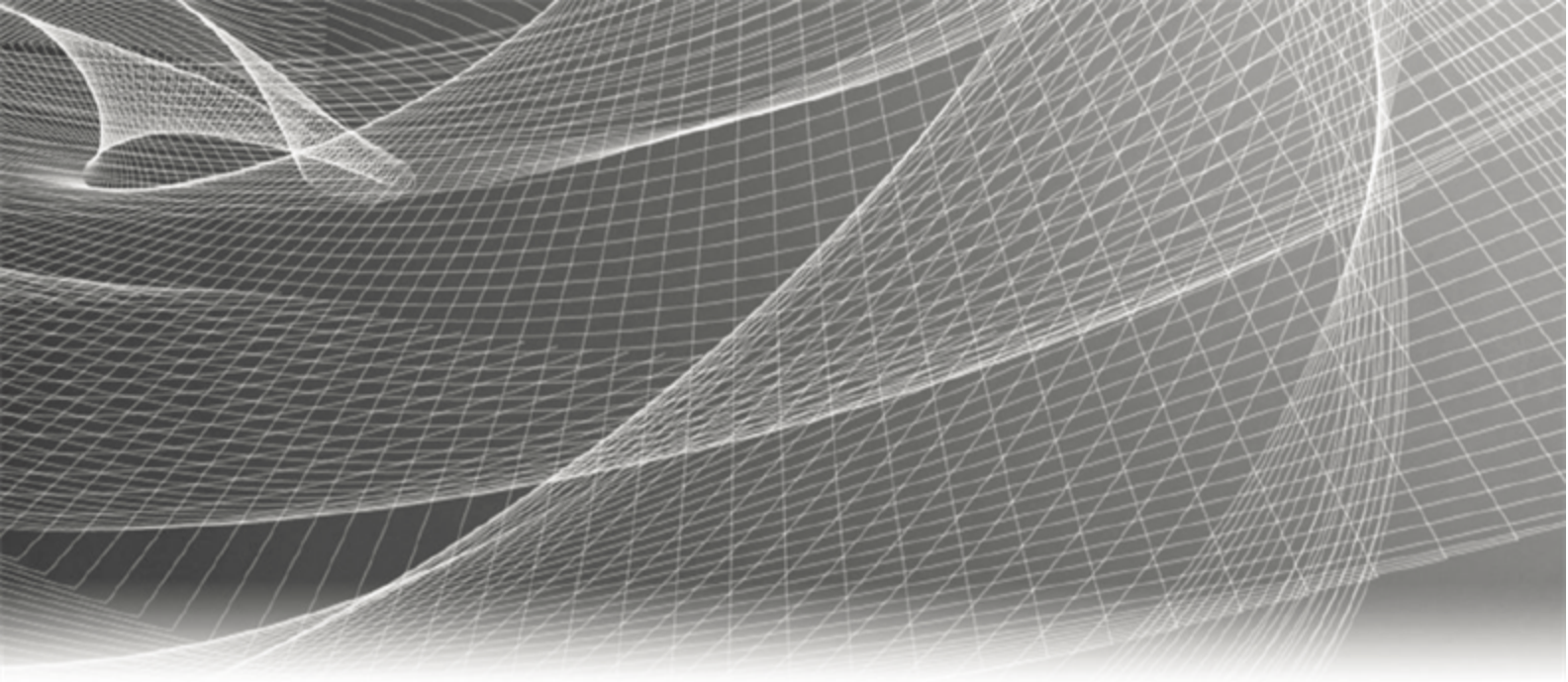

RSA SECURID® ACCESS

RSA® Authentication Agent 8.1 for PAM

インストールおよび構成ガイド(Solaris用)

連絡先情報

RSA Link(https://community.rsa.com)では、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

商標

Dell、RSA、RSAロゴ、EMC、および他の商標は、Dell Inc.またはその関連会社の商標又は登録商標です。その他の商標は、それぞれの所有者の商標又は登録商標です。RSAの商標のリストについては、japan.emc.com/legal/emc-corporation-trademarks.htmを参照してください。

使用許諾契約

本ソフトウェアと関連ドキュメントは、Dell Inc.またはその関連会社が著作権を保有しており、使用許諾契約に従って提供されます。本ソフトウェアと関連ドキュメントの使用と複製は、使用許諾契約の条項に従い、上記の著作権を侵害しない場合のみ許諾されます。本ソフトウェアと関連ドキュメント、およびその複製物を他人に提供することは一切認められません。

本使用許諾契約によって、本ソフトウェアと関連ドキュメントの所有権およびその他の知的財産権が譲渡されることはありません。本ソフトウェアと関連ドキュメントを不正に使用または複製した場合、民事および刑事上の責任が課せられる可能性があります。

本ソフトウェアは予告なく変更されることがありますので、あらかじめご承知おきください。

サード パーティ ライセンス

本製品にはRSA以外のサード パーティによって開発されたソフトウェアが含まれます。本製品内のサード パーティ製ソフトウェアに適用される使用許諾契約の内容については、RSA Linkの製品ドキュメント ページで確認できます。本製品を使用することにより、本製品のユーザーは、これらの使用許諾契約の条項に同意したものとみなされます。

暗号技術に関する注意

本製品には、暗号技術が組み込まれています。これらの暗号技術の使用、輸入、輸出は、各国の法律で禁止または制限されています。本製品を使用、輸入、輸出する場合は、各国における使用または輸出入に関する法律に従わなければなりません。

配布

この資料に記載される、いかなるDellソフトウェアの使用、複製、頒布も、当該ソフトウェア ライセンスが必要です。

Dell Inc.は、この資料に記載される情報が、発行日時点で正確であるとみなしています。この情報は予告なく変更されることがあります。

この資料に記載される情報は、「現状有姿」の条件で提供されています。Dell Inc. は、この資料に記載される情報に関する、どのような内容についても表明保証条項を設けず、特に、商品性や特定の目的に対する適応性に対する黙示の保証はいたしません。

2018年10月

目次

はじめに

対象読者

このガイドの対象読者は、RSA® Authentication Agent for PAM(Pluggable Authentication Module)のインストール、アップグレード、トラブルシューティングを行うネットワーク管理者とシステム管理者です。

サポートとサービス

RSA Link(https://community.rsa.com)で、コミュニティとサポート情報にアクセスできます。RSA Linkでは、よくある質問への回答や、既知の問題の解決方法を含むナレッジベースを公開しています。また、製品ドキュメント、コミュニティ ディスカッション、ケース管理なども公開されています。

RSA Ready Partner Program

RSA Ready Partner Program Webサイト(www.rsaready.com)では、RSA製品との連携が検証されたサード パーティのハードウェア製品およびソフトウェア製品に関する情報を利用できます。このWebサイトでは、RSA製品とこれらのサード パーティ製品の相互運用について、詳細な手順を説明した実装ガイドおよびその他の情報を提供しています。

第1章:PAM agentのインストール

RSA Authentication Agent 8.1 for PAMの概要

RSA Authentication Agent 8.1 for PAM(Pluggable Authentication Module)は、標準またはOpenSSHの接続ツールを使用したUNIXシステムでの認証をサポートしています。PAM agentは、RSAのカスタマイズされた共有ライブラリを使用し、クラウド認証サービスとRSA Authentication Managerによってサポートされている認証方法を使用してUNIXサーバおよびワークステーションへのアクセスをサポートします。

PAM agentがクラウド認証サービスまたはAuthentication Managerのどちらで認証するかを選択できます。RSA SecurID Access Enterprise EditionライセンスとPremium Editionライセンスには、この両方のRSA SecurID Accessコンポーネントが含まれています。PAM agentを使用するためにAuthentication Managerは必須ではありません。

PAM agentのバージョン8.1は、以下のメリットを新たにもたらします。

- クラウド認証サービスのサポート。クラウド認証サービスは、承認(モバイル向けに最適化されたプッシュ通知)、Authenticate Tokencode、デバイス生体認証、SMSトークンコード、音声トークンコード、RSA SecurIDトークンなどの多要素認証方法を使用して、SaaSおよびオンプレミスのWebアプリケーションへのユーザーのアクセスを保護します。
- UDPプロトコルではなくRESTプロトコルを使用してAuthentication Managerにアクセスする機能。
- 以前のバージョンのPAM agentによって使用されるUDPプロトコルの継続的サポート。
- Authentication Managerには、インストール済みのRESTプロトコルを使用するPAM agentの管理に役立つ、エージェントレポートが用意されています。RESTモードのPAM agentは、インストールされた各PAM agentに固有のソフトウェアID番号やエージェントが使用するオペレーティングシステムに関する情報などの追加的な情報をAuthentication Managerサーバに送信できます。

PAM agentをRESTモードで使用すると、UDPプロトコルを使用する場合にはない、以下のような追加的なメリットがあります。

- Authentication Manager導入環境にクラウド認証サービスを容易に統合できます。
- 1つの認証エージェント レコードをAuthentication Managerに追加して維持し、そのレコードを使用して複数のエージェントをインストールして管理することができます。
- UDPプロトコルを使用する場合よりも容易に、複数の認証エージェントを同じハードウェア上で実行できます。
- 認証エージェントがIPv4ネットワーク設定またはIPv4プロトコルを使用する必要がある導入環境で、TCPプロトコルを使用します。
- RESTプロトコルの認証モードでは、バージョン8.1のPAM agentは、FIPS準拠の暗号ライブラリモジュール**fips-2.0.16**とOpenSSLバージョン1.0.2lを使用します。詳細については、*OpenSSL FIPS 140-2 Security Policy Version 2.0.16* (https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf)を参照してください。
- RESTプロトコルを使用しない認証エージェントと比べて、新機能および機能拡張のための認証エージェントの更新回数が少なくてすみます。RESTプロトコルを使用する認証エージェントはAuthentication Managerの変更内容を活用できる可能性が高いため、エージェントの更新回数が少なくなります。

認証モード

PAM agentは3つの認証モードのいずれかでインストールできます。RSA SecurID認証はいずれのモードにも対応しています。必要に応じて、モードをインストール後に変更することもできます。手順については、「PAM agentの認証モードの変更 (33ページ)」を参照してください。

認証モード	説明
RSA Authentication ManagerとUDPプロトコル	RSA SecurIDのハードウェアおよびソフトウェアトークンは、RSA SecurIDトークンコードを生成します。エージェントはユーザーによって入力されたデータがAuthentication Managerに保存されているデータと一致しているかどうか検証し、その結果に基づいてアクセスを許可または拒否します。

