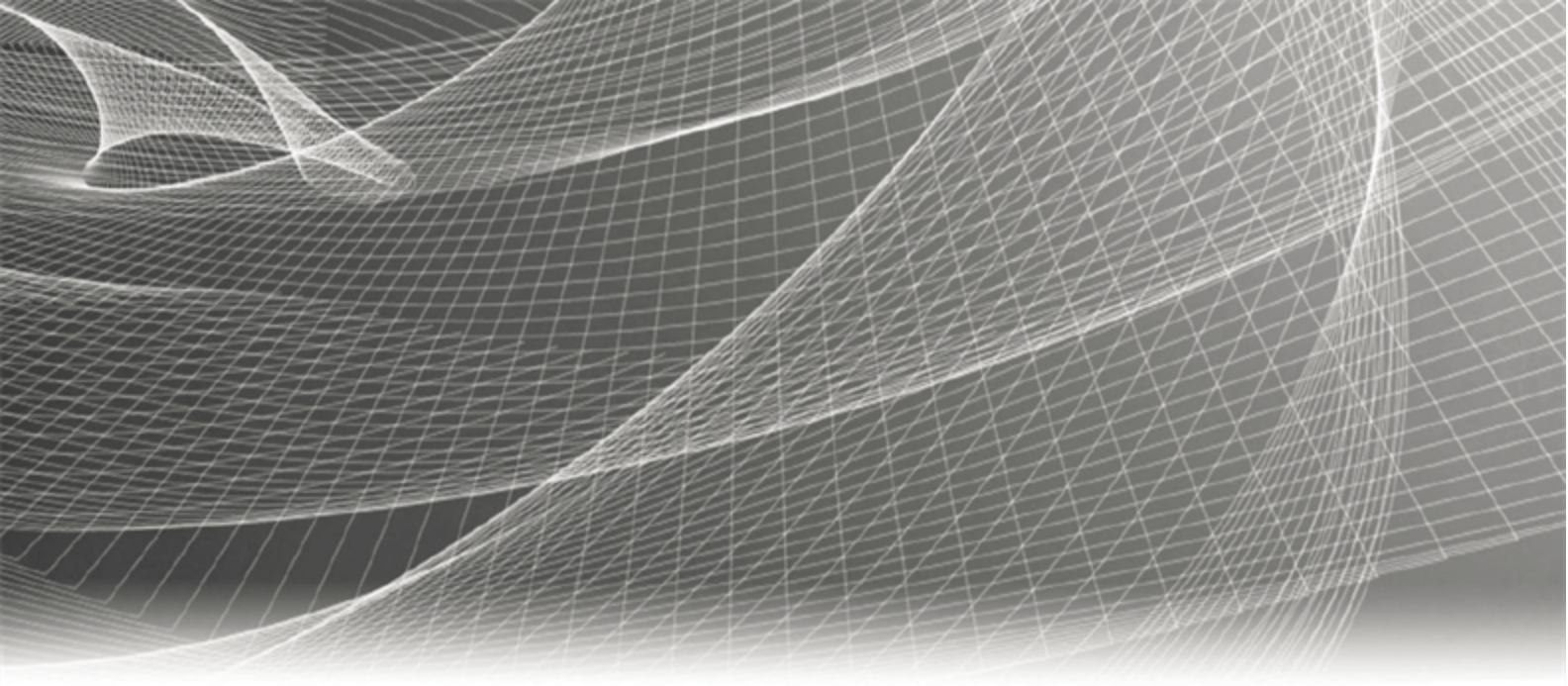

RSA SECURID® ACCESS

RSA SecurID® Authentifizierungs-Agent 8.0 for PAM

Installations- und Konfigurationsleitfaden für Oracle und RHEL

Kontaktinformationen

RSA Link (https://community.rsa.com) enthält eine Wissensdatenbank, in der allgemeine Fragen beantwortet und Lösungen für bekannte Probleme, Produktdokumentationen, Communitydiskussionen und Vorgangsmanagement bereitgestellt werden.

Marken

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

Lizenzvereinbarung

Diese Software und die zugehörige Dokumentation sind Eigentum von Dell Inc. oder ihren Tochtergesellschaften und vertraulich. Sie werden unter Lizenz bereitgestellt und dürfen nur gemäß den Bedingungen der betreffenden Lizenz und unter Einschluss des untenstehenden Copyright-Hinweises verwendet und kopiert werden. Diese Software und die Dokumentation sowie alle Kopien dürfen anderen Personen nicht überlassen oder auf andere Weise zur Verfügung gestellt werden.

Dabei werden keine Ansprüche oder Eigentumsrechte an der Software oder Dokumentation oder Rechte an geistigem Eigentum daran übertragen. Die unberechtigte Nutzung oder die Vervielfältigung dieser Software und der Dokumentation kann zivil- und/oder strafrechtlich verfolgt werden.

Diese Software kann ohne Vorankündigung geändert werden und sollte nicht als Verpflichtung seitens Dell Inc. ausgelegt werden.

Lizenzen von Drittanbietern

Dieses Produkt kann Software enthalten, die von anderen Anbietern als RSA entwickelt wurde. Der Text der Lizenzvereinbarungen, die sich auf Drittanbietersoftware in diesem Produkt beziehen, ist auf der Produktdokumentationsseite auf RSA Link verfügbar. Mit der Verwendung dieses Produkts verpflichtet sich der Benutzer zur uneingeschränkten Einhaltung der Bedingungen der Lizenzvereinbarungen.

Hinweis zu Verschlüsselungstechnologien

Dieses Produkt kann Verschlüsselungstechnologie enthalten. In vielen Ländern ist die Verwendung, das Importieren oder Exportieren von Verschlüsselungstechnologien untersagt. Die aktuellen Bestimmungen zum Verwenden, Importieren und Exportieren sollten beim Verwenden, Importieren und Exportieren dieses Produkts eingehalten werden.

Verteilung

Für die Nutzung, das Kopieren und die Verbreitung der in dieser Veröffentlichung beschriebenen Software von Dell ist eine entsprechende Softwarelizenz erforderlich.

Dell Inc. ist der Ansicht, dass die Informationen in dieser Veröffentlichung zum Zeitpunkt der Veröffentlichung korrekt sind. Diese Informationen können jederzeit ohne vorherige Ankündigung geändert werden.

DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN WERDEN OHNE GEWÄHR ZUR VERFÜGUNG GESTELLT. DELL INC. MACHT KEINE ZUSICHERUNGEN UND ÜBERNIMMT KEINE HAFTUNG JEDWEDER ART IM HINBLICK AUF DIE IN DIESEM DOKUMENT ENTHALTENEN INFORMATIONEN UND SCHLIESST INSBESONDERE JEDWEDE IMPLIZITE HAFTUNG FÜR DIE HANDELSÜBLICHKEIT UND DIE EIGNUNG FÜR EINEN BESTIMMTEN ZWECK AUS.

Dezember 2017

Inhalt

Vorwort **7**
Zielgruppe 7
Support und Service 7
RSA Ready Partner Program 7
Kapitel 1: Installieren von PAM Agent **9**
Übersicht über RSA SecurID Authentication Agent 8.0 for PAM 10
Authentifizierungsmodi 11
PAM Agent-Workflow 11
Softwareanforderungen 12
Erforderliche Betriebssysteme 12
SELinux-Anforderungen 13
RSA Authentication Manager-Versionsunterstützung 13
Cloudauthentifizierungsservice-Versionsunterstützung 14
Zertifikatanforderungen 14
Unterstützte Tools 14
OpenSSH-Unterstützung (optional) 14
Planung der Installation von PAM Agent 14
Installieren von RSA SecurID Authentication Agent 8.0 for PAM 17
Angeben der Agent-IP-Adresse für den UDP-Modus 17
Konfigurieren von OpenSSH 17
Installieren von PAM Agent 18
Installieren von PAM Agent auf einem Computer 18
Masseninstallation von PAM Agent mit der automatischen Installation 20
Aktivieren von SELinux 21
Durchführen eines Upgrades auf RSA SecurID Authentication Agent 8.0 for PAM 22
Konfigurieren von Tools 23
Konfigurieren von telnet 23
Konfigurieren von login 24
Konfigurieren von rlogin 24
Konfigurieren von su 24
Konfigurieren von ssh und zugehörigen Tools 25

Konfigurieren von sudo 25
Konfigurieren von ftp 25
Konfigurieren von gdm 26
Kapitel 2: Konfigurieren von Funktionen 27
Konfigurieren von Agent- und UNIX-Funktionen 28
Aktivieren des Agent-Reportings für RSA SecurID Authentication Agent 8.0 for PAM 28
Aktivieren der Debug-Ausgabe 28
Aktivieren der SecurID-Trace-Protokollierung für den UDP-Modus 29
Konfigurieren kombinierbarer Module 29
Verwenden von Reservepasswörtern 31
Aktivieren der selektiven SecurID-Authentifizierung 31
Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Gruppen 31
Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Benutzer 32
Konfigurieren der exponentiellen Backoff-Zeit 32
Ändern des PAM Agent-Authentifizierungsmodus 33
Wechseln vom UDP-Protokoll zum REST-Protokoll 33
Wechseln vom REST-Protokoll zum UDP-Protokoll 35
Wechseln zwischen RSA Authentication Manager und dem Cloudauthentifizierungsservice 36
Anhang A: Troubleshooting 39
Bekannte Konfigurationsprobleme 40
Probleme mit unterstützten Tools 40
Probleme bei Upgrade und Deinstallation 41
Authentifizierungsdienstprogramme für den UDP-Modus 41
Ausführen des acetest-Dienstprogramms 42
Ausführen des acestatus-Dienstprogramms 42
Konvertierungsdienstprogramm für den UDP-Modus 43
Node-Schlüssel für den UDP-Modus 43
Löschen des Node-Schlüssels aus RSA SecurID Authentication Agent 8.0 for PAM 44
Löschen des Node-Schlüssels vom PAM Agent-Computer 44
Erzeugen eines neuen Node-Schlüssels 45
Protokollierung für PAM Agent 45
Konfigurieren des Systemprotokolls 45
PAM Agent-Authentifizierungsprotokollmeldungen 45

Protokollierung für den REST-Modus 46
Troubleshooting von SELinux 47
Verwenden des REST-Protokolls auf einem aktualisierten Agent 47
Aktivieren der benutzerdefinierten Pfadeinstellungen 47
Konfigurieren der Werte für Timeout und Retry für die REST-Authentifizierung 48
Deinstallieren von RSA SecurID Authentication Agent 8.0 for PAM 49
Deinstallieren von PAM Agent von einem Computer 49
Massendeinstallation von PAM Agent im unbeaufsichtigten Modus 49
Anhang B: Wichtige Konfigurationsdateien 51
Wichtige Konfigurationsdateien 52

Vorwort

Zielgruppe

Dieses Handbuch richtet sich an Netzwerk- und Systemadministratoren, die für Installation, das Upgrade und das Troubleshooting von RSA SecurID® Authentication Agent for PAM (Pluggable Authentication Module) verantwortlich sind.

Support und Service

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

RSA Ready Partner Program

Die Website des RSA Ready Partner Program enthält unter www.rsaready.com Informationen über Hardware- und Softwareprodukte von Drittanbietern, die für den Einsatz mit RSA-Produkten zertifiziert sind. Die Website stellt Leitfäden für die Implementierung mit detaillierten Anweisungen sowie weitere Informationen zur Interoperabilität von RSA- und Drittanbieterprodukten bereit.

Kapitel 1: Installieren von PAM Agent

Übersicht über RSA SecurID Authentication Agent 8.0 for PAM 10
Softwareanforderungen 12
Planung der Installation von PAM Agent 14
Installieren von RSA SecurID Authentication Agent 8.0 for PAM 17
Durchführen eines Upgrades auf RSA SecurID Authentication Agent 8.0 for PAM 22
Konfigurieren von Tools 23

Übersicht über RSA SecurID Authentication Agent 8.0 for PAM

RSA SecurID Authentication Agent 8.0 for PAM (Pluggable Authentication Module) unterstützt die Authentifizierung auf UNIX-Systemen mit Standard- oder OpenSSH-Verbindungstools. PAM Agent verwendet angepasste gemeinsame RSA-Bibliotheken und unterstützt den Zugriff auf UNIX-Server und -Workstations mit den von Cloudauthentifizierungsservice und RSA Authentication Manager unterstützten Authentifizierungsmethoden.

Sie können auswählen, ob PAM Agent die Authentifizierung bei dem Cloudauthentifizierungsservice oder Authentication Manager durchführt. Die RSA SecurID Access Enterprise Edition-Lizenz und die Premium Edition-Lizenz enthalten beide Komponenten von RSA SecurID Access. Es ist nicht erforderlich, dass Authentication Manager PAM Agent verwendet.

Version 8.0 von PAM Agent bietet die folgenden neuen Vorteile:

- Unterstützung für den Cloudauthentifizierungsservice. Der Cloudauthentifizierungsservice verwendet Multifaktor-Authentifizierungsmethoden wie Approve (für Mobilgeräte optimierte Push-Benachrichtigung), Authenticate Tokencode, Gerätebiometrie und RSA SecurID-Token, um einen sicheren Zugriff auf Software as a Service (SaaS) und lokale Webanwendungen für Benutzer bereitzustellen.
- Möglichkeit für den Zugriff auf Authentication Manager mit dem REST-Protokoll anstelle des UDP-Protokolls
- Fortsetzung der Unterstützung für das UDP-Protokoll, das von früheren Versionen von PAM Agent verwendet wurde
- Authentication Manager bietet Agent Berichte, mit denen Sie Ihr in PAM Agent installiertes REST-Protokoll managen können. Im REST-Modus kann PAM Agent zusätzliche Informationen an den Authentication Manager-Server senden, beispielsweise eine eindeutige Software-ID-Nummer für jede installierte Instanz von PAM Agent und Informationen zu den vom Agent verwendeten Betriebssystem.

