# RSA® Authentication Manager 6.1 から 8.0 への移行ガイド

### 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

## 本書について

本書は、RSA® Authentication Manager 6.1 からバージョン 8.0 への移行を計画および実施する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 RSA Authentication Manager 8.0 での重要な変更

## RSA Authentication Manager 8.0 の概要

RSA Authentication Manager は、RSA SecurID 2 要素認証ソリューションの認証エンジンおよび導入環境管理コンポーネントです。

SecurID トークンにより、ランダムで常に変化する一連のトークンコードが生成されます。トークンコードは（一般的には 6 桁の）擬似乱数です。保護されているリソースにアクセスしようとすると、ネットワークにインストールされている認証エージェントから、トークンコードとユーザーの暗証番号（PIN）の入力を求められます。トークンコード（ユーザーが所有している要素）と PIN（ユーザーが記憶している要素）の組み合わせをパスコードと呼びます。

エージェントはパスコードを Authentication Manager に送信し、Authentication Manager はユーザーが本人であることを検証してからネットワークへのアクセスを許可します。

## 用語や概念についての重要な変更

RSA Authentication Manager の物理的および論理的構造が変更されました。次の表は、バージョン 8.0 で導入された新しい用語を古い用語と対応づけて説明しています。

| バージョン 6.1 での用語 | バージョン 8.0 での用語 | コメント |
|---|---|---|
| サーバ | インスタンス | インスタンスとは、Authentication Manager の物理的なインストールを指します。1 つの導入環境には、1 つのプライマリ インスタンスと、所有するライセンスに応じて最大 15 のレプリカ インスタンスを配置できます。プライマリ インスタンスとレプリカ インスタンスはそれぞれ内部データベースを持ちます。 |

| バージョン 6.1 での用語 | バージョン 8.0 での用語 | コメント |
|---|---|---|
| レルム | 導入環境 | バージョン 8.0 では、1 つのプライマリ インスタンスと、関連するレプリカ インスタンスによって 1 つの導入環境が構成されます。各導入環境には 1 つのレルムがあります。<br>バージョン 6.1 では、プライマリ Authentication Manager とそのレプリカ サーバから成る物理的なインストール環境をレルムと呼びます。すべてのオブジェクトはレルム内に存在しますが、組織の階層は、レルム、サイト、グループという、より単純なモデルに従います。 |
| レルム間 | トラステッド レルム | バージョン 8.0 では、レルム間の信頼を確立するには、信頼パッケージと呼ばれるファイルを送付する必要があります。 |
| サイト | セキュリティ ドメイン | セキュリティ ドメインとは、導入環境内の管理領域を定義する組織コンテナです。セキュリティ ドメインは、部門やパートナーなどのビジネスユニットごとに作成できます。導入環境内のオブジェクト（ユーザー、ロール、権限、他のセキュリティ ドメインなど）の所有権やネームスペースを設定します。セキュリティ ドメインは階層構造になっています。<br>バージョン 8.0 のセキュリティ ドメインには、下位のセキュリティ ドメインとユーザー グループを含めることができます。バージョン 6.1 のサイトはレルムよりも 1 つ下の階層にあり、ユーザーならびにユーザーのグループを含みますが、他のサイトを含めることはできません。 |

| バージョン 6.1 での用語 | バージョン 8.0 での用語 | コメント |
|---|---|---|
| グループ | ユーザー グループ | ユーザー グループはグループと同じです。エージェント ホストでグループをアクティブ化する機能や、アクセス時間を制御する機能は、バージョン 8.0 でも引き続き使用できます。<br>バージョン 8.0 のユーザー グループは階層構造になっており、ネストできます。 |
| ユーザー | ユーザー | バージョン 8.0 では、個別のユーザーに対するアクセス時間制限がサポートされなくなりました。この機能は、ユーザー グループごとに提供されます。<br>エージェントではユーザー アクティブ化は行えなくなり、グループ アクティブ化のみを行えます。 |
| エージェント | エージェント | バージョン 8.0 では、エージェントを追加するときに、特定のエージェント タイプ（UNIX エージェントやシングル トランザクション サーバなど）を指定する必要はありません。<br>移行処理の中で、エージェントを移行する際に自己登録エージェントの IP アドレスを維持するかどうかを指定できます。 |
| 管理者ロール | 管理者ロール | Authentication Manager 6.1 のデフォルト ロール（レルム、サイト、グループ）の権限適用範囲とタスク リストは移行されます。バージョン 8.0 では、権限の集合を定義することでロールを作成します。作成後、そのロールを管理者に割り当てます。ロールの権限適用範囲は、ロールが作成されたセキュリティ ドメインによって定義されます。 |

| バージョン 6.1 での用語 | バージョン 8.0 での用語 | コメント |
|---|---|---|
| 権限適用範囲 | 権限適用範囲 | バージョン 6.1 では、管理者ロールの権限適用範囲は管理対象者を定義します。たとえば、バージョン 6.1 では、管理者の権限適用範囲はレルム、サイト、グループのいずれかになります。<br>バージョン 8.0 では、管理者ロールの権限適用範囲をセキュリティ ドメインにしたことで、管理の柔軟性が大幅に向上しました。付与する権限を構成することにより、各ロールの管理機能を細かく区別できます。 |
| タスク リスト | 管理者ロール | デフォルトのタスク リスト（レルム、サイト、グループ）は、ロールと呼ばれる管理者権限の集合に移行されます。バージョン 8.0 のロールには、管理者にタスクの実行を許可する権限が含まれます。バージョン 6.1 のカスタム タスク リストは、同様の管理機能に近いロールに移行されます。バージョン 8.0 には、この他に事前定義のロールが用意されています。詳細については、32 ページの「事前定義の管理者ロール」を参照してください。 |
| 該当なし | アイデンティティ ソース | 内部データベースまたは指定した LDAP ディレクトリです。<br>ユーザーとユーザー グループのデータは、どちらのタイプのアイデンティティ ソースにも保存できます。製品固有のデータは、内部データベースに保存されます。 |