認証モード	説明
	PAM agentをアップグレードすると、デフォルトで、UDPプロトコルを使用するよう設定されます。RESTプロトコルを使用する別の認証モードに容易に切り替えることができます。
RSA Authentication ManagerとRESTプロトコル	RESTプロトコルを使用してAuthentication Managerによってサポートされているすべての認証タイプをサポートします。これには、RSA SecurIDのソフトウェアトークンおよびハードウェアトークン、クラウド認証サービスコンポーネントとの統合によるAuthenticate Tokencodeが含まれます。
クラウド認証サービスとRESTプロトコル	承認(モバイル向けに最適化されたプッシュ通知)、Authenticate Tokencode、デバイス生体認証、SMSトークンコード、音声トークンコード、RSA SecurIDトークンをサポートします。FIDOトークンおよび認証方法の組み合わせ(承認とRSA SecurIDトークンの組み合わせなど)を要求する認証条件はサポートされていません。

RSA Authentication Agent 8.1 for PAMはRSA Authentication Managerトラステッド レルムをサポートします。Authentication ManagerのRBA(リスク ベース認証)はサポートされていません。

PAM agentのワークフロー

PAM agentはUNIXサーバにインストールされ、認証を受けるユーザーとRSA Authentication Managerサーバまたはクラウド認証サービスのいずれかの間の仲介者のように機能します。

PAM agentはAuthentication Managerのセキュリティ機能をサポートしています。たとえば、特定のトークンに関連づけられたユーザーが新しいPINを設定する必要があるとAuthentication Managerが判断した場合、エージェントは、Authentication Managerで定義された条件のPINを設定するようユーザーにリクエストし、入力された情報をAuthentication Managerに送信します。Authentication Managerがユーザーのネクスト トークンコードをリクエストした場合、PAM agentはネクスト トークンコードの入力プロンプトをユーザーに表示します。正しいネクスト トークンコードがAuthentication Managerに送信されなかった場合、認証は失敗します。

以下のステップは、3つすべての認証モードにおけるPAM agentの認証の流れを示しています。

1. ユーザーがローカル(loginを使用)またはリモート(rlogin、telnet、SSH、FTPなどのツールを使用)から、PAM agentによって保護されているマシンにアクセスしようとします。

   このユーザーは、PAM agentがインストールされているマシン上にローカルに存在する必要があります。

2. UNIXのPAM(Pluggable Authentication Module)インフラストラクチャがすべてのログオン リクエストをインターセプトし、PAM構成ファイルを使用してRSA PAMモジュールにアクセスします。
   - ユーザーがRSA SecurID認証をするよう構成されていない場合、RSA PAMモジュールはリクエストを成功させます。
   - アクセスをリクエストしているユーザーがRSA SecurID認証をするよう構成されている場合、PAM agentはステップ3の認証に進みます。
3. PAM agentの認証モードに基づいて、エージェントがAuthentication Managerまたはクラウド認証サービスと通信します。

   UDP接続またはRESTプロトコルを使用するAuthentication Managerの場合は、以下のステップが実行されます。

   a. エージェントがユーザー名、続いてパスコードの入力をユーザーに求めます。
   b. エージェントがユーザー名とパスコードをAuthentication Managerに安全に送信します。
      - Authentication Managerがリクエストを承認した場合、エージェントはユーザーにアクセスを許可します。
      - Authentication Managerがリクエストを承認しなかった場合、エージェントはアクセスを拒否します。

   クラウド認証サービスの場合は、以下のステップが実行されます。

a. エージェントがユーザーにユーザー名の入力を求め、入力された情報をクラウド認証サービスに送信します。
b. クラウド認証サービスがクラウド認証サービスのアクセス ポリシーの保証レベルによってユーザーに設定された認証方法のリストをエージェントに送信します。
c. エージェントがユーザーに認証するよう求めます。
d. ユーザーが使用可能な認証方法を選択して、認証します。
   - クラウド認証サービスがリクエストを承認した場合、エージェントはユーザーにアクセスを許可します。
   - 認証が失敗した場合、クラウド認証サービスは次の認証方法を選択するようユーザーに求めます。
   - クラウド認証サービスがリクエストを承認しなかった場合、エージェントはアクセスを拒否します。

ソフトウェアの要件

このセクションでは、PAM agentによってサポートされているソフトウェアの最小バージョンについて説明します。

必要なオペレーティング システム

PAM agentには、次のいずれかのオペレーティング システムが必要です。

- Solaris SPARC 10.5(32ビットおよび64ビット)、ゾーン使用
- Solaris SPARC 11.2(32ビットおよび64ビット)
- Solaris x86 10.5アップデート11(32ビット)
- Solaris x86 11.3(32ビット)

オペレーティング システムに対応した32ビット版または64ビット版の**libuuid.so**(UUIDライブラリ)がPAM agentマシンにインストールされている必要があります。

RSA Authentication Managerのバージョンのサポート

RSA Authentication Agent 8.1 for PAMは、現行バージョンのREST APIである、RSA SecurID Authentication APIバージョン1.1をサポートしています。

次の表に、特定の機能をサポートするために必要となるRSA Authentication Managerのバージョンを示します。

必要なRSA Authentication Managerのバージョン	サポートされる機能
8.2 SP1以降	PAM agentにはRSA Authentication Manager 8.2 SP1以降が必要です。
8.2 SP1パッチ5以降	PAM agentでエージェント レポート機能を有効にする場合は、RESTモードでの認証失敗を防ぐため、RSA Authentication Manager 8.2 SP1 Patch 5以降が必要です。
8.3以降	RSA Authentication Manager 8.3以降のバージョンには、インストール済みのRESTプロトコルを使用するPAMエージェントの管理に役立つエージェント レポートが用意されています。これらのレポートには、PAM agentがAuthentication Managerに送信する追加情報が含まれています。

クラウド認証サービスのバージョンのサポート

RSA Authentication Agent 8.1 for PAMは、現行バージョンのREST APIである、RSA SecurID Authentication APIバージョン

1.1をサポートしています。

証明書の要件

PAM agentはRESTプロトコルではTLS 1.2証明書を使用します。クラウド認証サービスとRSA Authentication Manager 8.2以降は、これらの証明書を受け入れることができます。TLS 1.2証明書を使用していない導入環境では、認証モードとしてAuthentication ManagerとUDPプロトコルを使用する必要があります。

RESTプロトコルの認証モードでは、PAM agentは、FIPS準拠の暗号ライブラリモジュール**fips-2.0.16**とOpenSSLバージョン1.0.2lを使用します。詳細については、*OpenSSL FIPS 140-2 Security Policy Version 2.0.16* (https://www.openssl.org/docs/fips/SecurityPolicy-2.0.16.pdf)を参照してください。

サポートされるツール

PAM agentは次のツールをサポートしています。

- telnet
- login
- rlogin
- su
- ssh(ssh、sftp、scp)
- sudo

  サポートされているsudoバージョンを、https://www.sudo.wsからダウンロードしてインストールします。

- ftp(単一トランザクションに制限)
- dtlogin

OpenSSHのサポート(オプション)

PAM agentはOpenSSH 6.0 P1をサポートしています。OpenSSHを使用している場合は、お使いのプラットフォームと互換性のあるバージョンのOpenSSHを使用していることを確認してください。OpenSSHは必須ではありません。

サポートされているオプションのOpenSSHツールは以下のとおりです。

- ssh
- sftp
- scp

OpenSSHをエージェント マシンにインストールします。OpenSSHの動作条件や、ソースコードをコンパイルするために必要となる追加のソフトウェアなどについては、https://www.openssh.comを参照してください。

PAM agentのインストールの計画

PAM agentをインストールする前に、次のタスクを実行します。

- PAM agentをインストールするマシンで次の操作を実行します。
  1. root権限を取得します。
  2. PAM agentの構成ファイルを保存する**/var/ace**ディレクトリを作成し(まだ存在しない場合)、インストール ディレクトリを作成します。
  3. 信頼するルートCA証明書をRSA Authentication Managerまたはクラウド認証サービスから取得します(手順については、ナレッジベースの記事「How to export RSA SecurID Access Authentication Manager or Cloud

Authentication Service Root Certificate」を参照してください)。次の手順を実行します。

a. 証明書の有効期限が切れていないことを確認します。
b. 証明書をPEM形式で保存します。複数のCA証明書がある場合は、これらの証明書をPEM形式の単一ファイルに連結する必要があります。
c. ***filename*.pem**を**/var/ace/**ディレクトリにコピーします。
d. 証明書を保存する**/var/ace/**ディレクトリを適切な権限で保護します。

- RSA Authentication Managerを使用して認証するには、PAM agentの認証エージェント レコードを内部データベース上に作成します。詳細については、Authentication Managerのスーパー管理者に問い合わせるか、RSA Linkの Authentication Managerヘルプを参照してください。
- UDPプロトコルを使用して認証するには、Authentication Manager構成ファイルである**sdconf.rec**を生成するか、このファイルをAuthentication Managerのスーパー管理者から入手する必要があります。このファイルは、RESTプロトコルを使用する認証では必要ありません。

  sdconf.recファイルは、エージェントがAuthentication Managerのプライマリ インスタンスおよびレプリカ インスタンスと通信するためのIPアドレスを指定します。次の操作を実行します。

  - 最新バージョンの**sdconf.rec**ファイルが、エージェント マシン上のアクセス可能なディレクトリ(デフォルトの **/var/ace**ディレクトリなど)に存在することを確認します。
  - **sdconf.rec**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。
- クラウド認証サービスとRESTプロトコルの認証モードでは、PAM agentはロードロード バランシングとフェールオーバーをクラウド認証サービスに依存します。
- RSA Authentication ManagerとRESTプロトコルの認証モードでは、PAM agentはロード バランシングをサポートしません。PAM agentは、最大15個のAuthentication Managerレプリカ インスタンスに対するフェールオーバーをサポートします。
- PAM agentのインストール時に指定する情報を収集します。

  Authentication ManagerとUDPプロトコルの場合。デフォルト値をそのまま使用するか、新しいディレクトリを指定できます。

説明	**計画**
sdconf.recを保存するディレクトリ。デフォルト値は **/var/ace/**です。	
PAM agentディレクトリのルート パス。デフォルト値は **/opt**です。	