Die Verwendung von PAM Agent im REST-Modus bietet zusätzliche Vorteile im Vergleich zur Verwendung des UDP-Protokolls:

- Ihre Authentication Manager-Bereitstellung kann den Cloudauthentifizierungsservice einfacher integrieren.
- Sie können in Authentication Manager einen Authentifizierungs-Agent-Datensatz hinzufügen und verwalten und diesen verwenden, um mehrere installierte Agents darzustellen.
- Sie können mehrere Authentifizierungs-Agents einfacher auf derselben Hardware ausführen als mit dem UDP-Protokoll.
- Für Bereitstellungen, bei denen der Authentifizierungs-Agent IPv4-Netzwerkeinstellungen oder das IPv4-Protokoll verwenden muss, wird das TCP-Protokoll verwendet.
- In den REST-Protokollauthentifizierungsmodi wird in Version 8.0 von PAM Agent das FIPS-vorgabenkonforme kryptografische Bibliotheksmodul **fips-2.0.16** mit der OpenSSL-Version 1.0.2l verwendet. Weitere Informationen finden Sie in *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* unter https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.
- Es sind weniger Aktualisierungen des Authentifizierungs-Agent für neue Funktionen und Verbesserungen erforderlich als bei Authentifizierungs-Agents, die das REST-Protokoll nicht verwenden. Authentifizierungs-Agents, die das REST-Protokoll verwenden, nutzen mit höherer

Wahrscheinlichkeit Änderungen in Authentication Manager und reduzieren damit die Anzahl der erforderlichen Aktualisierungen für mehrere Agents.

Authentifizierungsmodi

Sie können PAM Agent in einem von drei Authentifizierungsmodi installieren. Alle Modi stellen eine Authentifizierung über RSA SecurID bereit. Sie können den Modus nach der Installation nach Bedarf ändern. Anweisungen dazu finden Sie unter Ändern des PAM Agent-Authentifizierungsmodus auf Seite 33.

Authentifizierungsmodus	Beschreibung
RSA Authentication Manager mit dem UDP-Protokoll	RSA SecurID-Hardware- und Softwareauthentifikatoren erzeugen RSA SecurID-Tokencodes. Der Agent überprüft, ob die vom Benutzer eingegebenen Daten mit den in Authentication Manager gespeicherten Daten übereinstimmen und gewährt oder verweigert den Zugriff basierend auf dem Ergebnis. Standardmäßig wird der Agent beim PAM Agent-Upgrade für die Verwendung des UDP-Protokolls konfiguriert. Sie können mühelos zu einem anderen Authentifizierungsmodus wechseln, der das REST-Protokoll verwendet.
RSA Authentication Manager mit dem REST-Protokoll	Diese Option bietet Unterstützung für alle Arten der Authentifizierung, die von Authentication Manager über das REST-Protokoll unterstützt werden, z. B. RSA SecurID-Software- und Hardwaretoken und Authenticate Tokencode über eine Integration in die Cloudauthentifizierungsservice-Komponente.
Cloudauthentifizierungsservice mit dem REST-Protokoll	Unterstützt Approve (für Mobilgeräte optimierte Push-Benachrichtigung), Authenticate Tokencode, Gerätebiometrie und RSA SecurID-Token. FIDO-Token, SMS-Tokencodes und Voice-Tokencodes werden nicht unterstützt.

RSA SecurID Authentication Agent 8.0 for PAM unterstützt vertrauenswürdige RSA Authentication Manager. Authentication Manager Risk-based Authentication (RBA) wird nicht unterstützt.

PAM Agent-Workflow

PAM Agent wird auf einem UNIX-Server installiert. Die Lösung fungiert als Vermittler zwischen sich authentifizierenden Benutzern und dem RSA Authentication Manager-Server oder dem Cloudauthentifizierungsservice.

PAM Agent unterstützt Authentication Manager-Sicherheitsfunktionen. Wenn Authentication Manager beispielsweise feststellt, dass für den mit einem bestimmten Token verbundenen Benutzer eine neue PIN erforderlich ist, fordert der Agent die PIN an, deren Merkmale in Authentication Manager definiert sind, und sendet die Informationen an Authentication Manager. Wenn Authentication Manager den nächsten im Token des Benutzers angezeigten Tokencode anfordert, zeigt PAM Agent eine Eingabeaufforderung für den Benutzer an. Wenn Sie der korrekte nächste Tokencode nicht an Authentication Manager gesendet wird, schlägt die Authentifizierung fehl.

In den folgenden Schritten ist der Authentifizierungsablauf für PAM Agent in allen drei Authentifizierungsmodi beschrieben:

1. Ein Benutzer versucht, auf einen von PAM Agent geschützten Computer zuzugreifen, entweder lokal mithilfe von „login“ oder remote mit Tools wie rlogin, telnet, SSH und FTP.

Der Benutzer muss lokal auf dem Computer vorhanden sein, auf dem PAM Agent installiert ist.

2. Die UNIX-PAM-Infrastruktur (Pluggable Authentication Module) fängt alle Anmeldeanforderungen ab und nutzt PAM-Konfigurationsdateien, um auf das RSA-PAM-Modul zuzugreifen:
    - Wenn ein Benutzer nicht für die RSA SecurID-Authentifizierung konfiguriert ist, lässt das RSA-PAM-Modul zu, dass die Anforderung erfolgreich ist.
    - Wenn der Benutzer, der den Zugriff anfordert, von RSA SecurID aufgefordert wird, setzt PAM Agent die Authentifizierung mit Schritt 3 fort.
3. Basierend auf dem PAM Agent-Authentifizierungsmodus kontaktiert der Agent entweder Authentication Manager oder den Cloudauthentifizierungsservice.

    Für Authentication Manager mit einer UDP-Verbindung oder dem REST-Protokoll finden die folgenden Schritte statt:

    a. Der Agent fordert den Benutzer auf, den Benutzernamen und dann den Passcode einzugeben.
    b. Der Agent sendet den Benutzernamen und Passcode auf sichere Weise an Authentication Manager:
        - Wenn Authentication Manager die Anforderung genehmigt, gewährt der Agent dem Benutzer den Zugriff.
        - Wenn Authentication Manager die Anforderung nicht genehmigt, verweigert der Agent den Zugriff.

    Für den Cloudauthentifizierungsservice finden die folgenden Schritte statt:

    a. Der Agent fordert den Benutzer auf, einen Benutzernamen einzugeben, und sendet die Informationen an den Cloudauthentifizierungsservice.
    b. Der Cloudauthentifizierungsservice stellt dem Agent die für den Benutzer in der Sicherheitsebene der Cloudauthentifizierungsservice-Zugriffsrichtlinie konfigurierten Authentifizierungsmethoden bereit.
    c. Der Agent fordert den Benutzer zur Authentifizierung auf.
    d. Der Benutzer wählt eine verfügbare Authentifizierungsmethode aus und authentifiziert sich:
        - Wenn der Cloudauthentifizierungsservice die Anforderung genehmigt, gewährt der Agent dem Benutzer den Zugriff.
        - Wenn eine Authentifizierungsmethode nicht erfolgreich ist, fordert der Cloudauthentifizierungsservice die nächste Authentifizierungsmethode beim Benutzer an.
        - Wenn der Cloudauthentifizierungsservice die Anforderung nicht genehmigt, verweigert der Agent den Zugriff.

Softwareanforderungen

In diesem Abschnitt werden die von PAM Agent unterstützten Mindestsoftwareversionen beschrieben.

Erforderliche Betriebssysteme

Für PAM Agent ist eins der folgenden Betriebssysteme erforderlich:

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

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

SELinux-Anforderungen

Wenn SELinux auf einem RHEL- oder Oracle Linux-System aktiviert ist, müssen Sie die folgenden Pakete vor der Installation von RSA Authentication Agent 8.0 for PAM installieren:

selinux-policy-devel*.noarch.rpm
policycoreutils-devel*.rpm

Wenn SELinux unter RHEL 6.8 32-Bit und 64-Bit oder Oracle Linux 6.8 64-Bit aktiviert ist, müssen Sie vor der Installation von RSA SecurID Authentication Agent 8.0 for PAM die folgenden Pakete installieren:

setools-libs-3.3.7-4.el6.x86_64.rpm
setools-libs-python-3.3.7-4.el6.x86_64.rpm
audit-libs-python-2.4.5-3.el6.x86_64.rpm
libsemanage-python-2.0.43-5.1.el6.x86_64.rpm
policycoreutils-python-2.0.83-29.0.1.el6.x86_64
setroubleshoot-plugins-3.0.40-2.0.1.el6.noarch
setroubleshoot-server-3.0.47-11.0.1.el6.x86_64

RSA Authentication Manager-Versionsunterstützung

RSA SecurID Authentication Agent 8.0 for PAM unterstützt die Version 1.1 der RSA SecurID-Authentifizierungs-API, die die aktuelle Version der REST APIs ist.

In der folgenden Tabelle sind die RSA Authentication Manager-Versionen aufgeführt, die erforderlich sind, um bestimmte Funktionen zu unterstützen.

Erforderliche RSA Authentication Manager-Version	Unterstützte Funktion
8.2 SP1 oder höher	Für PAM Agent ist RSA Authentication Manager 8.2 SP1 oder höher erforderlich.
8.2 SP1 Patch 5 oder höher	Wenn das Agent-Reporting-Flag in PAM Agent aktiviert ist, ist RSA Authentication Manager 8.2 SP1 Patch 5 oder höher erforderlich, um fehlgeschlagene Authentifizierungen im REST-Modus zu vermeiden.
8.3	RSA Authentication Manager 8.3 enthält Agent-Berichte, mit denen Sie Ihre installierten PAM Agent-Instanzen mit REST-Protokoll verwalten können. Diese Berichte beinhalten die zusätzlichen Informationen, die PAM Agent an Authentication Manager senden kann.

Cloudauthentifizierungsservice-Versionsunterstützung

RSA SecurID Authentication Agent 8.0 for PAM unterstützt die Version 1.1 der RSA SecurID-Authentifizierungs-API, die die aktuelle Version der REST APIs ist.

Zertifikatanforderungen

PAM Agent verwendet TLS 1.2-Zertifikate für das REST-Protokoll. Der Cloudauthentifizierungsservice und RSA Authentication Manager 8.2 oder höher können diese Zertifikate akzeptieren. Bereitstellungen, die keine TLS 1.2-Zertifikate verwenden, müssen den Authentifizierungsmodus nutzen, der Authentication Manager mit dem UDP-Protokoll unterstützt.

In den REST-Protokollauthentifizierungsmodi wird in PAM Agent das FIPS-vorgabenkonforme kryptografische Bibliotheksmodul **fips-2.0.16** mit der OpenSSL-Version 1.0.2l verwendet. Weitere Informationen finden Sie in *OpenSSL FIPS 140-2 Security Policy Version 2.0.16* unter https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf.

Unterstützte Tools

PAM Agent unterstützt die folgenden Tools:

- telnet
- login
- rlogin
- su
- sudo

  Sie können die unterstützte sudo-Version von https://www.sudo.ws herunterladen und installieren.

- ftp (begrenzt auf eine einzige Transaktion)
- gdm

OpenSSH-Unterstützung (optional)

PAM Agent unterstützt OpenSSH 6.0 P1. Wenn Sie OpenSSH nutzen, überprüfen Sie, ob Sie die kompatible Version von OpenSSH für Ihre Plattform verwenden. OpenSSH ist nicht erforderlich.

Die folgenden optionalen OpenSSH-Tools werden unterstützt:

- ssh
- sftp
- scp

Installieren Sie OpenSSH auf dem Agent-Computer. Weitere Informationen zu OpenSSH, einschließlich der Voraussetzungen und der zusätzlichen für die Kompilierung des Quellcodes erforderlichen Software, finden Sie unter https://www.openssh.com.

Planung der Installation von PAM Agent

Führen Sie vor der Installation von PAM Agent die folgenden Schritte aus:

- Auf dem Computer, auf dem Sie PAM Agent installieren:
    1. Sorgen Sie dafür, dass Sie Root-Berechtigungen erhalten.
    2. Erstellen Sie das Verzeichnis**/var/ace** für PAM Agent-Konfigurationsdateien, falls es noch nicht vorhanden ist, und erstellen Sie ein Installationsverzeichnis.
    3. Rufen Sie das vertrauenswürdige Serverstammzertifikat der Zertifizierungsstelle von RSA Authentication Manager oder dem Cloudauthentifizierungsservice ab. Gehen Sie folgendermaßen vor:
        a. Stellen Sie sicher, dass das Zertifikat nicht abgelaufen ist.
        b. Speichern Sie das Zertifikat im PEM-Format. Wenn mehrere Zertifizierungsstellenzertifikate vorhanden sind, müssen diese in einer einzigen Datei im PEM-Format verkettet werden.
        c. Kopieren Sie ***filename*.pem** in das Verzeichnis **/var/ace/**.
        d. Schützen Sie das Verzeichnis **/var/ace/**, in dem sich die Zertifikate befinden, mit den entsprechenden Berechtigungen.
- Erstellen Sie für die Authentifizierung mit RSA Authentication Manager einen Authentifizierungs-Agent-Datensatz für PAM Agent in der internen Datenbank. Weitere Informationen erhalten Sie von Ihrem Authentication Manager-Superadministrator oder in der Authentication Manager-Hilfe auf RSA Link.
- Zur Authentifizierung mit dem UDP-Protokoll müssen Sie die Authentication Manager-Konfigurationsdatei **sdconf.rec** erzeugen oder von Ihrem Authentication Manager-Superadministrator erhalten. Für die Authentifizierung mit dem REST-Protokoll ist diese Datei nicht erforderlich.

