RSA® Authentication Manager 8.0
セットアップと構成ガイド

商標について

RSA、RSA のロゴ、EMC は、EMC Corporation の登録商標または商標です。その他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。RSA の商標のリストについては、**http://japan.emc.com/legal/emc-corporation-trademarks.htm#rsa** 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、EMC が著作権を保有しており、ライセンス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、ライセンス契約の条項に従い、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。

本ライセンス契約によって、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、民事および刑事責任が課せられることがあります。
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

本製品は RSA 以外のサードパーティ製ソフトウェアを実装している場合があります。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書の内容については、製品 DVD の「Third-Party Licenses（サード パーティ ライセンス）」フォルダを参照してください。

暗号技術に関するご注意

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。

免責事項

本書に記載されている EMC ソフトウェアを使用、複製、および配布するには、適切なソフトウェア・ライセンスが必要です。

EMC Corporation 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。EMC Corporation は、本文書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。

Copyright © 1994-2013 EMC Corporation.All rights reserved.（不許複製・禁無断転載）
2013 年 3 月

目次

はじめに

本書について

このガイドは、RSA®Authentication Manager 導入環境のさまざまなコンポーネントのインストールとセキュリティ保護を担当するネットワークおよびシステム管理者を対象としています。

RSA Authentication Manager 8.0 マニュアル

RSA Authentication Manager 8.0 の詳細については、次のマニュアルを参照してください。RSA では、管理者のみがアクセス可能なネットワーク上の場所に製品マニュアルを保管することを推奨します。

リリース ノート。本リリースにおける新機能や変更点に加え、既知の不具合とその回避方法について説明しています。

Getting Started：Authentication Manager の Quick Setup プロセスを実行する方法について説明しています。

設計ガイド：Authentication Manager の上位レベルのアーキテクチャ、および既存ネットワークとの統合方法について説明しています。

セットアップと構成ガイド：Authentication Manager をセットアップおよび構成する方法について説明しています。

管理者ガイド：Authentication Manager とその機能の概要を示しています。システムを構成し、ユーザーやセキュリティ ポリシーの管理など、さまざまな管理タスクを実行する方法について説明しています。

Help Desk Administrator's Guide：ヘルプ デスク管理者が日々実行する最も一般的なタスクの手順について説明しています。

SNMP Reference Guide：SNMP（Simple Network Management Protocol）を構成して Authentication Manager のインスタンスを監視する方法について説明しています。

トラブルシューティング ガイド：RSA Authentication Manager の最も一般的なエラー メッセージと、各イベントをトラブルシューティングする適切なアクションについて説明します。

Developer's Guide：RSA Authentication Manager API（アプリケーション プログラミング インタフェース）を使用したカスタム プログラムの開発について説明しています。また、API の概要および Java API の Javadoc も含まれています。

Performance and Scalability Guide：最適なパフォーマンスを得るために環境を調整するときの考慮事項について説明しています。

6.1 から 8.0 への移行ガイド：RSA Authentication Manager 6.1 環境から RSA Authentication Manager 8.0 環境へ移行する方法について説明しています。

7.1 から 8.0 への移行ガイド：RSA Authentication Manager 7.1 環境から RSA Authentication Manager 8.0 環境へ移行する方法について説明しています。

Security Console ヘルプ：Security Console で日々実行される管理タスクについて説明しています。

Operations Console ヘルプ：Operations Console で実行される構成タスクおよび設定タスクについて説明しています。

Self-Service Console ヘルプ：Self-Service Console を使用する方法について説明しています。ヘルプを表示するには、Self-Service Console の［**Help（ヘルプ）**］タブで［**Self-Service Console Help（Self-Service Console ヘルプ）**］をクリックします。

RSA Token Management Snap-In ヘルプ：Active Directory アイデンティティ ソースが存在する環境で MMC（Microsoft 管理コンソール）と連携するソフトウェアを使用する方法について説明します。このスナップインを使用すると、トークンの有効化 / 無効化、トークンの割り当て、またはその他のトークン関連タスクを実行するために、Security Console にログオンする必要がなくなります。

関連ドキュメント

RADIUS リファレンス ガイド：RSA RADIUS で使用する初期設定ファイル、Dictionary ファイル、構成ファイルの使用法および設定について説明しています。

Security Configuration Guide：Authentication Manager で使用可能なセキュリティ構成設定について説明します。また、安全な導入と使用のための設定、安全な保守、物理的なセキュリティ管理に関する情報も提供します。

サポートとサービス

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
RSA Solution Gallery	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

RSA SecurCare Online では、よくある質問に対する回答や既知の問題に対する解決策を含むナレッジベースを参照できます。また、新しいリリースに関する情報や重要なテクニカル ニュース、ソフトウェアのダウンロードも利用できます。

RSA Solution Gallery では、RSA 製品との連携が検証されている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。このギャラリーには、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、連携手順を説明した Secured by RSA 実装ガイドおよびその他の情報が含まれています。

カスタマー サポートにご連絡される前に

ご連絡いただく際には、次の情報をご用意ください。

- ❑ RSA Authentication Manager アプライアンスにアクセスできることを確認してください。
- ❑ ライセンスのシリアル番号。シリアル番号は、次の方法で確認できます。
  - Security Console にログオンして、[**License Status（ライセンス ステータス**]をクリックします。[**View Installed License（インストール済みライセンスの表示)**]をクリックし、リストからライセンス ID を選択して内容を表示します。
- ❑ Authentication Manager アプライアンスのソフトウェアのバージョン情報。この情報は、Quick Setup の画面の右上隅、または Security Console に表示されます。Security Console にログオンして、[**Software Version Information（ソフトウェア バージョン情報)**]をクリックします。

1 導入の準備

計画の決定

RSA Authentication Manager 8.0 の導入環境のセットアップを開始する前に、インストールする Authentication Manager コンポーネントを決定する必要があります。導入環境には次のコンポーネントが含まれます。

プライマリ インスタンス。すべての管理操作を実行するインスタンスです。認証リクエストを処理することもできます。

レプリカ インスタンス。プライマリ インスタンスの冗長性を提供し、ユーザー認証を処理します。

Web Tier。RSA Self-Service Console、動的シード配布、RBA（リスクベース認証）サービスを DMZ（非武装地帯）内に安全に導入します。

ロードバランサ。プライマリ Web Tier とレプリカ Web Tier の間で認証リクエストを分散し、フェイルオーバーを容易にするために使用されます。

認証エージェント。保護対象の任意のリソースにインストールされます。

導入計画の詳細については、「設計ガイド」を参照してください。

VMware 仮想アプライアンスの要件

RSA Authentication Manager 8.0 は、RSA Authentication Appliance という名前の仮想アプライアンスとして VMware に導入されます。Quick Setup を実行するときに、RSA Authentication Appliance を Authentication Manager プライマリ インスタンスまたはレプリカ インスタンスとして構成します。

VMware vSphere Client は、VMware vCenter を使用して、または VMware ESXi プラットフォームで直接仮想アプライアンスを導入するために使用します。RSA Authentication Appliance を導入するために VMware vCenter は必須ではありません。

VMware ソフトウェア要件

必要なソフトウェア	説明
VMware プラットフォーム	仮想アプライアンスは、次のプラットフォームのいずれかに導入します。 • VMware ESXi 4.1 以降 • VMware ESXi 5.0 以降
VMware vSphere Client	サポートされている VMware ESXi および vCenter 環境で動作する任意のバージョンの vSphere Client。

VMware のホスト ハードウェア要件については、VMware のマニュアルを参照してください。

VMware ソフトウェア サポート

サポートされているソフトウェア	説明
（オプション）VMware vCenter Server	VMware vCenter は複数の仮想マシンの一元管理を実現し、vMotion などの管理機能を提供します。 RSA Authentication Appliance は、サポートする VMware ESXi のバージョンと互換性のあるバージョンの VMware vCenter をサポートしています。 • VMware vCenter Server 4.1 以降 • VMware vCenter Server 5.1 以降

プライマリまたはレプリカ インスタンスのハードウェア要件

各 RSA Authentication Manager インスタンス用の仮想アプライアンスは、最小要件を満たすかそれを超えるハードウェアを必要としています。各インスタンスは、デフォルト値を使用して導入されます。

説明	最小要件	デフォルト値
ディスク領域	100 GB 仮想アプライアンスを導入するときに、シン プロビジョニングされたストレージを選択します。	100 GB 仮想アプライアンスを導入するときに、シン プロビジョニングされたストレージを選択します。
メモリ要件	4 GB	8 GB
CPU 要件	1 個の仮想 CPU	2 個の仮想 CPU

仮想アプライアンスの自動チューニングは、4 GB、8 GB、16 GB のメモリをサポートしています。たとえば、16 GB を超えるメモリが利用可能な場合、アプライアンスは 16 GB のメモリを使用します。

仮想アプライアンスは、E1000 仮想ネットワーク アダプタのみサポートしています。デフォルトのネットワーク アダプタを変更したり、新しい仮想ネットワーク アダプタを仮想アプライアンスに追加しないでください。

VMware のホスト ハードウェア要件については、VMware のマニュアルを参照してください。

Authentication Manager により使用されるポートについては、63 ページの「使用するポート」を参照してください。

VMware 機能サポート

RSA Authentication Manager は、vMotion、Storage vMotion、High Availability、Fault Tolerance、DRS（Distributed Resource Scheduler）、スナップショットなどの VMware 機能をサポートしています。制限事項について、次の表で説明します。

機能	サポート
VMware Fault Tolerance	VMware vSphere 4.1 および 5.0 の VMware Fault Tolerance には、以下の要件があります。 • 1 つの仮想 CPU を持つ仮想アプライアンスのみ、Fault Tolerance との互換性があります。デフォルトでは、各 Authentication Manager インスタンスは、2 つの仮想 CPU とともに導入されます。 仮想 CPU の数は変更できます。手順については、VMware vSphere Client のマニュアルを参照してください。 • VMware Fault Tolerance は、IPv6 をサポートしていません。Fault Tolerance を使用する場合は、Authentication Manager プライマリ インスタンスまたはレプリカ インスタンスに対して IPv6 ネットワーク アドレスを設定しないでください。

機能	サポート
VMware スナップショット	Authentication Manager プライマリ インスタンスまたはレプリカ インスタンスの VMware スナップショットを作成できますが、スナップショットは、Operations Console のバックアップ機能に取って代わるものではありません。 Authentication Manager インスタンスのスナップショットを作成する場合、特定の設定が必要です。複雑な Authentication Manager 導入環境の場合は、スナップショットを復元した後、追加のタスクの実行が必要となる場合があります。 詳細については、「管理者ガイド」の「災害復旧」の章を参照してください。
VMware DRS（Distributed Resource Scheduler）	セキュリティと冗長性のため、プライマリ インスタンスとレプリカ インスタンスを別々のホストにインストールすることができます。 VMware DRS は、両方のインスタンスを同じホストに移動できます。各インスタンスが別々の物理ホストに配置されたままになるよう、DRS を構成してください。

サポートされるデータストア

次の場所にデータを格納できます。

- RSA Authentication Manager の内部データベース
- 1 つ以上の外部 LDAP ディレクトリ サーバ（Authentication Manager 内ではアイデンティティ ソースと呼びます）。

内部データベース

Authentication Manager は、内部データベースとともにインストールされます。次の情報は、内部データベースのみに格納されます。

- トークン データ、管理者ロール、パスワードポリシーなどの、Authentication Manager 特有のデータ。
- AuthenticationManager を LDAP ディレクトリのユーザーおよびユーザー グループ レコードとリンクするためのデータ。

ユーザー、ユーザー グループ、アイデンティティ属性データは、外部 LDAP ディレクトリまたは内部データベースに格納することができます。

サポートされているディレクトリ サーバ

RSA Authentication Manager は、ユーザー、ユーザーグループ、アイデンティティ属性データ用に、以下の外部 LDAP ディレクトリ サーバをサポートしています。

- Microsoft Active Directory 2008 R2
- Sun Java System Directory Server 7.0
- Oracle Directory Server Enterprise Edition 11G

ADAM（Active Directory アプリケーション モード）はサポートされていません。

Authentication Manager からすべての外部ディレクトリ サーバへのアクセスは読み取り専用です。ただし、認証時にユーザーが LDAP 上のパスワードを変更できるようシステムを構成できます。

Authentication Manager と LDAP の統合では、既存の LDAP スキーマを変更することなく、Authentication Manager で使用するデータへのマッピングを作成します。

Authentication Manager は、SSL-LDAP 接続をサポートしています。SSL は、Authentication Manager からユーザーが自分のパスワードを変更できるよう許可する場合に必要です。非 SSL 接続では、接続を通過する機密データが盗聴される可能性があります。たとえば、仮に非 SSL 接続を使用して LDAP バインド認証を行うと、パスワードが平文で送信されます。SSL-LDAP を使用するには、Authentication Manager が適切な証明書にアクセスできることが必須条件となります。

詳細については、「管理者ガイド」の「LDAP ディレクトリの統合」の章を参照してください。

サポートされる Web ブラウザ

RSA Authentication Manager の管理は Web ベースのインタフェースを使用するため、サポートされているブラウザからアクセスする必要があります。Authentication Manager は、次の Web ブラウザをサポートしています。

- Microsoft Internet Explorer 7.0 以降
- Mozilla Firefox 10.0 以降
- Google Chrome 18 以降
- Apple Safari 5.1 以降

Web ブラウザでは、JavaScript および Cookie が有効になっている必要があります。Web ブラウザの JavaScript および Cookie が有効になっていない場合は、JavaScript と Cookie を有効にする手順について Web ブラウザのドキュメントを参照してください。

サポートされる認証エージェント

認証エージェントは、RSA Authentication Manager との間でユーザー認証要求を安全にやりとりするためのソフトウェア アプリケーションです。認証エージェントは、ドメイン サーバ、Web サーバ、パーソナル コンピュータなどの Authentication Manager で保護する各マシンにインストールされます。SecurID 認証、ODA（On-Demand 認証）、RBA（リスク ベース認証）を使用するリソースには、すべて認証エージェントが必要です。

必要となるエージェントは、保護するリソースのタイプによって異なります。たとえば、Apache Web サーバを保護するには、RSA Authentication Agent for Apache をダウンロードする必要があります。また、RSA Authentication Agent ソフトウェアを組み込み済みの製品を購入することが可能です。たとえば、主要ブランドのリモート アクセス サーバおよびファイアウォール製品には RSA Authentication Agent が組み込まれています。

RSA Authentication Agent のリストについては、「**http://japan.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**」にアクセスしてください。

RSA Authentication Agent が組み込まれたサード パーティ製品のリストについては、RSA Secured® の Web サイト「**https://gallery.emc.com/community/marketplace/rsa?view=overview**」にアクセスしてください。

詳細については、「管理者ガイド」の「認証エージェントの導入」の章を参照してください。

ライセンス要件

RSA Authentication Manager を使用するにはライセンスが必要です。ライセンスは、Authentication Manager ソフトウェアの特定のバージョンを使用する権利を表します。

プライマリ アプライアンスの Quick Setup を実行する前に、ライセンス ファイルの場所を確認してください。このライセンス ファイルは、プライマリ アプライアンスの Quick Setup を実行するブラウザからアクセスできる場所に配置する必要があります。

正確なシステム時刻の設定

RSA Authentication Manager では、レプリケーションと認証のために正確な日時の設定が必須です。トークンの時刻と Authentication Manager のシステム時刻が一致しない場合、生成されたトークンコードが一致せず、認証が失敗します。インスタンスに NTP（ネットワーク タイム プロトコル）サーバを指定することにより、時刻ずれによるレプリケーションと認証の問題を回避できます。

重要：レプリカのある導入環境では、NTP サーバが必須です。すべての Authentication Manager インスタンスの時刻を同じ NTP サーバと同期させるようにしてください。

Authentication Manager に NTP サーバを設定しない場合、仮想アプライアンスは、仮想アプライアンスをホストする物理マシンの時刻を使用します。この場合、NTP サーバから正確な時刻情報を取得するよう、仮想アプライアンスをホストする物理マシンを構成する必要があります。

Quick Setup を実行する前に NTP サーバのホスト名や IP アドレスを入手するようにしてください。

プライマリ インスタンスの導入チェックリスト

RSA Authentication Manager プライマリ インスタンスをセット アップする前に、次の情報を収集する必要があります。仮想アプライアンスの導入および Quick Setup の実行中にこの情報を入力します。

- **VMware vSphere Client コンピュータ**。このコンピュータは、vSphere Client を使用してアプライアンスを導入し、サポートされる Web ブラウザを使用して Quick Setup を実行するために使用します。サポートされる Web ブラウザのリストについては、15 ページの「サポートされる Web ブラウザ」を参照してください。
- **RSA Authentication Appliance OVA ファイル**。OVA ファイルは仮想アプライアンスの作成に使用されます。OVA ファイルを VMware からアクセスできる場所にコピーします。
- **IPv4 ネットワーク設定**。仮想アプライアンスの完全修飾ドメイン名と固定 IP アドレス、サブネット マスクとデフォルト ゲートウェイ、ネットワーク内の DNS サーバの IP アドレスまたはホスト名の情報を取得します。

  Quick Setup の実行中に IPv4 ネットワーク設定が行われます。Quick Setup が完了した後、IPv6 対応のエージェントを使用する場合は、IPv6 を有効にできます。IPv4 と IPv6 のエージェントを同時にサポートできます。
- **アプライアンスのライセンス ファイル**。Quick Setup の実行中に、.zip 形式のライセンス ファイルにアクセスできる必要があります。ライセンス ファイルを入手されていない場合は、製品を購入された販売代理店または RSA カスタマーサポート窓口にお問い合わせください。

  プライマリ アプライアンスの Quick Setup を実行する前に、ライセンス ファイルの場所を確認してください。ライセンス ファイルは、プライマリ アプライアンスの Quick Setup を実行するブラウザからアクセスできる場所に配置する必要があります。このファイルは解凍しないでください。ライセンス ファイルは、許可された管理者のみがアクセスできる安全な場所に保管してください。

- **NTP サーバのホスト名または IP アドレス**。RSA では、ローカルまたはインターネット上の NTP（ネットワーク タイム プロトコル）サーバ（たとえば、nist.time.gov）を指定することを推奨します。Quick Setup の実行中に、少なくとも 1 台の NTP サーバのホスト名または IP アドレスを入力できます。

  重要：レプリケーション導入環境では、NTP サーバが必須です。すべての Authentication Manager インスタンスの時刻が同一の NTP サーバと同期している必要があります。