  Authentication ManagerとRESTプロトコルの場合。Authentication Managerのスーパー管理者から次の情報を入手します。

説明	**計画**
認証エージェントとAuthentication Managerプライマリ インスタンスの間の通信に使用するRESTサーバ URL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` プライマリ インスタンスのOperations Consoleで、	

説明	計画
[**管理**]>[**ネットワーク**]>[**アプライアンスのネットワーク設定**]ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。	
フェールオーバーに使用できるAuthentication Managerレプリカインスタンスの数。	
各レプリカインスタンスのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` レプリカインスタンスのOperations Consoleで、[**管理**]>[**ネットワーク**]>[**アプライアンスのネットワーク設定**]ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。	
ユーザー認証リクエストをAuthentication Managerに安全に渡すためのアクセスキー(クライアントキー)。この値は、Authentication Managerプライマリインスタンスの Security Consoleで生成されます。 アクセスキーの取得方法については、RSA Linkのトピック「認証エージェント用のRSA SecurID認証APIの構成」を参照してください。	
認証エージェント上に保存された信頼する証明書のディレクトリとファイル名。デフォルト値は**/var/ace/cert.pem**です。	
PAM agent用にAuthentication Managerで作成された認証エージェント名(クライアントID)。	
PAM agentディレクトリのルートパス。デフォルト値は**/opt**です。	

クラウド認証サービスとRESTプロトコルの場合。クラウド認証サービスのスーパー管理者から次の情報を入手します。

説明	計画
エージェントとクラウド認証サービスの間の通信に使用するRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT/mfa/v1_1/authn` クラウド認証サービスの場合、クラウド管理コンソールの任意のIdentity Routerの設定ページの[**Registration**]タブにある[**Authentication Service Domain**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は443です。	
ユーザー認証リクエストをクラウド認証サービスに安全	

説明	計画
に渡すためにクラウド管理コンソールで作成される認証APIキー(クライアント キー)。 認証APIキーの取得方法については、RSA Linkのトピック「Add an RSA SecurID Authentication API Key」を参照してください。	
認証エージェント上に保存された信頼する証明書のディレクトリとファイル名。デフォルト値は**/var/ace/cert.pem**です。	
クラウド認証サービスのテナントID。PAM agentは認証リクエストにテナントIDを指定することができますが、エージェントはこのデータを検証しません。このパラメータは、現時点ではクラウド認証サービスによってサポートされていません。	
クラウド認証サービスのアクセス ポリシー名。このポリシーはクラウド管理コンソールで定義されます。	
モバイル通知に表示するCLIENT_ID認証エージェント名。任意の値を入力できます。たとえば、「PAM_Agent」と入力します。	
PAM agentディレクトリのルート パス。デフォルト値は**/opt**です。	

RSA Authentication Agent 8.1 for PAMのインストール

PAM agentをインストールするには、次のタスクを完了します。

1. UDPモードのエージェントIPアドレスの指定 (16ページ)
2. OpenSSHの構成 (17ページ)
3. PAM agentのインストール (17ページ)
4. UDPモードの場合は、テスト認証を実行します。詳細については、「UDPモードの認証ユーティリティ (41ページ)」を参照してください。

   RESTプロトコル モードの場合は、ブラウザまたはhttpクライアントでRESTサーバのURLにアクセスして、接続をテストします。たとえば、「https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn」と入力します。現時点では認証されていないため、ブラウザまたはhttpクライアントには、「Forbidden」または「Unauthorized」というHTTP応答が表示されます。

UDPモードのエージェントIPアドレスの指定

UDPモードの場合、**sdconf.rec**ファイルと同じディレクトリに**sdopts.rec**ファイルを作成する必要があります。この手順は、RESTモードでは必要ありません。

ファイル	説明
sdopts.rec	エージェントをインストールしたマシンのIPアドレスのリストを指定します。エージェントは、**sdopts.rec**ファイルのIPアドレスを使用して、RSA Authentication Managerと通信します。
sdconf.rec	Authentication Managerが使用するIPアドレスのリストが含まれます。

手順

1. エージェント マシンで、テキスト エディタを使用して、**sdconf.rec**ファイルが保存されているパスに**sdopts.rec**ファイルを作成します。
2. ファイルに、次のように入力します。

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

   *x.x.x.x*はエージェント マシンのIPアドレスです。

   注:大文字のみを使用してください。また、スペースは入れないでください。

3. ファイルを保存します。

OpenSSHの構成

SSH(Secure Shell)プロトコルに基づくセキュリティ関連ネットワーク ユーティリティのスイートであるOpenSSHを使用する場合は、このソフトウェアをPAM agentと連携させ、パスコード認証メッセージをユーザーに表示するよう構成する必要があります。

開始する前に

OpenSSHをエージェント マシンにインストールします。OpenSSHの動作条件や、ソース コードをコンパイルするために必要となる追加のソフトウェアなどについては、https://www.openssh.comを参照してください。

手順

1. エージェント マシン上で**/etc/ssh/sshd_config**ファイルを開きます。
2. 次のパラメータを設定して、変更を保存します。

パラメータ	設定
PAMAuthenticationViaKBDInt	yes
PasswordAuthentication	no
ChallengeResponseAuthentication	yes

   PasswordAuthenticationパラメータを「no」に設定すると、OpenSSHのパスワード プロンプトが無効化され、PAM agentが代わりに使用されます。その結果、SecurID認証のプロンプトのみがユーザーに表示されます。

3. sshdを再起動します。次のように入力します。

   ```
   svcadm restart network/ssh
   ```

PAM agentのインストール

PAM agentは個々のマシンに手動でインストールするか、サイレント インストールを選択して、PAM agentの複数のコピーを自動的に導入することができます。

PAM agentをインストールする前に

1. 次のコマンドを実行します。

   ```
   $which echo
   ```

   /usr/ucb/echoが出力された場合は、**usr/bin**の「echo」バイナリを使用します。

2. 次のコマンドを実行します。

   ```
   $export PATH=/usr/bin:$PATH
   ```

3. Solaris 11をゾーンで使用する場合は、**group/system/solaris-desktop**パッケージをインストールし、PAM agentのインストールに必要なユーティリティを用意します。

1台のマシンへのPAM agentのインストール

1つのPAM agentをインストールします。PAM agentを複数のマシンにインストールするには、「サイレント インストールによるPAM agentの一括インストール (19ページ)」を参照してください。

手順

1. エージェント マシンで、PAM agentのインストール ディレクトリに移動します。
2. 次のように入力して、ファイルを解凍(untar)します。

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

3. 次のように入力して、インストール スクリプトを実行します。

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

4. 表示されるプロンプトに従います。Enterキーを押してデフォルト値を受け入れるか、適切な値を入力します。

   RSA Authentication Manager UDPモードの場合は、次の操作を実行します。

   - RSAソフトウェアの使用許諾契約に同意します。
   - 「0」を入力して、「RSA Authentication ManagerとUDPプロトコル」認証モードを選択します。
   - **sdconf.rec**を保存するディレクトリを入力します。
   - PAM agentのインストール ディレクトリを入力します。

   RSA Authentication Manager RESTモードの場合は、次の操作を実行します。

   - RSAソフトウェアの使用許諾契約に同意します。
   - 「1」を入力して、「RSA Authentication ManagerとRESTプロトコル」認証モードを選択します。
   - 認証エージェントとプライマリ インスタンスの間の通信のためのRESTサーバURLを入力します。
   - フェールオーバー用のAuthentication Managerレプリカ インスタンスがある場合は、「y」と入力します。
   - レプリカ インスタンスの数を指定します。
   - 各レプリカ インスタンスのRESTサーバURLを入力します。
   - 認証リクエストをAuthentication Managerに安全に渡すためのクライアント キー(アクセス キー)を入力します。
   - 認証エージェント上に保存された信頼する証明書のディレクトリとファイル名を入力します。
   - クライアントIDを入力します。これはAuthentication Managerの認証エージェント名です。
   - PAM agentのインストール ディレクトリを入力します。

   クラウド認証サービス RESTモードの場合は、次の操作を実行します。

   - RSAソフトウェアの使用許諾契約に同意します。
   - 「2」を入力して、「クラウド認証サービスとRESTプロトコル」認証モードを選択します。
   - 認証エージェントとクラウド認証サービスの間の通信のためのRESTサーバURLを入力します。
   - 認証リクエストをクラウド認証サービスに安全に渡すためのクライアント キー(認証APIキー)を入力します。
   - 認証エージェント上に保存された信頼する証明書のディレクトリとファイル名を入力します。
   - クラウド認証サービスのテナントIDを入力します。
   - クラウド認証サービスのアクセス ポリシー名を入力します。

- モバイル通知に表示するCLIENT_ID認証エージェント名を入力します。
- PAM agentのインストール ディレクトリを入力します。

5. UDPモードの場合のみ、**/etc/sd_pam.conf**ファイルのVAR_ACEに**sdconf.rec**ファイルの場所が正しく指定されていることを確認します。これは構成ファイルのパスです。パス全体が、-rw------- root権限でなければなりません。

終了後のステップ

- インストールを確認するには、PAM agentのインストール ディレクトリにある**installer.log**ファイルをチェックします。
- UDPモードの場合は、テスト認証を実行します。詳細については、「UDPモードの認証ユーティリティ (41ページ)」を参照してください。
- RESTプロトコル モードの場合は、ブラウザまたはhttpクライアントでRESTサーバのURLにアクセスして、接続をテストします。たとえば、「https://*HOSTNAME*:*PORT_NO*/mfa/v1_1/authn」と入力します。現時点では認証されていないため、ブラウザまたはhttpクライアントには、「Forbidden」または「Unauthorized」というHTTP応答が表示されます。

サイレント インストールによるPAM agentの一括インストール

同じ構成情報を使用して多数のPAM agentを導入します。たとえば、このタスクは、多数のエージェントをインストールする必要があり、そのエージェントが同じRSA Authentication Managerサーバや同じクラウド認証サービスと通信する場合に実行します。

開始する前に

PAM agentを手動でインストールして、表示されるプロンプトを記録します。手順については、「1台のマシンへのPAM agentのインストール (18ページ)」を参照してください。

手順

1. テキスト ベースの構成ファイルを作成し、PAM agentのインストール スクリプトの構成オプションを指定します。**installoptions.conf**など、構成ファイルには任意の名前を指定できます。
2. ファイルを開いて、選択する構成オプションを、PAM agentの手動インストール中に表示されるプロンプトと同じ順序で1行ごとに指定します。