  Die Datei **sdconf.rec** gibt an, wie der Agent mit der primären Instanz und Replikatinstanzen von Authentication Manager per IP-Adresse kommuniziert. Gehen Sie folgendermaßen vor:

    - Stellen Sie sicher, dass sich die neueste Version der Datei **sdconf.rec** in einem zugänglichen Verzeichnis auf dem Agent-Computer befindet, z. B. im Standardverzeichnis **/var/ace**.
    - Sie benötigen eine Schreibberechtigung für das Verzeichnis, in dem die Datei **sdconf.rec** gespeichert ist.
- Im Authentifizierungsmodus, der Cloudauthentifizierungsservice mit dem REST-Protokoll verwendet, nutzt PAM Agent den Cloudauthentifizierungsservice für Lastenausgleich und Failover.
- Im Authentifizierungsmodus, der RSA Authentication Manager mit dem REST-Protokoll verwendet, bietet PAM Agent keine Unterstützung für den Lastenausgleich. PAM Agent unterstützt das Failover auf maximal 15 Authentication Manager-Replikatinstanzen.
- Erfassen Sie die Informationen, die Sie während der Installation von PAM Agent bereitstellen werden.

  Authentication Manager mit dem UDP-Protokoll: Sie können die Standardwerte beibehalten oder neue Verzeichnisse angeben.

Beschreibung	**Ihr Plan**
Verzeichnis, in dem sich **sdconf.rec** befindet. Der Standardwert ist **/var/ace/**.	
Stammpfad für das Verzeichnis PAM Agent. Der Standardwert ist **/opt**.	

  Authentication Manager mit dem REST-Protokoll: Bitten Sie Ihren Authentication Manager-Superadministrator um die folgenden Informationen:

Beschreibung	Ihr Plan
REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und der primären Authentication Manager-Instanz. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn	
Anzahl der Authentication Manager-Replikatinstanzen, die für ein Failover verwendet werden können	
REST-Server-URL für jede Replikatinstanz. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn	
Zugriffsschlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an Authentication Manager. Dieser Wert wird in der Sicherheitskonsole auf der primären Authentication Manager-Instanz erzeugt.	
Geben Sie das Verzeichnis und den Dateinamen für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent ein. Der Standardwert ist **/var/ace/cert.pem**.	
Name des Authentifizierungs-Agent (Client-ID), der für PAM Agent in Authentication Manager erstellt wurde.	
Stammpfad für das Verzeichnis PAM Agent. Der Standardwert ist **/opt**.	

Cloudauthentifizierungsservice mit dem REST-Protokoll: Bitten Sie den Cloudauthentifizierungsservice-Superadministrator um die folgenden Informationen:

Beschreibung	Ihr Plan
REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und dem Cloudauthentifizierungsservice. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn	
Der in der Cloudadministrationskonsole erstellte Authentifizierungs-API-Schlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an den Cloudauthentifizierungsservice	
Verzeichnis und Dateiname für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent. Der Standardwert ist **/var/ace/cert.pem**.	
Mandanten-ID für den Cloudauthentifizierungsservice. PAM Agent kann die Mandanten-ID in Authentifizierungsanforderungen bereitstellen, aber die Daten werden nicht vom Agent überprüft. Dieser Parameter wird derzeit nicht vom Cloudauthentifizierungsservice unterstützt.	
Name der Zugriffs-Policy für den Cloudauthentifizierungsservice. Diese Policy wird in der Cloudadministrationskonsole definiert.	
CLIENT_ID für den Namen des Authentifizierungs-Agent, die in mobilen Benachrichtigungen angezeigt wird. Sie können einen beliebigen Wert eingeben. Beispiel: PAM_Agent.	
Stammpfad für das Verzeichnis PAM Agent. Der Standardwert ist **/opt**.	

Installieren von RSA SecurID Authentication Agent 8.0 for PAM

Führen Sie zum Installieren von PAM Agent die folgenden Aufgaben durch:

1. Angeben der Agent-IP-Adresse für den UDP-Modus unten
2. Konfigurieren von OpenSSH unten
3. Installieren von PAM Agent Auf der nächsten Seite
4. Führen Sie für den UDP-Modus eine Testauthentifizierung durch. Weitere Informationen finden Sie unter Authentifizierungsdienstprogramme für den UDP-Modus auf Seite 41.

   Testen Sie für den REST-Protokollmodus die Verbindung, indem Sie mit einem beliebigen Browser oder HTTP-Client auf die REST-Server-URL zugreifen. Geben Sie beispielsweise „https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn" ein. Da Sie derzeit keine Authentifizierung durchführen, sollte im Browser oder HTTP-Client die HTTP-Antwort „Forbidden" oder „Unauthorized" angezeigt werden.

5. Aktivieren von SELinux auf Seite 21 (falls erforderlich).

Angeben der Agent-IP-Adresse für den UDP-Modus

Für den UDP-Modus müssen Sie die Datei **sdopts.rec** in dem Verzeichnis erstellen, das von der Datei **sdconf.rec** verwendet wird. Dieses Verfahren gilt nicht für den REST-Modus.

Datei	Beschreibung
sdopts.rec	Listet die IP-Adresse für den Computer auf, auf dem der Agent installiert ist. Der Agent verwendet die IP-Adresse in der Datei **sdopts.rec**, um mit RSA Authentication Manager zu kommunizieren.
sdconf.rec	Gibt die IP-Adressen an, die von Authentication Manager verwendet werden.

Verfahren

1. Verwenden Sie auf dem Agent-Computer einen Texteditor, um eine **sdopts.rec**-Datei in dem Pfad zu erstellen, in dem die Datei **sdconf.rec** gespeichert ist.
2. Geben Sie in der Datei Folgendes ein:

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

   Dabei ist *x.x.x.x* die IP-Adresse des Agent-Hosts.

   Hinweis: Verwenden Sie nur Großbuchstaben und fügen Sie keine Leerzeichen ein.

3. Speichern Sie die Datei.

Konfigurieren von OpenSSH

Bei Verwendung von OpenSSH, der Suite mit sicherheitsbezogenen Netzwerkdienstprogrammen auf der Basis des SSH-Protokolls (Secure Shell) müssen Sie diese Software für die Zusammenarbeit mit PAM Agent und die Anzeige von Passcode-Authentifizierungsmeldungen für Benutzer konfigurieren.

Bevor Sie beginnen

Installieren Sie OpenSSH auf dem Agent-Computer. Weitere Informationen zu OpenSSH, einschließlich der Voraussetzungen und der zusätzlichen für die Kompilierung des Quellcodes erforderlichen Software, finden Sie unter https://www.openssh.com.

Verfahren

1. Öffnen Sie auf dem Agent-Computer die Datei **sshd_config**.
2. Legen Sie die folgenden Parameter fest und speichern Sie die Änderungen:

Parameter	Einstellung
UsePAM	yes
PasswordAuthentication	no
UsePrivilegeSeparation	no
ChallengeResponseAuthentication	yes

   Bei Festlegung des PasswordAuthentication-Parameters auf „no" wird die OpenSSH-Passworteingabeaufforderung deaktiviert. Stattdessen wird PAM Agent verwendet. Deshalb wird der Benutzer nur zur Eingabe der SecurID-Authentifizierung aufgefordert.

3. Starten Sie sshd neu. Geben Sie Folgendes ein:

```
service sshd restart
```

Installieren von PAM Agent

Sie können PAM Agent entweder manuell auf den einzelnen Computern installieren oder Sie können sich für eine automatische Installation entscheiden, um den Prozess der Bereitstellung mehrerer Kopien von PAM Agent zu automatisieren.

Installieren von PAM Agent auf einem Computer

Führen Sie die folgende Aufgabe aus, um eine PAM Agent-Instanz zu installieren. Informationen zum Installieren von PAM Agent auf mehreren Computern finden Sie unter Masseninstallation von PAM Agent mit der automatischen Installation auf Seite 20.

Verfahren

1. Wechseln Sie auf dem Agent-Computer zum Verzeichnis mit dem PAM Agent-Installationsprogramm.
2. Entpacken Sie die Datei, indem Sie Folgendes eingeben:

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

3. Führen Sie das Installationsskript aus, indem Sie Folgendes eingeben:

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

4. Befolgen Sie die Eingabeaufforderungen. Drücken Sie die EINGABETASTE, um den Standardwert zu übernehmen, oder geben Sie den entsprechenden Wert ein.

   Gehen Sie für den RSA Authentication Manager-UDP-Modus wie folgt vor:

   - Akzeptieren Sie die Lizenz für die RSA-Software.
   - Geben Sie 0 ein, um RSA Authentication Manager mit dem UDP-Protokollauthentifizierungsmodus auszuwählen.
   - Öffnen Sie das Verzeichnis, in dem sich **sdconf.rec** befindet.
   - Öffnen Sie das PAM Agent-Installationsverzeichnis.

   Gehen Sie für den RSA Authentication Manager-REST-Modus wie folgt vor:

- Akzeptieren Sie die Lizenz für die RSA-Software.
- Geben Sie 1 ein, um RSA Authentication Manager mit dem REST-Protokollauthentifizierungsmodus auszuwählen.
- Geben Sie die REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und der primären Instanz ein.
- Geben Sie „y" ein, wenn Authentication Manager-Replikatinstanzen für das Failover vorhanden sind.
- Geben Sie die Anzahl der Replikatinstanzen ein.
- Geben Sie die REST-Server-URL für jede Replikatinstanz ein.
- Geben Sie den Clientschlüssel (Zugriffsschlüssel) für die sichere Übergabe von Authentifizierungsanforderungen an Authentication Manager ein.
- Geben Sie das Verzeichnis und den Dateinamen für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent ein.
- Geben Sie die Client-ID ein, die dem Namen des Authentifizierungs-Agent in Authentication Manager entspricht.
- Öffnen Sie das PAM Agent-Installationsverzeichnis.

Gehen Sie für den Cloudauthentifizierungsservice-REST-Modus wie folgt vor:

- Akzeptieren Sie die Lizenz für die RSA-Software.
- Geben Sie 2 ein, um Cloudauthentifizierungsservice mit dem REST-Protokollauthentifizierungsmodus auszuwählen.
- Geben Sie die REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und dem Cloudauthentifizierungsservice ein.
- Geben Sie den Clientschlüssel (Authentifizierungs-API-Schlüssel) für die sichere Übergabe von Authentifizierungsanforderungen an den Cloudauthentifizierungsservice ein.
- Geben Sie das Verzeichnis und den Dateinamen für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent ein.
- Geben Sie die Mandanten-ID für den Cloudauthentifizierungsservice ein.
- Geben Sie den Namen der Zugriffs-Policy für den Cloudauthentifizierungsservice ein.
- Geben Sie CLIENT_ID für den Namen des Authentifizierungs-Agent ein, die in mobilen Benachrichtigungen angezeigt wird.
- Öffnen Sie das PAM Agent-Installationsverzeichnis.

5. Überprüfen Sie nur für den UDP-Modus nach der Installation, ob VAR_ACE in der Datei **/etc/sd_pam.conf** auf den korrekten Speicherort der Datei **sdconf.rec** verweist. Dies ist der Pfad zu den Konfigurationsdateien. Für den gesamten Pfad ist die Root-Berechtigung „-rw-------" erforderlich.

Nach Abschluss

- Sie können die Installation überprüfen, indem Sie die Datei **installer.log** im Verzeichnis mit dem PAM Agent-Installationsprogramm prüfen.
- Führen Sie für den UDP-Modus eine Testauthentifizierung durch. Weitere Informationen finden Sie unter Authentifizierungsdienstprogramme für den UDP-Modus auf Seite 41.
- Testen Sie für den REST-Protokollmodus die Verbindung, indem Sie mit einem beliebigen Browser oder HTTP-Client auf die REST-Server-URL zugreifen. Geben Sie beispielsweise „https://*HOSTNAME*:*PORT*_

NO/mfa/v1_1/authn" ein. Da Sie derzeit keine Authentifizierung durchführen, sollte im Browser oder HTTP-Client die HTTP-Antwort „Forbidden" oder „Unauthorized" angezeigt werden.

Masseninstallation von PAM Agent mit der automatischen Installation

Führen Sie diese Aufgabe aus, um eine große Anzahl von PAM Agent-Instanzen mit identischen Konfigurationsinformationen bereitzustellen. Führen Sie diese Aufgabe beispielsweise durch, wenn Sie eine große Anzahl von Agents installieren müssen, die mit denselben RSA Authentication Manager-Servern oder demselben Cloudauthentifizierungsservice kommunizieren.

Bevor Sie beginnen

Installieren Sie PAM Agent manuell und notieren Sie die Eingabeaufforderungen. Anweisungen dazu finden Sie unter Installieren von PAM Agent auf einem Computer auf Seite 18.

Verfahren

1. Erstellen Sie eine textbasierte Konfigurationsdatei, in der Sie die Konfigurationsoptionen für das PAM Agent-Installationsskript angeben. Sie können einen beliebigen Namen für die Konfigurationsdatei auswählen, z. B. **installoptions.conf**.
2. Öffnen Sie die Datei und listen Sie jede Konfigurationsoption, die Sie auswählen möchten, in einer separaten Zeile in derselben Reihenfolge auf, in der die Eingabeaufforderungen während einer manuellen Installation von PAM Agent zur Verfügung gestellt werden.

   Im folgenden Beispiel wird die entsprechende Eingabeaufforderung für die jeweilige Option beschrieben, die in der UDP-Konfiguration angegeben ist:

Beispielwert	Option
y	Automatische Installation fortsetzen? (y) Diese Eingabeaufforderung wird immer zuerst eingefügt.
Accept	Den allgemeinen Geschäftsbedingungen zustimmen? (Akzeptieren)
/var/ace	Verzeichnis mit sdconf.rec? (Verzeichnispfad)
/opt	Installationspfad für PAM Agent Verzeichnis? (Verzeichnispfad)
y	Upgrade/Überschreiben vorhandener Installation? (j/n)
	(Optional) Alternativer Stammpfad, falls vorherige Option „n"? (Verzeichnispfad)

   In diesem Fall würde die textbasierte Konfigurationsdatei Folgendes enthalten:

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

   Als weiteres Beispiel enthält die Konfigurationsdatei für den Authentication Manager-REST-Modus möglicherweise Daten, die den folgenden ähneln:

```
y
Accept
```

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

Hinweis: Die Anzahl und Reihenfolge der Installationseingabeaufforderungen sind je nach installiertem PAM Agent-Modus und installierter Plattform unterschiedlich.

