RSA® Authentication Manager 8.0

設計ガイド

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 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。

2013 年 3 月

目次

はじめに 5
本書について 5
RSA Authentication Manager 8.0 マニュアル 5
関連ドキュメント 6
サポートとサービス 6
カスタマー サポートにご連絡される前に 7

第 1 章 : 導入の計画 9
RSA Authentication Manager がネットワークを保護するしくみ 9
導入環境のコンポーネント 10
プライマリ インスタンス 10
レプリカ インスタンス 11
Web Tier 11
ロードバランサ 12
認証エージェント 12
RSA Authentication Manager 導入環境の例 13
導入環境に関する考慮事項 14
Web Tier の導入 14
負荷分散戦略の選択 15
導入環境タイプの選択 15
導入シナリオ 17
シナリオ 1 : プライマリ インスタンスのみ 17
シナリオ 1 の導入 18
シナリオ 2 : プライマリ インスタンスと Web Tier 18
シナリオ 2 の導入 19
シナリオ 3 : プライマリ インスタンスとレプリカ インスタンス 19
シナリオ 3 の導入 20
シナリオ 4 : 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 Web Tier 20
シナリオ 4 の導入 21

第 2 章 :RSA Authentication Manager のネットワーク統合の計画 23
ポート トラフィック 23
RSA Authentication Manager インスタンスが使用するポート 23
RSA コンソールに対するアクセスの制限 28
RSA RADIUS Server のリスニングポート要件 28
レガシー トラステッド レルムのポートの考慮事項 28
ロードバランサ導入時の Web Tier 上のポート 29
ロードバランサのない環境での Web Tier 上のポート 30
ファイアウォール経由のアクセス 30
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 31
ユーザー データ の格納場所 31
外部ディレクトリ サーバの使用 32

物理的なセキュリティの設計 33
DNS（ドメイン ネーム システム）の更新計画 34
システム管理者アカウント 34
Authentication Manager 管理者アカウント 35
アプライアンス オペレーティング システム アカウント 36
RSA RADIUS の概要 36
トラステッド レルム 37

第 3 章：設計ガイド チェックリスト 41
このチェックリストについて 41
導入の計画 41
ネットワーク構成の計画 41
インストール前 43
インストール 43

用語集 45

索引 55

はじめに

本書について

本書は、RSA ® Authentication Manager 導入環境の設計方法について説明しています。本書の内容は、システム設計者、ネットワーク プランナー、セキュリティ担当者に加え、職務としてシステム / ネットワーク / セキュリティに関与するその他の信頼されるユーザーを対象としています。一般ユーザー向けではないことにご注意ください。

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 導入の計画

RSA Authentication Manager がネットワークを保護するしくみ

RSA Authentication Manager は、ユーザーに対して多要素認証方式による認証を要求することにより、ネットワーク上のリソースを保護します。

Authentication Manager は次の多要素認証方式を提供します。

RSA SecurID トークン。ハードウェア トークンとソフトウェア トークンがトークンコードを提供し、ユーザーはトークンコードを使用して認証を行い、Authentication Manager で保護されたリソースにアクセスを許可されます。

トークンコードは（一般的には 6 桁の）擬似乱数です。トークンコードは時間をベースに計算され、定期的に変更されます。

保護されたリソースにアクセスするためには、ユーザーは暗証番号（SecurID PIN）とトークンに表示された数字（トークンコード）を入力します。SecurID PIN とトークンコードの組み合わせをパスコードと呼びます。

ユーザーは、Authentication Manager がパスコードが正しいと確認した場合のみ、アクセスを許可されます。そうでない場合、ユーザーはアクセスを拒否されます。Authentication Manager は、PIN レスの SecurID 認証もサポートしています。この場合、SecurID PIN は不要です。

RBA（リスク ベース認証）。ユーザーに気づかせることなくユーザーの行動パターンとデバイスを解析し、その解析結果を元に潜在的なリスクや不正な認証の試みを特定することによって、RSA SecurID 認証と従来のパスワード ベースの認証を強化します。RBA でネットワーク リソースを保護する場合、ユーザーが認証を試行するたびに、ユーザーのプロファイル、認証デバイス、認証履歴に基づいて、システムが保証レベルを決定します。

ODA（On-Demand 認証）。メールまたは SMS（Short Message Service）を利用して、ユーザーにワン タイム トークンコードを送信します。このトークンコードはユーザーだけが知っている PIN と組み合わせて使用します。物理的なトークンまたは専用の認証デバイスを使うことなく、強力な 2 要素認証を可能にします。ODA は、スタンドアロンの認証方式としても、RBA のユーザー確認方式としても使用することができます。

Authentication Manager は拡張性に優れ、最大 100 万人のユーザーを認証できます。また、多種多様なアプリケーションと相互運用性を持ちます。サポートされるアプリケーションのリストについては、https://gallery.emc.com/community/marketplace/rsa?view=overview を参照してください。

導入環境のコンポーネント

Authentication Manager 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。認証およびすべての管理操作が実行されるインストール環境。単独のインスタンスで Authentication Manager の管理とユーザー認証を処理できます。

レプリカ インスタンス。オプションです。認証を処理し、管理者が管理データを参照できるインストール環境。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。プライマリ インスタンスの冗長性を提供します。

注：RSA は、プライマリ インスタンスとレプリカ インスタンスの両方を導入することを推奨しています。

Web Tier。オプションです。Web Tier は、DMZ に Self-Service Console、動的シード配布、RBA（リスク ベース認証）サービスを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。詳細については、11 ページの「Web Tier」を参照してください。

ロードバランサ。オプションです。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導入されるコンポーネント。詳細については、12 ページの「ロードバランサ」を参照してください。

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。詳細については、12 ページの「認証エージェント」を参照してください。

プライマリ インスタンス

プライマリ インスタンスは、最初に導入する Authentication Manager システムです。プライマリ インスタンスを導入した後、レプリカ インスタンスを追加できます。保守や災害復旧時には、レプリカ インスタンスを昇格させ、プライマリ インスタンスと置換することができます。

導入環境の中で、Authentication Manager のすべての管理タスクを実行できるシステムはプライマリ インスタンスのみです。レプリカの昇格やログ ファイルの収集など、一部の管理タスクはレプリカ インスタンスでも実行できます。

プライマリ インスタンスの主な機能は、次のとおりです。

- ユーザーの認証。
- 内部データベースに格納されている Authentication Manager データの管理。SecurID トークンのインポートや割り当て、RBA（リスク ベース認証）の有効化、LDAP アイデンティティ ソースの追加、セルフ サービスの構成、レプリカ パッケージの生成、エージェント構成ファイル、ノード シークレットの生成などのタスクを実行できます。

- 管理や認証活動の結果生じた変更をレプリケーションする。
- プライマリ RSA RADIUS サーバをホストすること。
- セルフ サービス リクエストの処理。
- Authentication Manager データベースを最新の状態に維持する。

レプリカ インスタンス

レプリカ インスタンスは導入環境レベルでプライマリ インスタンスの冗長性を提供します。レプリカ インスタンスの管理データは、表示することはできますが更新することはできません。