- **オペレーティング システムのパスワード**。トラブルシューティングや高度な管理のためにアプライアンス オペレーティング システムにアクセスするときに使用するパスワードを選択します。パスワードは 8 ～ 32 文字の長さで、1 つ以上の英字と 1 つ以上の特殊文字（^、@、~ を除く）を含める必要があります。たとえば、gyz!8kMh は有効なパスワードです。詳細については、73 ページの「システム管理者アカウント」を参照してください。
- **初期の管理者アカウントのユーザー ID とパスワード**。次のユーザー ID とパスワードを選択します。
  - 初期のスーパー管理者のユーザー ID とパスワード（Security Console へのアクセスに使用）
  - Operations Console 管理者のユーザー ID とパスワード

  管理者アカウントとパスワードの管理については、73 ページの「システム管理者アカウント」を参照してください。

レプリカ インスタンスの導入チェックリスト

RSA Authentication Manager レプリカ インスタンスをセットアップする前に、セットアップする各レプリカについて次の情報を収集します。仮想アプライアンスの導入および Quick Setup の実行中にこの情報を入力します。

- **VMware vSphere Client コンピュータ**。このコンピュータは、vSphere Client を使用してアプライアンスを導入し、サポートされる Web ブラウザを使用して Quick Setup を実行するために使用します。サポートされる Web ブラウザのリストについては、15 ページの「サポートされる Web ブラウザ」を参照してください。

- **RSA Authentication Appliance OVA ファイル**。OVA ファイルは仮想アプライアンスの作成に使用されます。OVA ファイルを VMware からアクセスできる場所にコピーします。
- **IPv4 ネットワーク設定**。仮想アプライアンスの完全修飾ドメイン名と固定 IP アドレス、サブネット マスクとデフォルト ゲートウェイ、ネットワーク内の DNS サーバの IP アドレスまたはホスト名の情報を取得します。

  Quick Setup の実行中に IPv4 ネットワーク設定が行われます。Quick Setup が完了した後、IPv6 対応のエージェントを使用する場合は、IPv6 を有効にできます。IPv4 と IPv6 のエージェントを同時にサポートできます。
- **レプリカ パッケージ ファイルの場所**。レプリカ アプライアンスをセットアップするには、レプリカ パッケージ ファイルにアクセスできる必要があります。必要に応じて、レプリカ パッケージ ファイルを、Quick Setup の実行に使用するコンピュータにコピーします。

  レプリカ パッケージの作成の詳細については、33 ページの「レプリカ パッケージ ファイルの生成およびダウンロード」を参照してください。
- **NTP サーバのホスト名または IP アドレス**。ローカルまたはインターネット上の NTP（ネットワーク タイム プロトコル）サーバを使用して、プライマリ アプライアンスとレプリカ アプライアンスの時刻を同期する必要があります。Quick Setup の実行中に、少なくとも 1 台の NTP サーバのホスト名または IP アドレスを入力できます。
- **オペレーティング システムのパスワード**。トラブルシューティングや高度な管理のためにアプライアンス オペレーティング システムにアクセスするときに使用するパスワードを選択します。パスワードは 8 ～ 32 文字の長さで、1 つ以上の英字と 1 つ以上の特殊文字（^、@、~ を除く）を含める必要があります。たとえば、gyz!8kMh は有効なパスワードです。アプライアンスごとに一意のパスワードを選択します。詳細については、73 ページの「システム管理者アカウント」を参照してください。

セットアップおよび構成に関する情報リスト

次のリストを使用して、RSA Authentication Manager のセットアップおよび構成に関する情報を記入します。記入が完了したら、このリストを適切な担当者に配布してください。今後の参照のため、完成したリストのコピーを安全な場所に保管します。

注：このリストに記入する情報には、機密情報が含まれる場合があります。パスワードなどの機密情報をこのリストに記入する前に、自社のポリシーを確認してください。

仮想アプライアンスの導入

項目	値
RSA Authentication Appliance OVA パッケージの場所	
完全修飾ドメイン名	
IPv4 固定 IP アドレス	
IPv4 サブネット マスク	
IPv4 デフォルト ゲートウェイ	
DNS サーバの IP アドレス	

注：導入環境で IPv6 準拠のエージェントを使用する場合、Quick Setup が完了した後、Operations Console で IPv6 ネットワーク設定を追加できます。

プライマリ アプライアンスの構成

項目	値
RSA Authentication Manager ライセンス ファイル（.zip）の場所	
NTP サーバのホスト名または IP アドレス	
オペレーティング システムのパスワード	
スーパー管理者のユーザー名	
スーパー管理者のパスワード	
Operations Console 管理者のユーザー名	
Operations Console 管理者のパスワード	

レプリカ アプライアンスの構成

項目	値
レプリカ パッケージ ファイルの場所	
NTP サーバのホスト名または IP アドレス	
オペレーティング システムのパスワード	

ロードバランサの構成

説明	計画
ロードバランサの IP アドレス	
ロードバランサのホスト名 / 仮想ホスト名	
ポート番号	
DNS サーバに登録された仮想ホストまたはロードバランサの IP アドレス	

Web Tier のインストール

項目	値
Web Tier サーバの IP アドレス	
Web Tier サーバのホスト名	
DNS サーバの IP アドレス	

2 プライマリ アプライアンスの導入

導入タスクの実行

仮想アプライアンスを導入し、RSA Authentication Manager のプライマリ インスタンスを構成するには次のステップを実行します。

処理手順

1. RSA Authentication Appliance OVF テンプレートを導入します。VMware vCenter を使用した仮想アプライアンスの導入または、VMware ESXi への仮想アプライアンスの直接導入のいずれかを実行できます。
2. Quick Setup でアプライアンスを構成します。Quick Setup は、アクセス権限を作成し、アプライアンスがプライマリ インスタンスまたはレプリカ インスタンスのどちらかを指定するソフトウェア ウィザードです。プライマリ インスタンスでの Quick Setup の実行を参照してください。
3. 内部 RSA CA（認証局）証明書を受け入れます。SSL 証明書の管理を参照してください。
4. コンソールへのログオン。

VMware vCenter を使用した仮想アプライアンスの導入

仮想アプライアンスを管理するために VMware vCenter を使用している場合、この管理ツールを使用して仮想アプライアンスを導入できます。

開始する前に

- 導入するアプライアンスに関して必要な情報を収集します。17 ページの「プライマリ インスタンスの導入チェックリスト」を参照してください。
- RSA Authentication Appliance OVA ファイルを VMware からアクセスできる場所にコピーします。

処理手順

1. VMware vSphere Client で、VMware vCenter にログオンします。
2. **［File（ファイル）］＞［Deploy OVF Template（OVF テンプレートのデプロイ）］**の順に選択し、導入ウィザードを開始します。
3. ［Source（ソース）］ウィンドウで、**［Deploy from a File or URL（ファイルまたは URL からのデプロイ）］**を選択します。

4. ［**Browse（参照）**］をクリックし、RSA Authentication Appliance OVA ファイルを指定します。［**OK**］をクリックして、［Source（ソース）］ウィンドウに戻ります。［**Next（次へ）**］をクリックします。
5. ［OVF Template Details（OVF テンプレートの詳細）］ウィンドウで、「RSA Authentication Appliance」および正しいバージョン番号が表示されていることを確認します。［**Next（次へ）**］をクリックします。
6. ［End User License Agreement（エンド ユーザー使用許諾契約書）］ウィンドウで、契約書をスクロールして読みます。［**Accept（承諾）**］をクリックして、［**Next（次へ）**］をクリックします。
7. ［Name and Location（名前と場所）］ウィンドウで、仮想アプライアンスの名前を入力し、［**Next（次へ）**］をクリックします。
8. ［Host/Cluster（ホスト / クラスタ）］ウィンドウで、仮想アプライアンスのホストまたはクラスタを選択します。［**Next（次へ）**］をクリックします。
9. ［Resource Pool（リソース プール）］ウィンドウで、リソース プールを選択します。リソース プールを使用して、ホストまたはクラスタ内のリソースを管理することができます。［**Next（次へ）**］をクリックします。
10. ［Datastore（データストア）］ウィンドウで、仮想マシン ファイルを保存する既存の VMware データストアを選択します。VMware データストアには、VMFS（仮想マシン ファイル システム）のボリューム、ネットワーク接続型ストレージのディレクトリ、ローカル ファイル システムのパスなどの場所を指定できます。［**Next（次へ）**］をクリックします。
11. ［Disk Format（ディスクのフォーマット）］ウィンドウで、仮想ディスクを保存するフォーマットを選択します。
12. ［Network Mapping（ネットワーク マッピング）］ウィンドウで、仮想アプライアンスのネットワークを選択します。［**Next（次へ）**］をクリックします。
13. ［Properties（プロパティ）］ウィンドウで、仮想アプライアンスの IPv4 ネットワーク設定を入力します。
    - 完全修飾ドメイン名
    - IP アドレス
    - サブネット マスク
    - デフォルト ゲートウェイ
    - （オプション）プライマリ DNS サーバ
    - （オプション）セカンダリ DNS サーバ

    ［**Next（次へ）**］をクリックします。

注：導入環境で IPv6 準拠のエージェントを使用する場合、Quick Setup が完了した後、Operations Console で IPv6 ネットワーク設定を追加できます。

14. ［Ready to Complete（準備の完了）］ウィンドウで、設定を確認し、**［Finish（完了）］**をクリックします。VMware が RSA Authentication Appliance を導入するのに約 5 分必要です。
15. 仮想マシンをパワーオンします。
16. **［Launch Virtual Machine Console（仮想マシン コンソールの起動）］**ボタンをクリックします。
    仮想マシン コンソールに仮想アプライアンスの導入の進行状況が表示されます。
17. 30 秒待ち、デフォルトの英語（米国）のキーボード レイアウトを選択します。他のキーボード レイアウトを選択するには、任意のキーを押して、画面の指示を実行します。
18. ネットワーク設定が正しいことを確認します。設定を受け入れるには、「**y**」と入力して Enter キーを押すか、30 秒待ちます。
    仮想アプライアンスが導入されると、ステップ 13 で入力した IP アドレスを使用した Quick Setup URL が OS コンソールに表示されます。
19. https で始まる Quick Setup URL をブラウザに入力し、Enter キーを押します。

    `https://＜IP アドレス＞/`

注：仮想アプライアンスの信頼性を確認する場合は、Quick Setup の証明書の SHA-1 フィンガープリントが OS コンソールに表示された SHA-1 フィンガープリントと一致することを確認する必要があります。

VMware ESXi への仮想アプライアンスの直接導入

VMware ESXi に仮想アプライアンスを直接導入することができます。たとえば、中堅・中小企業（SMB）向けの VMware ESXi 無償版に仮想アプライアンスを導入することができます。仮想マシンの導入に VMware vCenter は必要ありません。

開始する前に

- 導入するアプライアンスに関して必要な情報を収集します。17 ページの「プライマリ インスタンスの導入チェックリスト」を参照してください。
- RSA Authentication Appliance OVA ファイルを VMware からアクセスできる場所にコピーします。

処理手順

1. VMware vSphere Client で、VMware ESXi サーバにログオンします。
2. **［File（ファイル）］＞［Deploy OVF Template（OVF テンプレートのデプロイ）］**の順に選択し、導入ウィザードを開始します。

3. ［Source（ソース）］ウィンドウで、**［Deploy from a File or URL（ファイルまたは URL からのデプロイ）］**を選択します。
4. **［Browse（参照）］**をクリックし、RSA Authentication Appliance OVA ファイルを指定します。**［OK］**をクリックして、［Source（ソース）］ウィンドウに戻ります。**［Next（次へ）］**をクリックします。
5. ［OVF Template Details（OVF テンプレートの詳細）］ウィンドウで、「RSA Authentication Appliance」および正しいバージョン番号が表示されていることを確認します。**［Next（次へ）］**をクリックします。
6. ［End User License Agreement（エンド ユーザー使用許諾契約書）］ウィンドウで、契約書をスクロールして読みます。**［Accept（承諾）］**をクリックして、**［Next（次へ）］**をクリックします。
7. ［Name and Location（名前と場所）］ウィンドウで、仮想アプライアンスの名前を入力し、**［Next（次へ）］**をクリックします。
8. ［Datastore（データストア）］ウィンドウで、仮想マシン ファイルのディレクトリを選択します。VMware データストアには、VMFS（仮想マシン ファイル システム）のボリューム、ネットワーク接続型ストレージのディレクトリ、ローカル ファイル システムのパスなどの場所を指定できます。**［Next（次へ）］**をクリックします。
9. ［Disk Format（ディスクのフォーマット）］ウィンドウで、仮想ディスクを保存するフォーマットを選択します。
10. ［Network Mapping（ネットワーク マッピング）］ウィンドウで、仮想アプライアンスのネットワークを選択します。**［Next（次へ）］**をクリックします。
11. ［Ready to Complete（準備の完了）］ウィンドウで、設定を確認し、**［Finish（完了）］**をクリックします。VMware が RSA Authentication Appliance を導入するのに約 5 分必要です。
12. 仮想マシンをパワーオンします。
13. RSA Authentication Appliance の**［Console（コンソール）］**タブをクリックします。
    OS コンソールに OVF 導入の進行状況が表示されます。
14. 30 秒待ち、デフォルトの英語（米国）のキーボード レイアウトを選択します。他のキーボード レイアウトを選択するには、任意のキーを押して、画面の指示を実行します。
15. OS コンソールのプロンプトに従って、仮想アプライアンスの IPv4 ネットワーク設定を入力します。
    - 完全修飾ホスト名
    - IP アドレス
    - サブネット マスク

- デフォルト ゲートウェイ
- （オプション）DNS サーバ構成

注：導入環境で IPv6 準拠のエージェントを使用する場合、Quick Setup が完了した後、Operations Console で IPv6 ネットワーク設定を追加できます。

16. ネットワーク設定が正しいことを確認します。設定を受け入れるには、「**y**」と入力して Enter キーを押すか、30 秒待ちます。
    仮想アプライアンスの導入が完了すると、ステップ 15 で入力した IP アドレスを使用した Quick Setup URL が OS コンソールに表示されます。
17. https で始まる Quick Setup URL をブラウザに入力し、Enter キーを押します。

    `https://` ＜ *IP* アドレス＞ `/`

注：仮想アプライアンスの信頼性を確認する場合は、Quick Setup の証明書の SHA-1 フィンガープリントが OS コンソールに表示された SHA-1 フィンガープリントと一致することを確認する必要があります。

プライマリ インスタンスでの Quick Setup の実行

Quick Setup は、RSA Authentication Appliance を RSA Authentication Manager プライマリ インスタンスとして構成します。Quick Setup が完了するまでは、RSA Authentication Appliance を信頼できるネットワークに接続した状態にします。Quick Setup を実行するクライアント コンピュータおよびブラウザも、信頼できるネットワーク上に接続する必要があります。

Quick Setup を完了していない場合、VMware vSphere Client で仮想マシンをパワーオンするたびに仮想アプライアンスのネットワーク設定を確認するよう求められます。

開始する前に

- 仮想アプライアンスの導入が完了している必要があります。
- ローカル コンピュータのブラウザが、Quick Setup の実行中に使用するライセンス ファイル（.zip）にアクセスできることを確認します。詳細については、17 ページの「プライマリ インスタンスの導入チェックリスト」を参照してください。

処理手順

1. 仮想アプライアンスの導入の終了時に表示される URL にアクセスし、Quick Setup を起動します。
2. Web ブラウザでセキュリティ レベルを高に設定している場合は、この URL が許可サイトまたは信頼済みサイトのリストにないことを知らせる警告が表示されます。続行するには、ブラウザに表示されているオプションをクリックし、信頼できないサイトへの接続を許可します。たとえば、ブラウザが、「I Understand the Risks.（危険性を理解した上で接続する）」というリンクをクリックするよう求める可能性があります。
3. ［Primary and Replica Quick Setup（プライマリおよびレプリカの Quick Setup）］ウィンドウで、**［Start Primary Quick Setup（プライマリの Quick Setup の開始）］**をクリックします。
4. ［Primary Quick Setup（プライマリの Quick Setup）］ページで、**［Start Step 1（ステップ 1 の開始）］**をクリックします。
5. RSA Authentication Appliance ライセンス ファイル（.zip）の場所を指定し、**［Upload（アップロード）］**をクリックします。
6. ライセンスの内容を確認して、**［Next（次へ）］**をクリックします。
7. ［Date & Time settings（日付と時刻設定）］ページで、次の操作を実行します。
   a. ［Region（地域）］を選択します（例：アメリカ）。
   b. ［Location（場所）］を選択します。夏時間を採用するタイムゾーンの場合、UTC（協定世界時）からの 2 つのオフセットが表示されます（例：（UTC-05/UTC-04）New York）。

c. 仮想アプライアンスの時刻を、VMware ホストまたは NTP サーバのどちらと同期するかを選択します。

d. ローカルまたはインターネット上の NTP サーバのホスト名または IP アドレスを入力します。
2 台目の NTP サーバを指定することもできます。アプライアンスは、リストの先頭にある NTP サーバから日付と時刻を取得します。Quick Setup が NTP サーバに接続できない場合は、Quick Setup が完了した後、Operations Console から NTP サーバを追加できます。

重要：レプリケーション環境では、NTP サーバが必須です。すべての Authentication Manager インスタンスの時刻が同一の NTP サーバと同期している必要があります。

e. NTP サーバへの接続をテストし、時刻が正確であることを確認するには、**［Preview Current Date & Time（現在の日付と時刻の確認）］**をクリックします。

f. **［Next（次へ）］**をクリックします。

8. ［OS Password（OS パスワード）］ページで、オペレーティング システムのパスワードの作成と確認を行い、**［Next（次へ）］**をクリックします。

注：オペレーティング システムのパスワードは、プライマリ インスタンスにログオンするために必要です。

オペレーティング システムのパスワードを記録し、必要な場合にアクセスできるようにします。セキュリティ上の理由から、RSA はオペレーティング システムのパスワードをリカバリするユーティリティを提供しません。

9. ［Initial Administration Accounts（初期の管理者アカウント）］ページで、Security Console スーパー管理者および OC（Operations Console）管理者のクレデンシャルを作成します。**［Next（次へ）］**をクリックします。

重要：ユーザー ID は一意である必要があります。1 ～ 255 の ASCII 文字を使用できます。&、%、>、<、' の各文字は使用できません。ユーザー ID に非サポート文字が含まれる場合、ユーザーは認証されません。

これらのユーザー ID とパスワードを記録します。

注：Quick Setup が完了した後、Security Console で追加のスーパー管理者および Operations Console 管理者アカウントを作成できます。