3. Wechseln Sie zum Verzeichnis mit dem PAM Agent-Installationsverzeichnis.
4. Entpacken Sie die Datei, indem Sie Folgendes eingeben:

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

5. Führen Sie das Installationsskript aus, indem Sie Folgendes eingeben:

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

   Dabei ist ***installoptions.conf*** die Konfigurationsdatei, die Sie in Schritt 1 erstellt haben. Wenn sich die Konfigurationsdatei an einem anderen Speicherort als dem aktuellen Verzeichnis befindet, geben Sie den vollständigen Pfad zur Datei ***installoptions.conf*** an.

Aktivieren von SELinux

Nach der Installation von PAM Agent können Sie SELinux (Security-Enhanced Linux) aktivieren.

Bevor Sie beginnen

- Überprüfen Sie auf dem Agent-Computer, ob PAM Agent erfolgreich funktioniert.

  Führen Sie beispielsweise im UDP-Modus eine Testauthentifizierung durch oder versuchen Sie, im REST-Modus, einen Authentication Manager-Server oder den Cloudauthentifizierungsservice anzupingen. Weitere Informationen zum Testen des UDP-Modus finden Sie unter Authentifizierungsdienstprogramme für den UDP-Modus auf Seite 41.

- Erstellen Sie Backups der Verzeichnisse **/etc/sd_pam.conf** und **/var/ace**.
- Um eine Blockierung des Zugriffs auf den PAM Agent-Computer zu vermeiden, konfigurieren Sie die geschützten RSA SecurID-Tools für die Verwendung des standardmäßigen PAM-Moduls, das mit dem Betriebssystem bereitgestellt wird, nicht für das RSA PAM-Modul. Setzen Sie die Toolkonfiguration zurück, damit Sie ohne RSA SecurID Authentication Agent 8.0 for PAM funktioniert.

  Schließen Sie alle aktiven Sitzungen, die das RSA PAM-Modul verwenden.

  Hinweis: Wenn Sie das RSA-Modul deinstallieren, während Verweise auf das RSA-Modul im Verzeichnis **/etc/pam.d** vorhanden sind, werden aus Ihrem System ausgesperrt.

Verfahren

1. Aktivieren Sie SELinux auf dem Agent-Computer.
2. Installieren Sie PAM Agent erneut, um SELinux-Policies für alle Tools zu erstellen:

a. Führen Sie das Installationsskript aus, indem Sie Folgendes eingeben:

   /<filename>/install_pam.sh

b. Geben Sie **y** ein, wenn das Installationsprogramm Sie auffordert, Ihre aktuelle Installation zu überschreiben.

c. Überschreiben Sie die vorhandene SELinux-Policy. Geben Sie bei Aufforderung **y** ein oder drücken Sie die EINGABETASTE, um den Standardwert **yes** auszuwählen.

Nach Abschluss

- Aktivieren Sie `auth required pam_securid.so` für alle konfigurierten Tools und testen Sie die Authentifizierung.
- Wenn SELinux aktiviert ist und die Datei **cert.pem** in einem benutzerdefinierten Verzeichnis statt dem Standardverzeichnis **/var/ace/** installiert ist, müssen Sie die SELinux-Policy für das benutzerdefinierte Verzeichnis aktivieren .

  Führen Sie die folgenden Befehle aus, wobei *cust_cert* das benutzerdefinierte Zertifikatverzeichnis ist:

  ```
  semanage fcontext -a -t var_t '/cust_cert/cert.pem'
  ```

  ```
  restorecon -v '/cust_cert/cert.pem'
  ```

Durchführen eines Upgrades auf RSA SecurID Authentication Agent 8.0 for PAM

Sie können ein Upgrade auf RSA SecurID Authentication Agent 8.0 for PAM von Version 7.1 Patch 2 (7.1.0.2) durchführen. Standardmäßig verwendet ein aktualisierter Agent RSA Authentication Manager und das UDP-Protokoll für die Authentifizierung. Sie können den Authentifizierungsmodus ändern, um den Cloudauthentifizierungsservice oder Authentication Manager und das REST-Protokoll zu nutzen. Anweisungen dazu finden Sie unter Ändern des PAM Agent-Authentifizierungsmodus auf Seite 33.

Bevor Sie beginnen

- Sie benötigen Root-Berechtigungen auf dem Agent-Host und eine Schreibberechtigung für das Verzeichnis, in dem die Datei **sdconf.rec** gespeichert ist. Für gewöhnlich ist diese Datei im Standardverzeichnis **/var/ace** gespeichert.
- Sichern Sie die Konfigurationsdateien vor dem Überschreiben, um die Konfigurationseinstellungen zu speichern. Weitere Informationen finden Sie unter Wichtige Konfigurationsdateien auf Seite 52.
- Konfigurieren Sie die geschützten RSA SecurID-Tools für die Verwendung des standardmäßigen PAM-Moduls, das mit dem Betriebssystem bereitgestellt wird, nicht für das RSA PAM-Modul. Alle aktiven Sitzungen, die RSA PAM-Module verwenden, müssen geschlossen werden, bevor Sie mit dem Upgrade fortfahren.

Verfahren

1. Wechseln Sie auf dem Agent-Computer zum Verzeichnis mit dem PAM Agent-Installationsprogramm.
2. Entpacken Sie die Datei, indem Sie Folgendes eingeben:

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

3. Führen Sie das Installationsskript aus, indem Sie Folgendes eingeben:

   /<filename>/install_pam.sh

4. Überschreiben Sie die vorhandenen Installationsdateien. Geben Sie **y** ein, wenn das Installationsprogramm Sie auffordert, Ihre aktuelle Installation zu überschreiben.
5. Wenn SELinux aktiviert ist und Sie das REST-Protokoll für die Authentifizierung verwenden möchten, müssen Sie die vorhandene SELinux-Policy überschreiben. Geben Sie bei Aufforderung **y** ein oder drücken Sie die EINGABETASTE, um den Standardwert **yes** auszuwählen.

   Wenn Sie **n** eingeben, können einige Tools keine Authentifizierung mit dem REST-Protokoll durchführen. Sie können die vorhandene SELinux-Policy jedoch überschreiben, indem Sie das Installationsskript ausführen. Dateien, die bereits aktualisiert wurden, sind nicht betroffen.

6. Rufen Sie die Agent-Versionsnummer ab, um zu ermitteln, ob das Upgrade erfolgreich war. Geben Sie Folgendes ein:

   strings pam_securid.so | grep "Agent"

   Damit wird die Versionsnummer des installierten Agent zurückgegeben.

Konfigurieren von Tools

Sie müssen die unterstützten Tools so konfigurieren, dass Benutzer für die von den Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Hinweis: Die Einstellungen für die Anzahl der gleichzeitig zulässigen Benutzer auf dem UNIX-Server müssen für jedes Tool, das verwendete Betriebssystem und die erwarteten gleichzeitigen Anmeldungen beim Server eingerichtet werden, insbesondere bei Verwendung des Cloudauthentifizierungsservice. Konfigurieren Sie beispielsweise die Einstellung „MaxStartups" in der Datei **/etc/ssh/sshd_config** für SSH und die Einstellung „Instances" in der Datei **/etc/xinetd.d/telnet** für Telnet.

Konfigurieren von telnet unten

Konfigurieren von login Auf der nächsten Seite

Konfigurieren von rlogin Auf der nächsten Seite

Konfigurieren von su Auf der nächsten Seite

Konfigurieren von ssh und zugehörigen Tools auf Seite 25

Konfigurieren von sudo auf Seite 25

Konfigurieren von ftp auf Seite 25

Konfigurieren von gdm auf Seite 26

Konfigurieren von telnet

Konfigurieren Sie telnet so, dass Benutzer für die von Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Verfahren

Hinweis: PAM Agent 8.0 bietet keine Unterstützung für Kerberos-Telnet.

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **remote**.
3. Kommentieren Sie alle Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

   ```
   auth required pam_securid.so
   ```

5. Wiederholen Sie nur bei Oracle Linux 6.8 (64-Bit) diese Schritte für die Datei **/etc/pam.d/login**.

   Für alle anderen Versionen von RHEL und Oracle Linux ist das Verfahren abgeschlossen.

Konfigurieren von login

Konfigurieren Sie den Befehl „login", um Benutzer für die von Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufzufordern.

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **login**.
3. Kommentieren Sie die Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

   ```
   auth required pam_securid.so
   ```

Konfigurieren von rlogin

Konfigurieren Sie das rlogin-Dienstprogramm, um Benutzer für die von Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufzufordern.

Bevor Sie beginnen

Wenn rlogin unter RHEL 6.8 oder Oracle Linux 6.8 nicht funktioniert, befolgen Sie die Verfahren unter Bekannte Konfigurationsprobleme auf Seite 40.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **rlogin**.
3. Kommentieren Sie die Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

   ```
   auth required pam_securid.so
   ```

Konfigurieren von su

Konfigurieren Sie den Befehl „su" so, dass Benutzer für die von Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **su**.
3. Kommentieren Sie alle Zeilen, die mit `auth` beginnen.

4. Fügen Sie die folgende Zeile hinzu:

```
auth required pam_securid.so
```

Konfigurieren von ssh und zugehörigen Tools

Sie können SSH und verwandte Tools wie scp und sftp so konfigurieren, dass Benutzer für die vom Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **sshd**.
3. Kommentieren Sie die Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

```
auth required pam_securid.so
```

Konfigurieren von sudo

Wenn bei Ihnen sudo erforderlich ist, müssen Sie den Befehl „sudo" so konfigurieren, dass Benutzer für die von Cloudauthentifizierungsservice und von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Bevor Sie beginnen

Sie können die unterstützte sudo-Version von https://www.sudo.ws herunterladen und installieren.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **sudo**.
3. Kommentieren Sie alle Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

```
auth required pam_securid.so
```

Konfigurieren von ftp

Konfigurieren Sie das FTP-Protokoll, um Benutzer für die von RSA Authentication Manager unterstützten Authentifizierungsmethoden aufzufordern.

Sie können den Cloudauthentifizierungsservice nicht zum Schutz von ftp verwenden. Sie können jedoch sftp benutzen. Anweisungen finden Sie unter Konfigurieren von ssh und zugehörigen Tools oben.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Öffnen Sie die Datei **vsftpd**.
3. Kommentieren Sie die Zeilen, die mit `auth` beginnen.
4. Fügen Sie die folgende Zeile hinzu:

```
auth required pam_securid.so
```

Konfigurieren von gdm

Sie können gdm so konfigurieren, dass Benutzer für die vom Cloudauthentifizierungsservice und RSA Authentication Manager unterstützten Authentifizierungsmethoden aufgefordert werden.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/pam.d**.
2. Ändern Sie die Dateien **gdm**,**gdm-password** und **gdm-autologin**wie folgt:
    a. Öffnen Sie jede gdm Datei.
    b. Kommentieren Sie alle Zeilen, die mit `auth` beginnen.
    c. Fügen Sie die folgende Zeile hinzu:

```
auth required pam_securid.so
```

Kapitel 2: Konfigurieren von Funktionen

Konfigurieren von Agent- und UNIX-Funktionen 28
Ändern des PAM Agent-Authentifizierungsmodus 33

Konfigurieren von Agent- und UNIX-Funktionen

Sie können die PAM Agent-Konfiguration für die Verwendung optionaler Agent- und UNIX-Funktionen anpassen.

Hinweis: Erstellen Sie vor der Anpassung des Agent Backupkopien der ursprünglichen Konfigurationsdateien.

Mehrere Konfigurationsdateien befinden sich im Verzeichnis **/etc/pam.d**. Jede Datei verwendet den Namen des Verbindungstools.

Weitere Informationen zum Anpassen des Agent finden Sie unter:

Aktivieren des Agent-Reportings für RSA SecurID Authentication Agent 8.0 for PAM unten

Aktivieren der Debug-Ausgabe unten

Aktivieren der SecurID-Trace-Protokollierung für den UDP-Modus Auf der gegenüberliegenden Seite

Konfigurieren kombinierbarer Module Auf der gegenüberliegenden Seite

Verwenden von Reservepasswörtern auf Seite 31

Aktivieren der selektiven SecurID-Authentifizierung auf Seite 31

Konfigurieren der exponentiellen Backoff-Zeit auf Seite 32

Aktivieren des Agent-Reportings für RSA SecurID Authentication Agent 8.0 for PAM

Sie können den Parameter ENABLE_AGENT_REPORTING in der Datei **mfa_api.properties** konfigurieren, um Agent-Details wie den Hostnamen, die Agent-Version und die Betriebssystemversion an RSA Authentication Manager zu senden. Sie können RSA Authentication Manager 8.3 zum Ausführen von Berichten verwenden, die diese Details beinhalten.

Bevor Sie beginnen

Sie benötigen Root-Berechtigungen für den Computer, auf dem der Agent installiert ist, und Schreibberechtigungen für das Verzeichnis, in dem die Datei **mfa_api.properties** gespeichert ist. Standardmäßig ist diese Datei in **/var/ace/conf** gespeichert.

Verfahren

1. Wechseln Sie zu dem Verzeichnis, in dem sich **mfa_api.properties** befindet. Standardmäßig lautet das Verzeichnis **/var/ace/conf**.
2. Öffnen Sie **mfa_api.properties**.
3. Ändern Sie den Parameter ENABLE_AGENT_REPORTING auf 1, wodurch das Agent-Reporting aktiviert wird. Der Standardwert ist 0.
4. Speichern Sie die Datei.

   Details zu PAM Agent und dem Computer, auf dem der Agent installiert ist, sind in den PAM Agent-Reportingdetails enthalten, die an Authentication Manager gesendet werden.

Aktivieren der Debug-Ausgabe

Für das Troubleshooting können Sie die Debug-Ausgabe für bestimmte Tools aktivieren, die von PAM Agent verwendet werden.