レプリカ インスタンスが提供するメリットは、次のとおりです。

- すべてのユーザーおよびシステム データのリアルタイムのミラーリング
- プライマリ インスタンスの応答がない場合、認証をフェイルオーバー
- 認証リクエストを複数インスタンスに負荷分散することによるパフォーマンスの向上
- リモートロケーションへのレプリカ インスタンスの導入
- プライマリ インスタンスの応答がない場合に、レプリカの昇格により管理機能を復旧可能

レプリカ インスタンスはオプション機能ですが、レプリカ インスタンスの導入を推奨します。

Web Tier

Web Tier は、DMZ にインストールされるプラットフォームです。プライベート ネットワークへの直接アクセスを許可することなく、リモート ユーザーにサービスを提供します。インバウンドのインターネット トラフィックがプライベート ネットワークに入る前に、WebTier で受信し、制御します。

Authentication Manager には、RBA（リスク ベース認証）、動的シード配布、Self-Service Console といった、企業ネットワークの外のユーザーからのアクセスが必要となる可能性のあるサービスが含まれています。ネットワークに DMZ が設置されている場合、Web Tier を導入し、これらのサービスを DMZ 内に導入することができます。

注：DMZ が設置されている環境であっても、On-Demand 認証または SecurID をそれぞれスタンドアロンの認証方式として使用する場合は、Web Tier を導入する必要はありません。

DMZ 内の Web Tier 上に Authentication Manager アプリケーションとサービスを導入すると、次のような利点があります。

- Self-Service Console や RBA のユーザーとやりとりされるフィルタリングされないインターネット トラフィックから内部ネットワークを保護します。Web Tier サーバで、プライベート ネットワークに入る前のインバウンド インターネット トラフィックを受信し、管理できます。
- RBA のログイン ページと Self-Service Console をカスタマイズできます。
- デフォルトの証明書を、認証機関から取得したカスタムの証明書と交換できます。
- 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。

1 つの導入環境に、最大 16 の Web Tier を導入できます。

ロードバランサ

ロードバランサは複数の Web Tier に認証要求を分散し、フェイルオーバーを容易にします。ロードバランサを導入環境に追加すると、次のような利点があります。

- ロードバランサはプライマリとレプリカの Web Tier に、RBA リクエストを分散します。
- ロードバランサは、HTTPS ポート経由で受信した Self-Service Console へのリクエストを、Self-Service Console が稼働する Web Tier またはプライマリ インスタンスに転送するよう構成できます。プライマリ インスタンスの障害により、レプリカ インスタンスを昇格した場合でも、ユーザーは同じ Self-Service Console の URL を使い続けることができます。
- Authentication Manager インスタンスまたは Web Tier の 1 つがダウンした場合には、フェイルオーバーを実行します。

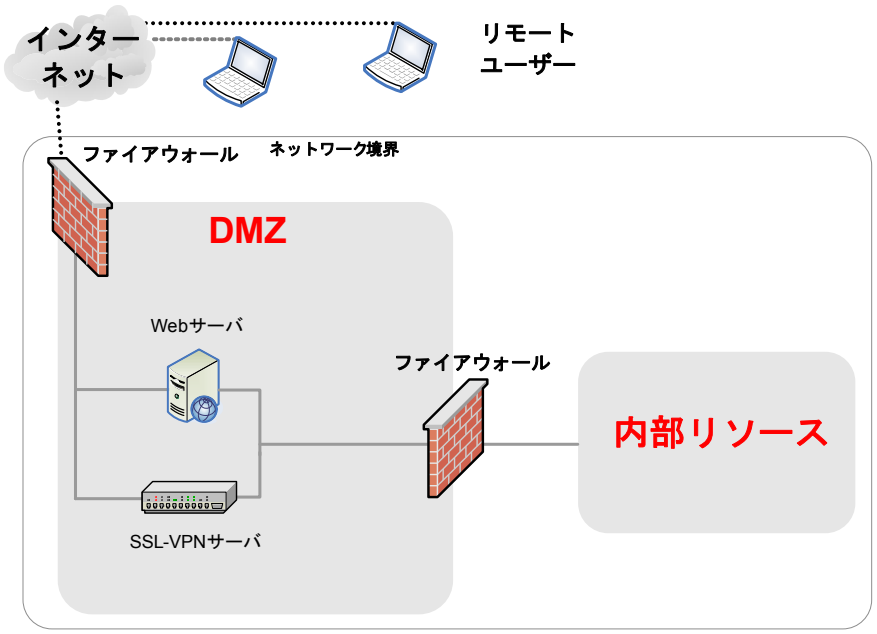
認証エージェント

認証エージェントは、保護対象のリソース上にインストールするソフトウェアです。Authentication Manager と通信して認証リクエストを処理します。Authentication Manager は多数の認証エージェントを処理できます。

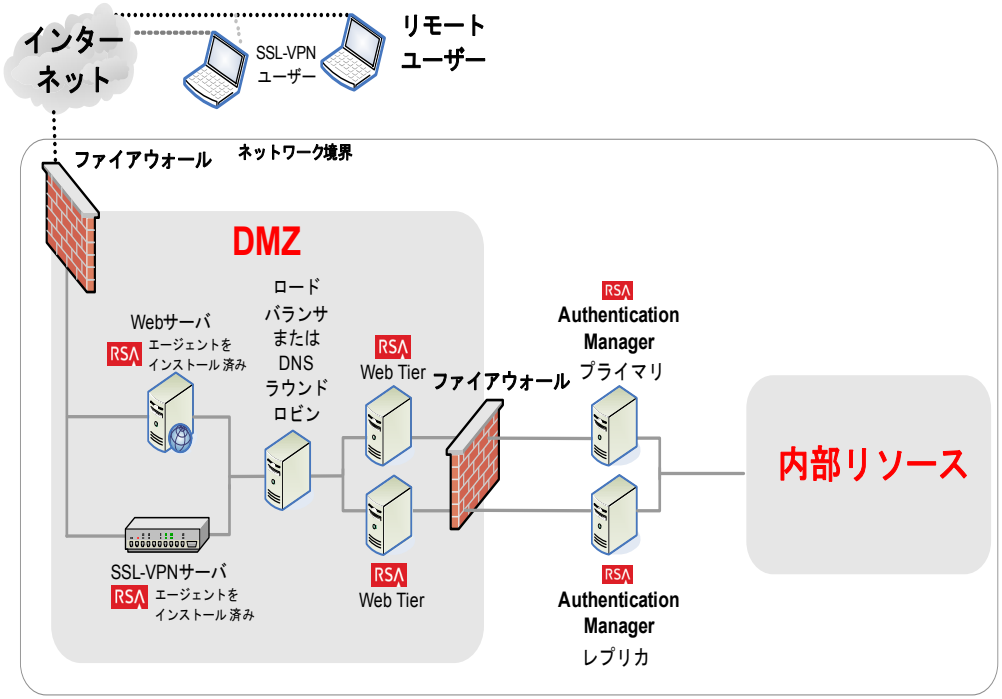
認証エージェントは、保護するリソースによってタイプが異なります。たとえば、Apache Web サーバを保護する場合は、RSA Authentication Agent 5.3 for Web for Apache が必要です。RSA Authentication Agent ソフトウェアは、Web サーバ以外にも数多くの製品に対応しています。リスク ベース認証が動作するのは Web ベースのエージェントのみであることに注意してください。RSA Authentication Agent が動作する製品の詳細については、**https://gallery.emc.com/community/marketplace/rsa?view=overview** を参照してください。