10. 入力した情報を確認します。いずれかの情報を変更する場合は、**［Back（戻る）］**をクリックして、該当するページを変更します。必要に応じて、ページ上部のナビゲーション リンクを使用します。

11. **［Start Configuration（構成の開始）］**をクリックします。
インスタンスの構成が完了すると、Security Console および Operations Console への直接リンクが表示されます。

次のステップ

- Authentication Manager の管理に使用する Web ブラウザでは、JavaScript を有効にする必要があります。JavaScript を有効にする手順については、ご使用の Web ブラウザのドキュメントを参照してください。
- Quick Setup が完了した後、Operations Console を使用して仮想アプライアンス ネットワーク設定を変更できます。変更により、VMware vSphere Client で行われたネットワーク設定の変更は無効になります。

SSL 証明書の管理

SSL（Secure Sockets Layer）は、RSA Authentication Manager の管理とレプリケーションに使用する通信ポートに対してデフォルトで有効になっています。Authentication Manager インスタンスの導入時に、長期使用可能な SSL 証明書によって通信が保護されます。この証明書は導入環境ごとに一意で、内部 RSA 認証局（CA）によって署名されます。

この SSL 証明書は内部 RSA CA によって署名されるため、ブラウザによっては、デフォルトの証明書を確認できないとの警告メッセージが出される場合があります。これは予期された動作です。

続行するには、ブラウザで提供されている、信頼できないサイトへの接続を許可するオプションをクリックします。たとえば、ブラウザによっては、「危険性を理解した上で接続する」などのリンクをクリックするように求められる場合があります。

この警告メッセージが表示されるのを防ぐには、内部 RSA CA を、ブラウザが信頼するルート証明機関のリストに追加するか、証明書を、ブラウザが信頼する認証局によって署名された証明書に置き換える必要があります。

内部 RSA CA を、ブラウザが信頼するルート証明機関のリストに追加する手順については、ブラウザのマニュアルを参照してください。

コンソールへのログオン

この処理手順では、Security Console、Operations Console、Self-Service Console にアクセスする方法について説明します。

処理手順

1. サポートされる Web ブラウザを開いて、以下の表のいずれかの URL を入力します。各コンソールは複数の URL をサポートします。

コンソール	URL
Security Console	https:// ＜完全修飾ドメイン名＞ https:// ＜完全修飾ドメイン名＞ /sc https:// ＜完全修飾ドメイン名＞ :7004/console-ims
Operations Console	https:// ＜完全修飾ドメイン名＞ /oc https:// ＜完全修飾ドメイン名＞ :7072/operations-console
Self-Service Console	Web Tier がない場合： https:// ＜完全修飾ドメイン名＞ /ssc https:// ＜完全修飾ドメイン名＞ :7004/console-selfservice Web Tier がある場合： https:// ＜完全修飾仮想ホスト名＞ https:// ＜完全修飾仮想ホスト名＞ /ssc https:// ＜完全修飾仮想ホスト名＞ /console-selfservice ロードバランサのデフォルトポートを変更した場合： https:// ＜完全修飾仮想ホスト名＞ : ＜仮想ホストのポート＞ / https:// ＜完全修飾仮想ホスト名＞ : ＜仮想ホストのポート＞ /ssc https:// ＜完全修飾仮想ホスト名＞ : ＜仮想ホストのポート＞ /console-selfservice

たとえば、アプライアンスの完全修飾ドメイン名が「host.mycompany.com」である場合に Security Console にアクセスするには、次の URL のいずれかを Web ブラウザに入力します。

https://host.mycompany.com

https://host.mycompany.com/sc

https://host.mycompany.com:7004/console-ims

2. Web ブラウザでセキュリティ レベルを高に設定している場合は、許可サイトまたは信頼済みサイトのリストにエントリーを追加する必要があります。許可サイトまたは信頼済みサイトの追加については、お使いのブラウザのドキュメントを参照してください。

3. Security Console にアクセスするには、Quick Setup の実行中に指定したスーパー管理者のユーザー ID とパスワードを入力します。Operations Console にアクセスするには、Quick Setup の実行中に指定した Operations Console 管理者のユーザー ID とパスワードを入力します。

   コンソールのアカウントとパスワードについて、詳細は 73 ページの「管理者アカウント」を参照してください。

   重要：Security Console は、初回起動が完了するまでに最大で 10 分かかる場合があります。

3 レプリカ アプライアンスの導入

導入タスクの実行

仮想アプライアンスを導入し、RSA Authentication Manager のレプリカ インスタンスを構成するには次のステップを実行します。

処理手順

1. レプリカ パッケージ ファイルの生成およびダウンロード
2. Quick Setup でアプライアンスを構成します。Quick Setup は、アクセス権限を作成し、アプライアンスがプライマリ インスタンスまたはレプリカ インスタンスのどちらかを指定するソフトウェア ウィザードです。レプリカ インスタンスでの Quick Setup の実行を参照してください。
3. レプリカ インスタンスをプライマリ インスタンスにアタッチする

レプリカ パッケージ ファイルの生成およびダウンロード

レプリカ インスタンスを導入環境に追加する前に、プライマリ インスタンスでレプリカ パッケージ ファイルを作成する必要があります。このファイルには、レプリカ インスタンスがプライマリ インスタンスに接続するための構成データが含まれています。レプリカ インスタンスはこのファイルにアクセスできる必要があります。

開始する前に

Operations Console 管理者である必要があります。

処理手順

1. プライマリ インスタンスで、Operations Console にログオンします。
2. **[Deployment Configuration（導入環境の構成）]** > **[Instances（インスタンス）]** > **[Generate Replica Package（レプリカ パッケージの生成）]** の順にクリックします。
3. **[Download（ダウンロード）]** をクリックしてレプリカ パッケージ ファイルをダウンロードし、**[Save（保存）]** をクリックしてローカル マシンにレプリカ パッケージを保存します。レプリカ パッケージ ファイルの名前は、「**replica_package.zip**」です。
4. **[Done（終了）]** をクリックして、Operations Console ホーム ページに戻ります。

レプリカ インスタンスでの Quick Setup の実行

Quick Setup で以下のタスクを実行し、導入環境にレプリカ アプライアンスを追加します。

- Quick Setup は RSA Authentication Appliance を RSA Authentication Manager レプリカ インスタンスとして構成します。
- Quick Setup はレプリカ インスタンスをプライマリ インスタンスにアタッチします。

Quick Setup がレプリカ インスタンスを構成した後、以下のいずれかのオプションを選択できます。

- レプリカ インスタンスを直ちにプライマリ インスタンスにアタッチする。
- レプリカ インスタンスのアタッチを延期する。

レプリカ インスタンスのアタッチの延期を選択した場合、Quick Setup はレプリカ インスタンスをパワーオフします。次回レプリカ インスタンスをパワーオンしたときに、Quick Setup にアクセスしてアタッチ処理を完了できます。

ベスト プラクティスとして、Quick Setup が完了するまでは、RSA Authentication Appliance を信頼できるネットワークに接続した状態にすることを推奨します。Quick Setup を実行するクライアント コンピュータおよびブラウザも、信頼できるネットワーク上に接続する必要があります。

Quick Setup を完了していない場合、VMware vSphere Client で仮想マシンをパワーオンするたびに仮想アプライアンスのネットワーク設定を確認するよう求められます。

開始する前に

- 仮想アプライアンスを導入します。手順については、23 ページの「VMware vCenter を使用した仮想アプライアンスの導入」または 25 ページの「VMware ESXi への仮想アプライアンスの直接導入」を参照してください。
- セットアップする レプリカ インスタンスに関して必要な情報を収集します。18 ページの「レプリカ インスタンスの導入チェックリスト」を参照してください。
- 33 ページの「レプリカ パッケージ ファイルの生成およびダウンロード」。

処理手順

1. ローカルマシンで、仮想アプライアンスの導入の終了時に表示される URL にアクセスし、Quick Setup を起動します。
2. Web ブラウザでセキュリティ レベルを高に設定している場合は、この URL が許可サイトまたは信頼済みサイトのリストにないことを知らせる警告が表示されます。続行するには、ブラウザに表示されているオプションをクリックし、信頼できないサイトへの接続を許可します。たとえば、ブラウザが、「I Understand the Risks.（危険性を理解した上で接続する）」というリンクをクリックするよう求める可能性があります。
3. ［Primary and Replica Quick Setup（プライマリおよびレプリカの Quick Setup）］ウィンドウで、**［Start Replica Quick Setup（レプリカの Quick Setup の開始）］**をクリックします。
4. ［Replica Quick Setup（レプリカの Quick Setup）］ページで、**［Start Step 1（ステップ 1 の開始）］**をクリックします。
5. ［Date & Time settings（日付と時刻設定）］ページで、次の操作を実行します。
   a. ［Region（地域）］を選択します（例：アメリカ）。
   b. ［Location（場所）］を選択します。夏時間を採用するタイムゾーンの場合、UTC（協定世界時）からの 2 つのオフセットが表示されます（例：（UTC-05/UTC-04）New York）。
   c. 仮想アプライアンスの時刻を、VMware ホストまたは NTP サーバのどちらと同期するかを選択します。
   d. ローカルまたはインターネット上の NTP サーバのホスト名または IP アドレスを入力します。
      2 台目の NTP サーバ アドレスを指定することもできます。アプライアンスは、リストの先頭にある NTP サーバから日付と時刻を取得します。Quick Setup が NTP サーバに接続できない場合は、Quick Setup が完了した後、Operations Console から NTP サーバを追加できます。

      重要：レプリケーション環境では、NTP サーバが必須です。すべての Authentication Manager インスタンスの時刻が同一の NTP サーバと同期している必要があります。

   e. NTP サーバへの接続をテストし、時刻が正確であることを確認するには、**［Preview Current Date & Time（現在の日付と時刻の確認）］**をクリックします。
   f. **［Next（次へ）］**をクリックします。
6. オペレーティング システム パスワードの作成と確認を行い、**［Next（次へ）］**をクリックします。

   注：オペレーティング システムのパスワードは、レプリカ インスタンスにログオンするために必要です。

今後の使用に備えてオペレーティング システム パスワードを記録します。セキュリティ上の理由から、RSA はオペレーティング システムのパスワードをリカバリするユーティリティを提供しません。

7. 入力した情報を確認します。いずれかの情報を変更する場合は、[**Back (戻る)**] をクリックして、該当するページを変更します。必要に応じて、ページ上部のナビゲーション リンクを使用します。
8. [**Start Configuration（構成の開始）**] をクリックします。
   インスタンスを構成した後、次のいずれかを実行します。
   - [**Begin Attach（アタッチの開始）**] をクリックして、レプリカ インスタンスをプライマリ インスタンスにアタッチします。詳細については、36 ページの「レプリカ インスタンスをプライマリ インスタンスにアタッチする」を参照してください。
   - [**Defer Attach（アタッチの延期）**] をクリックして、別の機会にレプリカ インスタンスをアタッチします。プロンプトが表示されたら、選択を確定します。レプリカ インスタンスがパワーオフされます。次回レプリカ インスタンスをパワーオンしたときに、レプリカ インスタンスをアタッチできます。

次のステップ

- 38 ページの「レプリカのアタッチの問題と解決方法」。

レプリカ インスタンスをプライマリ インスタンスにアタッチする

プライマリ インスタンスにレプリカ インスタンスをアタッチすると、レプリカ インスタンスがプライマリ インスタンスとデータを同期できるようになります。レプリカ インスタンスはすべての認証をローカルに記録し、認証とログ データを一定の間隔でプライマリ インスタンスに送信します。プライマリ インスタンスが使用不可の場合、レプリカ インスタンスは、プライマリ インスタンスが使用可能になるまでこのデータをローカルに保持します。

重要：レプリカ インスタンスは、アタッチ処理の間はユーザーの認証を行えません。

インスタンスは、データベースを安全に同期するために、暗号化されたリンク上で TCP/IP プロトコルを使用して通信します。インスタンスは、LAN（ローカル エリア ネットワーク）または WAN（ワイド エリア ネットワーク）を介して通信できます。

開始する前に

次のことを確認します。

- プライマリ インスタンスでレプリカ パッケージ ファイルを生成し、ローカル マシンにダウンロード済みであること。一般的な手順については、33 ページの「レプリカ パッケージ ファイルの生成およびダウンロード」を参照してください。
- プライマリ インスタンスとレプリカ インスタンスは、相互に名前解決が可能であり、次のポートで相互に接続可能であること。
  - 7002/TCP
  - 1812/TCP
  - 1813/TCP

注：ポート 1812 と 1813 は RSA RADIUS によって使用されます。RSA RADIUS を使用する予定がない場合でも、アタッチが成功するには、これらのポートをネットワークで（たとえば、プライマリ インスタンスとレプリカ インスタンスの間にあるファイアウォールなどで）開いておく必要があります。

- RSA RADIUS サービスがプライマリ インスタンスで実行されていること。RADIUS を使用する予定がない場合でも、レプリカのアタッチが成功するには、サービスが実行されている必要があります。
- プライマリ インスタンスとレプリカ インスタンスの時刻が同期していること。時刻のずれが 10 分を超える場合は、アタッチが失敗します。
- Quick Setup でレプリカ インスタンスを構成した後にアタッチの実施を延期していた場合は、レプリカ インスタンスの電源を入れた後に Quick Setup にアクセスします。Quick Setup は［Attach to Primary Instance（プライマリ インスタンスにアタッチ）］ページから再開します。

手順

1. ［Attach to Primary Instance（プライマリ インスタンスにアタッチ）］ページの［**Upload Replica Package（レプリカ パッケージのアップロード）**］で、［**Browse（参照）**］をクリックして、ローカル マシンからアップロードするレプリカ パッケージ ファイルを選択します。［**Next（次へ）**］をクリックします。
2. ［**Provide Credentials（クレデンシャルの提示）**］で、Operations Console 管理者のユーザー ID とパスワードを入力し、［**Next（次へ）**］をクリックします。

次のステップ

- レプリカ インスタンスのレプリケーション ステータス レポートを表示してレプリケーション ステータスを確認します。レプリカ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Instances（インスタンス）**］＞［**Status Report（ステータス レポート）**］の順にクリックします。

- RSA RADIUS を使用している場合、RADIUS サーバのレプリケーション ステータスを検証します。レプリカ インスタンスの Security Console で、［**RADIUS**］＞［**RADIUS Servers（RADIUS サーバ）**］の順にクリックします。
- Security Console または Operations Console のアクセスに使用する Web ブラウザの JavaScript が有効であることを確認します。JavaScript を有効にする手順については、ご使用の Web ブラウザのマニュアルを参照してください。
- レプリカ インスタンスがプライマリ インスタンスにアタッチされた後は、VMware vSphere Client で行われたネットワーク設定の変更は無効になります。レプリカ インスタンスの Operations Console を使用してネットワーク設定を変更します。

レプリカのアタッチの問題と解決方法

レプリカのアタッチの実行中に追加の情報を要求された場合、次の表のタスクを実行します。

問題	解決方法
レプリカ インスタンスがプライマリ インスタンスのホスト名を解決できない。	［**Associated Primary IP Address（関連づけるプライマリ IP アドレス）**］フィールドに、プライマリ インスタンス IP アドレスを入力し、［**Next（次へ）**］をクリックします。
レプリカ インスタンスがプライマリ インスタンスに到達できない。	［**Retry Options（再試行オプション）**］フィールドで、プライマリ インスタンス IP アドレスを修正します。以下のいずれかのオプションを選択してください。 • ネットワーク接続の問題を解決してから、プライマリ インスタンスへのアクセスを再試行します。 • ［**Override IP Address（IP アドレスの上書き）**］フィールドを選択し、プライマリ インスタンスの正しい IP アドレスを入力します。この情報はこの仮想アプライアンスの hosts ファイルに保存され、DNS サーバが使用できる場合は DNS 構成を上書きします。 ［**Next（次へ）**］をクリックし、Operations Console 管理者のクレデンシャルを入力します。

問題	解決方法
プライマリ インスタンスがレプリカ インスタンスのホスト名を解決できない	1. DNS サーバを更新します。または、プライマリ インスタンスのOperations Console を使用して、hosts ファイルを編集し、レプリカ インスタンスの正しい情報を記述します。 詳細については、Operations Console ヘルプのトピック「仮想アプライアンスの hosts ファイルの編集」を参照してください。 2. **［Next（次へ）］**をクリックします。
レプリカ インスタンスがプライマリ インスタンスの RADIUS ポートと通信できない。	プライマリ インスタンス上で RSA RADIUS サービスが実行中であることを確認します。以下の手順を実行します。 1. プライマリ インスタンスでOperations Console にログオンします。 2. **［Deployment Configuration（導入環境の構成）］＞［RADIUS Servers（RADIUS サーバ）］**の順に選択します。 3. プロンプトが表示されたら、スーパー管理者のユーザー ID とパスワードを入力します。 4. 再起動するサーバをクリックします。 5. コンテキスト メニューで**［Restart Server（サーバの再起動）］**を選択します。 6. **［Yes, restart RADIUS server（はい、RADIUS サーバを再起動します）］**を選択し、**［Restart Server（サーバの再起動）］**をクリックします。 1 分以内に、RSA RADIUS サービスが開始します。 7. ネットワーク構成で、ポート 1812/TCP および 1813/TCP 経由のリモート接続が許可されていることを確認します。 8. **［Next（次へ）］**をクリックします。
プライマリ インスタンスが通信ポート 7002/TCP、RADIUS ポート 1812/TCP、1813/TCP 経由でレプリカ インスタンスと通信できない。	1. ネットワーク構成で、通信ポート 7002/TCP、RADIUS ポート 1812/TCP、1813/TCP 経由のリモート接続が許可されていることを確認します。 2. **［Next（次へ）］**をクリックします。

問題	解決方法
プライマリ インスタンスとレプリカ インスタンス間の時間差が 10 分以上の場合、レプリカのアタッチに失敗する。	時間を変更できます。 プライマリ インスタンス側では、Operations Console にログオンし、［**Administration（管理）**］＞［**Date & Time（日付と時刻）**］の順に選択します。 レプリカ インスタンス側では、正しい時間を設定しレプリカ インスタンスを再導入します。以下の手順を実行します。 1. プライマリ インスタンスのOperations Console から、障害が発生したレプリカ インスタンスを削除します。手順については、RSA Operations Console ヘルプのトピック「レプリカ インスタンスの削除」を参照してください。 2. VMware vCenter または VMware ESXi 上で、障害が発生したレプリカ インスタンスの仮想アプライアンスをシャットダウンおよび削除します。 3. 新しいレプリカ インスタンスを導入します。