Sie können außerdem das Systemprotokoll so konfigurieren, dass alle PAM Agent-

Authentifizierungsprotokollmeldungen aufgezeichnet werden. Weitere Informationen finden Sie unter Protokollierung für PAM Agent auf Seite 45.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc/** und öffnen Sie die Datei **pam.d**.
2. Bearbeiten Sie die entsprechende Datei, indem Sie ein Debug-Argument für das pam_securid.so-Modul hinzufügen. Geben Sie Folgendes ein:

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

Aktivieren der SecurID-Trace-Protokollierung für den UDP-Modus

Sie können die detaillierte SecurID-Trace-Protokollierung für PAM Agent und für die Authentifizierungsdienstprogramme acetest und acestatus aktivieren. Standardmäßig ist die SecurID-Trace-Protokollierung bei der Installation von PAM Agent deaktiviert.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc** und öffnen Sie die Datei **sd_pam.conf**.
2. Legen Sie die folgende Variable fest, um die detaillierte Agent-Protokollierung zu aktivieren und das Protokollierungslevel festzulegen:

   `RSATRACELEVEL=`*`Wert`*

   Dabei ist *Wert* eine Einstellung aus der folgenden Tabelle.

Wert	Beschreibung
0	Deaktiviert die Protokollierung (Standardwert).
1	Protokolliert reguläre Meldungen.
2	Protokolliert Funktionseinstiegspunkte.
4	Protokolliert Funktionsausstiegspunkte.
8	Alle Logikflusskontrollen (ifs) verwenden diesen Wert.

   Fügen Sie für Kombinationen die entsprechenden Werte hinzu. Zum Protokollieren von regulären Meldungen und Funktionseinstiegspunkten legen Sie den Wert beispielsweise auf 3 fest.

3. Geben Sie den Pfad an, an den die Protokolle umgeleitet werden. Legen Sie die folgende Variable fest:

   `RSATRACEDEST=`*`filepath`*

   Dabei ist *filepath* der Dateipfad.

   Standardmäßig ist diese Variable leer. Wenn Sie diese Variable nicht festlegen, wird ein Standardfehler für die Protokolle für die Authentifizierungsdienstprogramme acetest und acestatus ausgegeben und es werden keine Protokolle für Authentifizierungstools erzeugt, selbst wenn der Wert`RSATRACELEVEL` angegeben wurde.

4. Speichern Sie Ihre Änderungen.

Konfigurieren kombinierbarer Module

In einer gestapelten Konfiguration verwenden Sie den Agent, um das RSA SecurID PAM-Authentifizierungsmodul in andere PAM-Authentifizierungsmodule in Ihrer Umgebung zu integrieren. Das

Passwort oder der Passcode wird von einem Authentifizierungsmodul zum nächsten übergeben. Sie können die Priorität der Authentifizierungs-Challenges konfigurieren, indem Sie die Konfigurationsdatei **/etc/pam.d*Name des Tools*** bearbeiten.

Hinweis: Die Argumente use_first_pass und try_first_pass werden bei Verwendung einer gestapelten Konfiguration mit dem Cloudauthentifizierungsservice nicht unterstützt.

Der Agent arbeitet mit den Argumenten use_first_pass und try_first_pass:

- **use_first_pass.** Der Agent verwendet nur das Passwort oder den Passcode, das bzw. der vom vorherigen Modul übergeben wurde, und verweigert den Zugriff, wenn die Anmeldeinformationen nicht übereinstimmen. Der Benutzer wird nicht erneut zur Authentifizierung aufgefordert.
- **try_first_pass.** Der Agent verwendet das Passwort oder den Passcode, das bzw. der vom vorherigen Modul übergeben wurde. Wenn die Anmeldeinformationen nicht übereinstimmen, wird der Benutzer zur Authentifizierung aufgefordert.

Hinweis: Wenn Benutzer, die von der SecurID-Authentifizierung ausgeschlossen sind, fehlgeschlagene Anmeldeversuche für den Zugriff auf das RSA PAM-Modul durchführen, sorgt die Funktion für das exponentielle Backoff dafür, dass das RSA PAM-Modul die Kontrolle behält, bis die Anmeldung erfolgreich ist oder die Sitzung beendet wird. Weitere Informationen zum Konfigurieren der exponentiellen Backoff-Zeit finden Sie unter Konfigurieren der exponentiellen Backoff-Zeit auf Seite 32.

Der folgende Abschnitt enthält ein Beispiel für die Konfiguration eines Verbindungstools (login-Tool) in einer gestapelten Umgebung.

Verfahren

1. Wechseln Sie zu **/etc/pam.d** und öffnen Sie die Datei **login**.

   Der folgende Text wird angezeigt:

   ```
   #%PAM-1.0
   auth required pam_securetty.so
   auth required pam_stack.so service=system-auth
   auth required pam_nologin.so
   account required pam_stack.so service=system-auth
   password required pam_stack.so service=system-auth
   # pam_selinux.so close should be the first session rule
   session required pam_selinux.so close
   session required pam_stack.so service=system-auth
   session required pam_loginuid.so
   session optional pam_console.so
   # pam_selinux.so open should be the last session rule
   session required pam_selinux.so open
   ```

2. Kommentieren Sie die folgenden Zeilen:

   ```
   auth required pam_securetty.so
   auth required pam_stack.so service=system-auth
   auth required pam_nologin.so
   ```

3. Fügen Sie die folgenden Zeilen hinzu. Geben Sie Folgendes ein:

   ```
   auth required pam_securid.so
   ```

Verwenden von Reservepasswörtern

Die Reservepasswortfunktion ist eine Notfallzugriffsmethode, mit der Sie als Administrator bei dem geschützten Computer, auf dem der Agent installiert ist, authentifiziert werden können, ohne einen RSA SecurID-Passcode einzugeben. PAM Agent lässt nur zu, dass Root-Administratoren Reservepasswörter unter unvorhergesehenen Bedingungen verwenden, beispielsweise bei einem Verlust der Kommunikation zwischen dem Agent und RSA SecurID Authentication Agent 8.0 for PAM. In diesen Situationen können Administratoren den Agent vorübergehend deaktivieren, wenn Benutzer sofortigen Zugriff auf die gehosteten Ressourcen benötigen.

Hinweis: Das UNIX-Kennwort ist das Reservepasswort.

Verfahren

1. Öffnen Sie die entsprechende Datei in **/etc/pam.d**.
2. Fügen Sie das Argument „reserve" zum pam_securid.so-Modul hinzu. Geben Sie Folgendes ein:

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

Aktivieren der selektiven SecurID-Authentifizierung

Sie können den Agent so konfigurieren, dass bestimmte UNIX-Benutzer oder -Gruppe selektiv immer oder nie zur SecurID-Authentifizierung aufgefordert werden:

Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Gruppen unten

Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Benutzer Auf der nächsten Seite

Hinweis: Wenn sowohl die Unterstützung für selektive Gruppen als auch die Unterstützung für selektive Benutzer aktiviert werden, wird nur die Unterstützung für selektive Benutzer aktiviert, während die Unterstützung für selektive Gruppen ignoriert wird.

In der folgenden Tabelle sind die möglichen Werte aufgeführt, die in der Datei **sd_pam.conf** festgelegt werden können.

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	Ergebnis
0	0	Keine Funktion ist aktiviert. Alle Benutzer und Benutzergruppe erhalten die Challenge.
0	1	Die Unterstützung für ausgewählte Benutzer wird aktiviert. PAM Agent fordert bestimmte UNIX-Benutzer entweder immer oder nie auf, sich mit SecurID zu authentifizieren.
1	0	Die Unterstützung für ausgewählte Gruppe wird aktiviert. PAM Agent fordert bestimmte UNIX-Gruppen entweder immer oder nie auf, sich mit RSA SecurID zu authentifizieren.
1	1	Die Unterstützung für ausgewählte Benutzer wird aktiviert. PAM Agent fordert bestimmte UNIX-Benutzer entweder immer oder nie auf, sich mit SecurID zu authentifizieren.

Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Gruppen

Sie können PAM Agent so konfigurieren, dass bestimmte UNIX-Gruppen immer oder nie aufgefordert werden, sich mit RSA SecurID zu authentifizieren. Wenn PAM Agent installiert ist, wird diese Funktion nicht aktiviert.

Mitglieder der Gruppe, die aus der SecurID-Authentifizierung ausgeschlossen sind, können entweder mit UNIX-Anmeldeinformationen oder über ein anderes PAM-Moduls im Stack authentifiziert werden. Konfigurieren Sie dafür den Parameter PAM_IGNORE_SUPPORT.

Hinweis: Geben Sie keine RSA Authentication Manager-Gruppen an. Diese Funktion ist für nur UNIX-Gruppen vorgesehen.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc** und öffnen Sie die Datei **sd_pam.conf**.
2. Legen Sie den Parameter ENABLE_GROUP_SUPPORT auf 1 fest. Der Standardwert ist 0.
3. Füllen Sie den Parameter LIST_OF_GROUPS aus.
4. Legen Sie den Wert für den Parameter INCL_EXCL_GROUPS fest.
   Gültige Werte:
   0: Die SecurID-Authentifizierung für die aufgeführten Gruppen wird deaktiviert (Standardwert).
   1: Die SecurID-Authentifizierung wird nur für die aufgeführten Gruppen aktiviert.
5. (Optional) Legen Sie den Parameter PAM_IGNORE_SUPPORT fest.
   Gültige Werte:
   0: Die UNIX-Passwortauthentifizierung wird aktiviert (Standardwert).
   1: Die UNIX-Passwortauthentifizierung wird deaktiviert.
   Dieser Parameter gilt nur für Gruppen, die von der SecurID-Authentifizierung ausgeschlossen sind.
6. Speichern Sie die Datei.

Aktivieren der selektiven SecurID-Authentifizierung für UNIX-Benutzer

Sie können PAM Agent so konfigurieren, dass bestimmte UNIX-Benutzer immer oder nie aufgefordert werden, sich mit SecurID zu authentifizieren. Wenn PAM Agent installiert ist, wird diese Funktion nicht aktiviert.

Benutzer, die aus der SecurID-Authentifizierung ausgeschlossen sind, können entweder mit UNIX-Anmeldeinformationen oder über ein anderes PAM-Moduls im Stack authentifiziert werden. Konfigurieren Sie dafür den Parameter PAM_IGNORE_SUPPORT_FOR_USERS.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc** und öffnen Sie die Datei **sd_pam.conf**.
2. Legen Sie den Parameter ENABLE_USERS_SUPPORT auf 1 fest. Der Standardwert ist 0.
3. Füllen Sie den Parameter LIST_OF_USERS aus.
4. Legen Sie den Wert für den Parameter INCL_EXCL_USERS fest.
   Gültige Werte:
   0: Die SecurID-Authentifizierung für die aufgeführten Benutzer wird deaktiviert (Standardwert).
   1: Die SecurID-Authentifizierung wird nur für die aufgeführten Benutzer aktiviert.
5. (Optional) Legen Sie den Parameter PAM_IGNORE_SUPPORT_FOR_USERS fest.
   Gültige Werte:
   0: Die UNIX-Passwortauthentifizierung wird aktiviert (Standardwert).
   1: Die UNIX-Passwortauthentifizierung wird deaktiviert.
   Dieser Parameter gilt nur für Benutzer, die von der SecurID-Authentifizierung ausgeschlossen sind.
6. Speichern Sie die Datei.

Konfigurieren der exponentiellen Backoff-Zeit

Sie können die Zeit konfigurieren, für die ein Benutzer, der von der RSA SecurID-Authentifizierung

ausgeschlossen ist, warten muss, bevor eine Authentifizierung nach jedem aufeinanderfolgenden fehlgeschlagenen Anmeldeversuch erfolgt. Standardmäßig können Benutzer die UNIX-Authentifizierung nach einem fehlgeschlagenen Anmeldeversuch mit pow(4, failattempts) Sekunden Verzögerung erneut versuchen. Drei fehlgeschlagene Anmeldeversuche führen beispielsweise zu einer Verzögerung von 64 Sekunden (vier hoch drei oder 4 x 4 x 4 = 64).

Hinweis: Das FTP-Protokoll bietet keine Unterstützung für die exponentielle Backoff-Verzögerung.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc** und öffnen Sie die Datei **sd_pam.conf**.
2. Legen Sie den Parameter BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERS wie folgt auf *N* fest:

N	**Authentifizierungsverhalten**
0	Ein erneuter UNIX-Authentifizierungsversuch wird nach einem fehlgeschlagenen Anmeldeversuch deaktiviert. Es gibt keine Authentifizierungsverzögerung für Anmeldeversuche, die auf einen fehlgeschlagenen Anmeldeversuch folgen.
1, 2, 3	Ein erneuter UNIX-Authentifizierungsversuch nach einem fehlgeschlagenen Anmeldeversuch wird mit pow(3, failattempts) Sekunden Verzögerung aktiviert.
4	Ein erneuter UNIX-Authentifizierungsversuch nach einem fehlgeschlagenen Anmeldeversuch wird mit pow(4, failattempts) Sekunden Verzögerung aktiviert.
5 und höher	Ein erneuter UNIX-Authentifizierungsversuch nach einem fehlgeschlagenen Anmeldeversuch wird mit pow(5/Above, failattempts) Sekunden Verzögerung aktiviert.

Ändern des PAM Agent-Authentifizierungsmodus

Sie können den Authentifizierungsmodus für PAM Agent ändern. Beispielsweise können Sie den Modus ändern, wenn Sie die erweiterten Authentifizierungsoptionen verwenden möchten, die vom Cloudauthentifizierungsservice bereitgestellt werden. Standardmäßig verwendet eine aktualisierte PAM Agent-Instanz RSA Authentication Manager mit dem UDP-Protokoll.