   次の例は、UDPモードで指定する各オプションと、それに対応するプロンプトについて説明しています。

値の例	オプション
y	サイレント インストールを続行しますか? (y)このプロンプトは常に最初に指定します。
Accept	使用許諾契約の条項に同意しますか? (Accept)
0	認証モードは? (目的のモードに対応する数値) 0:RSA Authentication ManagerとUDPプロトコル 1:RSA Authentication ManagerとRESTプロトコル 2:クラウド認証サービスとRESTプロトコル
/var/ace	sdconf.recを保存したディレクトリは? (ディレクトリ パス)
/opt	PAM agentディレクトリのインストール パスは? (ディレクトリ パス)
y	既存のインストールをアップグレード/上書きしますか? (y/n)

   この場合、テキスト ベースの構成ファイルの内容は、次のようになります。

```
y
```

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

また、Authentication Manager RESTモードの場合、構成ファイルには、次のようなデータが含まれます。

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

注:インストール プロンプトの数と順序は、インストールするPAM agentのモードとプラットフォームによって異なります。

3. PAM agentインストール ディレクトリに移動します。
4. 次のように入力して、ファイルを解凍(untar)します。

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

5. 次のように入力して、インストール スクリプトを実行します。

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

   installoptions.confは、ステップ1で作成した構成ファイルです。構成ファイルがカレント ディレクトリと異なる場所にある場合は、***installoptions.conf***ファイルへのフル パスパスを指定します。

RSA Authentication Agent 8.1 for PAMへのアップグレード

RSA Authentication Agent 8.1 for PAMにはバージョン7.1 Patch2(7.1.0.2)またはバージョン8.0からアップグレードできます。

7.1.0.2からアップグレードした場合、アップグレードしたエージェントが認証に使用するのは、RSA Authentication ManagerとUDPプロトコルです。認証モードは、クラウド認証サービスまたはAuthentication ManagerのRESTプロトコルを使用するように変更できます。手順については、「PAM agentの認証モードの変更 (33ページ)」を参照してください。

8.0からアップグレードした場合、アップグレードしたエージェントは、前のバージョンと同じ認証モードを使用します。

開始する前に

- エージェント ホストでのroot権限と、**sdconf.rec**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。このファイルは、通常、デフォルトの**/var/ace**ディレクトリに保存されます。
- 上書きされる前に構成ファイルをバックアップして、構成を保存します。詳細については、「重要な構成ファイル (50ページ)」を参照してください。
- RSA SecurIDで保護されたツールの構成を変更し、RSA PAMモジュールではなく、オペレーティング システムに付属の標準PAMモジュールを使用するようにします。アップグレードを行う前に、RSA PAMモジュールを使用するアクティブなセッションを閉じる必要があります。

手順

1. エージェント マシンで、PAM agentのインストール ディレクトリに移動します。
2. 次のように入力して、ファイルを解凍(untar)します。

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

3. 次のように入力して、インストール スクリプトを実行します。

   ```
   /<filename>/install_pam.sh
   ```

4. 既存のインストール ファイルを上書きします。インストーラが現在のインストールを上書きするか確認するプロンプトを表示したら、「**y**」と入力します。
5. エージェントのバージョン番号を取得して、アップグレードが成功したかどうかを確認します。次のように入力します。

   strings pam_securid.so | grep "Agent"

   インストールされたエージェントのバージョン番号が表示されます。

ツールの構成

クラウド認証サービスおよびRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するためには、サポート対象のツールを構成する必要があります。

Solaris 10では、**/etc/pam.conf**ファイルを構成します。Solaris 11では、**/etc/pam.d/others**ファイルまたは**/etc/pam.conf**ファイルを構成できます。どちらのファイルを構成するかについては、Solaris 11または各ツールのマニュアルを参照してください。

注:UNIXサーバでの同時使用ユーザー数の設定は、特にクラウド認証サービスを使用しているときは、各ツール、使用中のオペレーティング システム、サーバへの予想される同時ログオンに対して設定する必要があります。

telnetの構成 (21ページ)

loginの構成 (22ページ)

rloginの構成 (22ページ)

suの構成 (23ページ)

sshと関連ツールの構成 (23ページ)

sudoの構成 (24ページ)

ftpの構成 (24ページ)

dtloginの構成 (25ページ)

telnetの構成

クラウド認証サービスおよびRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにtelnetを構成します。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

```
telnet auth requisite pam_authtok_get.so.1
telnet auth required pam_dhkeys.so.1
telnet auth required pam_unix_cred.so.1
telnet auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
telnet auth required pam_securid.so
```

loginの構成

クラウド認証サービスとRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにloginコマンドを構成します。

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

```
login auth requisite pam_authtok_get.so.1
login auth required pam_dhkeys.so.1
login auth required pam_unix_cred.so.1
login auth required pam_unix_auth.so.1
login auth required pam_dial_auth.so.1
```

4. 次の行を追加します。

```
login auth required pam_securid.so
```

rloginの構成

クラウド認証サービスとRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにrloginユーティリティを構成します。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

```
rlogin auth sufficient pam_rhosts_auth.so.1
rlogin auth requisite pam_authtok_get.so.1
```

```
rlogin auth required pam_dhkeys.so.1
rlogin auth required pam_unix_cred.so.1
rlogin auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
rlogin auth required pam_securid.so
```

suの構成

クラウド認証サービスおよびRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにsuコマンドを構成します。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメントアウトします。

```
su auth requisite pam_authtok_get.so.1
su auth required pam_dhkeys.so.1
su auth required pam_unix_cred.so.1
su auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
su auth required pam_securid.so
```

sshと関連ツールの構成

クラウド認証サービスとRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するように、SSHとその関連ツール(scpやsftpなど)を構成できます。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメントアウトします。

```
sshd-kbdint auth requisite pam_authtok_get.so.1
sshd-kbdint auth required pam_dhkeys.so.1
sshd-kbdint auth required pam_unix_cred.so.1
sshd-kbdint auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
sshd-kbdint auth required pam_securid.so
```

sudoの構成

sudoが必要な場合は、クラウド認証サービスおよびRSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにsudoコマンドを構成します。

開始する前に

サポートされているsudoバージョンを、https://www.sudo.wsからダウンロードしてインストールします。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authenticationセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

```
sudo auth requisite pam_authtok_get.so.1
sudo auth required pam_dhkeys.so.1
sudo auth required pam_unix_cred.so.1
sudo auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
sudo auth required pam_securid.so
```

ftpの構成

RSA Authentication Managerでサポートされている認証方法のプロンプトをユーザーに表示するようにftpプロトコルを構成します。

ftpの保護にクラウド認証サービスを使用することはできませんが、sftpは使用できます。手順については、「sshと関連ツールの構成 (23ページ)」を参照してください。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

```
ftp auth requisite pam_authtok_get.so.1
ftp auth required pam_dhkeys.so.1
ftp auth required pam_unix_cred.so.1
ftp auth required pam_unix_auth.so.1
```

4. 次の行を追加します。

```
ftp auth required pam_securid.so
```

dtloginの構成

クラウド認証サービスとRSA Authentication Managerによってサポートされている認証方式のプロンプトをユーザーに表示するように、dtloginを構成することができます。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. Authentication Managementセクションまでスクロールします。
3. 次の行がある場合はコメント アウトします。

   ```
   dtlogin auth requisite pam_authtok_get.so.1
   dtlogin auth required pam_dhkeys.so.1
   dtlogin auth required pam_unix_cred.so.1
   dtlogin auth required pam_unix_auth.so.1
   ```

4. 次の行を追加します。

   ```
   dtlogin auth required pam_securid.so
   ```

第2章:機能の構成

エージェントとUNIXの機能の構成

エージェントとUNIXのオプション機能を使用するよう、PAM agent構成をカスタマイズできます。

注:エージェントをカスタマイズする前に、元の構成ファイルのバックアップコピーを作成しておいてください。

Solaris 10では、**pam.conf**という名前の単一の構成ファイルが**/etc**ディレクトリに含まれています。

Solaris 11では、**/etc/pam.d/others**ファイルまたは**/etc/pam.conf**ファイルを構成できます。どちらのファイルを構成するかについては、Solaris 11または各ツールのマニュアルを参照してください。

エージェントをカスタマイズするには、以下を参照してください。

RSA Authentication Agent 8.1 for PAMのエージェント レポート機能の有効化 (28ページ)

デバッグ出力の有効化 (28ページ)

UDPモードでのSecurIDトレース ログの有効化 (29ページ)

スタッカブル モジュールの構成 (29ページ)

予備パスワードの使用 (30ページ)

選択的SecurID認証の有効化 (31ページ)

指数バックオフ時間の構成 (32ページ)

RSA Authentication Agent 8.1 for PAMのエージェント レポート機能の有効化

mfa_api.propertiesファイルのENABLE_AGENT_REPORTINGパラメータの構成により、ホスト名、エージェントのバージョン、OSのバージョンなどのエージェントの詳細情報をRSA Authentication Managerに送信できるようになります。RSA Authentication Manager 8.3以降を使用すると、このような詳細情報のレポートを実行できます。

開始する前に

エージェントがインストールされているマシンのroot権限と、**mfa_api.properties**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/var/ace/conf**に保存されます。

手順

1. **mfa_api.properties**を保存するディレクトリに移動します。デフォルトで、このディレクトリは**/var/ace/conf**です。
2. **mfa_api.properties**を開きます。
3. ENABLE_AGENT_REPORTINGパラメータを1に変更します。これにより、エージェント レポート機能が有効になります。デフォルト値は0です。
4. ファイルを保存します。

   PAM agentとインストールされているマシンの詳細情報が、Authentication Managerに送信されるPAM agentのレポートに含まれるようになります。

デバッグ出力の有効化

トラブルシューティングのため、PAM agentが使用する特定のツールに対してデバッグ出力を有効にできます。

また、すべてのPAM agent認証ログ メッセージをシステム ログに記録するよう構成することもできます。詳細については、「PAM agentのログ (44ページ)」を参照してください。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. debug引数をpam_securid.soモジュールに追加します。次のように入力します。

   ```
   tool name auth required pam_securid.so debug
   ```

   *tool name*は、デバッグ出力を有効にするツールの名前です。

UDPモードでのSecurIDトレース ログの有効化

PAM agentや、認証ユーティリティacetestおよびacestatusに対して、詳細なSecurIDトレース ログを有効にできます。デフォルトでは、PAM agentをインストールしたとき、SecurIDトレース ログは無効になっています。