4 仮想ホストとロードバランサの構成

仮想ホストとロードバランサの概要

仮想ホストとは、外部ネットワークから RBA（リスク ベース認証）、Self-Service Console、動的シード配布を使用するユーザーのための DMZ へのゲートウェイです。仮想ホストを構成し、各 Web Tier に仮想ホストを割り当てる必要があります。

ロード バランシングにより Web Tier トラフィックを Web Tier サーバ間に分散させることができます。これを実現するため、Web Tier 導入環境にロードバランサを含めることができます。または、ラウンドロビン DNS を使用できます。仮想ホストは最大 2 台のロードバランサに関連づけることができます。

ロードバランサを必要とするネットワーク構成の詳細については、「設計ガイド」を参照してください。

ロードバランサの要件

ロードバランサが以下の要件を満たしている必要があります。

セッション維持機能。ロードバランサは、セッション中のクライアントを、同一のサーバに繰り返し接続させる必要があります。ロードバランサは、1 つの認証セッション中は、クライアントを同一の Authentication Manager インスタンスまたは Web Tier サーバ（導入シナリオによる）に接続させる必要があります。

X-Forwarded-For ヘッダ。アプリケーション レイヤーのロードバランサは、すべてのリクエストがロードバランサから送信されているように見せます。ロードバランサが、元のクライアント IP アドレスを「X-Forwarded-For」ヘッダに含めて送信するように構成する必要があります。この構成は、ほとんどのアプリケーション レイヤーのロードバランサにおいてデフォルトの構成です。

必要な機能に加えて、以下の点を考慮します。

HTTPS リダイレクト。ロードバランサは HTTPS リクエストを別の URL にリダイレクトできる必要があります。これにより、ユーザーはロードバランサのホスト名を使用して Self-Service Console にアクセスできます。

ロードバランサと仮想ホストの構成

ロードバランサを追加する場合、仮想ホスト名、IP アドレス、リスニング ポートを構成する必要があります。ロードバランサは、DMZ（非武装地帯）へのエントリー ポイントを提供する仮想ホストとして機能します。Web Tier をインストールする前に仮想ホストを構成する必要があります。

導入環境にロードバランサがある場合、仮想ホスト名はロードバランサのパブリック IP アドレスに解決される必要があります。

導入環境にロードバランサがない場合、仮想ホスト名は Web Tier のパブリック IP アドレスに解決される必要があります。

ロードバランサの名前を変更する場合、または別のロードバランサを使用する場合、それに応じて仮想ホスト名を変更する必要があります。

開始する前に

- スーパー管理者である必要があります。
- 仮想ホスト名が、ロードバランサをポイントするよう DNS（ドメイン名システム）を構成する必要があります。

手順

1. プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Virtual Host & Load Balancing（仮想ホストとロード バランシング）**］の順にクリックします。
2. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力します。
3. ［Virtual Host & Load Balancing（仮想ホストとロード バランシング）］ページで、以下の操作を実行します。
   a. ［**Configure a virtual host and load balancers（仮想ホストとロードバランサを構成する）**］を選択します。
   b. 仮想ホスト名として、導入環境で一意の完全修飾ホスト名を入力します。
   c. （オプション）デフォルトのポート番号を変更します。
   d. 最大 2 つのロードバランサ IP アドレスを入力します。ロードバランサを使用しない場合は、IP アドレスは空白のままにします。
   e. ［**Add（追加）**］をクリックします。
4. ［**Save（保存）**］をクリックします。
   システムは仮想ホスト名およびキー指定要素をキーストア ファイルに保存します。
5. 確認ページで、［**Mandatory Next Steps（次の必須ステップ）**］を読みます。
6. ［**Done（終了）**］をクリックします。

次のステップ

Operations Console で、適切な次の必須ステップを実行します。

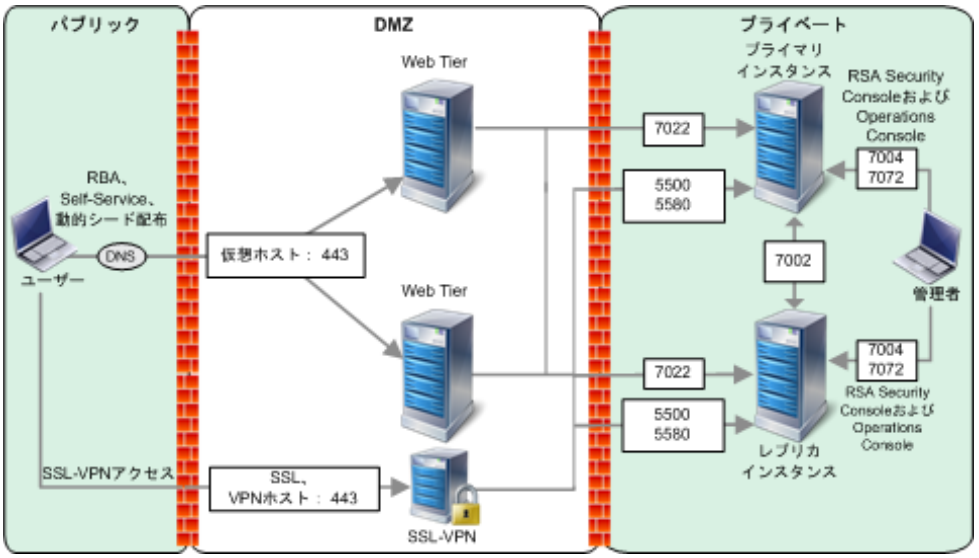
- ロードバランサの詳細を更新した場合、プライマリ インスタンスとレプリカ インスタンスをリブートする必要があります。Operations Console で、［**Maintenance（保守）**］＞［**Reboot Appliance（アプライアンスのリブート）**］の順にクリックして、各インスタンスをリブートします。
- 仮想ホスト名を更新した場合は、RBA を使用する各 Web ベース アプリケーション用に新しい統合スクリプトを生成し、統合スクリプトを再導入します。詳細については、「管理者ガイド」を参照してください。
- 導入環境に Web Tier が含まれる場合は Web Tier を更新します。Operations Console で、［**Deployment Configuration**（導入環境の構成）］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックします。各 Web Tier で更新リンクをクリックします。
- 導入環境に Web Tier が含まれる場合、ロードバランサとファイアウォールにある証明書を仮想ホストの証明書で置換します。
- 導入環境で動的シード配布を使用する場合、CT-KIP URL のホスト名とポートを、仮想ホストのホスト名とポートに更新します。Security Console で、［**Setup（セットアップ）**］＞［**System Settings（システム設定）**］の順にクリックします。［**Tokens（トークン）**］をクリックします。
- 導入環境で RSA Self-Service Console を使用する場合、Self-Service Console URL を仮想ホストのホスト名とポートに更新します。Security Console で、［**Setup（セットアップ）**］＞［**Self-Service Settings（セルフ サービス設定）**］の順にクリックします。［**E-Mail Notifications for User Account Changes（ユーザー アカウント変更のメール通知）**］をクリックします。

Web Tier とラウンドロビン DNS を使用したロード バランシング

ロードバランサを使用しない場合、ラウンド ロビン DNS（ドメイン名システム）を使用して、Web Tier サーバ間に RBA（リスク ベース認証）リクエストを負荷分散させるよう構成できます。

ラウンドロビン DNS によるロード バランシングを実現する場合は、DNS の構成で、仮想ホスト名に Web Tier サーバのパブリックからアクセス可能な IP アドレスを割り当て、ラウンド ロビンを有効にします。これにより、DNS サーバによって、RBA リクエストを複数の Web Tier サーバに送信できるようになります。

次の図では、ラウンドロビン DNS によるロード バランシングを使用した Authentication Manager の導入環境の例を示しています。



5 Web Tier のインストール

Web Tier の概要

Web Tier は、Self-Service Console、動的シード配布、RBA（リスク ベース認証）サービスをインストールおよび導入するための信頼性の高いプラットフォームです。

Web Tier は、企業のプライベート ネットワークの手前でインバウンド インターネット トラフィックを受信および管理し、プライベート ネットワークを保護します。これにより、Self-Service Console や Web ベース アプリケーション（SSL-VPN、シン クライアント、Web ポータルなど）を使用するエンド ユーザーがプライベート ネットワークにアクセスするのを防ぎます。Web Tier サーバは、認証トラフィックなどのトラフィックのサブセットのみを安全にプライベート ネットワークに送信します。

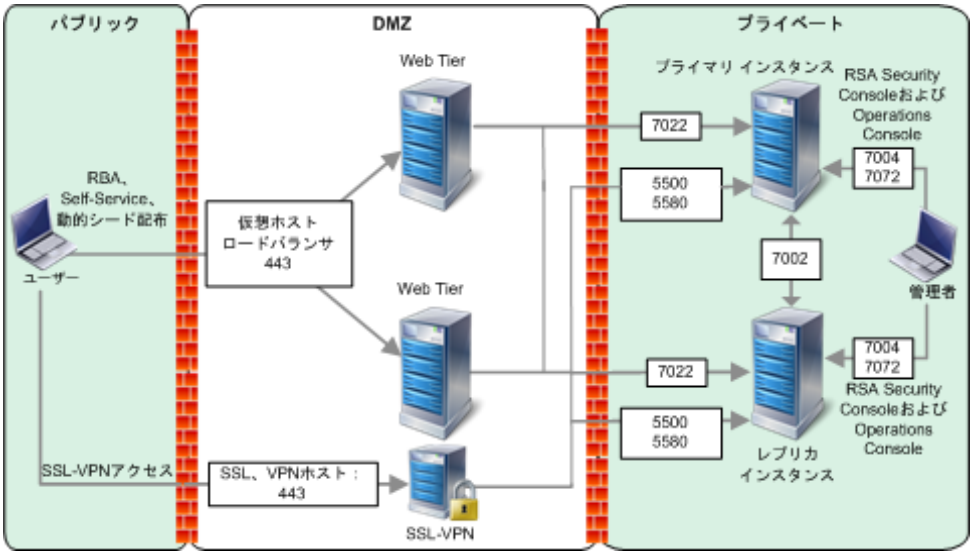
ネットワーク セキュリティの提供に加えて、DMZ（非武装地帯）内の Web Tier サーバ上に Authentication Manager を導入すると、次のような利点があります。

- RBA サービスや Web ベース アプリケーションのエンド ユーザー インタフェースをカスタマイズできます。
- 一部のタスク処理をバックエンド サーバから切り離すことにより、システム パフォーマンスが向上します。

Web Tier をインストールするにはプライマリ インスタンスが必要です。プライベート ネットワークに少なくとも 1 つの Authentication Manager レプリカ インスタンスを配置し、DMZ にロードバランサと複数の Web Tier サーバを配置するのが理想的な構成です。1 つのインスタンスは最大 16 個の Web Tier を持つことができます。Authentication Manager および Web Tier サーバを管理するには、スーパー管理者の権限が必要です。

Web Tier は必須ではありませんが、導入環境によっては、ネットワークの構成や要件を満たすために必須となる場合があります。Authentication Manager の導入タイプの詳細については、「設計ガイド」を参照してください。

次の図は、一般的な Web Tier の導入環境のトラフィック フローとポートを示しています。

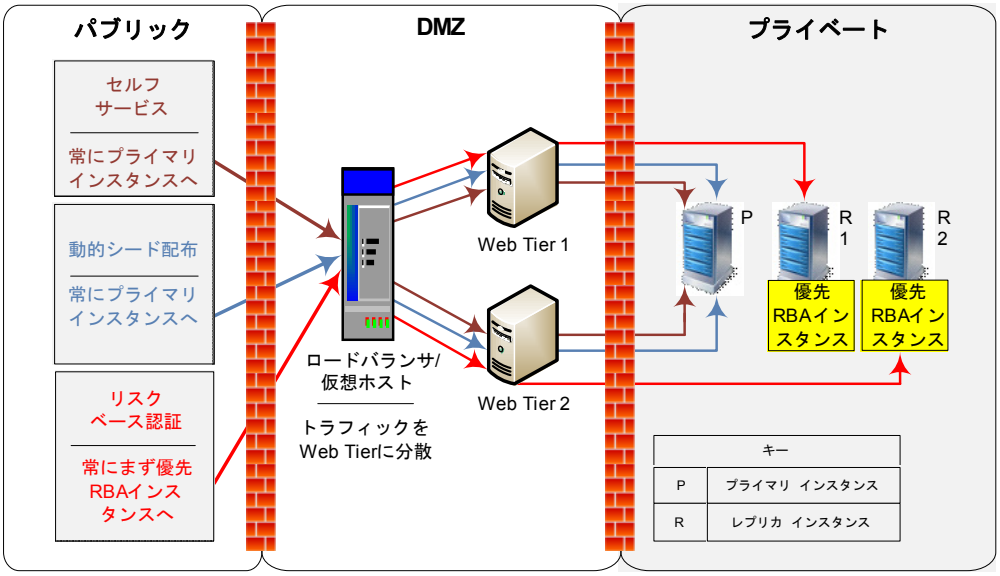


Web Tier を経由したセルフサービス、動的シード配布、RBA のトラフィック

Authentication Manager では、セルフサービスおよび動的シード配布サービスはプライマリ インスタンス上でのみ実行できるため、これらのトラフィックはプライマリ インスタンスに送信されます。RBA サービスは任意のインスタンスで実行できますが、負荷分散のため、Web Tier は常に RBA トラフィックを優先 RBA インスタンスに送信します。

優先 RBA インスタンスとは、Web Tier が RBA トラフィックを送信する最初のインスタンスのことです。Web Tier を導入する時に、優先 RBA インスタンスを選択する必要があります。RSA では、各 Web Tier に対して異なる優先 RBA インスタンスを選択することを推奨します。優先 RBA インスタンスとして、任意の Authentication Manager インスタンスを選択できます。

次の図に、Web Tier を経由したセルフ サービス、動的シード配布、RBA のトラフィックのフローを示します。



優先 RBA インスタンスが使用できない場合、Web Tier は RBA トラフィックをサーバ リスト上の次のインスタンスに送信します。

優先 RBA インスタンスに指定されたレプリカを削除する場合、指定した Web Tier も削除されることに注意してください。削除された Web Tier を介した RBA トラフィック フローが停止します。導入環境にロードバランサおよび仮想ホストがある場合、それらが削除されたレプリカや Web Tier を参照していないことを確認します。

Web Tier のハードウェアとオペレーティング システムの要件

次の表は、Web Tier サーバの最小要件を示しています。RSA では、予想される使用率に基づき要件を上方修正することを推奨します。

説明	要件
ハードウェア	• ハード ディスク ドライブ：2 GB（Web Tier インストール用） • ハード ディスク ドライブ：4 GB-20 GB の空きスペース（ログおよび更新されたコンポーネントのダウンロード用） • RAM：2 GB
ポート	外部ファイアウォール：443 HTTPS（TCP） DMZ：443 HTTPS（TCP） 内部ファイアウォール：7022 T3S（TCP）
オペレーティング システム	• Red Hat Enterprise Linux 5 Server（64 ビット版） • Red Hat Enterprise Linux 6 Server（64 ビット版） • Windows Server 2008 R2（64 ビット版）

Web Tier プリインストール タスクの実行

Web Tier をインストールする前に、次のタスクを実行して Web Tier 環境をセットアップします。

処理手順

1. スーパー管理者の権限およびソフトウェアをインストールする権限を持っていることを確認します。
2. Operations Console へのアクセス権があることを確認します。
3. Linux システムの場合は、ローカル ユーザーのオープン可能ファイル数のハード制限が少なくとも 4,096 であることを確認します。
4. Web Tier サーバがハードウェアとオペレーティング システムの要件を満たしていることを確認します。詳細については、47 ページの「Web Tier のハードウェアとオペレーティング システムの要件」を参照してください。
5. ネットワークの DMZ 内で Web Tier サーバをセットアップします。
6. Web Tier サーバと、Web Tier を関連づけるインスタンス（プライマリまたはレプリカ）のシステム時刻のずれが 1 分以内であることを確認します。タイム ゾーンが同じである必要はありません。たとえば、Web Tier サーバの時刻を午前 7:00（GMT）、関連づけられるインスタンスの時刻を午前 9:00（GMT + 2）に設定することができます。
7. 仮想ホストを構成します。仮想ホスト名として、ロードバランサのホスト名またはラウンド ロビン DNS（ドメイン名システム）を使用することができます。手順については、第 4 章、仮想ホストとロードバランサの構成。を参照してください
8. （オプション）仮想ホストで、デフォルトの証明書を置き換えます。手順については、「管理者ガイド」を参照してください。
9. ロードバランサおよびファイアウォールで、証明書を仮想ホストの証明書に置き換えます。手順については、お使いのロードバランサおよびファイアウォールのドキュメントを参照してください。

Web Tier のインストール

以下の処理手順は、プライマリ インスタンスに関連づける Web Tier をインストールするためのタスクを示しています。レプリカ インスタンスを Web Tier に関連づける前に、これらのタスクを実行する必要があります。

開始する前に

- 仮想ホストおよびロードバランサが構成されていることを確認します。
- 各 Web Tier の優先 RBA インスタンスを決定します。

処理手順

1. パブリックおよびプライベート DNS サーバに、Web Tier のホスト名と IP アドレスを追加します。
2. プライマリ インスタンスで、Web Tier 導入レコードを追加し、Web Tier 導入パッケージを作成します。操作手順については、50 ページの「Web Tier 導入レコードの追加」を参照してください。
3. Web Tier サーバで、ご使用のプラットフォームに応じた RSA Authentication Web Tier インストーラを実行します。手順については、以下を参照してください。
   52 ページの「グラフィカル ユーザー インタフェースを使用した Windows での Web Tier のインストール」。
   53 ページの「コマンド ラインを使用した Windows での Web Tier のインストール」。
   55 ページの「グラフィカル ユーザー インタフェースを使用した Linux での Web Tier のインストール」。
   57 ページの「コマンド ラインを使用した Linux での Web Tier のインストール」。
4. 導入環境で RSA Self-Service Console を使用する場合、Self-Service Console URL が仮想ホストのホスト名とポートを指すよう変更します。手順については、Security Console ヘルプのトピック「セルフサービス ユーザー アカウント変更のメール通知の構成」を参照してください。
5. 導入環境で動的シード配布を使用する場合、CT-KIP URL が仮想ホストのホスト名とポートを指すよう変更します。手順については、Security Console ヘルプのトピック「トークン設定の構成」を参照してください。

Web Tier 導入レコードの追加

Web Tier をインストールする前に、プライマリ インスタンスのデータベースに Web Tier 導入レコードが存在する必要があります。Web Tier 導入レコードにより、プライマリ インスタンスから Web Tier への通信が確立します。