RSA Authentication Manager 導入環境の例

次の図は、Authentication Manager が統合される前の基本的なネットワーク構成を示しています。



次の図は、Authentication Manager が統合された後の基本的なネットワーク構成を示しています。



導入環境に関する考慮事項

RSA Authentication Manager は、プライマリ インスタンスおよびレプリカ インスタンスによって、導入環境の耐障害性をサポートします。冗長構成により、導入環境が予期しない障害から保護され、定期的な保守が容易になり、すべての認証サービスの可用性が保証されます。

システム レベルの冗長性が必要ですか？

いいえ。システム レベルの冗長性が必要ない場合、プライマリ インスタンスを単独で導入することができます。プライマリ インスタンスが応答を停止すると、認証は不可能となり、エンド ユーザーは保護されたリソースにアクセスできなくなる点に留意してください。このため、RSA では、ビジネス クリティカルなアプリケーションを保護する場合には、レプリカ インスタンスを導入し、システム レベルの冗長性を確保するよう強く推奨します。

はい。システム レベルの冗長性が必要な場合、プライマリ インスタンスと 1 つ以上のレプリカ インスタンスを導入します。

Web Tier の導入

多くの企業ネットワークでは、不要、または悪意のあるインターネット トラフィックをフィルタリングするために DMZ を設置し、内部ネットワークの保護されたリソースが直接アクセスされるのを防止しています。そのようなネットワーク構成に対応するため、RSA Authentication Manager では、DMZ 内に独立した Web Tier サーバを配置し、その上に RBA（リスク ベース認証）サービス、動的シード配布、Self-Service Console を導入できます。

自社のネットワークには DMZ がありますか？

いいえ。自社のネットワークに DMZ がない場合、Web Tier サーバの導入は必要ありません。この場合、提供できるサービスが制限される可能性があること、また、自社のファイアウォールのポートを 1 つ以上開く必要が出てくる可能性があることに留意してください。詳細については、17 ページの「シナリオ 1：プライマリ インスタンスのみ」または 19 ページの「シナリオ 3：プライマリ インスタンスとレプリカ インスタンス」を参照してください。

はい。自社のネットワークに DMZ がある場合、提供する予定のサービスに応じて、各インスタンス（プライマリおよびレプリカ）ごとに、1 つ以上の Web Tier を導入する必要があります。

RBA と動的シード配布を使用する予定がありますか？企業ネットワークの外部からの Self-Service Console へのアクセスを許可する予定がありますか？

いいえ。認証方式として On-Demand 認証または SecurID を単独で使用し、かつ、企業ネットワークの外からの Self-Service Console へのアクセスを許可しない場合には、Web Tier サーバの導入は必要ありません。詳細については、17 ページの「シナリオ 1：プライマリ インスタンスのみ」または 19 ページの「シナリオ 3：プライマリ インスタンスとレプリカ インスタンス」を参照してください。

はい。DMZ のある環境では、企業ネットワークの外からアクセスできるように、Web Tier 上に RBA、動的シード配布、Self-Service Console を導入する必要があります。各インスタンス（プライマリおよびレプリカ）ごとに、1 つの Web Tier を導入する必要があります。詳細については、18 ページの「シナリオ 2：プライマリ インスタンスと Web Tier」または 20 ページの「シナリオ 4：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 Web Tier」を参照してください。

負荷分散戦略の選択

プライマリ インスタンス、レプリカ インスタンス、Web Tier から構成される導入環境では、プライマリ インスタンスとレプリカ インスタンスに RBA（リスク ベース認証）リクエストを分散させるため、そしてどちらか一方のサーバが応答を停止した場合にサービスの継続性を保証するために、追加のステップが必要です。

DNS ラウンド ロビンは、2 つのサーバに負荷を均等に分散する最も簡単な方法です。しかし、この方法では、2 つのサーバの内 1 つが応答を停止した場合に、自動的に対処できません。RBA の自動フェイルオーバーが必要な場合には、RSA ではハードウェアまたはソフトウェアのロードバランサの使用を推奨します。