手順

1. **/etc**ディレクトリに移動し、**sd_pam.conf**ファイルを開きます。
2. 詳細なエージェント ログを有効にして、ログのレベルを設定するには、次の変数を設定します。

   RSATRACELEVEL=*value*

   *value*には次の表の値を設定します。

値	説明
0	ログを無効にします(デフォルト)
1	通常のメッセージをログに記録します
2	関数のエントリー ポイントをログに記録します
4	関数の終了ポイントをログに記録します
8	すべてのロジックのフロー制御がこれ(ifs)を使用します

   組み合わせる場合は、対応する値を加算します。たとえば、通常のメッセージと関数のエントリー ポイントをログに記録するには、3を設定します。

3. ログのリダイレクト先のファイル パスを指定します。次の変数を設定します。

   RSATRACEDEST=*filepath*

   *filepath*はファイル パスです。

   デフォルトでは、この変数は空白です。この変数を設定しないと、RSATRACELEVEL値が指定されていても、認証ツールに関するログは生成されません。認証ユーティリティacetestおよびacestatusの場合は標準エラーにログが出力されます。

4. 変更を保存します。

スタッカブル モジュールの構成

スタック構成では、RSA SecurID PAM認証モジュールと他のPAM認証モジュールを統合することができます。パスワードまたはパスコードは、1つの認証モジュールから次の認証モジュールに渡されます。**etc/pam.d/others**ファイルまたは**/etc/pam.conf**ファイルを編集し、認証の優先度を構成することができます。

注:スタック構成がクラウド認証サービスで使用されているとき、引数use_first_passおよび try_first_passはサポートされません。

エージェントは次の引数と連携します。

- **use_first_pass。**エージェントは、前のモジュールから渡されたパスワードまたはパスコードのみを使用し、認証情報が一致しない場合はアクセスを拒否します。ユーザーが再度認証を求められることはありません。
- **try_first_pass。**エージェントは、前のモジュールから渡されたパスワードまたはパスコードを使用します。認証情報が一致しない場合、ユーザーは認証を求められます。
- **not_set_pass。**エージェントは、スタックされたパスワード モジュールにパスワードまたはパスコードを送信しません。

注:SecurID認証の対象外のユーザーが、RSA PAMモジュールでログイン試行に失敗すると、ログインが成功するか認証セッションが終了するまで、指数バックオフ機能によってRSA PAMモジュールが確実に制御を維持します。指数バックオフ時間の構成の詳細については、「指数バックオフ時間の構成 (32ページ)」を参照してください。

次のセクションでは、スタック環境で接続ツール(ログイン ツール)を構成する方法の例について説明します。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

   次のテキストが表示されます。

   ```
   # Authentication management
   # login service (explicit because of pam_dial_auth)
   login auth requisite pam_authtok_get.so
   login auth required pam_dhkeys.so.1
   login auth required pam_unix_cred.so.1
   login auth required pam_unix_auth.so.1
   login auth required pam_dial_auth.so.1
   ```

2. 前掲の行をコメント アウトします。
3. 次の行を追加します。

   ```
   login auth required pam_securid.so
   ```

予備パスワードの使用

予備パスワード機能は、管理者がエマージェンシー アクセスの手段として使用でき、エージェントによって保護されたマシンに、RSA SecurIDパスコードを入力することなくアクセスすることができます。PAM agentでは、root管理者のみが、エージェントとRSA Authentication Agent 8.1 for PAMの間の通信喪失など、不測の事態が発生したときに予備パスワードを使用できます。こうした状況で、ユーザーが即座にマシン上のリソースにアクセスする必要がある場合、管理者はエージェントを一時的に無効にできます。

注:UNIXパスワードは予備パスワードです。

手順

1. Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

   Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

2. reserve引数をpam_securid.soモジュールに追加します。次のように入力します。

   ```
   tool name auth required pam_securid.so reserve
   ```

   *tool name*は、予備パスワードを構成する必要があるツールの名前です。

選択的SecurID認証の有効化

特定のUNIXユーザーまたはグループを選択し、常にSecurID認証を求めるか、またはSecurID認証を求めないようにエージェントを構成できます。

UNIXグループに対する選択的SecurID認証の有効化 (31ページ)

UNIXユーザーに対する選択的SecurID認証の有効化 (32ページ)

注:選択的グループ サポートと選択的ユーザー サポートの両方が有効になっている場合は、選択的ユーザー サポートのみが有効になり、選択的グループ サポートは無視されます。

次の表は、**sd_pam.conf**ファイルで設定できる値の組み合わせを示しています。

ENABLE_ GROUPS_ SUPPORT	ENABLE_ USERS_ SUPPORT	結果
0	0	どちらの機能も有効になっていません。すべてのユーザーとユーザー グループがSecurID認証を求められます。
0	1	選択的ユーザー サポートが有効です。 PAM agentは、特定のUNIXユーザーに対して常にSecurIDによる認証を求めるか、特定のユーザーに対してSecurIDによる認証を求めません。
1	0	選択的グループ サポートが有効です PAM agentは、特定のUNIXグループに対して常にSecurIDによる認証を求めるか、特定のグループに対してSecurIDによる認証を求めません。
1	1	選択的ユーザー サポートが有効です。 PAM agentは、特定のUNIXユーザーに対して常にSecurIDによる認証を求めるか、特定のユーザーに対してSecurIDによる認証を求めません。

UNIXグループに対する選択的SecurID認証の有効化

特定のUNIXグループに対して常にRSA SecurIDによる認証を求めるか、RSA SecurID認証を求めないようにPAM agentを構成できます。PAM agentのインストール時には、この機能は有効化されていません。

SecurID認証から除外されたグループ メンバーは、UNIX認証情報を使用するか、スタック内の別のPAMモジュールを通じて認証できます。これを行うには、PAM_IGNORE_SUPPORTパラメータを構成します。

注:RSA Authentication Managerグループは指定しないでください。この機能は、UNIXグループのみを対象にしています。

手順

1. **/etc**ディレクトリに移動し、**sd_pam.conf**ファイルを開きます。
2. ENABLE_GROUP_SUPPORTパラメータを1に設定します。デフォルト値は0です。
3. LIST_OF_GROUPSパラメータに値を入力します。
4. INCL_EXCL_GROUPSパラメータの値を設定します。
   有効な値:
   0:リストに指定したグループに対してSecurID認証を無効にします(デフォルト)。
   1:リストに指定したグループに対してのみSecurID認証を有効にします。
5. (オプション)PAM_IGNORE_SUPPORTパラメータを設定します。
   有効な値:
   0:UNIXパスワード認証を有効にします(デフォルト)。

1:UNIXパスワード認証を無効にします。
このパラメータは、SecurID認証から除外されたグループにのみ適用されます。

6. ファイルを保存します。

UNIXユーザーに対する選択的SecurID認証の有効化

特定のUNIXユーザーに対して常にSecurIDによる認証を求めるか、SecurIDによる認証を求めないようにPAM agentを構成できます。PAM agentのインストール時には、この機能は有効化されていません。

SecurID認証から除外されたユーザーは、UNIX認証情報を使用するか、スタック内の別のPAMモジュールを通じて認証できます。これを行うには、PAM_IGNORE_SUPPORT_FOR_USERSパラメータを構成します。

手順

1. **/etc**ディレクトリに移動し、**sd_pam.conf**ファイルを開きます。
2. ENABLE_USERS_SUPPORTパラメータを1に設定します。デフォルト値は0です。
3. LIST_OF_USERSパラメータに値を入力します。
4. INCL_EXCL_USERSパラメータの値を設定します。
   有効な値:
   0:リストに指定したユーザーに対してSecurID認証を無効にします(デフォルト)。
   1:リストに指定したユーザーに対してのみSecurID認証を有効にします。
5. (オプション)PAM_IGNORE_SUPPORT_FOR_USERSパラメータを設定します。
   有効な値:
   0:UNIXパスワード認証を有効にします(デフォルト)。
   1:UNIXパスワード認証を無効にします。
   このパラメータは、SecurID認証から除外されたユーザーにのみ適用されます。
6. ファイルを保存します。

指数バックオフ時間の構成

RSA SecurID認証から除外されているユーザーによるログイン試行が連続して失敗した後、このユーザーが認証を受ける前に待つ必要のある時間の長さを構成できます。デフォルトで、ユーザーはログイン試行に失敗した後で「pow(4, 失敗回数)」秒分の遅延をはさんで、UNIX認証を再試行できます。たとえば、ログイン試行が3回失敗した場合は、64秒(4の3乗、つまり4 X 4 X 4 = 64)の遅延が生じます。

注: ftpプロトコルは指数バックオフ遅延をサポートしていません。

手順

1. **/etc**ディレクトリに移動し、**sd_pam.conf**ファイルを開きます。
2. BACKOFF_TIME_FOR_RSA_EXCLUDED_UNIX_USERSパラメータに、次の表のように*N*を設定します。

N	**認証動作**
0	ログイン試行が失敗した後のUNIX認証の再試行を無効化します。ログイン試行が失敗した後のログイン試行では、認証の遅延が生じません。
1、2、3	ログイン試行に失敗した後、「pow(3, 失敗回数)」秒分の遅延をはさんでUNIX認証の再試行を有効化します。
4	ログイン試行に失敗した後、「pow(4, 失敗回数)」秒分の遅延をはさんでUNIX認証の再試行を有効化します。
5またはそ	ログイン試行に失敗した後、「pow(5またはそれ以上, 失敗

N	認証動作
れ以上	回数)」秒分の遅延をはさんでUNIX認証の再試行を有効化します。

信頼するルートCA証明書の置換

たとえば、RSA Authentication Managerまたはクラウド認証サービスの現在の証明書が更新された場合などに、信頼するルートCA証明書を置換する必要が生じることがあります。

この証明書を取得する手順については、ナレッジベースの記事「How to export RSA SecurID Access Authentication Manager or Cloud Authentication Service Root Certificate」を参照してください。

開始する前に

- PAM agentがインストールされているマシン上の**/var/ace**ディレクトリに対するroot権限が必要です。
- 新しい証明書がPEM形式であることを確認します。複数のCA証明書がある場合は、これらの証明書をPEM形式の単一ファイルに連結する必要があります。

  ファイル形式は次のようになります。

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

  Thawte (BASE64)

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

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

  Entrust (BASE64)