インスタンスには最大 16 個の Web Tier を追加できます。各 Web Tier に、Web Tier 導入レコードが必要です。

この手順の最終ステップで、今すぐ Web Tier 導入パッケージを生成するか、後日生成するかを選択できます。Web Tier 導入パッケージには、Web Tier を関連インスタンスに接続するために RSA Authentication Manager が使用する情報が含まれています。Web Tier 導入パッケージは、Web Tier をインストールする前に生成する必要があります。Web Tier 導入パッケージを生成後、すぐに Web Tier をインストールできます。

開始する前に

- スーパー管理者である必要があります。
- 新しい Web Tier をインストールする場合、仮想ホスト名、リスニング ポート、ロードバランサを構成してください。一般的な手順については、ロードバランサと仮想ホストの構成を参照してください。

手順

1. プライマリ インスタンスの Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Add New（新規追加）**］の順にクリックします。
2. プロンプトに従って、スーパー管理者のユーザー ID とパスワードを入力します。
3. ［Add New Web-Tier Deployment（Web Tier 導入環境の新規追加）］ページにある［**Details（詳細）**］セクションで、次の情報を入力します。
   - **導入名**。Web Tier 導入環境の名前（0 ～ 255 文字。&、%、>、<、’、” の文字は使用不可）。
   - **ホスト名**。Web Tier をインストールする Web Tier サーバの完全修飾ホスト名。
   - **優先 RBA インスタンス**。この Web Tier に接続し、RBA（リスク ベース認証）トラフィックの宛先となるインスタンスです。
4. ［**Web-Tier Service Options（Web Tier サービス オプション）**］セクションで、次のサービスをオンまたはオフにします。
   - Self-Service Console
   - リスク ベース認証
   - 動的シード配布

5. ［Virtual Host（仮想ホスト）］セクションで、次の情報を確認します。
   - **仮想ホスト名**。仮想ホストの完全修飾名を指定する必要があります。
   - **ポート番号**。デフォルトは、443。
6. 以下のいずれかの操作を実行します。
   - ［**Save（保存）**］をクリックします。システムは、関連するプライマリ インスタンスにあるデータベースにレコードを保存します。信頼証明書は、Web Tier 導入パッケージを生成すると更新されます。
   - ［**Save & Generate Web-Tier Package（保存して Web Tier パッケージを生成）**］をクリックします。［Generate Web-Tier Deployment Package（Web Tier 導入パッケージの生成）］画面が表示されます。

注：Web Tier のホスト名を解決できない場合、確認画面が表示されます。画面の指示に従います。

次のステップ

- この Web Tier 導入レコードの詳細を確認します。手順については、Operations Console ヘルプ トピック「View Web Tier Deployments（Web Tier 導入環境の表示）」を参照してください。
- Web Tier 導入パッケージを生成せずに Web Tier 導入レコードを保存することにした場合、Web Tier をインストールする前に Web Tier 導入パッケージを生成します。
- Web Tier をインストールします。

Web-Tier インストールのチェックリスト

RSA Authentication Manager には Windows および Linux 向けの Web Tier インストーラが含まれており、RSA Authentication Manager 8.0 – Virtual Appliance DVD に収録されています。Web Tier インストーラを起動する前に、次の点を確認します。

- Web Tier プリインストール タスクが完了している。
- Web Tier サーバがシステム要件を満たしている。
- パブリックおよびプライベート DNS サーバに、Web Tier サーバの IP アドレスが追加されている。
- Web Tier 導入パッケージを生成し、プライマリ インスタンスから Web Tier サーバに転送済みである。
- Web Tier を関連づける Authentication Manager インスタンスが稼働中である。
- 次の情報を把握している。
  - Web Tier ソフトウェアをインストールする場所およびディレクトリ名
  - Web Tier サーバの完全修飾ホスト名

  - Web Tier サーバのプライマリ NIC IP アドレス（IPv4）
  - Web Tier 導入パッケージの名前、保存場所、パスワード
  - Linux の場合、ローカル ユーザー名（root 以外）
- Web Tier 導入パッケージ内のホスト名がインストール先の Web Tier サーバのホスト名と一致している。
- Linux の場合、root 権限を持っている。

チェックリストの項目を確認した後、使用するインストーラを起動して Web Tier をインストールします。

- グラフィカル ユーザー インタフェースを使用した Windows での Web Tier のインストール
- コマンド ラインを使用した Windows での Web Tier のインストール
- グラフィカル ユーザー インタフェースを使用した Linux での Web Tier のインストール
- コマンド ラインを使用した Linux での Web Tier のインストール

グラフィカル ユーザー インタフェースを使用した Windows での Web Tier のインストール

Web Tier サーバで RSA Authentication Web Tier インストーラを実行します。インストールにより、動的シード配布、Self-Service Console、RBA（リスクベース認証）サービスがインストールされます。

パスとファイル名を指定するときは、英字と数字のみを使用してください。英語以外の 1 バイト文字および 2 バイト文字はサポートされていません。

開始する前に

- 51 ページの「Web-Tier インストールのチェックリスト」のタスクを完了します。
- RSA Authentication Manager 8.0 – Virtual Appliance DVD を挿入します。

処理手順

1. RSA Authentication Manager 8.0 – Virtual Appliance DVD で、**Webtier/windows-x86_64** に進み、**install_webtier.bat** を検索します。
2. 以下のいずれかの操作を実行します。
   - UAC（ユーザー アクセス制御）がオンになっている場合、**install_webtier.bat** を右クリックし、**[Run As Administrator（管理者として実行）]** を選択します。
   - UAC（ユーザー アクセス制御）がオフになっている場合、**install_webtier.bat** をダブル クリックします。
3. **[Welcome（ようこそ）]** 画面で、概要と操作方法を確認します。**[Next（次へ）]** をクリックします。

4. ［**License Agreement（使用許諾契約書）**］画面で、使用許諾契約書を確認して、［**Next**（次へ）］をクリックします。
5. ［**Installation Folder（インストール フォルダ）**］画面でインストール フォルダを指定して、［**Next**（次へ）］をクリックします。
6. ［**Choose Web-Tier Package File（Web Tier パッケージ ファイルの選択）**］画面で、次の手順を実行します。
   a. この Web Tier サーバを関連づけるインスタンスの **Web Tier パッケージ**を選択します。
   b. パスワードを入力します。
   c. ［**Next（次へ）**］をクリックします。
7. ［**Summary（サマリー）**］画面で、次のいずれかを実行します。
   - サマリーの内容が正しい場合は、［**Next（次へ）**］をクリックします。
   - サマリーの内容が正しくない場合は、［**Previous（前へ）**］をクリックして、情報を修正します。
8. ［**Installation Progress（インストール進行状況）**］画面で、進捗バーにインストールが完了したことが表示されるまで待ち、［**Next**（次へ）］をクリックします。
9. ［**Run Configuration（構成の実行）**］画面で構成が完了するまで待ち、［**Next**（次へ）］をクリックします。
10. ［**Installation Summary（インストール サマリー）**］画面で、［**Done（終了）**］をクリックします。

次のステップ

Web Tier インストーラを終了した後、Web Tier Update Service がプライマリ サーバに接続し、必要なサービスをインストールします。この処理のステータスをチェックするには Operations Console を使用します。

Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックし、Web Tier インストールのステータスを参照します。

コマンド ラインを使用した Windows での Web Tier のインストール

Web Tier サーバで RSA Authentication Web Tier インストーラを実行します。インストールにより、動的シード配布、Self-Service Console、RBA（リスクベース認証）サービスがインストールされます。

パスとファイル名を指定するときは、英字と数字のみを使用してください。英語以外の 1 バイト文字および 2 バイト文字はサポートされていません。

開始する前に

51 ページの「Web-Tier インストールのチェックリスト」のタスクを完了します。

処理手順

1. Web Tier サーバ上で、**Webtier/windows-x86_64** に進み、コンソール モードで **install.bat** を起動します。
2. コマンド ラインで次のように入力して Enter キーを押します。

   ```
   install_webtier.bat -console
   ```

3. ［**Welcome（ようこそ）**］画面で、Enter キーを押します。
4. ［**License Agreement（使用許諾契約書）**］画面で、Enter キーを押して続行します。
5. 以降の［**License Agreement（使用許諾契約書）**］画面で、以下の操作を実行できます。
   a. 使用許諾契約書の次ページの内容を表示するには、Enter キーを押します。
      最終ページまで進んだら、使用許諾契約書の条項に同意する場合は、「**YES**」と入力し、Enter キーを押します。
   b. 使用許諾契約書の表示を終了するには「Q」と入力します。
      使用許諾契約書の条項に同意する場合は、「**YES**」と入力し、Enter キーを押します。
6. ［**Installation Folder（インストール フォルダ）**］画面で、インストール フォルダの場所を入力し、Enter キーを押します。
7. ［**Choose Web Tier Package（Web Tier パッケージの選択）**］画面で、次の手順を実行します。
   a. Web Tier パッケージの場所とファイル名を入力し、Enter キーを押します。
   b. Web Tier パッケージのパスワードを入力し、Enter キーを押します。
   c. Enter キーを押します。
8. ［**Summary（サマリー）**］画面でサマリーを確認し、次のいずれかを実行します。
   - サマリーの内容が正しい場合、続行するには「**1**」と入力して Enter キーを押します。
     インストールが開始し、インストールが正常に完了すると［**Finish（完了）**］画面が表示されます。
   - サマリーの内容が正しくない場合は、「**2**」を入力し、Enter キーを押して終了します。
     インストールは終了するため、再度インストールを開始する必要があります。
9. ［**Finish（完了）**］画面で、Enter キーを押して終了します。

次のステップ

Web Tier インストーラを終了した後、Web Tier Update Service がプライマリサーバに接続し、必要なサービスをインストールします。この処理のステータスをチェックするには Operations Console を使用します。

Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Web-Tier Deployments（Web Tier の導入）**] > [**Manage Existing（既存項目の管理）**] の順にクリックし、Web Tier インストールのステータスを参照します。

グラフィカル ユーザー インタフェースを使用した Linux での Web Tier のインストール

Web Tier サーバで RSA Authentication Web Tier インストーラを実行します。インストールにより、動的シード配布、Self-Service Console、RBA（リスクベース認証）サービスがインストールされます。

- パスとファイル名を指定するときは、英字と数字のみを使用してください。英語以外の 1 バイト文字および 2 バイト文字はサポートされていません。
- インストール ユーザーには、Web Tier をインストールするフォルダに対する実行権限が必要です。
- /root ディレクトリの下に Web Tier インストーラおよび Web Tier パッケージを保存しないでください。
- インストール パスにスペースを含めないでください。

開始する前に

- ローカル ユーザーのオープン可能ファイル数のハード制限が少なくとも 4,096 であることを確認します。
- 51 ページの「Web-Tier インストールのチェックリスト」のタスクを完了します。
- RSA Authentication Manager 8.0 – Virtual Appliance DVD を挿入します。

処理手順

1. root としてログオンします。
2. コマンド ラインで、ディレクトリを RSA Authentication Manager 8.0 – Virtual Appliance DVD に変更し、次のいずれかを実行します。
   - Red Hat Enterprise Linux 5 Server（64 ビット版）の場合は、次のように入力して Enter キーを押します。

     ```
     cd  Webtier/linux-x86_64
     ```

   - Red Hat Enterprise Linux 6 Server（64 ビット版）の場合は、次のように入力して Enter キーを押します。

     ```
     cd  Webtier/linux-x86_64
     ```

3. コマンド ラインで次のように入力して Enter キーを押します。

   ```
   ./install_webtier.sh
   ```

4. ［RSA Authentication Manager Web-Tier Installer（RSA Authentication Web Tier インストーラ）］画面で、［**Next（次へ）**］をクリックします。
5. ［**Welcome（ようこそ）**］画面で概要と操作方法を確認し、［**Next（次へ）**］をクリックします。
6. ［**License Agreement（使用許諾契約書）**］画面で、使用許諾契約書を読みます。条項に同意し、［**Next（次へ）**］をクリックします。
7. ［**Installation Folder（インストール フォルダ）**］画面でインストール フォルダを指定して、［**Next（次へ）**］をクリックします。
8. ［**Choose Web-Tier Package File（Web Tier パッケージ ファイルの選択）**］画面で、次の手順を実行します。
   a. この Web Tier サーバを関連づけるインスタンスの **Web Tier** パッケージを選択します。
   b. パスワードを入力します。
   c. ［**Next（次へ）**］をクリックします。
9. ［Install User（インストール ユーザー）］画面でローカル ユーザー名を入力して、［Next（**次へ**）］をクリックします。
10. ［**Summary（サマリー）**］画面で、次のいずれかを実行します。
    - サマリーの内容が正しい場合は、［**Next（次へ）**］をクリックします。
    - サマリーの内容が正しくない場合は、［**Previous（前へ）**］をクリックして、情報を修正します。
11. ［**Installation Progress（インストール進行状況）**］画面で、進捗バーにインストールが完了したことが表示されるまで待ち、［**Next（次へ）**］をクリックします。
12. ［**Run Configuration（構成の実行）**］画面で構成が完了するまで待ち、［**Next（次へ）**］をクリックします。
13. ［**Installation Summary（インストール サマリー）**］画面で、［**Done**（終了）］をクリックします。

次のステップ

Web Tier インストーラを終了した後、Web Tier Update Service がプライマリ サーバに接続し、必要なサービスをインストールします。この処理のステータスをチェックするには Operations Console を使用します。

Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックし、Web Tier インストールのステータスを確認します。

コマンド ラインを使用した Linux での Web Tier のインストール

Web Tier サーバで RSA Authentication Web Tier インストーラを実行します。インストールにより、動的シード配布、Self-Service Console、RBA（リスクベース認証）サービスがインストールされます。

- パスとファイル名を指定するときは、英字と数字のみを使用してください。英語以外の 1 バイト文字および 2 バイト文字はサポートされていません。
- インストール ユーザーには、Web Tier をインストールするフォルダに対する実行権限が必要です。
- /root ディレクトリの下に Web Tier インストーラおよび Web Tier パッケージを保存しないでください。
- インストール パスにスペースを含めないでください。

開始する前に

- ローカル ユーザーのオープン可能ファイル数のハード制限が少なくとも 4,096 であることを確認します。
- 51 ページの「Web-Tier インストールのチェックリスト」のタスクを完了します。

処理手順

1. root としてログオンします。
2. コマンド ラインで、ディレクトリを *RSA Authentication Manager 8.0 – Virtual Appliance* DVD に変更し、次のいずれかを実行します。
   - Red Hat Enterprise Linux 5 Server（64 ビット版）の場合は、次のように入力して Enter キーを押します。

     ```
     cd  Webtier/linux-x86_64
     ```
   - Red Hat Enterprise Linux 6 Server（64 ビット版）の場合は、次のように入力して Enter キーを押します。

     ```
     cd  Webtier/linux-x86_64
     ```
3. コマンド ラインで次のように入力して Enter キーを押します。

   ```
   ./install_webtier.sh -console
   ```
4. **［Welcome（ようこそ）］**画面で、続行すには「**1**」を入力して Enter キーを押します。
5. **［License Agreement（使用許諾契約書）］**画面で、Enter キーを押して続行します。
6. 以降の**［License Agreement（使用許諾契約書）］**画面で、以下の操作を実行できます。
   - 使用許諾契約書の次ページの内容を表示するには、Enter キーを押します。

最終ページまで進んだら、使用許諾契約書の条項に同意する場合は、「**YES**」と入力し、Enter キーを押します。

- 使用許諾契約書の表示を終了するには「Q」と入力します。
  使用許諾契約書の条項に同意する場合は、「**YES**」と入力し、Enter キーを押します。

7. ［**Installation Folder（インストール フォルダ）**］画面で、次の手順を実行します。
   a. インストール フォルダの場所を入力します。
   b. Enter キーを押します。
8. ［**Choose Web Tier（Web Tier の選択）**］画面で、次の手順を実行します。
   a. Web Tier パッケージの場所とファイル名を入力し、Enter キーを押します。
   b. Web Tier パッケージのパスワードを入力し、Enter キーを押します。
   c. Enter キーを押します。
9. ［**Installation User（インストール ユーザー）**］画面で、次の手順を実行します。
   a. インストール ユーザーを入力し、Enter キーを押します。
   b. Enter キーを押します。
10. ［**Summary（サマリー）**］画面でサマリーを確認し、次のいずれかを実行します。
    a. サマリーの内容が正しい場合、続行するには「**1**」と入力して Enter キーを押します。
       インストールが開始し、インストールが正常に完了すると［**Finish（完了）**］画面が表示されます。
    b. サマリーの内容が正しくない場合は、「**2**」を入力し、Enter キーを押して終了します。
       インストールは終了するため、再度インストールを開始する必要があります。
11. ［**Finish（完了）**］画面で、Enter キーを押して終了します。

次のステップ

Web Tier インストーラを終了した後、Web Tier Update Service がプライマリ サーバに接続し、必要なサービスをインストールします。この処理のステータスをチェックするには Operations Console を使用します。

Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Web-Tier Deployments（Web Tier の導入）**］＞［**Manage Existing（既存項目の管理）**］の順にクリックし、Web Tier インストールのステータスを確認します。

6 導入環境の次のステップ

RSA Authentication Manager の導入後、必要な構成タスクを実行する必要があります。導入環境の要件に応じて、追加の構成タスクを実行してください。

トピック	説明	詳細情報
すべての導入環境に必要なステップ		
使用するポート	認証、管理、レプリケーション、その他のサービスがネットワーク上で問題なく稼働するよう、プライマリ インスタンスとレプリカ インスタンス、およびそれぞれの Web Tier サーバ上のポートがアクセスできることを確認します。	詳細については、付録 A、使用するポート。を参照してください
RSA Authentication Manager ユーザー アカウント	RSA Authentication Manager では、各ユーザーがアカウントを持っている必要があります。ユーザー アカウントを作成して内部データベースに格納するか、Authentication Manager を 1 つ以上の外部 LDAP（Lightweight Directory Access Protocol）ディレクトリに直接リンクすることができます。	内部データベースの使用方法の詳細については、「管理者ガイド」の「ユーザーの管理」の章を参照してください。 既存の LDAP ディレクトリの使用方法の詳細については、「管理者ガイド」の「LDAP ディレクトリの統合」の章を参照してください。
認証エージェント	認証エージェントは、RSA Authentication Manager と通信し、認証リクエストを処理する、保護対象リソース上のコンポーネントです。SecurID 認証、ODA（On-Demand 認証）、RBA（リスク ベース認証）を使用するリソースには、すべて認証エージェントが必要です。	RSA Authentication Agent のリストについては、「**http://japan.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm#!offerings**」にアクセスしてください。 RSA Authentication Agent が組み込まれたサードパーティ製品のリストについては、RSA Secured® の Web サイト「**https://gallery.emc.com/community/marketplace/rsa?view=overview**」にアクセスしてください。