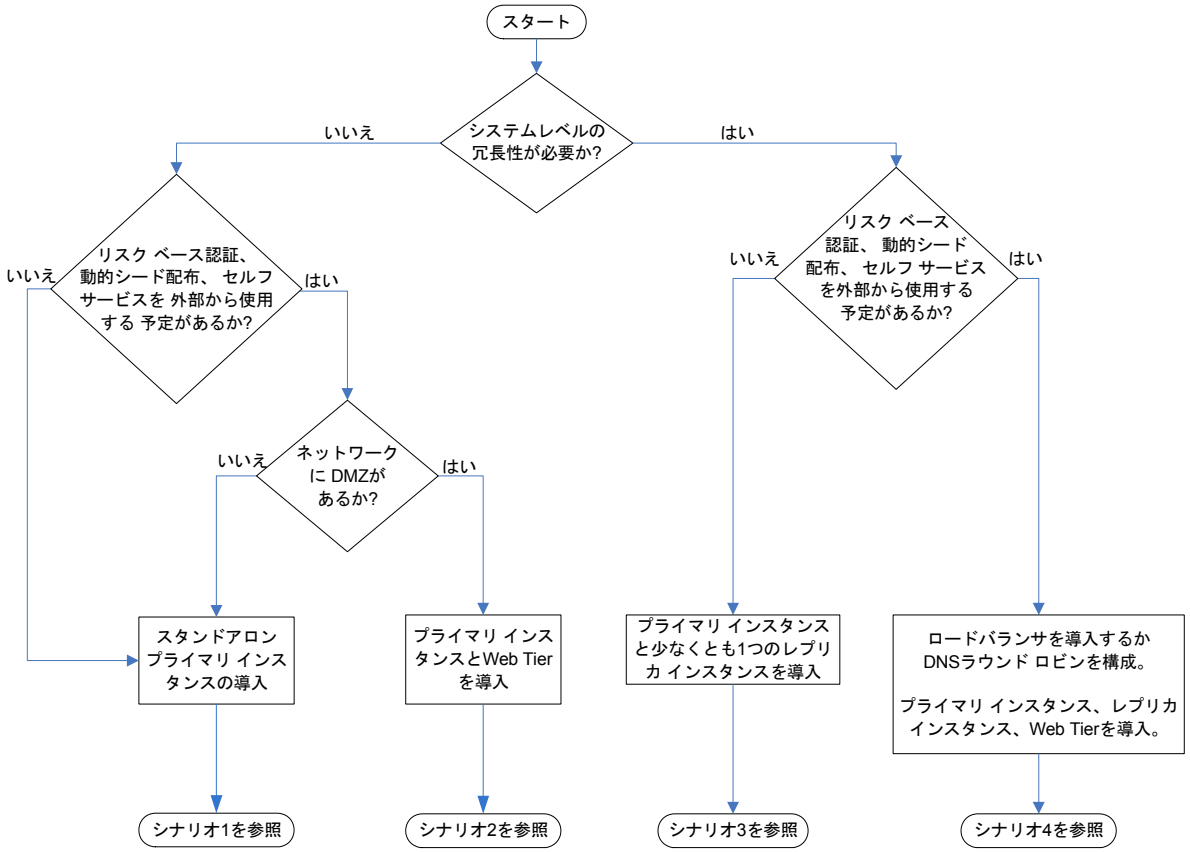
導入環境タイプの選択

Authentication Manager は、ネットワーク トポロジーやビジネス要件に応じて、多数の導入オプションをサポートしています。

Authentication Manager の導入前に、既存のネットワーク構成を確認します。この情報は、ネットワークに Authentication Manager を統合する最善の方法を決定するのに役立ちます。

確認すべき情報	説明
ネットワーク トポロジー図	すべてのサーバ、その他のハードウェア、内部リソース、ファイアウォール、ポータル、ユーザーのマシンが物理的にどこに配置されているのかを示します。
認証プロセスのフロー チャート	既存の認証プロセスを示します。

ネットワーク トポロジーに関する情報を収集し、確認した後は、意思決定ツリーを使い、自社にとって最適な Authentication Manager のネットワーク構成を決定します。



導入シナリオ

次のシナリオは、Authentication Manager の一般的な導入環境を示しています。

シナリオ / サポートする機能	RBA（リスクベース認証）	ODA（On-Demand 認証）	SecurID	負荷分散とフェイルオーバー
17 ページの「シナリオ 1：プライマリ インスタンスのみ」を参照。	X	X	X	
18 ページの「シナリオ 2：プライマリ インスタンスと Web Tier」を参照。	X	X	X	
19 ページの「シナリオ 3：プライマリ インスタンスとレプリカ インスタンス」を参照。		X	X	X
20 ページの「シナリオ 4：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 Web Tier」を参照。	X	X	X	X

シナリオ 1：プライマリ インスタンスのみ

スタンドアロンプライマリ インスタンス導入環境では、次の機能を使用できます。

- 認証方式：ODA（完全サポート）、RBA（条件付きサポート）、SecurID（完全サポート）

シナリオ 1 を選択する際は、次の要素を考慮してください。

- プライマリ インスタンス上では、Self-Service Console、Security Console、RBA のすべてがポート 7004 番を共有します。したがって、この構成で RBA、Self-Service Console、動的シード配布をインターネット経由で使用すると、Security Console もインターネットからアクセスできるようになります。RBA または Self-Service Console の使用を検討している場合、RSA では Web Tier サーバの導入を強く推奨します。ポートの詳細については、23 ページの「ポート トラフィック」を参照してください。
- RBA は標準 SSL ポート（443 番）ではなく、ポート 7004 番を使用するため、クライアント側のファイアウォール越しにアクセスするエンドユーザー（たとえばホテルからの認証）の場合、このサービスにアクセスできない可能性があります。厳しい制限が設定されたクライアント側ファイアウォールに対応する必要がある場合には、RSA では、Web Tier サーバの導入を強く推奨します。ポートの詳細については、23 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 インスタンスでは Authentication Manager の内部ルート CA（認証局）が署名した SSL 証明書が使用されるため、RBA を使用する際、または Self-Service Console にアクセスする際に、ユーザーに証明書のセキュリティ警告が表示される可能性があります。これらの警告を表示させたくない場合は、Operations Console を使用して、既存の証明書をサードパーティの CA が発行した新しい証明書と交換できます。詳細については、「管理者ガイド」の「SSL 証明書の管理」を参照してください。
- プライマリ インスタンスのみの環境では、冗長性や負荷分散が提供されません。

シナリオ 1 の導入

スタンドアロン プライマリ インスタンスを導入するには、次の手順を実行します。

手順

1. 導入を計画し、インストール前チェックリストを完成させます。手順については、「セットアップと構成ガイド」の「導入の準備」の章を参照してください。
2. プライマリ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「プライマリ アプライアンスの導入」の章を参照してください。
3. 導入環境を保護し、ポートを構成し、ユーザーを追加し、認証方式およびセルフ サービスを構成します。手順については、「セットアップと構成ガイド」の「導入の次のステップ」の章を参照してください。

シナリオ 2：プライマリ インスタンスと Web Tier

プライマリ インスタンスと Web Tier からなる導入環境では、次の機能を使用できます。

- 認証方式：ODA、RBA、SecurID
- RBA ログオン ページのカスタマイズ
- Self-Service Console のカスタマイズ
- Web Tier サーバの SSL 証明書の交換

シナリオ 2 を選択する際は、次の要素を考慮してください。

- プライマリ インスタンスが応答を停止した場合、フェイルオーバーは実行されません。プライマリ インスタンスが応答を停止した場合、認証は不可能となり、エンド ユーザーは保護されたリソースにアクセスできなくなります。このため、RSA では、ビジネス クリティカルな アプリケーションを保護する場合は、プライマリ インスタンスとレプリカ インスタンスの導入を強く推奨します。
- 負荷分散は行われません。

シナリオ 2 の導入

プライマリ インスタンスと Web Tier からなる環境を導入するには、次の手順を実行します。

手順

1. 導入を計画し、インストール前チェックリストを完成させます。手順については、「セットアップと構成ガイド」の「導入の準備」の章を参照してください。
2. プライマリ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「プライマリ アプライアンスの導入」の章を参照してください。
3. Web Tier を追加します。手順については、「セットアップと構成ガイド」の「Web Tier のインストール」の章を参照してください。
4. 導入環境を保護し、ポートを構成し、ユーザーを追加し、認証方式およびセルフ サービスを構成します。手順については、「セットアップと構成ガイド」の「導入の次のステップ」の章を参照してください。

シナリオ 3：プライマリ インスタンスとレプリカ インスタンス

プライマリ インスタンスとレプリカ インスタンスからなる導入環境では、次の機能を使用できます。

- 認証方式：ODA と SecurID
- 災害復旧時のフェイルオーバー
- 地理的に分散した導入環境

シナリオ 3 を選択する際は、次の要素を考慮してください。

- プライマリ インスタンス上では、Self-Service Console、Security Console、Operations Console がポート 7004 番を共有します。したがって、ファイアウォールでこのポートを開放すると、これらのサービスがすべてインターネットから利用できるようになります。企業ネットワークの外部から Self-Service Console の利用を許可する必要がある場合、RSA では、Web Tier サーバの導入を強く推奨します。ポートの詳細については、23 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 インスタンスでは Authentication Manager の内部ルート CA（認証局）が署名した SSL 証明書が使用されるため、RBA を使用する際、または Self-Service Console にアクセスする際に、ユーザーに証明書のセキュリティ警告が表示される可能性があります。これらの警告を表示させたくない場合は、Operations Console を使用して、既存の証明書をサードパーティの認証局が発行した新しい証明書と交換できます。詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「SSL 証明書の管理」を参照してください。