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

手順

1. 新しいルート証明書の名前を変更して、置換する証明書と同じ名前にします。
2. PAM agentがインストールされているマシンで、***new_cert_file*.pem**を**/var/ace/**ディレクトリにコピーして置換します。

PAM agentの認証モードの変更

PAM agentの認証モードは変更できます。たとえば、クラウド認証サービスに用意されている拡張認証オプションを使用する場合にモードを変更します。アップグレードされたPAM agentでは、デフォルトでRSA Authentication ManagerとUDPプロトコルが使用されます。

UDPプロトコルからRESTプロトコルへの変更

UDPプロトコルの認証モードは、Authentication Managerまたはクラウド認証サービスの RESTプロトコルの認証モードに変更できます。

開始する前に

- エージェントがインストールされているマシンに対するroot権限が必要です。
- **sdconf.rec**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/etc**に保存されます。

- **mfa_api.properties**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/var/ace/conf**に保存されます。
- 必要な情報を収集します。

  RESTプロトコルを使用したAuthentication Manager認証の場合は、Authentication Managerのスーパー管理者から次の情報を入手します。

パラメータ	説明
REST_URL	認証エージェントとAuthentication Managerプライマリインスタンスの間の通信のためのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` プライマリインスタンスのOperations Consoleで、**[管理]>[ネットワーク]>[アプライアンスのネットワーク設定]**ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。
REPLICA_*number* *number*は1～15です。	フェールオーバーに使用できる各レプリカインスタンスのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` レプリカインスタンスのOperations Consoleで、**[管理]>[ネットワーク]>[アプライアンスのネットワーク設定]**ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。
CLIENT_KEY	認証リクエストをAuthentication Managerに安全に渡すためのアクセスキー(クライアントキー)。この値は、Authentication Managerプライマリインスタンスの Security Consoleで生成されます。 アクセスキーの取得方法については、RSA Linkのトピック「認証エージェント用のRSA SecurID認証APIの構成」を参照してください。
CA_CERT_FILE_PATH	認証エージェント上に保存された信頼する証明書のディレクトリとファイル名。デフォルト値は**/var/ace/cert.pem**です。
CLIENT_ID	PAM agent用にAuthentication Managerで作成された認証エージェント名(クライアントID)。

クラウド認証サービスを使用した認証の場合は、クラウド認証サービスのスーパー管理者から次の情報を入手します。

パラメータ	説明
REST_URL	エージェントとクラウド認証サービスの間の通信のためのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT/mfa/v1_1/authn` クラウド認証サービスの場合、クラウド管理コンソールの任意のIdentity Routerの設定ページの[**Registration**]タブにある[**Authentication Service Domain**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は443です。
CLIENT_KEY	ユーザー認証リクエストをクラウド認証サービスに安全に渡すためにクラウド管理コンソールで作成される認証APIキー(クライアントキー)。 認証APIキーの取得方法については、RSA Linkのトピック「Add an RSA SecurID Authentication API Key」を参照してください。
CA_CERT_FILE_PATH	認証エージェント上に保存された信頼する証明書のディレクトリとファイル名。デフォルト値は**/var/ace/cert.pem**です。
TENANT_ID	クラウド認証サービスのテナントID。PAM agentは認証リクエストにテナントIDを指定することができますが、エージェントはこのデータを検証しません。このパラメータは、現時点ではクラウド認証サービスによってサポートされていません。

パラメータ	説明
ASSURANCE_POLICY_ID	クラウド認証サービスのアクセスポリシー名。
CLIENT_ID	モバイル通知に表示する認証エージェント名。任意の値を入力できます。たとえば、「PAM_Agent」と入力します。

手順

1. **sd_pam.conf**が置かれているディレクトリに移動します。デフォルトの場所は**/etc**です。
2. **sd_pam.conf**を開きます。
3. OPERATION_MODEパラメータを次のように変更します。
   - Authentication ManagerとRESTプロトコルの場合は「1」を入力します。
   - クラウド認証サービスとRESTプロトコルの場合は「2」を入力します。

   OPERATION_MODEパラメータが「0」であるか、指定されていないか、コメント アウトされている場合、PAM agentのデフォルトはUDPモードです。
4. **/var/ace/conf**ディレクトリに移動します。**mfa_api.properties**ファイルを更新する必要があります。
5. **mfa_api.properties**を開きます。
6. コメントを削除して、必要なパラメータを有効にします。
7. 必要な各パラメータの値を入力します。
8. ファイルを保存します。

   RESTプロトコルを使用できるようになりました。

RESTプロトコルからUDPプロトコルへの変更

RESTプロトコルを使用するようPAM agentをインストールした後で、Authentication ManagerのUDPプロトコルを使用するよう認証モードを変更することができます。

UDPプロトコルを使用するよう認証モードを変更すると、**mfa_api.properties**ファイル内のRESTプロトコル設定は適用されなくなります。

開始する前に

- Authentication Managerの構成ファイルである**sdconf.rec**が必要です。このファイルはAuthentication Managerで生成するか、Authentication Managerのスーパー管理者から取得します。詳細については、「PAM agentのインストールの計画 (13ページ)」を参照してください。
- エージェントがインストールされているマシンのroot権限と、**sd_pam.conf**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/etc**ディレクトリに保存されます。

手順

1. **sd_pam.conf**が置かれているディレクトリに移動します。デフォルトの場所は**/etc**です。
2. **sd_pam.conf**を開きます。
3. OPERATION_MODEパラメータを、UDPプロトコルを表す「0」に変更します。

   ```
   OPERATION_MODE=0
   ```

   OPERATION_MODEパラメータが「0」であるか、指定されていないか、コメント アウトされている場合、PAM agentのデフォルトはUDPモードです。

4. **sdconf.rec**を**/var/ace**ディレクトリにコピーします。

   UDPプロトコルを使用できるようになりました。

RSA Authentication Managerとクラウド認証サービスの変更

PAM agentがRESTプロトコルで、Authentication Managerを使用するか、またはクラウド認証サービスを使用するかを変更できます。

開始する前に

- エージェントがインストールされているマシンに対するroot権限が必要です。
- **sdconf.rec**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/var/ace**に保存されます。
- **mfa_api.properties**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/var/ace/conf**に保存されます。
- 信頼する証明書のパスを指定するCA_CERT_FILE_PATHパラメータはそのままで構いません。その他のパラメータについては、必要な情報を収集します。

  RESTプロトコルを使用したAuthentication Manager認証の場合は、Authentication Managerのスーパー管理者から次の情報を入手します。

パラメータ	説明
REST_URL	認証エージェントとAuthentication Managerプライマリインスタンスの間の通信のためのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` プライマリインスタンスのOperations Consoleで、**[管理]>[ネットワーク]>[アプライアンスのネットワーク設定]**ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。
REPLICA_*number* *number*は1～15です。	フェールオーバーに使用できる各レプリカインスタンスのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT_NO/mfa/v1_1/authn` レプリカインスタンスのOperations Consoleで、**[管理]>[ネットワーク]>[アプライアンスのネットワーク設定]**ページを表示し、[**完全修飾ドメイン名**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は5555です。
CLIENT_KEY	認証リクエストをAuthentication Managerに安全に渡すためのアクセスキー(クライアントキー)。この値は、Authentication Managerプライマリインスタンスの Security Consoleで生成されます。 アクセスキーの取得方法については、RSA Linkのトピック「認証エージェント用のRSA SecurID認証APIの構成」を参照してください。
CLIENT_ID	PAM agent用にAuthentication Managerで作成された認証エージェント名(クライアントID)。

クラウド認証サービスを使用した認証の場合は、クラウド認証サービスのスーパー管理者から次の情報を入手します。

パラメータ	説明
REST_URL	エージェントとクラウド認証サービスの間の通信のためのRESTサーバURL。次の形式で指定します。 `https://HOSTNAME:PORT/mfa/v1_1/authn`

パラメータ	説明
	クラウド認証サービスの場合、クラウド管理コンソールの任意のIdentity Routeの設定ページの[**Registration**]タブにある[**Authentication Service Domain**]フィールドから*HOSTNAME*の値を取得します。デフォルトの*PORT*の値は443です。
CLIENT_KEY	ユーザー認証リクエストをクラウド認証サービスに安全に渡すためにクラウド管理コンソールで作成される認証APIキー(クライアント キー)。 認証APIキーの取得方法については、RSA Linkのトピック「Add an RSA SecurID Authentication API Key」を参照してください。
TENANT_ID	クラウド認証サービスのテナントID。PAM agentは認証リクエストにテナントIDを指定することができますが、エージェントはこのデータを検証しません。このパラメータは、現時点ではクラウド認証サービスによってサポートされていません。
ASSURANCE_POLICY_ID	クラウド認証サービスのアクセス ポリシー名。
CLIENT_ID	モバイル通知に表示する認証エージェント名。任意の値を入力できます。たとえば、「PAM_Agent」と入力します。

手順

1. **sd_pam.conf**が置かれているディレクトリに移動します。デフォルトの場所は**/etc**です。
2. **sd_pam.conf**を開きます。
3. OPERATION_MODEパラメータを次のように変更します。
   - Authentication ManagerとRESTプロトコルの場合は「1」を入力します。
   - クラウド認証サービスとRESTプロトコルの場合は「2」を入力します。

   OPERATION_MODEパラメータが「0」であるか、指定されていないか、コメント アウトされている場合、PAM agentのデフォルトはUDPモードです。
4. **/var/ace/conf**ディレクトリに移動します。**mfa_api.properties**ファイル内の必要なパラメータ値を更新する必要があります。
5. **mfa_api.properties**を開きます。
6. 必要なパラメータのコメントを外して有効にし、必要でなくなったパラメータをコメント アウトします。
7. 必要な各パラメータの値を入力します。
8. ファイルを保存します。