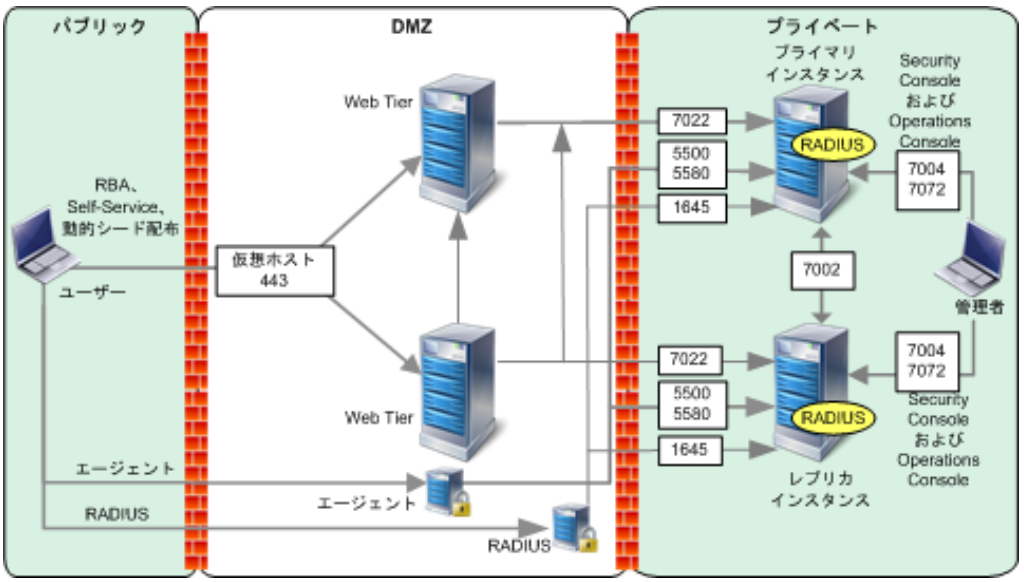
トピック	説明	詳細情報
RSA RADIUS 構成		
RSA RADIUS 構成	RADIUS で保護されたネットワークでは、RADIUS クライアントがネットワーク境界でユーザー アクセスを制御します。 RADIUS クライアント（VPN サーバ、ワイヤレス アクセス ポイント、ダイヤル イン モデムに接続されたネットワーク アクセス サーバ）が RSA RADIUS サーバと通信することにより、ユーザー認証が実行され、適切なアクセス制御パラメータが確立されます。 認証が成功すると、セッション制御のために属性のセットが RADIUS サーバから RADIUS クライアントへ返されます。	詳細については、「管理者ガイド」の「RSA RADIUS の管理」の章を参照してください。
認証方式の構成		
ハードウェア トークンおよびソフトウェア トークン	**ハードウェア トークン** RSA 製のデバイスで、トークンコードを生成して表示します。トークンコードは常に表示された状態で、たとえば 60 秒に 1 回のように、一定間隔で自動的に変化します。認証を行うためのパスコードを作成するには、このトークンコードをユーザーの PIN と組み合わせる必要があります。ハードウェア トークンには、PINPad、キー フォブ、USB トークンが含まれます。 **ソフトウェア トークン** RSA SecurID Software Token アプリケーションとともに、Windows デスクトップ / ラップトップ、Web ブラウザ、RSA Smart Card、モバイル デバイスなどにインストールされた、ソフトウェア ベースのセキュリティ トークンです。 ほとんどの場合、ソフトウェア トークンはユーザーに PIN の入力を要求するよう構成されています。ソフトウェア トークンはユーザーが入力した PIN とトークンコードを組み合わせ、認証を行うためのパスコードを表示します。	詳細については、「管理者ガイド」の「RSA SecurID トークンの導入と管理」の章を参照してください。
RBA（リスクベース認証）	RBA は、ユーザーの行動パターンやアクセスに使用するデバイスをユーザーに気づかせることなく分析することにより、潜在的なリスクや不正な認証試行を識別します。RBA は RSA SecurID 認証を強化します。	詳細については、「管理者ガイド」の「リスク ベース認証の導入」の章を参照してください。

トピック	説明	詳細情報
ODA（On-Demand 認証）	ODA は、メールまたはテキスト メッセージでユーザーに ワン タイム トークンコードを送信します。On-Demand トークンコードの提供方法を構成する必要があります。エージェントが保護対象リソースにすでに組み込まれている場合を除き、保護対象リソース上に RSA Authentication Agent ソフトウェアをインストールします。	詳細については、「管理者ガイド」の「On-Demand 認証の導入」の章を参照してください。
追加の導入ステップ		
セルフ サービスの構成	ユーザーが Self-Service Console を使用してユーザー情報の保守およびトラブルシューティング タスクを実行できるように RSA Authentication Manager を構成できます。	詳細については、「管理者ガイド」の「RSA セルフ サービス」の章を参照してください。
導入環境の保護	ネットワーク トポロジーや、使用する RSA Authentication Manager の機能によっては、安全な運用のために、追加のネットワーク構成や製品の構成が必要となる場合があります。 また、各 RSA Authentication Manager インスタンスには ClamAV（Clam Antivirus）ソフトウェアが含まれます。ClamAV は、侵入や悪意のあるコードによるシステムまたはデータへのアクセスに対するリスクを低減することを目的としたオープン ソース ソフトウェア ツールキットです。	詳細については、「Security Configuration Guide」を参照してください。

A 使用するポート

ポート トラフィック

次の図は、プライマリ インスタンスとレプリカ インスタンス、Web Tier、ロードバランサで構成された一般的な RSA Authentication Manager の導入環境を示しています。1 つの外部ファイアウォールがプライマリ インスタンスとレプリカ インスタンスを保護し、もう 1 つの外部ファイアウォールが DMZ を保護しています。RADIUS ポートの詳細については、63 ページの RSA Authentication Manager インスタンスが使用するポートを参照してください。



RSA Authentication Manager インスタンスが使用するポート

RSA Authentication Manager インスタンスには、特定のポートへのトラフィックを制限する内部ファイアウォールがあります。内部ファイアウォールは、ホストや製品の機能を提供するサービスへのインバウンド トラフィックを制限します。アウトバウンド トラフィックは制限されません。RSA では、外部ファイアウォールによって他のネットワークから分離されたサブネットにインスタンスを設置することを推奨します。

次の表は、Authentication Manager インスタンスが使用するポートを示しています。説明に IPv6 サポートが明記されている場合を除き、すべてのポートは IPv4 のみサポートしています。

ポート番号とプロトコル	機能	ソース	説明
22、TCP	SSH	SSH クライアント	デフォルトでは無効です。オペレーティング システム アカウント（rsaadmin）によるオペレーティング システムへのアクセスを許可します。
49、TCP	TACACS 認証	TACACS クライアント	NAD（Network Access Device）から認証リクエストを受信するために使用します。
80、TCP	Quick Setup	管理者のブラウザ	RSA Authentication Manager アプライアンスの Quick Setup の間のみ開きます。Quick Setup の完了後、アプライアンスはこのポートでリスンしません。
161、UDP	SNMP	SNMP クライアント	Authentication Manager SNMP エージェントが、GET リクエストをリスンし、NMS（Network Management System）にレスポンスを送信するために使用します。SNMP が有効でないかぎり、このポートは閉じられます。これは Security Console で構成できます。
443、TCP	Quick Setup Operations Console、Security Console、Self-Service Console	管理者のブラウザ	RSA Authentication Manager アプライアンスの Quick Setup に使用します。Quick Setup の完了後、アプライアンスはこのポートから適切なコンソールに接続をリダイレクトします。
1645、UDP	RADIUS 認証（レガシー ポート）	RADIUS クライアント	このポートは、RADIUS クライアントから認証リクエストを受信します。
1646、UDP	RADIUS アカウンティング（レガシー ポート）	RADIUS クライアント	このポートは、RADIUS クライアントからインバウンドのアカウンティング リクエストを受信します。

ポート番号とプロトコル	機能	ソース	説明
1812、TCP	RADIUS レプリケーションポート	他の RADIUS サーバ	このポートは、プライマリ RADIUS サービスとレプリカ RADIUS サービスの間の通信で使用されます。 RSA RADIUS を使用していなくても、導入環境にレプリカ インスタンスがある場合は、このポートを常に開いておく必要があります。詳細については、68 ページの RSA RADIUS Server のリスニングポート要件の項を参照してください。
1812、UDP	RADIUS 認証	RADIUS クライアント	このポートは、RADIUS クライアントから認証リクエストを受信します。 RSA RADIUS 認証を使用する計画がない場合は、このポートを閉じることができます。
1813、TCP	RADIUS 管理機能	RADIUS サーバ	このポートは、保護された RADIUS リモート管理チャネル経由で Security Console から RADIUS を管理するために使用します。 RSA RADIUS を使用していなくても、導入環境にレプリカ インスタンスがある場合は、このポートを常に開いておく必要があります。詳細については、68 ページの RSA RADIUS Server のリスニングポート要件を参照してください。
1813、UDP	RADIUS アカウンティング	RADIUS クライアント	このポートは、RADIUS クライアントからアカウンティング リクエストを受信します。 RSA RADIUS 認証を使用する計画がない場合は、このポートを閉じることができます。

ポート番号とプロトコル	機能	ソース	説明
5500、TCP	エージェント認証	RSA SecurID 認証プロトコルエージェント	TCP を使用する認証エージェントからのリクエストを受信し、返信します。RSA SecurID および ODA（On-Demand 認証）のために必要です。このポートは、IPv4 準拠エージェントと IPv6 準拠エージェントの両方をサポートしています。
5500、UDP	エージェント認証	RSA SecurID 認証プロトコルエージェント	UDP を使用する認証エージェントからのリクエストを受信し、返信します。RSA SecurID、ODA、RBA（リスク ベース認証）に必要です。このポートは、IPv4 準拠のエージェントのみサポートしています。
5550、TCP	Agent Auto-Registration	RSA エージェント	Authentication Manager への自動登録を試行する認証エージェントとの通信に使用します。
5580、TCP	オフライン認証サービス	RSA エージェント	エージェントからのオフライン認証データ追加要求の受信と、エージェントへのオフライン認証データの送信に使用します。エージェント上のサーバ リストの更新にも使用します。 導入環境でオフライン認証を使用しておらず、ログイン パスワード統合 API を使用するエージェントが存在しない場合は、閉じることができます。
7002、TCP SSL 暗号化	Authentication Manager	他のアプライアンス	Authentication Manager プライマリ インスタンスとレプリカ インスタンスの間の通信に使用します。 RSA API（Application Programming Interface）により使用されます。 レプリカ インスタンスが少なくとも 1 つある場合に有効化します。

ポート番号とプロトコル	機能	ソース	説明
7002、TCP SSL 暗号化	MMC（Microsoft Management Console）用の RSA Token Management スナップイン	Microsoft 管理コンソール	RSA Token Management スナップインを使用して MMC からユーザーおよびトークンを管理する場合は、このポートを有効化します。
7004、TCP SSL 暗号化	Security Console	管理者のブラウザ	Security Console を使用して導入環境を管理するために必要です。Security Console 機能に対するリクエストを受信します。
7004、TCP SSL 暗号化	Self-Service Console および RBA	ユーザーのブラウザ	Self-Service Console または RBA を使用するために必要です。Self-Service Console 機能と RBA 認証に対するリクエストを受信します。
7004、TCP SSL 暗号化	CT-KIP（Cryptographic Token-Key Initialization Protocol）	ユーザーのブラウザ	動的シード配布を使用するために必要です。
7022、TCP SSL 暗号化	トラステッドレルムのネットワーク アクセス ポイントまたは Web Tier。	トラステッドレルム、または Web Tier と他のアプライアンス	このポートは、トラステッド レルムまたは Web Tier がある場合にのみ有効化します。トラステッドレルムとの通信に使用します。アプライアンスとその Web Tier の間の通信を許可します。
7072、TCP SSL 暗号化	Operations Console	スーパー管理者のブラウザ	Operations Console から導入環境を管理するために必要です。Operations Console 機能に対する要求を受信します。
7082、TCP SSL 暗号化	RADIUS 構成 SSL	Authentication Manager インスタンス	Operations Console から RADIUS を構成したり、RADIUS サービスを再起動するために使用します。

RSA コンソールに対するアクセスの制限

Security Console（ポート 7004）および Operations Console（ポート 7072）へのアクセスは、社内管理者に限定する必要があります。ポート 7004 は Security Console、動的シード配布、Self-Service Console によって使用されますが、イントラネットの外から直接アクセスできないようにする必要があります。外部ユーザーによる Self-Service Console または動的シード配布サービスへのアクセスを許可する場合は、Web Tier を導入し、ポート 7004 を保護して Security Console へのアクセスを制限します。

RSA RADIUS Server のリスニングポート要件

RSA RADIUS は、RSA Authentication Manager を使用してインストールおよび構成します。Authentication Manager サーバ上のすべての RADIUS 関連ポート（1645、1646、1812、1813、7082）は、デフォルトで開かれています。

初期の RADIUS 標準では、RADIUS 認証パケットとアカウンティング パケットのために UDP ポート 1645 および 1646 を使用しました。その後、RADIUS 標準化グループは、ポートの割り当てを 1812 および 1813 に変更しました。Authentication Manager RADIUS サーバは、下位互換性のために、4 つのポートすべてでリスンします。すべての RADIUS クライアントが、ポート 1812 および 1813 でのみ RADIUS サーバと通信するように構成されている場合、外部ファイアウォールでレガシー ポート 1645 および 1646 をブロックする必要があります。

RSA RADIUS を使用する計画がなくても、導入環境にレプリカ インスタンスがある場合は、TCP ポート 1812 および 1813 を常に開いておく必要があります。これらのポートは、レプリカのアタッチ、レプリカの昇格、IP アドレスとホスト名の変更などのタスクを実行する時に使用されます。RADIUS 認証 UDP ポート 1812 および 1813 は閉じることができます。

レガシー トラステッド レルムのポートの考慮事項

RSA Authentication Manager 8.0 のトラステッド レルムは、63 ページの RSA Authentication Manager インスタンスが使用するポートでリストされているポートを使用して、RSA Authentication Manager 7.1 または 8.0 のトラステッド レルムと通信します。RSA Authentication Manager 6.1 のトラステッド レルムと通信するには、Authentication Manager 8.0 が認証に使用するポート範囲を構成する必要があります。このポート範囲は、Security Console を使用して構成します。デフォルトは以下のとおりです。

- ポート範囲 = 10 ポート
- 最小ポート = 10001
- 最大ポート = 10010

Authentication Manager 6.1 とのレガシー信頼関係が確立されている場合を除き、これらのポートは閉じられます。すべてのファイアウォールを、導入環境間のアクセスを許可するように構成する必要があります。

デフォルトの設定を変更して、パフォーマンスを改善したり、導入環境内の他のネットワーク サービスと共存させたりすることができます。たとえば、Authentication Manager 8.0 の多数のユーザーが、複数のレガシー トラステッド レルムとの間で同時に認証を行うのであれば、デフォルトの設定からポート範囲を増やすことを推奨します。

指定するポート数を決定するには、レガシー トラステッドレルムの数と、レガシー トラステッドレルムとの間で 5 秒間に標準的に予想される認証の回数を乗算します。たとえば、10 個のレガシー トラステッドレルムがあり、5 秒間に 2 回ずつ認証が発生すると予想される場合は、ポート範囲に 20 を指定します。

Security Console は、ポートがすでに使用中かどうか検証しません。そのため、任意の変更を加える前に、ポートが使用可能であることを確認する必要があります。ポート範囲を 10 未満に設定しないでください。レガシー レルムの場合、認証のために少なくとも 10 個のポートが必要です。

手順については、「Security Console Help」で「Configure Ports for Trusted Legacy Realm Authentication（レガシー トラステッド レルム認証用のポートの構成）」のトピックを参照してください。

ロードバランサ導入時の Web Tier 上のポート

次の表は、ロードバランサを使用する環境における Web Tier サーバ上のデフォルトのリスニング ポートを示しています。

ファイアウォールまたはプロキシ サーバを使用する環境の場合、Web Tier が、Authentication Manager の機能を提供するその他すべてのホストやサービスと通信できるよう、ファイアウォールまたはプロキシ サーバを設定する必要があります。そのようなホストやサービスは、表の「ソース」列に示されており、Authentication Manager アプライアンス、ロードバランサ、ブラウザが含まれます。

ポート番号とプロトコル	機能	ソース	ターゲット	説明
443、TCP	Self-Service Console、RBA（リスク ベース認証）、動的シード配布	ユーザーのブラウザ	プライマリ Web Tier ホスト名	Self-Service Console 機能、RBA 認証、動的シード配布へのリクエストを受信します。
443、TCP	RBA	ユーザーのブラウザ	ロードバランサ	仮想ホスト名を指定した、RBA 認証リクエストを受信します。
443、TCP	RBA	ロードバランサ	Web Tier 仮想ホスト名	仮想ホスト名を指定した、RBA 認証リクエストを受信します。

ロードバランサのない環境での Web Tier 上のポート

次の表は、ロードバランサを使用しない環境における Web Tier サーバ上のデフォルトのリスニング ポートを示しています。

ファイアウォールまたはプロキシ サーバを使用する環境の場合、Web Tier が、Authentication Manager の機能を提供するその他すべてのホストおよびサービスと通信できるよう、ファイアウォールまたはプロキシ サーバを設定する必要があります。そのようなホストおよびサービスは、表の「ソース」列に示されており、Authentication Manager アプライアンス、ロードバランサ、ブラウザが含まれます。

ポート番号とプロトコル	機能	ソース	ターゲット	説明
443、TCP	Self-Service Console、RBA（リスク ベース認証）、動的シード配布	ユーザーのブラウザ	プライマリ Web Tier ホスト名	Self-Service Console 機能、RBA 認証、動的シード配布に対するリクエストを受信します。
443、TCP	RBA	ユーザーのブラウザ	Web Tier 仮想ホスト名	RBA 認証に対するリクエストを受信します。