- 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には、Operations Console 管理者のクレデンシャルが必要です。Operations Console 管理者は多くの重要な機能を実行できるため、これらのクレデンシャルは最も信頼できる人にのみ提供してください。リモート レプリカ インスタンスをセットアップする際は、リモート ロケーションにいる管理者がレプリカ インスタンスの導入だけを行う（アタッチは行わない）ようにすることで、これらのクレデンシャルの提供を回避できます。リモート管理者がレプリカ インスタンスを導入した後、ローカル管理者がリモート レプリカ インスタンスにアクセスしてアタッチ手順を実行できます。
- レプリカ インスタンスを導入するには、プライマリ インスタンス上で作成したレプリカ パッケージ ファイルが必要です。レプリカ パッケージを信頼できる管理者に送信する場合は、このファイルの完全性が維持されるよう注意する必要があります。レプリカ パッケージ ファイルを送信する際は、署名付きメールなどの安全で検証可能な手段を常に使用してください。

シナリオ 3 の導入

プライマリ インスタンスと 1 つ以上のレプリカ インスタンスからなる環境を導入するには、次の手順を実行します。

手順

1. 導入を計画し、インストール前チェックリストを完成させます。手順については、「セットアップと構成ガイド」の「導入の準備」の章を参照してください。
2. プライマリ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「プライマリ アプライアンスの導入」の章を参照してください。
3. レプリカ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「レプリカ アプライアンスの導入」の章を参照してください。
4. 導入環境を保護し、ポートを構成し、ユーザーを追加し、認証方式およびセルフ サービスを構成します。手順については、「セットアップと構成ガイド」の「導入の次のステップ」の章を参照してください。

シナリオ 4：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 Web Tier

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 Web Tier からなる導入環境では、次の機能を使用できます。

- 認証方式：ODA、RBA、SecurID
- 災害復旧時のフェイルオーバー

- RBA ログオン ページのカスタマイズ
- Self-Service Console のカスタマイズ
- Web Tier サーバの SSL 証明書の交換

シナリオ 4 を選択する際は、次の要素を考慮してください。

- RBA 自体は、Web Tier 間の負荷分散機能を持っていません。負荷分散は外部のロードバランサまたは DNS ラウンド ロビンによって提供されます。
- この構成では、個々の Web Tier のホスト名および共有の仮想ホスト名の両方とも、インターネットからアクセス可能な名前である必要があります。

シナリオ 4 の導入

プライマリ インスタンスおよび 1 つ以上のレプリカ インスタンスと Web Tier からなる環境を導入するには、次の手順を実行します。

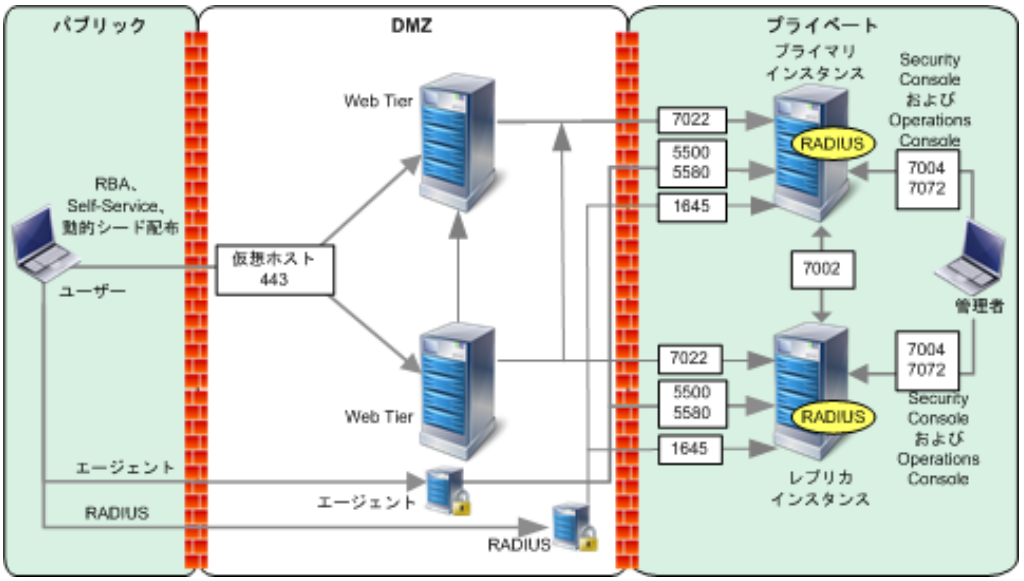
手順

1. 導入を計画し、インストール前チェックリストを完成させます。手順については、「セットアップと構成ガイド」の「導入の準備」の章を参照してください。
2. プライマリ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「プライマリ アプライアンスの導入」の章を参照してください。
3. レプリカ アプライアンスをセットアップします。手順については、「セットアップと構成ガイド」の「レプリカ アプライアンスの導入」の章を参照してください。
4. ロードバランサを追加するか、または DNS ラウンド ロビンを構成します。手順については、「セットアップと構成ガイド」の「仮想ホストとロードバランサの構成」の章を参照してください。
5. Web Tier を追加します。手順については、「セットアップと構成ガイド」の「Web Tier のインストール」の章を参照してください。
6. 導入環境を保護し、ポートを構成し、ユーザーを追加し、認証方式およびセルフ サービスを構成します。手順については、「セットアップと構成ガイド」の「導入の次のステップ」の章を参照してください。

2 RSA Authentication Manager のネットワーク統合の計画

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、23 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、28 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、28 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、23 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、23 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。

ユーザー データ の格納場所

次の場所にユーザー データを格納できます。

- 内部データベース
- 外部ディレクトリ サーバ（Authentication Manager ではアイデンティティ ソースと呼ぶ）

外部ディレクトリ サーバを統合すると、管理者は RSA Security Console を使用して次のことを行えます。

- 外部ディレクトリ サーバに存在するユーザーおよびユーザー グループ データを表示すること（ただし追加、変更はできない）。
- 外部ディレクトリ サーバに存在する個々のユーザーに対して、SecurID 認証、On-Demand 認証、リスクベース認証のような Authentication Manager 機能を有効化または無効化すること。
- 内部データベースに格納されたポリシー データなどの RSA 固有のデータを管理すること。

注：ユーザー データやグループ データを変更するには、外部ディレクトリ サーバのネイティブ ユーザー インタフェースを使用する必要があります。RSA Security Console からは、変更できません。

内部データベースと外部ディレクトリ サーバのどちらを使用するかを選択する際には、現在のネットワークの構成とニーズを検討してください。Authentication Manager には内部データベースが含まれます。内部データベースには、すべてのアプリケーション データおよびポリシー データが格納されます。内部データベースには、ユーザー データおよびユーザー グループ データを格納することもできます。