Wechseln vom UDP-Protokoll zum REST-Protokoll

Sie können für RSA SecurID Authentication Agent 8.0 for PAM oder den Cloudauthentifizierungsservice vom UDP-Protokollauthentifizierungsmodus zum REST-Protokoll wechseln

Bevor Sie beginnen

- Sie benötigen Root-Berechtigungen auf dem Computer, auf dem der Agent installiert ist.
- Sie benötigen eine Schreibberechtigung für das Verzeichnis, in dem die Datei **sdconf.rec** gespeichert ist. Standardmäßig ist diese Datei in **/etc** gespeichert.
- Sie benötigen eine Schreibberechtigung für das Verzeichnis, in dem die Datei **mfa_api.properties** gespeichert ist. Standardmäßig ist diese Datei in **/var/ace/conf** gespeichert.
- Stellen Sie die erforderlichen Informationen zusammen.

  Für eine Authentication Manager-Authentifizierung mit dem REST-Protokoll müssen Sie Ihren Authentication Manager-Superadministrator um die folgenden Informationen bitten.

Parameter	Beschreibung
REST_URL	REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und der primären Authentication Manager-Instanz. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
REPLICA_*number* Dabei ist *number* eine Zahl von 1 bis 15.	Eine REST-Server-URL für jede Replikatinstanz, die für das Failover verwendet werden kann. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	Zugriffsschlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an Authentication Manager. Dieser Wert wird in der Sicherheitskonsole auf der primären Authentication Manager-Instanz erzeugt.
CA_CERT_FILE_ PATH	Verzeichnis und Dateiname für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent. Der Standardwert ist **/var/ace/cert.pem**.
CLIENT_ID	Name des Authentifizierungs-Agent (Client-ID), der für PAM Agent in Authentication Manager erstellt wurde.

  Für eine Authentifizierung mit dem Cloudauthentifizierungsservice müssen Sie Ihren Cloudauthentifizierungsservice-Superadministrator um die folgenden Informationen bitten.

Parameter	Beschreibung
REST_URL	REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und dem Cloudauthentifizierungsservice. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	Der in der Cloudadministrationskonsole erstellte Authentifizierungs-API-Schlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an den Cloudauthentifizierungsservice
CA_CERT_FILE_PATH	Geben Sie das Verzeichnis und den Dateinamen für das vertrauenswürdige Serverzertifikat auf dem Authentifizierungs-Agent ein. Der Standardwert ist **/var/ace/cert.pem**.
TENANT_ID	Mandanten-ID für den Cloudauthentifizierungsservice. PAM Agent kann die Mandanten-ID in Authentifizierungsanforderungen bereitstellen, aber die Daten werden nicht vom Agent überprüft. Dieser Parameter wird derzeit nicht vom Cloudauthentifizierungsservice unterstützt.
ASSURANCE_ POLICY_ID	Name der Zugriffs-Policy für den Cloudauthentifizierungsservice.

Parameter	Beschreibung
CLIENT_ID	Name des Authentifizierungs-Agent, der in mobilen Benachrichtigungen angezeigt wird. Sie können einen beliebigen Wert eingeben. Beispiel: PAM_Agent.

Verfahren

1. Wechseln Sie zum Verzeichnis, in dem sich **sd_pam.conf** befindet. Der Standardspeicherort ist **/etc**.
2. Öffnen Sie **sd_pam.conf**.
3. Ändern Sie den Parameter OPERATION_MODE:
   - Für Authentication Manager mit dem REST-Protokoll geben Sie 1 ein.
   - Für den Cloudauthentifizierungsservice mit dem REST-Protokoll geben Sie 2 ein.

   Wenn der Parameter OPERATION_MODE 0, nicht angegeben oder auskommentiert ist, verwendet PAM Agent standardmäßig den UDP-Modus.
4. Wechseln Sie zum Verzeichnis **/var/ace/conf**. Sie müssen die Datei **mfa_api.properties** aktualisieren.
5. Öffnen Sie **mfa_api.properties**.
6. Entfernen Sie Kommentare, um die erforderlichen Parameter zu aktivieren.
7. Geben Sie einen Wert für jeden erforderlichen Parameter ein.
8. Speichern Sie die Datei.

   Jetzt können Sie das REST-Protokoll verwenden.

Nach Abschluss

Wenn SELinux aktiviert ist, müssen Sie den folgenden Befehl ausführen, wobei *REST_port_number* der für die REST-Authentifizierung verwendete Port ist (der Standardport ist 5555):

```
semanage port -a -t dns_port_t -p tcp REST_port_number
```

Wechseln vom REST-Protokoll zum UDP-Protokoll

Nach der Installation von PAM Agent für die Verwendung des REST-Protokolls können Sie den Authentifizierungsmodus ändern, um RSA SecurID Authentication Agent 8.0 for PAM mit dem UDP-Protokoll zu verwenden.

Nachdem Sie den Authentifizierungsmodus für die Verwendung des UDP-Protokolls geändert haben, sind die Konfigurationseinstellungen für das REST-Protokoll in der Datei **mfa_api.properties** nicht mehr gültig.

Bevor Sie beginnen

- Die Authentication Manager-Konfigurationsdatei **sdconf.rec** ist erforderlich. Sie können diese Datei in Authentication Manager erzeugen oder sie von Ihrem Authentication Manager-Superadministrator erhalten. Weitere Informationen finden Sie unter Planung der Installation von PAM Agent auf Seite 14.
- Sie benötigen Root-Berechtigungen für den Computer, auf dem der Agent installiert ist, und eine Schreibberechtigung für das Verzeichnis, in dem die Datei **sd_pam.conf** gespeichert ist. Standardmäßig ist diese Datei im Verzeichnis **/etc** gespeichert.

Verfahren

1. Wechseln Sie zum Verzeichnis, in dem sich **sd_pam.conf** befindet. Der Standardspeicherort ist **/etc**.
2. Öffnen Sie **sd_pam.conf**.
3. Ändern Sie den Parameter OPERATION_MODE auf 0 für das UDP-Protokoll:

   ```
   OPERATION_MODE=0
   ```

   Wenn der Parameter OPERATION_MODE 0, nicht angegeben oder auskommentiert ist, verwendet PAM Agent standardmäßig den UDP-Modus.

4. Kopieren Sie **sdconf.rec** in das Verzeichnis **/var/ace**.

   Jetzt können Sie das UDP-Protokoll verwenden.

Wechseln zwischen RSA Authentication Manager und dem Cloudauthentifizierungsservice

Sie können ändern, ob PAM Agent das REST-Protokoll mit Authentication Manager oder dem Cloudauthentifizierungsservice verwendet.

Bevor Sie beginnen

- Sie benötigen Root-Berechtigungen auf dem Computer, auf dem der Agent installiert ist.
- Sie benötigen eine Schreibberechtigung für das Verzeichnis, in dem die Datei **sdconf.rec** gespeichert ist. Standardmäßig ist diese Datei in **/var/ace** gespeichert.
- Sie benötigen eine Schreibberechtigung für das Verzeichnis, in dem die Datei **mfa_api.properties** gespeichert ist. Standardmäßig ist diese Datei in **/var/ace/conf** gespeichert.
- Der Parameter CA_CERT_FILE_PATH für das vertrauenswürdige Serverzertifikat kann gleich bleiben. Stellen Sie für andere Parameter die erforderlichen Informationen zusammen:
  Für eine Authentication Manager-Authentifizierung mit dem REST-Protokoll müssen Sie Ihren Authentication Manager-Superadministrator um die folgenden Informationen bitten.

Parameter	**Beschreibung**
REST_URL	REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und der primären Authentication Manager-Instanz. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
REPLICA_*number* Dabei ist *number* eine Zahl von 1 bis 15.	Eine REST-Server-URL für jede Replikatinstanz, die für das Failover verwendet werden kann. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	Zugriffsschlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an Authentication Manager. Dieser Wert wird in der Sicherheitskonsole auf der primären Authentication Manager-Instanz erzeugt.
CLIENT_ID	Name des Authentifizierungs-Agent (Client-ID), der für PAM Agent in Authentication Manager erstellt wurde.

Für eine Authentifizierung mit dem Cloudauthentifizierungsservice müssen Sie Ihren Cloudauthentifizierungsservice-Superadministrator um die folgenden Informationen bitten.

Parameter	Beschreibung
REST_URL	REST-Server-URL für die Kommunikation zwischen dem Authentifizierungs-Agent und dem Cloudauthentifizierungsservice. Beispiel: https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn
CLIENT_KEY	Der in der Cloudadministrationskonsole erstellte Authentifizierungs-API-Schlüssel (Clientschlüssel) für die sichere Übergabe von Benutzerauthentifizierungsanforderungen an den Cloudauthentifizierungsservice
TENANT_ID	Mandanten-ID für den Cloudauthentifizierungsservice. PAM Agent kann die Mandanten-ID in Authentifizierungsanforderungen bereitstellen, aber die Daten werden nicht vom Agent überprüft. Dieser Parameter wird derzeit nicht vom Cloudauthentifizierungsservice unterstützt.
ASSURANCE_ POLICY_ID	Name der Zugriffs-Policy für den Cloudauthentifizierungsservice.
CLIENT_ID	Name des Authentifizierungs-Agent, der in mobilen Benachrichtigungen angezeigt wird. Sie können einen beliebigen Wert eingeben. Beispiel: PAM_ Agent.

Verfahren

1. Wechseln Sie zum Verzeichnis, in dem sich **sd_pam.conf** befindet. Der Standardspeicherort ist **/etc**.
2. Öffnen Sie **sd_pam.conf**.
3. Ändern Sie den Parameter OPERATION_MODE:
   - Für Authentication Manager mit dem REST-Protokoll geben Sie 1 ein.
   - Für den Cloudauthentifizierungsservice mit dem REST-Protokoll geben Sie 2 ein.

   Wenn der Parameter OPERATION_MODE 0, nicht angegeben oder auskommentiert ist, verwendet PAM Agent standardmäßig den UDP-Modus.
4. Wechseln Sie zum Verzeichnis **/var/ace/conf**. Sie müssen die erforderlichen Werte für die Parameter in der Datei **mfa_api.properties** aktualisieren.
5. Öffnen Sie **mfa_api.properties**.
6. Entfernen Sie Kommentare, um die erforderlichen Parameter zu aktivieren, und kommentieren Sie alle Parameter aus, die nicht mehr benötigt werden.
7. Geben Sie einen Wert für jeden erforderlichen Parameter ein.
8. Speichern Sie die Datei.

   Jetzt können Sie das REST-Protokoll mit dem neuen Authentifizierungsmodus verwenden.

Anhang A: Troubleshooting

Bekannte Konfigurationsprobleme 40
Authentifizierungsdienstprogramme für den UDP-Modus 41
Konvertierungsdienstprogramm für den UDP-Modus 43
Node-Schlüssel für den UDP-Modus 43
Protokollierung für PAM Agent 45
Protokollierung für den REST-Modus 46
Troubleshooting von SELinux 47
Konfigurieren der Werte für Timeout und Retry für die REST-Authentifizierung 48
Deinstallieren von RSA SecurID Authentication Agent 8.0 for PAM 49

Bekannte Konfigurationsprobleme

In diesem Abschnitt werden bekannte Probleme beschrieben.

Probleme mit unterstützten Tools

Tool	Bekanntes Problem
dtlogin	**Problem:** Anzeigeeinschränkungen können zu zwei Problemen für Benutzer führen: • Authentifizierenden Benutzern wird nicht die komplette Meldung über verfügbare Authentifizierungsmethoden angezeigt. • Benutzer mit Reservepasswort sehen ein partielles Texteingabefeld auf Bildschirmen, auf denen es nicht erforderlich ist. **Lösung:** Authentifizierende Benutzern können gemäß der Anweisung auf dem Bildschirm die EINGABETASTE drücken, um die komplette Meldung anzuzeigen. Benutzer mit Reservepasswort können das überflüssige Feld ignorieren.
ftp	• **Problem:** Wenn Sie SecurID für den Schutz von ftp verwenden, werden Benutzern keine Eingabeaufforderungen und Fehlermeldungen für die SecurID-Authentifizierung angezeigt. Nur Standardeingabeaufforderungen und -fehlermeldungen des Betriebssystems werden angezeigt. **Lösung:** Weisen Sie Benutzer an, ihren Benutzernamen an der Betriebssystem-Eingabeaufforderung für den Benutzernamen und den SecurID-Passcode an der Betriebssystem-Eingabeaufforderung für das Passwort einzugeben. Wenn ein Benutzer den Tokenstatus nicht kennt (wenn sich das Token beispielsweise im Modus „Nächster Tokencode" oder „Neue PIN" befindet), muss sich der Benutzer mit einem anderen Verbindungstool wie rlogin authentifizieren, um sicherzustellen, dass die PIN oder der Tokencode noch gültig ist. • FTP bietet keine Unterstützung für eine exponentielle Backoff-Verzögerung. • Sie können den Cloudauthentifizierungsservice nicht für den Schutz von ftp verwenden, sftp wird jedoch unterstützt.
ssh	**Problem:** Nachdem ein Benutzer in einer einzigen Sitzung drei erfolglose SecurID-Authentifizierungsversuche durchgeführt hat, wird die Verbindung geschlossen. **Lösung:** Der Benutzer kann die Sitzung beenden und eine andere Sitzung starten.
ftp mit SELinux	**Problem:**Wenn SELinux aktiviert ist, wird einem ftp-Toolbenutzer die Meldung „500 OOPS: cannot change directory:/home/tzfFjG_9su" angezeigt. **Lösung:** Führen Sie auf dem Agent-Computer den Befehl „setsebool -P ftp_*home_dir* on" aus, wobei *home_dir* das Stammverzeichnis des Benutzers ist.
gdm	**Problem:**PAM Agent Nachrichten werden möglicherweise gekürzt. **Lösung:**Das gdm-Design kann entsprechend konfiguriert werden, um dieses Problem zu vermeiden.
rlogin	**Problem:** In RHEL 6.8 werden rlogin-Verbindungen vor der Konfiguration von rlogin zur Zusammenarbeit mit PAM Agent geschlossen. **Lösung:** Stellen Sie sicher, das rlogin funktioniert, bevor Sie PAM Agent konfigurieren. Führen Sie die folgenden Schritte aus: 1. Öffnen Sie die Datei **/etc/xinet,d/rlogin**.