重要：レプリカ Web Tier ではポート 443 を常に開いておきます。

ファイアウォール経由のアクセス

RSA Authentication Manager のすべてのインスタンスを、外部ファイアウォールによって他のネットワークから分離されたサブネットにセットアップすることを推奨します。外部ファイアウォールを経由して認証を行う場合は、静的 NAT（Network Address Translation）に適合するため、Authentication Manager インスタンスのエイリアス IP アドレスと、認証エージェントの代替 IP アドレスを構成できます。次のものを割り当てることができます。

- Authentication Manager の各インスタンスには、4 つの異なる IP アドレス（元の IP アドレスと最大 3 つのエイリアス）を割り当てることができます。作業手順については、「Security Console Help」で「Add Alternative IP Addresses for Instances（インスタンスの代替 IP アドレスの追加）」のトピックを参照してください。
- エージェントには、代替 IP アドレスを無制限に（プライマリ IP アドレスは 1 つ）割り当てることが可能です。作業手順については、RSA Security Console ヘルプのトピック「Add an Authentication Agent（認証エージェントの追加）」を参照してください。

それぞれ異なる IP アドレスを、Authentication Manager インスタンスに割り当てる必要があります。すべての Authentication Manager インスタンスは、NAT によって隠蔽される場合でも、IP アドレスを共有することはできません。

各 Authentication Manager インスタンスのプライマリ IP アドレスとエイリアスを把握しておく必要があります。導入環境が複数の場所に分散している場合、Authentication Manager の通信や内部プロセスがどのポートを使用するか、把握しておく必要があります。環境に合わせてファイアウォールで新しいポートを開くか、既存のいくつかのポートを閉じる必要があります。ポート変換は、プライマリ インスタンスとレプリカ インスタンスが Authentication Manager の標準のポートで通信している場合にサポートされます。たとえば、プライマリ インスタンスとレプリカ インスタンスは、ポート 7002（TCP）で通信している必要があります。ポートの詳細については、63 ページのポート トラフィックを参照してください。

プライマリ インスタンスとレプリカ インスタンス間の接続の保護

Authentication Manager は、プライマリ インスタンス データベースとレプリカ インスタンス データベース間でデータを複製するために、ポート 7002 番を使用します。このチャネルを不正使用から保護するために、次のことを推奨します。

- 導入環境にレプリカがない場合、またはプライマリ インスタンスおよびレプリカ インスタンスが同じ LAN 上にある場合、外部ファイアウォール（アプライアンスのファイアウォールではありません）のポート 7002 番を閉じます。これにより、外部トラフィックがプライマリまたはレプリカ インスタンスまで届くことはありません。
- プライマリ アプライアンスとレプリカ アプライアンスが WAN 経由で接続され、その間にファイアウォールが存在する場合、ファイアウォールのポート 7002 番を開きます。ただし、プライマリおよびレプリカ インスタンスの IP アドレスから発信されたもののみが許可されるよう、このポート上のトラフィックを制限します。

B 管理者アカウント

システム管理者アカウント

次のアカウントは、AuthenticationManager 導入環境の変更、保守、修復を行う権限を持っています。これらのアカウントは Quick Setup 中に作成されます。

- Authentication Manager 管理者アカウント
- アプライアンス オペレーティング システム アカウント

これらのアカウントのログオン クレデンシャルを媒体に記録する場合は、保存方法と保存場所が安全であることを確認します。

Authentication Manager 管理者アカウント

次の表に、AuthenticationManager の管理者アカウントを示します。プライマリ インスタンスを導入する管理者が、Quick Setup 中にこれらのアカウントを作成します。

名前	権限の内容	管理
スーパー管理者	スーパー管理者は、導入環境内のすべてのセキュリティ ドメインで完全な管理者権限を持ち、Security Console 内のすべての管理タスクを実行できます。	すべてのスーパー管理者は、Security Console で他のスーパー管理者ユーザーを作成できます。 Operations Console 管理者は、すべてのスーパー管理者アカウントがシステムにアクセスできなくなった場合にいずれかのスーパー管理者アカウントを復旧できます。

名前	権限の内容	管理
Operations Console 管理者	Operations Console 管理者は Operations Console 内の管理タスクを実行できます。また、コマンド ライン ユーティリティを使用して、スーパー管理者アカウントの復旧などの処理を実行できます。コマンド ライン ユーティリティを使用するには、アプライアンス オペレーティング システム アカウントのパスワードが必要です。 **注：**Operations Console の一部のタスクの実行には、スーパー管理者のクレデンシャルも必要になります。Operations Console が許可するのは、ユーザーレコードが内部データベースに格納されたスーパー管理者のみです。	すべてのスーパー管理者は、Security Console で Operations Console 管理者を作成して管理できます。たとえば、紛失した Operations Console 管理者パスワードを復旧することはできませんが、スーパー管理者であれば新しいパスワードを作成できます。 Operations Console 管理者アカウントは、Authentication Manager 内部データベースの外に格納されます。そのため、データベースが接続不能になっても、Operations Console 管理者は引き続き Operations Console とコマンド ライン ユーティリティにアクセスできます。

スーパー管理者と非管理者ユーザーのユーザー ID は同じ規則で検証されます。有効なユーザー ID は一意の識別子でなければならず、1 ～ 255 文字の ASCII 文字を使用できます。&、%、>、<、' の各文字は使用できません。

Operations Console 管理者の有効なユーザー ID は一意の識別子でなければならず、1 ～ 255 文字の ASCII 文字を使用できます。@、~ の各文字とスペースは使用できません。

注：Operations Console を使用するユーザーごとに Operations Console 管理者アカウントを作成します。複数の管理者の間で、アカウント情報（特にパスワード）を共有しないでください。

アプライアンス オペレーティング システム アカウント

アプライアンス オペレーティング システム アカウントのユーザー ID は rsaadmin です。このユーザー ID は変更できません。オペレーティング システム アカウントのパスワードは、Quick Setup 中に指定します。このアカウントは、高度な保守またはトラブルシューティング タスクの実行時にオペレーティング システムにアクセスするために使用します。

すべてのアプライアンスには root ユーザー アカウントもあります。このアカウントは通常のタスクでは必要ありません。このアカウントを使用してアプライアンスにログオンすることはできません。

オペレーティング システムには、SSH（Secure Shell）または VMware vSphere Client を使用してアクセスできます。SSH でアプライアンス オペレーティング システムにアクセスするには、事前に Operations Console を使用してアプライアンスの SSH を有効化する必要があります。

Operations Console 管理者は、rsaadmin のパスワードを変更できます。

セキュリティ上の理由から、オペレーティング システム パスワードを復旧するためのユーティリティは提供していません。

スーパー管理者アカウントの管理

スーパー管理者のみがスーパー管理者アカウントを管理できます。

手順

1. Security Console で、**［Identity（アイデンティティ）］＞［Users（ユーザー）］＞［Manage Existing（既存項目の管理）］**の順にクリックします。
2. 検索フィールドを使用して、編集するユーザーを検索します。
3. 編集するユーザーをクリックして、**［Edit（編集）］**を選択します。
4. ユーザー設定を更新します。
5. **［Save（保存）］**をクリックします。

C RSA Authentication ManagerToken Management スナップインのインストール

概要

RSA Token Management スナップインは、Active Directory アイデンティティ ソースを持つ導入環境で、RSA SecurID トークンを管理するための便利な方法を提供します。RSA Token Management スナップインは、MMC（Microsoft Management Console）の「Active Directory ユーザーとコンピュータ」スナップインのコンテキスト メニュー、プロパティ ページ、コントロール バー、ツールバーを拡張します。RSA Token Management スナップインを使用すると、トークンの有効化または無効化、トークンの割り当て、その他のトークン関連タスクを Security Console にログオンすることなく実行できます。この拡張機能によって有効になる管理アクションの詳細については、「管理者ガイド」を参照してください。

システム要件

RSAToken Management スナップインは次のプラットフォームにインストールできます。

- Windows Server 2008 R2 ドメイン コントローラ
- AD DS（Active Directory ドメイン サービス）スナップインおよびコマンド ライン ツール
  がインストールされた Windows Server 2008 R2 Server
- AD DS スナップインおよびコマンド ライン ツールがインストールされた Windows Server 2008 Server
- AD DS スナップインおよびコマンド ライン ツールがインストールされた Windows 7

ローカル アクセス環境での Token Management スナップインのインストール

Active Directory がインストールされているホストで直接 Token Management スナップインを使用して Authentication Manager を管理する場合、この処理手順を使用します。

開始する前に

管理者権限が必要です。ドメイン レベルなど、これらの権限は、Windows のネットワーク構成によって異なります。少なくともドメイン管理者およびローカル マシンの管理者である必要があります。

処理手順

1. RSA Token Management スナップインのインストール ファイルを取得します。インストール ファイルは RSA Authentication Manager 8.0 – Token Management Snap-In for MMC.zip ファイルに含まれます。このファイルは RSA SecurCare Online からダウンロードできます。
2. スナップインをインストールするマシン上のディレクトリにすべてのインストール ファイルを解凍します。
3. 以下のいずれかの操作を実行します。
   - 32 ビット オペレーティング システムの場合は、**setup32.exe** を実行します。
   - 64 ビット オペレーティング システムの場合は、**setup64.exe** を実行します。

   注：まだ Visual C++ 再頒布可能パッケージと Microsoft .NET Framework がインストールされてない場合は、インストーラがそれらもインストールします。
4. **［Welcome（ようこそ）］**、**［Select Region（地域の選択）］**、**［License Agreement（使用許諾契約書）］**のプロンプトに応答します。
5. Authentication Manager サーバ設定について、次の値を入力します。
   - Authentication Manager サーバ ホスト名
   - Authentication Manager サーバ ポート番号
   - Authentication Manager コマンド サーバ ポート
6. **［Destination Location（インストール場所）］**を入力するプロンプトが表示されたら、デフォルトの場所をそのまま指定するか、代替の場所を入力します。
7. ［Pre-installation（プリインストール）］画面を確認し、**［Next（次へ）］**をクリックして続行します。
8. **［Finish（完了）］**をクリックします。

リモート アクセス環境での Token Management スナップインのインストール

Active Directory がインストールされていない Windows 7 または Windows Server 2008 から Token Management スナップインをリモートで使用して Authentication Manager を管理する場合、この処理手順を使用します。

AD DS（Active Directory ドメイン サービス）スナップインおよびコマンド ライン ツールはリモート サーバ管理ツールの一部であり、Windows Server 2008 R2、Windows Server 2008、Windows 7 マシンから Active Directory ドメイン コントローラをリモートで管理する場合に使用します。

Windows 7 の場合、リモート サーバ管理ツールを使用してリモート管理を実行できます。このツール パッケージは別途ダウンロードしてインストールする必要があります。また、Windows 7（32 ビットおよび 64 ビット）にのみインストールできます。

Windows 2008 では、リモート サーバ管理ツールの機能はオペレーティング システムの一部であり、サーバーマネージャーから追加することができます。

リモート サーバ管理ツールのインストール後に、AD DS スナップインおよびコマンド ライン ツールを有効にできます。

開始する前に

- Windows 7 の場合、Microsoft Web サイトからリモート サーバ管理ツール パッケージをダウンロードしてインストールします。
- 適切な権限を持っている必要があります。ドメイン レベルなど、これらの権限は、Windows のネットワーク構成によって異なります。少なくともドメイン管理者およびローカル マシンの管理者である必要があります。
- 管理者は AD DS スナップインおよびコマンド ライン ツールを使用してリモートで Active Directory を管理するために、適切な管理者権限を持っている必要があります。ドメイン レベルなど、これらの権限は、Windows のネットワーク構成によって異なります。

処理手順

1. リモート サーバ管理ツールの **AD DS** スナップインおよびコマンド ライン ツールの機能を有効にします。
2. RSA Token Management スナップインのインストール ファイルを取得します。インストール ファイルは RSA Authentication Manager 8.0 – Token Management Snap-In for MMC.zip ファイルに含まれます。このファイルは RSA SecurCare Online からダウンロードできます。
3. スナップインをインストールするマシン上のディレクトリにすべてのインストール ファイルを解凍します。

4. 以下のいずれかの操作を実行します。
   - 32 ビット オペレーティング システムの場合は、**setup32.exe** を実行します。
   - 64 ビット オペレーティング システムの場合は、**setup64.exe** を実行します。
5. **［Welcome（ようこそ）］**、**［Select Region（地域の選択）］**、**［License Agreement（使用許諾契約書）］**のプロンプトに応答します。
6. Authentication Manager サーバ設定について、次の値を入力します。
   - Authentication Manager サーバ ホスト名
   - Authentication Manager サーバ ポート番号
   - Authentication Manager コマンド サーバ ポート
7. **［Destination Location（インストール場所）］**を入力するプロンプトが表示されたら、デフォルトの場所をそのまま指定するか、代替の場所を入力します。
8. ［Pre-installation（プリインストール）］画面を確認し、**［Next（次へ）］**をクリックして続行します。
9. **［Finish（完了）］**をクリックします。

インストール後タスクの実行

正常にインストールが完了したら、次のタスクを実行して MMC 拡張機能の構成を完了します。

処理手順

1. Authentication Manager のセットアップが完了し、実行中であることを確認します。
2. Active Directory が、アイデンティティ ソースとして構成されていることを確認します。詳細については、「管理者ガイド」の「LDAP ディレクトリの統合」の章を参照してください。
3. 「Active Directory ユーザーとコンピュータ」管理コンソールの起動の後、RSA Token Management スナップインを開きます。
4. Authentication Manager との接続の構成
5. Token Management スナップインを使用する Windows ユーザーが、有効な Active Directory 管理者であり、かつ有効な Authentication Manager 管理者ユーザーであることを確認します。管理者と管理者権限の詳細については、「管理者ガイド」で「RSA Authentication Manager による管理の準備」の章を参照してください。

「Active Directory ユーザーとコンピュータ」管理コンソールの起動

Token Management スナップインを使用して Authentication Manager を管理するには、「Active Directory ユーザーとコンピュータ」管理コンソールを起動する必要があります。

開始する前に

インストール後タスクの実行に記述された先行ステップをすべて実行します。

処理手順

以下のいずれかの操作を実行します。

- **［Control Panel（コントロール パネル）］＞［Administrative Tools（管理ツール）］＞［Active Directory Users and Computers（Active Directory ユーザーとコンピュータ）］**の順にクリックします。
- コマンド プロンプトから **dsa.msc** を実行します。

Authentication Manager との接続の構成

Token Management スナップインから Authentication Manager サーバにアクセスするには、サーバ情報および認証情報などの接続設定を行う必要があります。

開始する前に

インストール後タスクの実行に記述された先行ステップをすべて実行します。

処理手順

1. 「Active Directory ユーザーとコンピュータ」管理コンソールにアクセスします。
2. 任意のユーザーをクリックします。これにより、RSA ボタンがツールバーに表示されます。
3. ツールバーの［**RSA**］をクリックします。
   ［RSA Token Management Setting（RSA トークン管理設定）］ページが表示されます。
4. **［Server Information（サーバ情報）］**セクションで、次の操作を実行します。
   a. **［AM Server Host（AM サーバ ホスト）］**フィールドに、RSA Authentication Manager が実行中のマシンの名前を入力します。
   b. **［AM Server port（AM サーバ ポート）］**フィールドに、RSA Authentication Manager が実行中のポート番号を入力します。
   c. **［Command Server Port（コマンド サーバ ポート）］**フィールドに、Authentication Manager サーバ上でコマンド サーバが実行中のポート番号を入力します。

5. ［**Authentication Information（認証情報）**］セクションで、次の操作を実行します。

   a. ユーザーのユーザー **ID** タイプを選択します。

      ［**Login User（ログイン ユーザー）**］フィールドに表示されるユーザー名の形式は、選択したユーザー ID タイプに基づいています。

      重要：ユーザー ID タイプは、Authentication Manager 側でこのアイデンティティ ソースに対して定義したユーザー ID タイプと同一である必要があります。
      このユーザーは Active Directory のドメイン管理者グループのメンバーである必要があり、同時に Authentication Manager のスーパー管理者である必要があります。

   b. ［**User Password（ユーザー パスワード）**］フィールドに、ユーザーのパスワードを入力します。

   c. ［**Test Authentication（テスト認証）**］をクリックして、テスト認証を実行します。
      複数のアイデンティティ ソースにユーザー ID が存在する場合、アイデンティティ ソースを選択してテストできます。選択したアイデンティティ ソースが［**Identity Source Name（アイデンティティ ソース名）**］フィールドに表示されます。証明書を今後の通信でも使用するか確認のプロンプトが表示されたら、［yes（はい）］をクリックします。

用語集

Active Directory

Microsoft Windows Server 2003 SP2、Microsoft Windows Server 2008、Microsoft Windows Server 2008 R2 に搭載されているディレクトリ サービス。

Active Directory フォレスト

Windows Server 環境で使用する認証サーバの集合体。すべての認証サーバで、共通のスキーマ、構成、グローバル カタログが使用されます。

CLU（コマンド ライン ユーティリティ）

コマンド ライン ユーザー インタフェースを提供するユーティリティ。

CT-KIP（Cryptographic Token-Key Initialization Protocol）

ソフトウェア トークンの安全な初期化と構成のためのクライアント サーバ プロトコル。このプロトコルでは、トークン内の秘密鍵機能および確立された公開鍵基盤のどちらも必要ありません。プロトコルが正常に実行されると、サーバとトークンの両方で、同じ共有シークレットが生成されます。

DMZ（非武装地帯）

2 つのファイアウォールの間に構成されるネットワークの領域。

DMZ

「DMZ（非武装地帯）」を参照してください。

On-Demand トークンコード

SMS または SMTP により配布されるトークンコード。ユーザーに PIN の入力を要求することにより、2 要素認証を実現します。On-Demand トークンコードはユーザー始動のコードで、Authentication Manager はユーザー要求を受け取った場合のみユーザーにトークンコードを送信します。On-Demand トークンコードは一度だけ使用できます。管理者が On-Demand トークンコードの有効期間を構成します。「On-Demand トークンコード サービス」を参照してください。

On-Demand トークンコード サービス

有効化されたユーザーがトークンの代わりにテキスト メッセージまたはメールでトークンコードを受信できるサービス。On-Demand トークンコード サービスの構成とユーザーの有効化は、Security Console で行います。

Operations Console

ユーザーが Authentication Manager の構成や設定（アイデンティティ ソースの追加と管理、インスタンスの追加と管理、災害復旧など）を行う管理ユーザー インタフェース。

RADIUS

「RADIUS（Remote Authentication Dial-In User Service）」を参照してください。

RADIUS（Remote Authentication Dial-In User Service）

ネットワークへのリモート アクセスを管理および保護するためのプロトコル。RADIUS サーバは、VPN などの RADIUS クライアントからユーザー アクセス リクエストを受信します。