   RESTプロトコルを新しい認証モードで使用できるようになりました。

付録A:トラブルシューティング

構成に関する既知の問題

このセクションでは、既知の問題を説明します。

サポートされているツールの問題

ツール	既知の問題
dtlogin	**問題**:ディスプレイの制限により、次の2つの問題が発生することがあります。 • 認証を受けるユーザーの画面に、使用可能な認証方法に関するメッセージの一部が表示されないことがあります。 • 予備パスワードのユーザーの画面に、不要なテキスト入力フィールドの一部が表示されることがあります。 **解決方法**:認証を受けるユーザーは、画面の指示どおりにENTERキーを押すことで、メッセージ全体を表示できます。予備パスワードのユーザーは、不要なフィールドを無視してかまいません。
ftp	• **問題**:SecurIDを使用してFTPを保護するときに、SecurIDの認証プロンプトとエラー メッセージがユーザーに表示されません。OS(オペレーティング システム)の標準のプロンプトとエラー メッセージのみ表示されます。 **解決方法**: OSのユーザー名プロンプトでユーザー名を入力し、OSのパスワード プロンプトでSecurIDパスコードを入力するようユーザーに指示します。 ユーザーはトークンのステータスがわからない場合(たとえば、トークンがネクスト トークンコード モードまたはNew PINモードの場合)、rloginなどの別の接続ツールを認証に使用して、PINまたはトークンコードがまだ有効であることを確認する必要があります。 • FTPは指数バックオフ遅延をサポートしていません。 • クラウド認証サービスを使用してFTPを保護することはできませんが、sftpはサポートされています。
ssh	**問題**:ユーザーによるSecurID認証試行が1回のセッションで3回失敗すると、接続が閉じられます。 **解決方法**: ユーザーはセッションを終了し、別のセッションを開始できます。
dtlogin	**問題**:Solaris 10とSolaris SPARC 10のロック画面には、パスコードが必要な場合に、パスワードの入力をユーザーに求めるプロンプトが表示されます。 **解決方法**:認証を受けるユーザーは、RSA SecurIDのパスコードを入力する必要があります。
rlogin、telnet	**問題**:NFS環境では、ユーザーのホーム ディレクトリにある**.rhosts**ファイルにより、ネットワーク内の他のマシンおよびリソースへのリモート アクセスを構成できます。このような環境では、ユーザーが自分のワークステーションにローカルでアクセスする時に、SecurIDによる認証を求められます。しかし、ユーザーがローカル アクセスを取得した後で他のリソースへのネットワーク アクセスのためにtelnetまたはrloginを使用する場合、SecurIDの認証は要求されません。 **解決方法**: このような環境では、必要に応じてユーザーを制限することを推奨します。
rlogin、telnet	**問題**:Solaris 11では、rloginとtelnetのセッションで接続が正しく閉じられません。いずれのツールも、ログアウト後、前のセッションのプロンプトを返しません。この問題は、他のバージョンのSolarisでは発生しません。 **解決方法**: アクティブなセッションを閉じるか、別のセッションを使用して応答のないセッションを終了します。

アップグレードとアンインストールの問題

問題: RSA PAMモジュールを無効にしないでPAM agentをアップグレードまたはアンインストールしようとすると、「pam_securid.soはビジー状態のため、削除/置換できません」というエラー メッセージが表示されることがあります。
解決方法:この問題を解決するには、ssh以外のツールを使用してログオンし、**pam_securid.so**を削除する必要があります。

UDPモードの認証ユーティリティ

認証ユーティリティは次のディレクトリにあります。

- 32ビット オペレーティング システム: ***PAM agentのインストール ディレクトリ*/bin/32bit**
- 64ビット オペレーティング システム: ***PAM agentのインストール ディレクトリ*/bin/64bit**

これらのユーティリティを使用して、以下を行うことができます。

- テスト認証を実行する。詳細については、「acetestユーティリティの実行 (41ページ)」を参照してください。
- PAM agentとRSA Authentication Manager間の通信を検証する。詳細については、「acestatusユーティリティの実行 (41ページ)」を参照してください。

これらのユーティリティのログを有効にすることができます。詳細については、「UDPモードでのSecurIDトレース ログの有効化 (29ページ)」を参照してください。

acetestユーティリティの実行

このユーティリティは、テスト認証を実行することによって、エージェントが正しく機能していることを確認します。

手順

1. PAM agent認証ユーティリティのディレクトリに移動します。
   - 32ビット オペレーティング システム: ***PAM agentのインストール ディレクトリ*/bin/32bit**
   - 64ビット オペレーティング システム: ***PAM agentのインストール ディレクトリ*/bin/64bit**
2. 次のように入力します。

   ```
   ./acetest
   ```

3. 有効なユーザー名とパスコードを入力します。

アクセスを繰り返し拒否される場合は、acestatusユーティリティを使用してAuthentication Managerサーバとの接続をテストするか、Authentication Manager管理者に問い合わせてください。acestatusユーティリティの実行 (41ページ)

acestatusユーティリティの実行

このユーティリティは、PAM agentがエージェント ホストとして登録されている各Authentication Managerのステータスをチェックします。表示される情報に関する質問がある場合は、Authentication Manager管理者に問い合わせてください。

手順

1. PAM agentユーティリティのディレクトリに移動します。
2. 次のように入力します。

   ```
   ./acestatus
   ```

次の表に、Authentication Managerセクションに表示される情報を示します。

表示される情報	説明
Configuration Version	使用中の**sdconf.rec**ファイルのバージョン。RSA Authentication Manager 8.0以降の場合、この番号は14です。
DES Enabled	導入環境でレガシー プロトコルがサポートされる場合は、YESと表示されます。
Client Retries	タイムアウトが発生する前にPAM agentによって認証データがAuthentication Managerに送信され

表示される情報	説明
	る回数。
Client Timeout	PAM agentが認証データをAuthentication Managerに再送信する前に待機する時間(秒単位)。
Server Release	Authentication Managerのバージョン番号。
Communication	Authentication ManagerとPAM agentによって使用されるプロトコルのバージョン。

次の表に、Authentication Managerセクションに表示されるステータス情報を示します。

ステータス情報	説明
Server Active Address	PAM agentがサーバとの通信に使用するIPアドレス。このアドレスは、選択したサーバの実際のIPアドレスである場合と、サーバに割り当てられているエイリアスIPアドレスの場合があります。0.0.0.0というIPアドレスは、エージェントがサーバからの通信をまだ受信していないことを意味します。

次の表に、Authentication Managerセクションに表示されるサーバ ステータス情報を示します。

サーバ ステータス	説明
Available for Authentications	このサーバは認証リクエストの処理に使用できます。
Unused	このサーバは認証リクエストをまだ受信していません。
For Failover only	このサーバはフェールオーバー専用に予約されています。
Default Server During initial requests	現時点でリクエストの処理に使用できるのは、このサーバだけです。

UDPモードの変換ユーティリティ

変換ユーティリティは、UDPベースのPAM agentが、他のSecurIDエージェントと共存するときに使用されます。

変換ユーティリティ ns_conv_utilは、次のディレクトリにあります。

- 32ビット オペレーティング システム: ***pam agent home*/bin/32bit**
- 64ビット オペレーティング システム: ***pam agent home*/bin/64bit**

手順

1. PAM agentユーティリティのディレクトリに移動します。
2. 次のように入力します。

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

   *<Existing_Securid_file_path>*は、現在のSecurIDファイルが存在するパスです。

   *<New_Securid_dir_path>*は、新しく生成されたSecurIDファイルを保存するディレクトリです。

   コマンドの例:

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

3. 新しい場所が、VAR_ACEに指定された場所と異なる場合は、新しいSecurIDファイルをこの場所にコピーします。

UDPモードのノード シークレット

ノード シークレットは、RSA Authentication ManagerとPAM agentが、ネットワーク経由で送受信するデータのパケットを暗号化および復号するときに使用する対称暗号化キーです。UDPプロトコルを使用するエージェントには、ノード シークレットが必要です。共有ノード シークレットは、Authentication Managerデータベースと、PAM agentがインストールされているマシン上のファイルの両方に保存されます。RESTプロトコルを使用するエージェントの場合、ノード シークレット ファイルは使用されません。チャネルの暗号化には、ノード シークレットではなく、動的にネゴシエートされたキーが、強力な暗号化アルゴリズムとともに使用されます。

UDPモードのエージェントの場合、ノード シークレットが、Authentication Managerサーバ、またはPAM agentがインストールされているマシンのどちらかに存在しなくなったときは、もう一方に存在するノード シークレットをクリアします。Authentication Managerのノード シークレット ファイルとPAM agentマシンのノード シークレット ファイルが一致しない場合は、両方の場所でノード シークレットをクリアします。ノード シークレットをクリアしたら、新しいノード シークレットを生成する必要があります。

RSA Authentication Agent 8.1 for PAMのノード シークレットのクリア

Authentication Managerに登録されたノード シークレットと、PAM agentがインストールされているマシンのノード シークレットが一致しない場合、またはPAM agent マシンにノード シークレットがない場合は、Authentication Managerからノード シークレットをクリアする必要があります。たとえば、PAM agentを再インストールした場合、PAM agent マシンにはノード シークレットはありません。

手順

1. Authentication ManagerのSecurity Consoleで、**[アクセス]＞[認証エージェント]＞[既存項目の管理]**の順にクリックします。
2. 対象のエージェント マシンを特定し、ドロップダウン メニューから[**ノード シークレットの管理**]を選択します。
3. [**ノード シークレットをクリアします**]チェックボックスをオンにして、[**保存**]をクリックします。

終了後のステップ

- PAM agent マシンにノード シークレットがある場合は、「PAM agentマシンでのノード シークレットのクリア (43ページ)」を参照してください。
- PAM agent マシンにノード シークレットがない場合は、「 新しいノード シークレットの生成 (44ページ)」の手順に従ってください。

PAM agentマシンでのノード シークレットのクリア

RSA Authentication Managerインスタンス のノード シークレットとPAM agent マシンのノード シークレットが一致しない場合、またはAuthentication Managerにノード シークレットがない場合は、PAM agent マシンからノード シークレットをクリアする必要があります。たとえば、新しいAuthentication Managerインスタンスをインストールし、既存のPAM agentを追加した場合、Authentication Managerにはノード シークレットはありません。

開始する前に

Authentication Managerにノード シークレットがある場合は、「 RSA Authentication Agent 8.1 for PAMのノード シークレットのクリア (43ページ)」を参照してください。

手順

1. PAM agentがインストールされているマシンにログオンし、**/var/ace**ディレクトリでノード シークレット ファイル**securid**を見つけます。
2. ノード シークレット ファイルの名前を変更するか、そのファイルを削除します。

3. ノード シークレットは、サーバのキャッシュにも保存されています。マシンを再起動して、キャッシュからノード シークレットをクリアします。

終了後のステップ

新しいノード シークレットの生成 (44ページ)

新しいノード シークレットの生成

手順

1. PAM agent マシンからacetestユーティリティを実行して、ノード シークレット ファイルを生成します。詳細については、「UDPモードの認証ユーティリティ (41ページ)」を参照してください。
2. 認証ログをチェックし、新しいノード シークレットが送信されたことを確認します。
3. PAM agent マシンを再起動して、エージェントにノード シークレット ファイルを読み込ませます。