外部ディレクトリ サーバの使用

Authentication Manager では、ユーザー データおよびユーザー グループ データの保存に外部ディレクトリ サーバを使用できます。これを実現するには、アイデンティティ ソースを作成し、Authentication Manager に対してユーザー データおよびユーザー グループ データの場所を指定します。

外部ディレクトリ サーバの統合については、次の点に留意してください。

- 登録済みデバイスのように、Authentication Manager に固有のユーザー データは、内部データベースに保存されます。
- Authentication Manager ディレクトリ サーバを統合するために、既存のディレクトリ スキーマを変更する必要はありません。代わりに、Authentication Manager が使用するデータへのマッピングを定義します。
- Authentication Manager は、1 つの例外を除き、外部ディレクトリ サーバに対して、読み取り専用アクセスを行います。唯一の例外は、ユーザーが認証時に自身のパスワード変更を許可されている場合です。
- ユーザーが自身のパスワードの変更を許可されている場合、ネットワーク上を通過する機密データが第三者に開示されることがないよう、外部ディレクトリ サーバとの接続には SSL-LDAP を使用する必要があります。SSL-LDAP 接続を使用するには、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。
- Active Directory の場合、Authentication Manager は、1 つの導入環境につき、グローバル カタログ アイデンティティ ソースと、最大 30 の非グローバル カタログ アイデンティティ ソースをサポートします。

サポートされる外部ディレクトリ サーバ

Authentication Manager では、次のバージョンがサポートされています。

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

注：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。

外部ディレクトリ サーバの統合に必要な情報のリストは、41 ページの第 3 章「設計ガイド チェックリスト」を参照してください。

物理的なセキュリティの設計

Authentication Manager を導入する場合、導入環境内に存在する物理的なシステムを、不正ユーザーやさまざまな攻撃から保護するよう計画する必要があります。

- **装置**。Authentication Manager を実行する装置の物理的なセキュリティを確保するために、RSA では、最小限の信頼できる担当者のみがアクセス可能な、施錠可能な場所に装置を設置することを推奨します。
- **接続とポート**。アプライアンスへの接続の数および種類を最小限に抑えるようにしてください。システムの機能に必要ないポートを経由するアクセスをブロックします。
- **パスワードとキー指定要素**。内部データベースなどの内部サービスへのアクセスに使用するキーとパスワードは、Authentication Manager の Quick Setup によって生成されます。これらのクレデンシャルは、Authentication Manager 内のセキュア ヴォルトに保存され、無人起動のためのシステム固有キーおよび対話式オペレーションのための Operations Console 管理者のクレデンシャルの両方を使用して保護されます。Operations Console 管理者のクレデンシャルは、Quick Setup 中に作成されます。

  Operations Console 管理者のクレデンシャルにより、Authentication Manager の実行に必要なすべてのシステム パスワードが保護されるため、Operations Console 管理者のクレデンシャルは安全に保護する必要があります。

  フェイルオーバーおよび災害復旧戦略を計画する際には、すべてのシステム パスワードのバックアップの一部として、システムのキーとパスワードを、パスワード保護された暗号化ファイルにエクスポートすることができます。災害復旧時には、このファイルをインポートして導入環境に戻すことができます。エクスポートしたファイルは安全が確保された保管庫で保管することを強く推奨します。
- **仮想アプライアンスをホストする物理マシン**。仮想ディスク、仮想メモリ、すべての VMware スナップショットが格納されるホストを保護します。

DNS（ドメイン ネーム システム）の更新計画

ユーザーが Web Tier とロードバランサ（オプション）にインターネット経由でアクセスできるようにするには、それらのシステムに対してパブリックに解決可能な名前を購入する必要があります。次の手順を実行します。

- ドメイン名を定義します（例：*mydomain.com*）
- ホスト名を定義します（例：*myhost.mydomain.com*）
- ドメイン名の登録機関に連絡して、ドメイン名とホスト名を登録します。

セルフ サービスおよびリスク ベース認証（RBA）を使用するクライアントは、DNS（ドメイン ネーム システム）を使用して仮想ホスト名を解決できる必要があります。

- 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。

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。
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。

RSA RADIUS の概要

RSA RADIUS と RSA Authentication Manager を共に使用すると、RADIUS 対応デバイスを通じてネットワーク リソースにアクセスしようとするユーザーを直接認証できます。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。RADIUS サーバが受信したアクセス リクエストは RSA Authentication Manager に転送され、検証されます。Authentication Manager が許可または拒否メッセージを RADIUS サーバに送信し、RADIUS サーバがそのメッセージをリクエスト送信元の RADIUS クライアントに転送します。

RADIUS は、Authentication Manager のインストール中に自動的にインストールされて構成されます。インストール後、RADIUS は Authentication Manager と同じインスタンス上で稼働するように構成されます。

RSA RADIUS の構成と、RSA RADIUS が稼働する個々のインスタンスに必要な設定の管理は、Operations Console を使用して行います。

RADIUS の日常的な運用管理に関連するほとんどのタスクは、Security Console から実行できます。

Security Console を通じて、次のオブジェクトを管理できます。

- **RADIUS サーバ**。RADIUS クライアントからユーザーのアクセス リクエストを受信し、検証のため Authentication Manager に転送するサーバ。RADIUS サーバは、Authentication Manager から受信した許可または拒否メッセージをリクエスト送信元の RADIUS クライアントに転送します。
- **RADIUS クライアント**。ネットワーク境界に設置され、ネットワーク リソースにアクセスしようとするユーザーに対してアクセス制御を執行する、RADIUS に対応したデバイス。
- **RADIUS プロファイル**。リモート ネットワーク アクセスを要求するユーザーのセッション要件を指定するチェックリスト属性およびリターンリスト属性の名前付きコレクション。
- **RADIUS ユーザー属性**。プロファイルの外でユーザーまたはトラステッド ユーザーに割り当てる RADIUS 属性。
- **RADIUS アカウンティング**。課金や監査の目的で使用される、RADIUS サーバとクライアントの使用統計。
- **RADIUS レプリケーション**。RSA RADIUS は、RADIUS アクティビティの結果生じた変更を自動的に RADIUS レプリカ サーバに送信します。手動でレプリケーションを行うこともできます。

トラステッド レルム

導入環境とは、プライマリ インスタンスと必要に応じて追加された 1 つ以上のレプリカ インスタンスで構成される RSA Authentication Manager インストール環境のことです。

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。

たとえば、ロンドンに本部がある会社がニューヨークにオフィスを持っているとします。ロンドンのオフィスとニューヨークのオフィスのそれぞれに Authentication Manager の導入環境があります。各導入環境で管理されるオブジェクトがレルムを構成します。ロンドン レルムとニューヨーク レルムです。

複数のレルム間で、信頼関係を持つことができます。これにより、あるレルムのユーザーが、別のレルムで認証し、その別のレルムのリソースにアクセスすることができるようになります。