RBA

「RBA（リスクベース認証）」を参照してください。

RBA（リスクベース認証）

保護対象のリソースへのアクセスを許可する前に、ユーザーのプロファイル、認証履歴、認証デバイスを分析する認証方式。

RBA 統合スクリプト

Web ベース アプリケーションのデフォルト ログオン ページからカスタマイズされたログオン ページにユーザーをリダイレクトするスクリプト。これにより、Authentication Manager は、リスク ベース認証を使用してユーザーを認証できます。統合スクリプトを作成するには、統合スクリプトのテンプレートが必要です。

Request Approver

ユーザーからのアカウント登録、トークン、ユーザー グループ メンバーシップのリクエストを許可する権限を付与する、事前定義された管理者ロール。

Security Console

日常的な管理作業の大半を実行するために使用する管理ユーザー インタフェース。

Self-Service Console

ユーザー プロファイルの更新、Self-Service Console のパスワードの変更、セキュリティ クエスチョンの設定、リスク ベース認証で登録したデバイスのクリア、On-Demand トークン用の電子メール アドレスまたは電話番号の変更、On-Demand トークンの PIN の管理などを行う、エンドユーザー向けのユーザー インタフェース。エンドユーザーは、Self-Service Console からトークンのリクエスト、保守、トラブルシューティングも実行できる。

SSL

「SSL（Secure Socket Layer）」を参照してください。

SSL（Secure Socket Layer）

暗号化を使用してインターネット経由のセキュア通信を可能にするプロトコル。SSL は主要な Web ブラウザや Web サーバで広くサポートされています。

Trace ログ

トレース情報を永続的に記録したもの。

UDP

「UDP（User Datagram Protocol）」を参照してください。

UDP（User Datagram Protocol）

データグラムと呼ばれる短いメッセージを送信することで、ネットワーク コンピュータのプログラム同士が通信できるようにするプロトコル。

Web Tier

Web Tier は、DMZ に Self-Service Console、動的シード配布サービスおよび RBA（リスク ベース認証）サービスをインストールおよび導入するためのプラットフォームです。Web Tier は、企業のプライベート ネットワークの手前でエンド ユーザーからのインバウンド インターネット トラフィックを受信および管理し、プライベート ネットワークが直接アクセスされるのを防ぎます。

アイデンティティ ソース

ユーザーおよびユーザー グループのデータが保存されているデータストア。内部データベースまたは外部ディレクトリ サーバ（Microsoft Active Directory など）を使用できます。

アイデンティティ属性

カスタム定義の属性。常にユーザーまたはユーザー グループのコア属性データと同じ物理リポジトリに保存されます。これらの属性で検索、クエリ、レポートを実行できます。各アイデンティティ属性定義は、LDAP ディレクトリの既存の属性にマッピングする必要があります。

アプライアンス

RSA Authentication Manager がインストールされている仮想アプライアンス。アプライアンスは、プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。

委譲管理

管理者の権限の集合とそれらの適用範囲を定義するためのスキーム。管理者が一部の権限を別の管理者に委譲することを許可します。

インスタンス

RSA Authentication Manager の単一のインストール。プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。1 つのインスタンスには、1 つの RADIUS サーバも含まれます。

エージェント ホスト

エージェントがインストールされたマシン。

下位のセキュリティ ドメイン

セキュリティ ドメインの階層において、他のセキュリティ ドメインの下にネストされたセキュリティ ドメイン。

鍵ストア

鍵と証明書を保管するための機能。

カスタム属性

ユーザーが Authentication Manager に作成する属性です。LDAP ディレクトリのフィールドにマッピングされます。たとえば、ユーザーの部署を表すカスタム属性を作成できます。

仮想アプライアンス

Authentication Manager がインストールされている仮想マシン。仮想アプライアンスは、プライマリ インスタンスまたはレプリカ インスタンスとしてセットアップできます。

仮想ホスト

仮想マシンがインストールされている物理コンピュータ。仮想ホストは、Web ベースのアプリケーション、Web Tier、Web Tier に関連づけられたプライマリ インスタンスとレプリカ インスタンスの間のトラフィックを管理するのに役立ちます。

仮想ホスト名

パブリックにアクセス可能なホスト名。エンド ユーザーは Web Tier 経由で認証を受ける場合、この仮想ホスト名にアクセスします。また、仮想ホスト名に基づいて SSL 情報が生成されます。仮想ホスト名は、ロードバランサのホスト名と同じにする必要があります。

監査情報

システムのイベントやアクティビティ（ポリシーや構成の変更、認証、承認など）の履歴を示す監査ログに含まれているデータ。

監査ログ

システムのイベントやアクティビティを記録したシステム生成ファイル。システムには Trace ログ、Administrative ログ、Runtime Audit ログ、System ログと呼ばれる 4 つのファイルがあります。

管理者

システムを管理するための管理者権限を付与する管理者ロールを 1 つ以上割り当てられたユーザー。

管理者ロール

権限の集合とそれらの権限が適用される範囲。

許可

リソースに対する操作をユーザーに許可するかどうかを判別するプロセス。

グローバル カタログ

レプリケートされた読み取り専用のリポジトリであり、Active Directory フォレストにある全エントリーの属性のサブセットが格納されます。

グローバル カタログ アイデンティティ ソース

Active Directory グローバル カタログと関連づけられているアイデンティティ ソース。このアイデンティティ ソースは、ユーザーの検索と認証、フォレスト内のグループ メンバーシップの解決に使用されます。

権限

管理者が実行できるタスクを指定します。

権限適用範囲

導入環境内で、ロールの権限が適用されるセキュリティ ドメイン。

コア属性

すべての RSA 製品でユーザーの作成に共通して利用される固定の属性セット。導入環境が LDAP か内部データベースかに関係なく、これらの属性は常にプライマリ ユーザー レコードの一部となります。コア属性を非表示にすることはできませんが、委譲には利用できます。

固定パスコード

ユーザーがアクセス権を得るために PIN およびトークンコードの代わりに入力します。パスワードに似ています。固定パスコードの形式は、セキュリティ ドメインに割り当てられたトークン ポリシーで定義されます。管理者は、各ユーザーの認証設定ページで固定パスコードを作成します。固定パスコードには英数字を使用できます。トークン ポリシーによっては、特殊文字を含めることができる場合があります。

最上位のセキュリティ ドメイン

最上位のセキュリティ ドメインは、セキュリティ ドメイン階層における 1 番目のセキュリティ ドメインです。1 つまたは複数のアイデンティティ ソースにリンクし、導入環境全体のパスワード ポリシー、ロックアウト ポリシー、認証ポリシーを管理するという点で、他のセキュリティ ドメインとは異なります。

最低保証レベル

「保証レベル」を参照してください。

サイレント収集

リスクベース認証において、各ユーザーのプロファイル、認証履歴、認証デバイスに関するデータを、ログオン時にユーザー確認をすることなく、サイレントに収集する期間。

システム イベント

システムが生成するイベントのうち、製品の機能に関するもの以外のイベント（サーバの起動とシャットダウン、フェイルオーバー イベント、レプリケーション イベントなど）。

システム ログ

システム イベントを永続的に記録したもの。

昇格

レプリカ インスタンスを新しいプライマリ インスタンスにするための構成処理。昇格処理により、元のプライマリ インスタンスは導入環境からデタッチされます。元のプライマリ インスタンスを参照しているすべての構成データは、新しいプライマリ インスタンスから削除されます。

承認者

Request Approver、つまり承認者の権限を持つ管理者。

証明書

秘密鍵に対応する非対称公開鍵。証明書には自己署名または別の証明書の秘密鍵で署名します。

証明書 DN

認証用にユーザーに発行される証明書の識別名。

除外単語辞書

ユーザーのパスワードに使用できない単語を記録した辞書。除外単語辞書を使用すると、一般的で容易に推測される単語をパスワードとして使用できなくなります。

信頼パッケージ

導入環境に関する構成情報が含まれている XML ファイル。

スーパー管理者

Security Console 内のすべての管理タスクを実行する権限を持つ管理者。スーパー管理者には次の権限があります。

- アイデンティティ ソースのシステムへのリンク
- 1 つの導入環境におけるすべての権限
- 1 つの導入環境における管理者ロールの割り当て

セキュリティ クエスチョン

ユーザーが標準的な方法を使用せずに認証を行えるようにする方法。このサービスを利用するには、ユーザーは複数のセキュリティ クエスチョンに回答し、あらかじめ回答を登録しておく必要があります。このサービスを使用して認証を行う時は、元々回答していた質問のすべてまたは一部に正しく回答する必要があります。

セキュリティ ドメイン

一般にビジネスユニット、部門、取引先などの単位に応じて、管理運営の責任領域を定義するコンテナ。セキュリティ ドメインはシステム内のオブジェクト（ユーザー、ロール、権限など）の所有権やネームスペースを構築します。セキュリティ ドメインは階層構造になっています。

セッション

ユーザーとソフトウェア アプリケーションのやり取りに関するデータを含むアプリケーションとユーザーが行う対話。ユーザーがソフトウェア アプリケーションにログオンするとセッションが開始され、ログオフすると終了します。

セルフ サービス

ユーザー プロファイルの更新、Self-Service Console のパスワードの変更、セキュリティ クエスチョンの設定、リスク ベース認証で登録したデバイスのクリア、On-Demand トークン用の電子メール アドレスまたは電話番号の変更、On-Demand トークンの PIN の管理などを行う、エンドユーザー向けの Authentication Manager のコンポーネント。エンドユーザーは、トークンのリクエスト、保守、トラブルシューティングも実行できる。

送付先住所

配布者がハードウェア トークンを送付する住所。

属性

状態、外見、値、または何らかの設定を定義する特性。Authentication Manager では、属性とはユーザーおよびユーザー グループに関連づけられた値を指します。たとえば、各ユーザー グループには 3 つの標準的な属性（「名前」、「アイデンティティ ソース」、「セキュリティ ドメイン」）があります。

属性のマッピング

User ID や Last Name などのユーザーまたはユーザー グループの属性を、システムにリンクされた 1 つ以上のアイデンティティ ソースと関連づけるプロセス。内部データベースをプライマリ アイデンティティ ソースとして使用する導入環境では、属性のマッピングは不要です。

タイムアウト

指定した時間が経過するまでにユーザーがデスクトップ上で何も操作を行わないと再認証が要求されます（秒単位）。

データストア

リレーショナル データベース（Oracle や DB2）またはディレクトリ サーバ（Microsoft Active Directory または Oracle Directory Server）などのデータ ソース。データ ソースのタイプごとに別々にデータを管理したり、データにアクセスします。

デバイス登録

リスクベース認証において、認証に使用したデバイスをユーザーのデバイス履歴に保存するプロセス。

デバイス履歴

リスクベース認証の場合、システムが各ユーザーのデバイス履歴を保持します。デバイス履歴には、保護対象のリソースへのアクセスに使用したデバイスの情報が含まれます。

電子メール テンプレート

管理者がユーザーの要求（アカウント登録、トークン、ユーザー グループ メンバーシップ、On-Demand トークンコード サービス）に関する電子メール通知をカスタマイズする際に使用できるテンプレート。「メール通知」を参照してください。

動的シード配布

Web ブラウザなどのソフトウェア トークンをホストするデバイスに、CT-KIP（Cryptographic Token-Key Initialization Protocol）を使用してトークン ファイルを提供するために必要なすべてのステップの自動化。

導入環境

1 つのプライマリ インスタンスと、オプションで 1 つ以上のレプリカ インスタンスで構成される、Authentication Manager のインストール環境。

トークン

Authentication Manager で本人確認に使用するデバイス。ハードウェア トークン（キー フォブなど）またはソフトウェア トークンがあります。

トークン プロビジョニング

アカウント登録、ユーザー グループ メンバーシップ、RSA SecurID トークン、On-Demand トークンコード サービスをユーザーに提供するために必要な全ステップを自動化したもの。「セルフ サービス」も参照してください。

トークン配布者

ユーザーからのトークン リクエストを処理する権限を付与する、事前定義された管理者ロール。配布者は、ユーザーにどのようにトークンを配布してリクエストを完了する予定かを記録します。

トラステッド レルム

トラステッド レルムとは、別のレルムと信頼関係にあるレルムのことです。トラステッド レルムのユーザーは、別のレルムで認証を受け、別のレルムのリソースにアクセスすることができます。2 つ以上のレルムが存在すれば、信頼関係を持つことができます。信頼関係は一方向でも双方向でも可能です。

内部データベース

Authentication Manager 独自のデータ ソース。

認証

ユーザーまたはプロセスが確かにそのユーザーまたはプロセスであるということを確実に判別するプロセス。

認証エージェント

ドメイン サーバ、Web サーバ、デスクトップ コンピュータなどのデバイスにインストールされ、ネットワーク上の Authentication Manager との認証通信を行うソフトウェア アプリケーション。「エージェント ホスト」を参照してください。

認証サーバ

認証リクエスト処理、データベース操作、Security Console への接続を提供するサービスで構成されるコンポーネント。

認証プロトコル

認証時にユーザーのクレデンシャルを転送するために使用される規則（HTTP-BASIC/DIGEST、NTLM、Kerberos、SPNEGO など）。

認証方式

ワンステップ認証、マルチ オプション認証（ユーザー名やパスワードなど）、チェーン認証などの認証要求手続きの種類。

ノード シークレット

認証要求時にエージェントがデータの暗号化に使用する長寿命の対称鍵。ノード シークレットは Authentication Manager とエージェントのみが知っています。

配信先

On-Demand トークンコードの送付先となる電子メール アドレスまたは携帯電話番号。

配布者

Token Distributor、つまり配布者権限を持つ管理者。

配布ファイル用パスワード

配布ファイルを電子メールでユーザーに送る際に、配布ファイルの保護に使用されるパスワード。

バックアップ

プライマリ インスタンス データのコピーを含むファイル。バックアップ ファイルを使用して、災害復旧時にプライマリ インスタンスをリストアできます。RSA Authentication Manager バックアップ ファイルには、次のものが含まれます。内部データベース、アプライアンス固有のデータと構成、内部サービスにアクセスするために使用される鍵とパスワード、内部データベース ログ ファイル。アプライアンスおよびオペレーティング システムのログ ファイルは含まれません。

プライマリ インスタンス

認証およびすべての管理アクションが実行される導入環境。

プロビジョニング

「トークン プロビジョニング」を参照してください。

プロビジョニング データ

プロビジョニング のサーバ定義のデータ。トークン デバイスのプロビジョニングを完了させるために必要な情報のコンテナです。

保証レベル

リスクベース認証では、ユーザーの毎回の認証試行が、ユーザーのプロファイル、デバイス、認証履歴に基づいて保証レベルに分類されます。その認証試行の保証レベルが、RBA ポリシーで設定された最低保証レベルに達している場合、ユーザーは RBA で保護されたリソースへのアクセスを許可されます。最低保証レベルに達していない場合、ユーザーはユーザー確認方法により本人であることを証明しなければ、RBA で保護されたリソースへのアクセスを許可されません。

ホスト

仮想マシンがインストールされている物理コンピュータ。

メール通知

アカウント登録、トークン、ユーザー グループ メンバーシップの要求に関するステータス情報が記載されており、要求を提出したユーザーに送信されます。トークンを要求した場合の電子メール通知には、トークンのダウンロードやアクティブ化の方法に関する情報も含まれています。Request Approver と Token Distributor は、それぞれに必要なアクションを要求する電子メール通知を受信します。「電子メール テンプレート」を参照してください。

ユーザー ID

システムが認証を試みているユーザーの識別に使用する文字列。
通常、ユーザー ID はユーザーの名前の頭文字と、その後ろに苗字を続けたものです。たとえば、Jane Doe のユーザー ID は *jdoe* となります。

ユーザー確認方法

リスクベース認証において、ユーザーが本人であることを確認するために使用する認証方法。

優先インスタンス

Web Tier 上のリスク ベース認証サービスが最初に通信する Authentication Manager インスタンス。また、Web Tier への更新を提供するインスタンス。任意のインスタンスを優先インスタンスとして構成できます。たとえば、レプリカ インスタンスを優先インスタンスとして構成できます。

ラウンドロビン DNS

専用のソフトウェアまたはハードウェアを必要としない、ロード バランシングの代替方法。DNS（ドメイン ネーム システム）サーバを構成してラウンド ロビンを有効化した場合、DNS サーバにより、RBA（リスク ベース認証）リクエストを複数の Web Tier サーバに送信することができます。「ロードバランサ」を参照してください。

リクエスト

ユーザーは、アカウント登録、トークン、On-Demand トークンコード サービス、ユーザー グループ メンバーシップをリクエストすることができます。

リスクエンジン

Authentication Manager では、リスクエンジンが、ユーザーごとの認証リスクをインテリジェントに評価します。リスクエンジンは、各ユーザーのデバイスと行動パターンに関する情報を長期間にわたり蓄積します。ユーザーが認証を試行すると、リスクエンジンは収集したデータを参照してそのリスクを評価します。そのリスク評価に基づき、ユーザーの認証試行に、保証レベル（高、中、低など）を割り当てます。

レプリカ インスタンス

認証を処理し、管理者が管理データを参照できる導入環境。レプリカ インスタンスではどの管理操作も実行されません。

レプリカ パッケージ

レプリカ アプライアンスがプライマリ アプライアンスに接続するための構成データを含んだファイル。レプリカ アプライアンスのセットアップを開始する前に、レプリカ パッケージ ファイルを生成する必要があります。

レルム

レルムは 1 つの組織単位であり、ユーザーとユーザー グループ、トークン、パスワード ポリシー、エージェントなど、1 つの導入環境で管理されるすべてのオブジェクトが含まれます。各導入環境にはレルムが 1 つだけあります。

ロードバランサ

リソース使用率の最適化を目的として、認証リクエストを複数のコンピュータに分散させるために導入するコンポーネント。通常、ロードバランサは、専用のハードウェアまたはソフトウェアとして実装され、冗長性の実現、信頼性の向上、レスポンス タイムの最小化を可能にします。「ラウンドロビン DNS」を参照してください。

ワークフロー

作業やビジネスの過程における情報やタスクの一連の動き。ワークフローは、ユーザーからのさまざまな要求に対して、1 つまたは 2 つの承認ステップと 1 つの配布ステップで構成できます。

ワークフロー参加者

承認者または配布者。承認者は、ユーザーからの要求をレビュー、承認、または保留します。配布者は、要求されたトークンの配布方法を決定したり、各要求に対する配布方法を記録します。「ワークフロー」も参照してください。

索引