Tool	Bekanntes Problem
	2. Fügen Sie **nice = 5** am Ende der rlogin-Konfiguration hinzu. 3. Starten Sie xinetd-Services neu: `service xinetd restart`
rlogin	**Problem:** In Oracle Linux 6.8 funktioniert rlogin nicht. **Lösung:** Führen Sie ein Downgrade auf die folgenden RPMs durch: **util-linux-ng-2.17.2-12.18.el6.x86_64.rpm** **libblkid-2.17.2-12.18.el6.x86_64.rpm** **libuuid-2.17.2-12.18.el6.x86_64.rpm**
rlogin	**Problem:** Wenn der erste Versuch der Verarbeitung einer rlogin-Anforderung fehlschlägt, wird die Sitzung an den Anmelde-Daemon übergeben. **Lösung:** Wenn Sie Linux für die Verwendung von rlogin konfigurieren, müssen Sie die Datei für die Remoteanmeldung in **/etc/pam.d** konfigurieren.
rlogin	**Problem:** rlogin fordert ein Passwort statt einen Passcode an, wenn mehrdeutige Einträge in der Datei **/etc/hosts** vorhanden sind. **Lösung:** Wenn neben der Loopback-IP-Adresse und der tatsächlichen Computeradresse ein Computername vorhanden ist, entfernen Sie den Computernamen neben der Loopback-IP-Adresse. rlogin verhält sich dann wie erwartet.
rlogin	**Problem:** Wenn ein Benutzer versucht, mit dem rlogin-Tool auf das System zuzugreifen und falsche Anmeldeinformationen eingibt, leitet das System den Authentifizierungsprozess an das telnet-Tool um. Möglicherweise fordert das System außerdem dazu auf, je nach telnet-Konfiguration das Passwort oder den Passcode einzugeben. **Lösung:** Wenn rlogin durch SecurID geschützt ist, muss telnet ebenfalls durch SecurID geschützt werden und umgekehrt.

Probleme bei Upgrade und Deinstallation

Problem: Wenn Sie versuchen, ein Upgrade oder eine Deinstallation von PAM Agent durchzuführen, ohne das RSA-PAM-Modul zu deaktivieren, erhalten Sie möglicherweise die Fehlermeldung „pam_securid.so is busy, not able to remove/replace".
Lösung: Um dieses Problem zu beheben, müssen Sie sich mit anderen Tools als ssh anmelden und **pam_securid.so** manuell entfernen.

Authentifizierungsdienstprogramme für den UDP-Modus

Authentifizierungsdienstprogramme befinden sich in den folgenden Verzeichnissen:

- 32-Bit-Betriebssystem: ***Pam Agent-Installationsverzeichnis*/bin/32bit**
- 64-Bit-Betriebssystem: ***Pam Agent-Installationsverzeichnis*/bin/64bit**

Verwenden Sie diese Dienstprogramme für Folgendes:

- Durchführen einer Testauthentifizierung. Weitere Informationen finden Sie unter Ausführen des acetest-Dienstprogramms Auf der nächsten Seite.
- Überprüfen der Kommunikation zwischen PAM Agent und RSA Authentication Manager. Weitere Informationen finden Sie unter Ausführen des acestatus-Dienstprogramms Auf der nächsten Seite.

Sie können die Protokollierung für diese Dienstprogramme aktivieren. Weitere Informationen finden Sie unter Aktivieren der SecurID-Trace-Protokollierung für den UDP-Modus auf Seite 29.

Ausführen des acetest-Dienstprogramms

Dieses Dienstprogramm prüft mithilfe einer Testauthentifizierung, ob der Agent ordnungsgemäß funktioniert.

Verfahren

1. Wechseln Sie zum Verzeichnis mit den PAM Agent-Authentifizierungsdienstprogrammen:
   - 32-Bit-Betriebssystem: ***PAM Agent-Installationsverzeichnis*/bin/32bit**
   - 64-Bit-Betriebssystem: ***PAM Agent-Installationsverzeichnis*/bin/64bit**
2. Geben Sie Folgendes ein:

   ```
   ./acetest
   ```

3. Geben Sie einen gültigen Benutzernamen und Passcode ein.

Wenn der Zugriff wiederholt verweigert wird, testen Sie die Verbindung mit dem Authentication Manager-Server mithilfe des Dienstprogramms Ausführen des acestatus-Dienstprogramms unten oder wenden Sie sich an Ihren Authentication Manager-Administrator.

Ausführen des acestatus-Dienstprogramms

Dieses Dienstprogramm prüft den Status jeder Authentication Manager-Instanz, in der PAM Agent als Agent-Host registriert ist. Wenn Sie Fragen zu den angezeigten Informationen haben, wenden Sie sich an Ihren Authentication Manager-Administrator.

Verfahren

1. Wechseln Sie zum Verzeichnis mit den PAM Agent-Dienstprogrammen.
2. Geben Sie Folgendes ein:

   ```
   ./acestatus
   ```

In der folgenden Tabelle sind die im Authentication Manager-Abschnitt angezeigten Informationen aufgeführt.

Zurückgegebene Informationen	Beschreibung
Configuration Version	Version der verwendeten **sdconf.rec**-Datei. Für RSA Authentication Manager 8.0 oder höher ist diese Zahl 14.
DES Enabled	Wenn Ihre Konfigurationsumgebung Legacy-Protokolle unterstützt, wird YES angezeigt.
Client Retries	Gibt an, wie oft PAM Agent Authentifizierungsdaten an Authentication Manager sendet, bevor es zu einem Timeout kommt.
Client Timeout	Zeit (in Sekunden), für die PAM Agent wartet, bevor Authentifizierungsdaten erneut an Authentication Manager gesendet werden
Server Release	Versionsnummer von Authentication Manager
Communication	Von Authentication Manager und PAM Agent verwendete Protokollversion

In der folgenden Tabelle sind die im Authentication Manager-Abschnitt angezeigten Statusinformationen aufgeführt.

Statusinformationen	Beschreibung
Server Active Address	Die IP-Adresse, die von PAM Agent für die Kommunikation mit dem Server verwendet wird. Diese Adresse kann die tatsächliche IP-Adresse des von Ihnen ausgewählten Servers oder eine dem Server zugewiesene Alias-IP-Adresse sein. Die IP-Adresse 0.0.0.0 weist darauf hin, dass der Agent bisher keine Kommunikation vom Server erhalten hat.

In der folgenden Tabelle sind die im Authentication Manager-Abschnitt angezeigten Serverstatusinformationen aufgeführt.

Serverstatus	Beschreibung
Verfügbar für Authentifizierungen	Dieser Server ist verfügbar, um Authentifizierungsanforderungen zu verarbeiten.
Nicht verwendet	Der Server hat noch keine Authentifizierungsanforderung erhalten.
For Failover only	Der Server ist nur für Failover-Zwecke reserviert.
Default Server During initial requests	Derzeit ist nur dieser Server für die Verarbeitung von Anforderungen verfügbar.

Konvertierungsdienstprogramm für den UDP-Modus

Das Konvertierungsdienstprogramm wird verwendet, wenn eine UDP-basierte PAM Agent-Instanz gemeinsam mit anderen SecurID-Agents vorhanden ist.

Das Konvertierungsdienstprogramm ns_conv_util befindet sich in den folgenden Verzeichnissen:

- 32-Bit-Betriebssystem: ***pam agent home*/bin/32bit**
- 64-Bit-Betriebssystem: ***pam agent home*/bin/64bit**

Verfahren

1. Wechseln Sie zum Verzeichnis der PAM Agent-Dienstprogramme.
2. Geben Sie Folgendes ein:

   ```
   ./ns_conv_util <Existing_Securid_file_path> <New_Securid_dir_path>
   ```

   Dabei ist *<Existing_Securid_file_path>* der Pfad, in dem sich die aktuelle SecurID-Datei befindet,

   und *<New_Securid_dir_path>* ist das Verzeichnis, in dem die neu erzeugte SecurID-Datei gespeichert werden soll.

   Beispiel:

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

3. Wenn der neue Zielspeicherort nicht mit dem von VAR_ACE angegebenen Speicherort identisch ist, kopieren Sie die neue SecurID-Datei an diesen Speicherort.

Node-Schlüssel für den UDP-Modus

Der Node-Schlüssel ist ein symmetrischer Chiffrierschlüssel, den RSA Authentication Manager und PAM Agent

zum Verschlüsseln und Entschlüsseln von Datenpaketen verwenden, während diese über das Netzwerk übertragen werden. Node-Schlüssel sind für Agents erforderlich, die das UDP-Protokoll verwenden. Die gemeinsam Node-Schlüssel ist sowohl in der Authentication Manager-Datenbank als auch in einer Datei auf dem Computer gespeichert, auf dem PAM Agent installiert ist. Für Agents, die das REST-Protokoll verwenden, wird keine Node-Schlüsseldatei verwendet. Anstelle eines Node-Schlüssels wird zusammen mit einem starken Verschlüsselungsalgorithmus ein dynamisch ausgehandelter Schlüssel zum Verschlüsseln des Kanals verwendet.

Wenn für UDP-basierte Agents der Node-Schlüssel auf dem Authentication Manager-Server oder dem Computer, auf dem PAM Agent installiert ist, fehlt, deaktivieren Sie den Node-Schlüssel am anderen Speicherort. Wenn die Node-Schlüsseldateien auf dem Authentication Manager- und dem PAM Agent-Computer nicht übereinstimmen, löschen Sie den Node-Schlüssel an beiden Speicherorten. Nachdem Sie den Node-Schlüssel gelöscht haben, müssen Sie einen neuen Node-Schlüssel erzeugen.

Löschen des Node-Schlüssels aus RSA SecurID Authentication Agent 8.0 for PAM

Wenn der Node-Schlüssel in RSA SecurID Authentication Agent 8.0 for PAM und auf dem Computer, auf dem PAM Agent installiert ist, nicht übereinstimmen oder der Node-Schlüssel auf dem PAM Agent-Computer fehlt, müssen Sie den Node-Schlüssel aus Authentication Manager löschen. Wenn Sie PAM Agent neu installieren, fehlt der Node-Schlüssel auf dem PAM Agent-Computer.

Verfahren

1. Klicken Sie in der Authentication Manager-Sicherheitskonsole auf **Zugriff > Authentifizierungs-Agents > Vorhandene managen**.
2. Suchen Sie nach dem betroffenen Agent-Computer und wählen Sie **Node-Schlüssel managen** aus dem Drop-down-Menü aus.
3. Aktivieren Sie das Kontrollkästchen **Node-Schlüssel löschen** und klicken Sie dann auf **Speichern**.

Nach Abschluss

- Wenn ein Node-Schlüssel auf dem PAM Agent-Computer vorhanden ist, finden Sie weitere Informationen unter Löschen des Node-Schlüssels vom PAM Agent-Computer unten.
- Wenn auf dem PAM Agent-Computer kein Node-Schlüssel vorhanden ist, befolgen Sie das Verfahren unter Erzeugen eines neuen Node-Schlüssels Auf der gegenüberliegenden Seite.

Löschen des Node-Schlüssels vom PAM Agent-Computer

Wenn der Node-Schlüssel in der RSA Authentication Manager-Instanz und auf dem PAM Agent-Computer nicht übereinstimmen oder der Node-Schlüssel in Authentication Manager fehlt, müssen Sie den Node-Schlüssel vom PAM Agent-Computer löschen. Wenn Sie beispielsweise eine neue Authentication Manager-Instanz installieren und eine vorhandene PAM Agent-Instanz hinzufügen, fehlt der Node-Schlüssel in Authentication Manager.

Bevor Sie beginnen

Wenn ein Node-Schlüssel in Authentication Manager vorhanden ist, finden Sie weitere Informationen unter Löschen des Node-Schlüssels aus RSA SecurID Authentication Agent 8.0 for PAM oben.

Verfahren

1. Melden Sie sich bei dem Computer an, auf dem PAM Agent installiert ist, und suchen Sie nach der Node-Schlüsseldatei **securid**, die sich im Verzeichnis **/var/ace** befindet.

2. Benennen Sie die Node-Schlüsseldatei um oder löschen Sie die Datei.
3. Der Node-Schlüssel wird auch im Servercache gespeichert. Starten Sie den Computer neu, um den Node-Schlüssel aus dem Cache zu löschen.

Nach Abschluss

Erzeugen eines neuen Node-Schlüssels unten

Erzeugen eines neuen Node-Schlüssels

Verfahren

1. Führen Sie das acetest-Dienstprogramm auf dem PAM Agent-Computer aus, um die Node-Schlüsseldatei zu erzeugen. Weitere Informationen finden Sie unter Authentifizierungsdienstprogramme für den UDP-Modus auf Seite 41.
2. Prüfen Sie Ihre Authentifizierungsprotokolle und stellen Sie sicher, dass ein neuer Node-Schlüssel gesendet wurde.
3. Starten Sie den PAM Agent-Computer neu, damit der Agent die Node-Schlüsseldatei lesen kann.

Protokollierung für PAM Agent

Wenn die Protokollierung aktiviert ist, werden PAM Agent-Authentifizierungsmeldungen standardmäßig im Systemprotokoll aufgezeichnet. Für Verfolgungszwecke können Sie Ihr Systemprotokoll so konfigurieren, dass PAM Agent-Authentifizierungsprotokollmeldungen für bestimmte Tools aufgezeichnet werden. Weitere Informationen finden Sie unter Aktivieren der Debug-Ausgabe auf Seite 28.

Konfigurieren des Systemprotokolls

Mit dem folgenden Verfahren werden alle Authentifizierungsmeldungen an das Systemprotokoll gesendet.

Verfahren

1. Wechseln Sie zum Verzeichnis **/etc /**.
2. Öffnen Sie die Datei **syslog.conf**.
3. Fügen Sie den Parameter `auth.notice` zu der Zeile hinzu, in der Ihre Systemprotokolldatei angegeben ist.
4. Entfernen Sie den Parameter`authpriv.none`, wenn er für die Systemprotokolldatei angegeben ist.
5. Wenn Sie telnet oder login verwenden, fügen Sie den Parameter `authpriv.notice` zu der Zeile hinzu, in der die Systemprotokolldatei angegeben ist.
6. Speichern Sie Ihre Änderungen.
7. Starten Sie den Syslog-Daemon neu.