たとえば、ロンドン レルムがニューヨーク レルムとの信頼関係を持っているとします。これは、ニューヨーク レルムがロンドン レルムのユーザーを「信頼」し、ニューヨーク レルムのユーザーと同じ権限を与えることを意味します。ロンドン オフィスのユーザーは、ニューヨークに滞在中、他のすべてのニューヨーク オフィスの ユーザーと同様にニューヨーク オフィスで認証を受けられます。

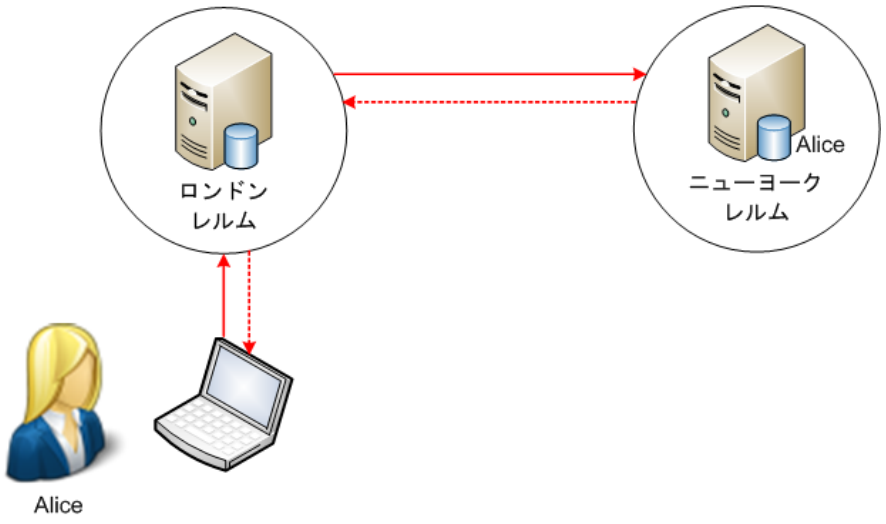
信頼関係は次のタスクを実行して作成します。

- 外部レルムをトラステッド レルムとして追加します。
- トラステッド レルムに属するトラステッド ユーザーを認証するエージェントを指定します。
- トラステッド ユーザーを指定します。トラステッド レルムの全ユーザーが認証を受けられるようにはしたくない場合があります。その場合は、トラステッド レルムのどのユーザーをトラステッド ユーザーとするかを指定します。トラステッド ユーザーだけが、認証を受けることができます。

信頼関係には単方向の信頼または双方向の信頼があります。単方向の信頼では、一方のレルムのトラステッド ユーザーだけが相手レルムで認証を受けることができます。

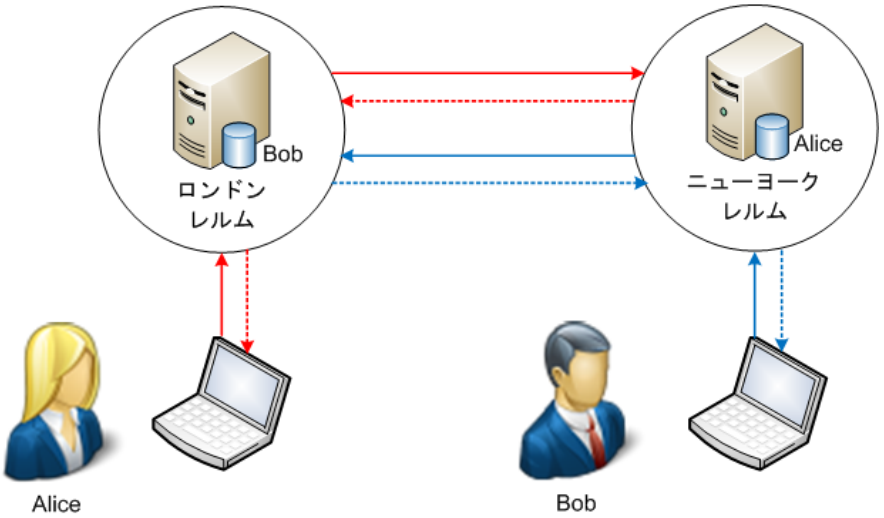
たとえば、ロンドンとニューヨークの間の信頼関係が単方向である場合、ロンドンのトラステッド ユーザーがニューヨークで認証を受けるか、ニューヨークのトラステッド ユーザーがロンドンで認証を受けるか、そのどちらか一方のみが可能です。双方向の信頼では、どちらのレルムのトラステッド ユーザーも、相手方のレルムで認証を受けられます。たとえば、ロンドンとニューヨークの間の信頼関係が双方向である場合、ロンドンのトラステッド ユーザーはニューヨークで認証を受けることができ、ニューヨークのトラステッド ユーザーもロンドンで認証を受けることができます。

次の図に、単方向の信頼を示します。ロンドンはニューヨークをトラステッド レルムとして追加しました。これにより、ニューヨーク レルムのトラステッド ユーザーである Alice は、ロンドン出張中にロンドン レルムで認証を受けることが可能になります。



ロンドン滞在中に、Alice はニューヨーク レルムの自分のクレデンシャル（ユーザー名とパスコード）を使用してロンドンの VPN（バーチャル プライベート ネットワーク）へアクセスを試行します。ロンドンの VPN サーバはエージェントによって保護されており、そのエージェントはトラステッドレルム認証に対応するよう構成されています。このエージェントは自分のレルム内では Alice というユーザーが見つからないため、他のレルムに Alice というユーザーがいないか探します。エージェントがニューヨーク レルムで Alice を見つけた後、ニューヨーク レルムは Alice のクレデンシャルを検証し、Alice を認証した後、Alice のアクセスを許可するようエージェントに指示します。

次の図に、双方向の信頼を示します。ロンドンはニューヨークをトラステッド レルムとして追加し、ニューヨークはロンドンをトラステッド レルムとして追加しました。これにより、ニューヨーク レルムのトラステッド ユーザーである Alice がロンドン レルムで認証を受けられるのと同時に、ロンドン レルムのトラステッド ユーザーである Bob がニューヨーク レルムで認証を受けられるようになります。



トラステッド レルムの詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「トラステッド レルムの管理」の章を参照してください。

3 設計ガイド チェックリスト

このチェックリストについて

次のチェックリストを使用して、設計およびインストール情報を指定します。RSA では、このチェックリストへの記入を完了し、適切な導入担当者へ配布することを推奨します。今後の参照用に、記入したチェックリストのコピーを安全な場所に保管します。

注：このチェック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チェックリストに記入する前に、自社のセキュリティ ポリシーを参照してください。

導入の計画

要素	計画
レプリカ インスタンスが必要かどうかを決定します。	
使用する認証方法を決定します。	
Web Tier をインストールする必要があるかどうかと、Web Tier で利用する機能を決定します。	
ロードバランサまたはラウンド ロビン DNS が必要かどうかを決定します。	
インスタンスを同期するタイム サーバが必要かどうかを決定します。	

ネットワーク構成の計画

要素	計画
プライマリおよびレプリカ インスタンスのために、どのポートを開く必要があるかを決定します。	
ロードバランサ用にデフォルトのポートを使用するかどうかを決定します。	