PAM agentのログ

ログ機能を有効にすると、デフォルトで、PAM agent認証メッセージはシステム ログに記録されます。トレース目的で必要な場合は、特定のツールに関するPAM agent認証ログ メッセージをシステム ログに記録するよう構成できます。「デバッグ出力の有効化 (28ページ)」を参照してください。

システム ログの構成

次の手順を実行すると、すべての認証メッセージがシステム ログに送信されます。

手順

1. **/etc/**ディレクトリに移動します。
2. **syslog.conf**ファイルを開きます。
3. システム ログ ファイルを指定する行に`auth.notice`パラメータを追加します。
4. `authpriv.none`パラメータがシステム ログ ファイルに指定されている場合は、それを削除します。
5. telnetまたはloginを使用している場合は、システム ログ ファイルを指定する行に`authpriv.notice`パラメータを追加します。
6. 変更を保存します。
7. syslogデーモンを再起動します。

PAMエージェント認証ログ メッセージ

次の表は、認証ログ メッセージを示しています。

メッセージ	説明
Cannot locate **sd_pam.conf** file	構成ファイル**sd_pam.conf**が**/etc**ディレクトリにありません。**/etc**に正しい構成ファイルが存在しないと、VAR_ACEを正しく設定できません。
AceInitialize failed	AceInitializeは、ワーカー スレッドを初期化して**sdconf.rec**から設定を読み込むAPI関数です。**sdconf.rec**の最新のコピーをAuthentication Manager管理者から受け取っており、VAR_ACEが正しく設定されていることを確認してください。
Cannot communicate with RSA ACE/Server	Authentication Managerブローカーが起動されていないか、ネットワーク障害が発生しています。Authentication Managerの管理者またはネットワーク管理者に問い合わせてください。
Reserve password	文字数の上限は256文字です。

メッセージ	説明
exceeds character limit	
Invalid reserve password	予備パスワードがホストのシステム パスワードと同じです。Authentication Managerが認証リクエストを処理できない場合は、このパスワードを知っている必要があります。
User name exceeds character limit	ユーザー名は31文字以下でなければなりません。
Reserve password not allowed. User is not root.	rootユーザーであることを確認してください。予備パスワードを使用できるのは、rootユーザーだけです。

RESTモードのログ

RESTモードは、**log4cxx**ライブラリにより追加のログ機能をサポートしています。RESTレイヤーのログはPAM agentのログとは別のものです。RollingFileAppenderとSyslogAppenderがサポートされます。RollingFileAppenderはデフォルトで有効になります。INFOのログレベルのログが、**/var/ace/log/mfa_rest.log**に送られます。サイズによるローテーションが有効化されており、10 MBでローテーションされます。

時間によるローテーションはサポートされません。sshやsuなどのサポートされるツールでは、リクエストのたびに認証エージェントが読み込まれます。そのため、PAM agentは時間に基づいてログをローテーションできません。PAM agentは、サイズによるログのローテーションをサポートしています。

RESTモードのデフォルトのログ設定は変更できます。

手順

1. **/var/ace/conf**ディレクトリに移動します。
2. **log.properties**ファイルを開きます。
3. 以下のエントリーを設定して、サイズによるローテーションを有効にします。

```
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. 以下のエントリーを設定して、ローカルおよびリモートのSyslogへの転送を有効にします。

```
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. 変更を保存します。
6. syslogデーモンを再起動します。

REST認証のタイムアウト値と再試行値の構成

PAM agentからRSA Authentication Managerまたはクラウド認証サービスへの接続にかかる時間、およびPAM agentが応答を待つ時間を構成できます。PAM agentがAuthentication Managerのプライマリまたはレプリカ インスタンス、またはクラウド認証サービスに対して接続を試行する回数を構成することもできます。これらのパラメータは、RESTプロトコルでのみ使用されます。

ネットワークの速度を考慮してください。低速なネットワークで認証を成功させるには、タイムアウト値を長く設定してください。

開始する前に

エージェントがインストールされているマシンのroot権限と、**mfa_api.properties**ファイルが保存されているディレクトリに対する書き込みアクセス権が必要です。デフォルトで、このファイルは**/var/ace/conf**に保存されます。

手順

1. **mfa_api.properties**を保存するディレクトリに移動します。デフォルトで、このディレクトリは**/var/ace/conf**です。
2. **mfa_api.properties**を開きます。
3. 次のパラメータを変更できます。
   - CONNECT_TIMEOUT。エージェントがサーバへの接続に許容する最大秒数。デフォルトは60秒です。
   - READ_TIMEOUT。サーバへの接続と応答の読み取りに許容する最大秒数。READ_TIMEOUT値には、CONNECT_TIMEOUT値と、応答の読み取りに許容される最大秒数の合計を指定する必要があります。デフォルトは120秒です。
   - MAX_RETRIES。PAM agentがAuthentication Managerまたはクラウド認証サービスに対して接続を試行する回数。デフォルト値は3です。
   - Authentication ManagerのRESTインターフェイスの初期化フェーズ、つまりPAM agentが認証の試行を開始する場合、MAX_RETRIESは、そのエージェントが他のサーバにフェールオーバーする前に、同じサーバに対してアクセスを試行する回数です。検証フェーズ、つまりPAM agentが認証情報を送信する場合、フェールオーバーはサポートされず、MAX_RETRIESは、認証が失敗する前に、そのエージェントが同じサーバに対してアクセスを試行する回数です。
   - クラウド認証サービスはフェールオーバーをサポートしていません。初期化フェーズと検証フェーズの両方で、MAX_RETRIESは、認証が失敗する前に、エージェントが同じサーバに対してアクセスを試行する回数です。
4. ファイルを保存します。

RSA Authentication Agent 8.1 for PAMのアンインストール

PAM agentは個々のマシンで手動でアンインストールするか、PAM agentの複数のコピーをサイレント モードで自動的にアンインストールできます。

Solaris 10では、**/etc**ディレクトリに移動し、**pam.conf**ファイルを開きます。

Solaris 11では、**/etc/pam.d**ディレクトリに移動して**others**ファイルを開くか、**/etc**ディレクトリに移動して**pam.conf**ファイルを開きます。

開始する前に

- RSA SecurIDで保護されたツールの構成を変更し、RSA PAMモジュールではなく、オペレーティング システムに付属の標準PAMモジュールを使用するようにします。アンインストールを行う前に、RSA PAMモジュールを使用するアクティブなセッションを閉じる必要があります。「ツールの構成 (21ページ)」で行った処理手順を元に戻す必要があります。

  注:/etc/pam.d/othersファイルまたは**/etc/pam.conf**ファイルにRSAモジュールへの参照が存在する状態で、RSAモジュールをアンインストールすると、システムからロックアウトされます。

- root権限があることを確認します。

1台のマシンからのPAM agentのアンインストール

1つのPAM agentをアンインストールします。

手順

1. PAM agentのホーム ディレクトリに移動します。たとえば、**/opt/pam**です。
2. アンインストール スクリプトを実行します。次のように入力します。

   ```
   ./uninstall_pam.sh
   ```

3. インストール ディレクトリが削除されたことを確認します。ディレクトリがまだ存在する場合は、手動で削除する必要があります。
4. PAM agentが正常に削除されたことを確認するには、**/var/pam_uninstaller/uninstaller.log**ファイルをチェックします。

サイレント モードでのPAM agentの一括アンインストール

多数のPAM agentをアンインストールします。

手順

1. **unconfig**という名前のテキスト ベースの構成ファイルを作成します。このファイルには次の情報を追加します。

   ```
   y
   y
   y
   ```

   yはそれぞれ、次のプロンプトに対する応答です。

   - Are you sure that you would like to uninstall the RSA Authentication Agent 8.1.0 [101] for PAM?
   - The RSA Authentication Agent for PAM will be deleted from the <*install_path*> directory. Ok?

- If you uninstall the RSA module while there are references to the RSA module in the PAM configuration file (file **pam.conf** or inside the directory **pam.d**), you will be locked out of your system. Proceed with uninstall? Ok?

2. PAM agentのホーム ディレクトリに移動します。たとえば、**/opt/pam**です。
3. アンインストール スクリプトを実行します。次のように入力します。

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

付録B: 重要な構成ファイル

重要な構成ファイル

デフォルトのPAM agentインストール ディレクトリは**/opt/pam**であり、インストール時に変更できます。デフォルトで、**/var/ace**ディレクトリにはREST関連のライブラリとファイルが含まれています。このディレクトリは変更できません。

PAM agentには、バイナリ(**pam_securid.so**、**acetest**、**acestatus**、**ns_conv_util**)に加え、次の表に示す重要な構成ファイルが含まれます。

ファイル	説明
log.properties	RESTプロトコル用のPAM agentログ構成ファイル。PAM agentは、RESTモードのログに**log4cxx**ライブラリを使用します。
mfa_api.properties	Authentication Managerとクラウド認証サービスの RESTプロトコルの認証に使用される設定が含まれます。
sdconf.rec	このファイルはRSA Authentication Managerによって生成され、PAM agentの動作を制御する構成情報を含んでいます。このファイルの権限は-rw------- root rootにする必要があります。 このファイルはUDPモードでのみ使用されます。
sdopts.rec	このファイルは、手動でロード バランシングする場合に使用され、Authentication Managerインスタンスの IPアドレスのリストを指定します。このファイルの権限は-rw------- root rootにする必要があります。 このファイルはUDPモードでのみ使用されます。
sdstatus.12	このファイルは、Authentication Managerサーバの最後に確認されたステータスをトラッキングするためにPAM agentの認証APIによって生成されます。このファイルの権限は-rw------- root rootにする必要があります。
sd_pam.conf	PAM agentの動作を制御する構成情報を含んでいます。このファイルの権限は-rw-r--r-- root rootにする必要があります。
securid	このファイルは、ローカル マシンとAuthentication Managerの間のUDPプロトコル通信を保護するために使用される共有シークレット キーを含んでいます。このファイルの名前は、エージェントがAuthentication Managerとの通信に使用するポートに構成されたプロトコル名(通常は「services」ファイル経由)から命名されます。このファイルの権限は-r--------- root rootにする必要があります。ただし、OSのumask設定によっても異なります。 UDPプロトコルにはこのファイルが必要です。このファイルは、RESTプロトコルを使用する認証の場合はオプションです。