PAM Agent-Authentifizierungsprotokollmeldungen

In der folgenden Tabelle sind die Authentifizierungsprotokollmeldungen aufgeführt.

Meldung	Beschreibung
Cannot locate **sd_ pam.conf** file	Die Konfigurationsdatei **sd_pam.conf** befindet sich nicht im Verzeichnis **/etc.**; **/etc.** muss die richtige Konfigurationsdatei enthalten, damit VAR_ACE ordnungsgemäß festgelegt werden kann.
AceInitialize	AceInitialize ist ein API-Funktionsaufruf, mit dem Worker Threads initialisiert und

Meldung	Beschreibung
failed	Konfigurationseinstellungen aus **sdconf.rec** geladen werden. Überprüfen Sie, ob Sie die neueste Kopie von **sdconf.rec** von Ihrem Authentication Manager-Administrator erhalten haben und ob VAR_ACE ordnungsgemäß festgelegt ist.
Cannot communicate with RSA ACE/Server	Entweder wurden die Authentication Manager-Broker nicht gestartet oder es ist ein Netzwerkausfall aufgetreten. Wenden Sie sich an Ihren Authentication Manager-Administrator oder Ihren Netzwerkadministrator.
Reserve password exceeds character limit	Die maximale Anzahl der Zeichen ist auf 256 Zeichen beschränkt.
Invalid reserve password	Das Reservepasswort ist mit dem Systempasswort für den Host identisch. Sie müssen dieses Passwort kennen, wenn Authentication Manager Authentifizierungsanforderungen nicht verarbeiten kann.
User name exceeds character limit	Der Benutzername darf nicht länger als 31 Zeichen sein.
Reserve password not allowed. User is not root.	Stellen Sie sicher, dass Sie ein Root-Benutzer sind. Nur Root-Benutzer können das Reservepasswort verwenden.

Protokollierung für den REST-Modus

Der REST-Modus unterstützt die zusätzliche Protokollierung, die von der **log4cxx**-Bibliothek implementiert wird. Die Protokollierung für die REST-Ebene erfolgt separat von den PAM Agent-Protokollen. RollingFileAppender und SyslogAppender werden unterstützt. RollingFileAppender ist standardmäßig aktiviert. Protokolle werden in **/var/ace/log/mfa_rest.log** mit der Protokollebene „INFO" gespeichert. Die größenbasierte Rotation wird mit einer Rotationsgröße von 10 MB aktiviert.

Die zeitbasierte Protokollrotation wird nicht unterstützt. Da unterstützte Tools wie ssh und su den Authentifizierungs-Agent für jede Anforderung laden, können die Protokolle in PAM Agent nicht basierend auf der Zeit rotiert werden. PAM Agent unterstützt die größenbasierte Protokollrotation.

Sie können die Standardprotokolleinstellungen für den REST-Modus ändern.

Verfahren

1. Wechseln Sie zum Verzeichnis **/var/ace/conf**.
2. Öffnen Sie die Datei **log.properties**.
3. Konfigurieren Sie die folgenden Einträge für die größenbasierte Rotation :

```
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. Konfigurieren Sie die folgenden Einträge, um die lokale und Remoteprotokollierung an syslog zu unterstützen:

```
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. Speichern Sie Ihre Änderungen.
6. Starten Sie den Syslog-Daemon neu.

Troubleshooting von SELinux

Für SELinux (Security-Enhanced Linux) sind manchmal die unten angegebenen zusätzlichen Verfahren erforderlich.

Verwenden des REST-Protokolls auf einem aktualisierten Agent

Um das REST-Protokoll für die Authentifizierung zu verwenden, müssen Sie die vorhandene SELinux-Policy überschreiben, bei ein Upgrade von PAM Agent durchführen. Andernfalls können einige Tools keine Authentifizierung mit dem REST-Protokoll ausführen.

Zum Aktualisieren der SELinux-Policy können Sie das Installationsskript erneut ausführen und die vorhandene Policy überschreiben. Dateien, die bereits aktualisiert wurden, sind nicht betroffen.

Aktivieren der benutzerdefinierten Pfadeinstellungen

Wenn SELinux aktiviert ist, funktionieren benutzerdefinierte Pfadeinstellungen für VAR_ACE und RSATRACEDEST standardmäßig nicht.

Verfahren

Um benutzerdefinierte Pfadeinstellungen zu aktivieren, müssen Sie die folgenden Befehle eingeben, wobei

<custom_directory_path> der Pfad des benutzerdefinierten VAR_ACE-Verzeichnisses oder des RSATRACEDEST-Verzeichnisses ist, das Sie verwenden möchten:

```
semanage fcontext -a -t var_t <custom_directory_path>
```

```
restorecon -R <custom_directory_path>
```

Konfigurieren der Werte für Timeout und Retry für die REST-Authentifizierung

Sie können konfigurieren, wie die Herstellung einer Verbindung von PAM Agent mit RSA Authentication Manager oder dem Cloudauthentifizierungsservice dauern kann und wie lange PAM Agent auf eine Antwort wartet. Sie können außerdem konfigurieren, wie oft PAM Agent versucht, eine primäre Instanz oder Replikatinstanz von Authentication Manager oder den Cloudauthentifizierungsservice zu kontaktieren. Diese Parameter werden nur vom REST-Protokoll verwendet.

Stellen Sie sicher, dass Sie die Geschwindigkeit Ihres Netzwerks berücksichtigen. Die Festlegung hoher Timeout-Werte in einem langsameren Netzwerk sorgt dafür, dass die Authentifizierung erfolgreich ist.

Bevor Sie beginnen

Sie benötigen Root-Berechtigungen für den Computer, auf dem der Agent installiert ist, und Schreibberechtigungen für das Verzeichnis, in dem die Datei **mfa_api.properties** gespeichert ist. Standardmäßig ist diese Datei in **/var/ace/conf** gespeichert.

Verfahren

1. Wechseln Sie zu dem Verzeichnis, in dem sich **mfa_api.properties** befindet. Standardmäßig lautet das Verzeichnis **/var/ace/conf**.
2. Öffnen Sie **mfa_api.properties**.
3. Sie können die folgenden Parameter ändern:
    - CONNECT_TIMEOUT: Die maximale Anzahl von Sekunden, die für die Herstellung der Verbindung vom Agent mit dem Server zulässig sind. Der Standardwert beträgt 60 Sekunden.
    - READ_TIMEOUT: Die maximale Anzahl von Sekunden, die für die Herstellung der Verbindung vom Agent mit dem Server und das Lesen der Antwort zulässig sind. Der Wert für READ_TIMEOUT muss der Summe aus dem Wert für CONNECT_TIMEOUT und der maximal zulässigen Zeit für das Lesen der Antwort entsprechen. Der Standardwert beträgt 120 Sekunden.
    - MAX_RETRIES: Die Anzahl der Versuche für die Herstellung der Verbindung von PAM Agent mit Authentication Manager oder dem Cloudauthentifizierungsservice. Der Standardwert ist 3.
    - Für die Initialisierungsphase der Authentication Manager-REST-Schnittstelle gibt MAX_RETRIES beim Starten eines Authentifizierungsversuchs durch PAM Agent an, wie oft der Agent versucht, denselben Server zu kontaktieren, bevor ein Failover zu einem anderen Server erfolgt. Wenn PAM Agent während der Überprüfungsphase Authentifizierungsinformationen bereitstellt und kein Failover unterstützt wird, gibt MAX_RETRIES an, wie oft der Agent versucht, denselben Server zu kontaktieren, bevor die Authentifizierung fehlschlägt.
    - Der Cloudauthentifizierungsservice bietet keine Unterstützung für Failover. Sowohl für die Initialisierungs- als auch die Überprüfungsphase gibt MAX_RETRIES an, wie oft der Agent versucht, denselben Server zu kontaktieren, bevor die Authentifizierung fehlschlägt.
4. Speichern Sie die Datei.

Deinstallieren von RSA SecurID Authentication Agent 8.0 for PAM

Sie können PAM Agent entweder manuell auf den einzelnen Computern deinstallieren oder Sie können sich für eine automatische Deinstallation mehrerer Kopien von PAM Agent entscheiden.

Bei der Deinstallation von RSA SecurID Authentication Agent 8.0 for PAM werden die konfigurierten SELINUX-Beschriftungen für REST-Bibliotheken entfernt, die während der Installation von PAM Agent erstellt wurden.

Bevor Sie beginnen

- Konfigurieren Sie die geschützten RSA SecurID-Tools für die Verwendung des standardmäßigen PAM-Moduls, das mit dem Betriebssystem bereitgestellt wird, nicht für das RSA PAM-Modul. Alle aktiven Sitzungen, die RSA PAM-Module verwenden, müssen geschlossen werden, bevor Sie mit der Deinstallation fortfahren. Sie müssen die Verfahren, die Sie unter Konfigurieren von Tools auf Seite 23 befolgt haben, rückgängig machen.

  Hinweis: Wenn Sie das RSA-Modul deinstallieren, während Verweise auf das RSA-Modul im Verzeichnis **/etc/pam.d** vorhanden sind, werden aus Ihrem System ausgesperrt.

- Überprüfen Sie, ob Sie über Root-Berechtigungen auf dem Host verfügen.

Deinstallieren von PAM Agent von einem Computer

Führen Sie die folgende Aufgabe aus, um eine PAM Agent-Instanz zu deinstallieren.

Verfahren

1. Wechseln Sie zum PAM Agent-Stammverzeichnis. Beispiel: **/opt/pam**.
2. Führen Sie das Deinstallationsskript aus. Geben Sie Folgendes ein:

   ```
   ./uninstall_pam.sh
   ```

3. Überprüfen Sie, ob das Installationsverzeichnis entfernt wurde. Wenn das Verzeichnis noch vorhanden ist, müssen Sie es manuell entfernen.
4. Zum Überprüfen, ob PAM Agent erfolgreich entfernt wurde, prüfen Sie die Datei **/var/pam_uninstaller/uninstaller.log**.

Massendeinstallation von PAM Agent im unbeaufsichtigten Modus

Führen Sie die folgende Aufgabe aus, um eine große Anzahl von PAM Agent-Instanzen zu deinstallieren.

Verfahren

1. Erstellen Sie eine textbasierte Konfigurationsdatei mit dem Namen **unconfig**. Die Datei muss die folgenden Informationen enthalten:

   ```
   /opt/
   y
   y
   y
   ```

   Dabei ist */opt/* der PAM Agent-Stammpfad, der normalerweise **/opt/** ist.

Jedes „y" ist eine Antwort auf eine Eingabeaufforderung:

- Are you sure that you would like to uninstall the RSA Authentication Agent 8.0.0 [101] for PAM?
- The RSA Authentication Agent for PAM will be deleted from the */opt* 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. Wechseln Sie zum PAM Agent-Stammverzeichnis. Beispiel: **/opt/pam**.
3. Führen Sie das Deinstallationsskript aus. Geben Sie Folgendes ein:

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

Anhang B: Wichtige Konfigurationsdateien

Wichtige Konfigurationsdateien 52

Wichtige Konfigurationsdateien

Der Standardinstallationsverzeichnis für PAM Agent ist **/opt/pam**. Dies kann während der Installation geändert werden. Standardmäßig enthält das Verzeichnis **/var/ace** REST-relevante Bibliotheken und Dateien. Dieser Verzeichnisspeicherort kann nicht geändert werden.

Zusätzlich zu den Binärdateien (**pam_securid.so**, **acetest**, **acestatus** und **ns_conv_util**) verwaltet PAM Agent die wichtigen Konfigurationsdateien, die in der folgenden Tabelle aufgeführt sind.

Datei	Beschreibung
log.properties	PAM Agent-Protokollierungskonfigurationsdatei für das REST-Protokoll. PAM Agent verwendet die Bibliothek **log4cxx** für die Protokollierung im REST-Modus.
mfa_ api.properties	Enthält die vom REST-Protokoll für die Authentifizierung bei Authentication Manager und dem Cloudauthentifizierungsservice verwendeten Einstellungen.
sdconf.rec	Diese Datei wird von RSA Authentication Manager erzeugt und enthält Konfigurationsinformationen, die das Verhalten von PAM Agent steuern. Diese Datei benötigt die Berechtigung „-rw------- root root“. Diese Datei wird nur im UDP-Modus verwendet.
sdopts.rec	Diese Datei wird für den manuellen Lastausgleich verwendet. Sie enthält eine Liste mit IP-Adressen für Authentication Manager-Instanzen. Diese Datei benötigt die Berechtigung „-rw------- root root“. Diese Datei wird nur im UDP-Modus verwendet.
sdstatus.12	Diese Datei wird von der PAM Agent-Authentifizierungs-API zum Nachverfolgen des letzten bekannten Status der Authentication Manager-Server verwendet. Diese Datei benötigt die Berechtigung „-rw------- root root“.
sd_pam.conf	Enthält die Konfigurationseinstellungen, die das Verhalten von PAM Agent steuern. Diese Datei benötigt die Berechtigung „-rw-r--r-- root root“.
securid	Diese Datei enthält einen gemeinsamen geheimen Schlüssel für den Schutz der UDP-Protokollkommunikation zwischen dem lokalen Computer und Authentication Manager. Der Name dieser Datei wird vom konfigurierten Protokollnamen des lokalen Systems für den Port abgeleitet, über den der Agent mit Authentication Manager kommuniziert, in der Regel über die Datei „services“. Diese Datei benötigt die Berechtigung „-r-------- root root“. Das hängt jedoch von der Umask-Einstellung des Betriebssystems ab. Für das UDP-Protokoll ist diese Datei erforderlich. Für die Authentifizierung mit dem REST-Protokoll ist die Datei optional.