要素	計画
Web Tier 用にデフォルトのポートを使用するかどうかを決定します。	
ファイアウォールを構成するために、どのような情報を入手する必要があるかを決定します。 次に例を挙げます。 • インスタンスの IP アドレス • エージェントの IP アドレス • ロードバランサのホスト名と IP アドレス • ロードバランサのポート • Web Tier サーバのホスト名と IP アドレス • Web Tier のポート • 仮想ホスト名	
デフォルトの証明書を使用するかカスタム証明書で置き換えるかを決定します。	
ユーザー データの格納場所を決定します。 • 内部データベース • 外部ディレクトリ サーバ • 両方	
ディレクトリ サーバ • サポート対象バージョンのディレクトリ サーバを使用していることを確認します。 • ディレクトリ サーバの管理者アカウントを取得します。 • ディレクトリ サーバの URL を確認します。 • （オプション）フェイルオーバー用のディレクトリ サーバの URL を確認します。 • ユーザーに Authentication Manager 経由のパスワード変更を許可するかどうかを決定します。 • Web Tier サーバ、ロードバランサ、仮想ホスト名に対して、（インターネット上に）公開する DNS 名およびアドレスを取得します。 • パスワード変更を許可する場合： – Active Directory 上で CA（認証局）サービスを有効化します。 – ドメイン ルート CA 証明書か、ディレクトリ サーバの証明書と同じルート CA によって署名された証明書をエクスポートし、使用可能であることを確認します。	

インストール前

要素	計画
ライセンス ファイルの場所を確認します。	
名前およびパスワードを計画します。 • スーパー管理者のユーザー ID • スーパー管理者パスワード • Operations Console 管理者の名前とパスワード • OS のパスワード • Web Tier のパスワード	
Web Tier サーバの物理的な設置場所を決定します。	
エージェントが必要かどうかを決定します。	
ロードバランサが必要かどうかを決定します。	

インストール

要素	計画
プライマリ インスタンスをインストールします。	
1 つ以上のレプリカ インスタンスをインストールします。	
Web Tier をインストールします。	
必要に応じてエージェントをインストールします。	
必要に応じてロードバランサをインストールします。	

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

A

Active Directory, 32
administrators
    system administrator accounts, 34

D

DMZ
    Web Tier の導入 , 11

I

IP アドレス
    エイリアス , 30

L

LDAP ディレクトリ
    統合のガイドライン , 32
license
    ID, 7
    serial number, 7

N

NAT。ネットワーク アドレス変換を参照

O

On-Demand 認証
    エージェントの使用 , 12
    概要 , 9
    定義 , 9
    概要 , 9
one-way trust, 38
operating system
    account, 36
Operations Console
    administrator permissions, 35
Oracle Directory Server, 32

P

passwords
    lost, 35–36

R

RADIUS
    accounting, 37
    clients, 37
    profiles, 37
    replication, 37
    servers, 37
    user attributes, 37
replica instances
    definition, 11
RSA Self-Service Console
    ロードバランサの使用 , 12

S

Secure Shell
    for accessing the appliance, 36
SecurID
    概要 , 9
SSH. *See* Secure Shell.
Sun Java System Directory Server, 32
Super Admin
    permissions, 35
system administrator accounts, 34

T

trusted realms
    authentication, 37
    one-way trust, 38
    two-way trust, 39
trusts. *See* trusted realms
two-way trust, 39

U

User IDs
    valid characters, 35

V

valid characters
    for User IDs, 35
version
    viewing, 7
Virtual Private Network
    trusted realm, 39

W

Web Tier, 20
- 概要 , 10
- サポートされる数 , 12
- 導入 , 14
- メリットの概要 , 12
- ラウンド ロビン DNS ポート , 30
- ロードバランサの使用 , 12
- ロードバランサ ポート , 29
- RBA ログオンページの カスタマイズ , 12

あ

アイデンティティ ソース
- LDAP の使用 , 32

い

インストール
- ファイアウォール アクセス , 30

え

エイリアス
- 許可される数 , 30

か

外部ディレクトリ サーバ
- サポートされるタイプ , 33
- ユーザー機能の有効化と無効化 , 32

拡張性 , 9

カスタマイズ
- RBA ログオン ページ , 12

管理
- 外部ディレクトリ サーバ , 31

き

キーストア , 33

既存ネットワークの確認 , 15

く

グローバル カタログ
- サポートされる数 , 32

さ

サブネット
- アプライアンスの導入 , 23

し

証明書
- SSL-LDAP, 32
- デフォルトをカスタムに置き 換え , 12

す

スキーマ
- ディレクトリ サーバの統合 , 32

せ

セキュア シェル
- ポート , 24

セキュリティ
- キー指定要素とシステム パスワード , 33
- 接続 , 33
- 装置 , 33

セキュリティ。「キーストア」を 参照 , 33

た

代替 IP アドレス , 30

多要素認証
- 概要 , 9

て

ディレクトリ サーバの統合
- スキーマ , 32

と

トークン
- SecurID の概要 , 9
- タイプ , 9

統合
- 設計 , 23

導入
- Web Tier, 14
- オプション , 10
- サブネットの使用 , 23
- サポートされるシナリオ , 17
- 設計 , 9
- タイプの選択 , 15
- ファイアウォールの使用 , 30
- プライマリ , 20
- プライマリと Web Tier, 18
- プライマリとレプリカ , 19
- プライマリのみ , 17

登録済みデバイス
- データの保存場所 , 32

に

認証
- On-Demand, 9
- ユーザー確認 , 9
- ユーザー履歴 , 9
- リスク ベース , 9

認証エージェント
　概要，10
　代替 IP アドレス，30
　タイプ，12

ね
ネットワーク アドレス変換，30
　エージェントの IP アドレスの
　　エイリアス，30
ネットワーク保護，9

は
パスコード
　概要，9

ふ
ファイアウォール
　Web Tier での使用，14
　エイリアス，30
　ネットワーク アドレス変換，30
フェイルオーバー
　ロードバランサの使用，12
プライマリ インスタンス
　概要，10
　レプリカ インスタンスへの安全な
　　接続，31

ほ
ポートの使用
　トラフィック フロー図，23
ポート使用
　ポートの一覧，23
ポートの使用
　Web Tier での，29, 30
　Web Tier 内，14
　セキュリティ，33
ポート変換，31
ポリシー データ
　外部ディレクトリ サーバ内の，31
　内部データベース内の，32

ま
マスター パスワード
　セキュリティの確保，33
　バックアップのための
　　エクスポート，33
　リカバリ，33

ゆ
ユーザー グループ データ
　管理，31
　内部データベース内の，32

ら
ラウンド ロビン DNS
　ポート，30
ラウンドロビン DNS
　導入戦略，15

り
リスク ベース認証
　エージェントの使用，12
　概要，9
　保証レベル，9

れ
レプリカ，20
プライマリ インスタンス
　レプリカ インスタンスへの安全な
　　接続，31
レプリカ インスタンス
　概要，10
　許可される数，14

ろ
ロードバランサ
　概要，10
　使用，12
ロード バランス
　導入戦略，15