| バージョン 6.1 での用語 | バージョン 8.0 での用語 | コメント |
|---|---|---|
| LDAP 同期ジョブ | 該当なし | バージョン 6.1 と同様に、バージョン 8.0 でも既存のユーザー データとユーザー グループ データを使用できます。ただし、バージョン 8.0 では、定期的または手動により LDAP 同期ジョブを実行して内部データベースを更新するのではなく、最新の LDAP データに実行時にアクセスできるようになりました。<br>この結果、最新の LDAP データが常に使用可能になり、認証に使用できるようになりました。 |

## Authentication Manager 8.0 の機能拡張

次の表では、RSA Authentication Manager 8.0 仮想アプライアンスの機能を、RSA SecurID Appliance のバージョン 2.0、2.0.1、2.0.2 と比較しています。

| | RSA SecurID Appliance 2.0、2.0.1、2.0.2 の機能 | Authentication Manager 8.0 の新機能 |
|---|---|---|
| **オペレーティング システム** | Microsoft Windows 2003 | SuSE Linux |
| **必要な経験** | Microsoft Windows に精通している。 | システム管理者が Linux オペレーティング システムにログオンする必要が生じることはほとんどありません。 |
| **オペレーティング システムの保守** | 基本的なシステム管理タスクには、Appliance の Web UI（ユーザー インタフェース）からアクセスできます。<br>システム管理者がオペレーティング システムの保守を行うには、Microsoft Windows のリモート デスクトップ機能を使用して Appliance にログオンする必要があります。ログオンは、クライアント コンピュータから直接実行することも、Appliance の Web UI にある［**Advanced（詳細）**］タブを使用することもできます。 | システム管理者は、Web ベースの Operations Console にログオンします。ほとんどのシステム保守タスクについても、このコンソールから実行できます。 |

| | RSA SecurID Appliance 2.0、2.0.1、2.0.2 の機能 | Authentication Manager 8.0 の新機能 |
|---|---|---|
| **プリインストールされている Authentication Manager のバージョン** | Appliance のバージョンに応じて、RSA Authentication Manager 6.1、6.1.1、6.1.2、6.1.3、6.1.4 のいずれか。 | RSA Authentication Manager 8.0 |
| **RSA RADIUS サーバ** | RSA RADIUS サーバをダウンロードし、RSA SecurID Appliance 2.0 にインストールできます。RSA RADIUS のアップグレードは、Appliance アップグレードに含まれています。 | RSA RADIUS 8.0 は、RSA Authentication Manager 8.0 に完全に統合されたコンポーネントとしてプリインストールされています。 |
| **Web ベースのインタフェースで利用できる機能** | 2 つの Web インタフェースを使用して、いくつかの機能にアクセスできます。<br>• Authentication Manager の一般的な機能は、Appliance の Web UI から利用できます。<br>• システム管理者やヘルプ デスク管理者は、Authentication Manager の Quick Admin を使用して、RSA Authentication Manager プライマリ データベースに保存されたユーザー、トークン、拡張レコード データの、表示と変更を実行できます。<br>その他すべての機能に関しては、Appliance のデスクトップにログオンして Authentication Manager 管理ツールを使用する必要があります。 | Authentication Manager のほとんどの機能は、Security Console、Operations Console、Self-Service Console から実行できます。使用頻度が低いいくつかの管理タスクは、コマンド ライン ユーティリティで実行します。 |
| **サポートされている認証方式** | Appliance の Web UI では、ハードウェア トークンを管理できます。<br>ソフトウェア トークンは、Windows リモート デスクトップ経由の Authentication Manager 管理ツールで管理できます。 | Security Console を使用して、ハードウェア トークンとソフトウェア トークンを管理できます。<br>Authentication Manager 8.0 では、RBA（リスク ベース認証）がサポートされます。<br>On-Demand トークンコードがサポートされます。On-Demand トークンコードを有効にした場合は、モバイル デバイスまたはメール アカウントを所有しているユーザーが、ワン タイム トークンコードをテキスト メッセージとして受信できます。 |

| | RSA SecurID Appliance 2.0、2.0.1、2.0.2 の機能 | Authentication Manager 8.0 の新機能 |
|---|---|---|
| **LDAP の統合** | LDAP ディレクトリから RSA Authentication Manager 6.1 データベースにユーザー データをコピーできます。LDAP を同期するには、Appliance に含まれる Windows ベースの 4GL インタフェースを使用します。 | RSA Authentication Manager 8.0 データベースは、LDAP ディレクトリからユーザー データおよびユーザー グループ データをリアルタイムで読み取ります。LDAP 管理者のみが、LDAP ネイティブ インタフェース経由でユーザーとユーザー グループを変更できます。Authentication Manager はこの目的には使用できません。 |
| **リモート トークン キー生成（CT-KIP）** | リモート トークン キー生成（CT-KIP）はサポートされていません。 | リモート トークン キー生成（CT-KIP）はサポートされています。CT-KIP を使用すると、ソフトウェア トークンをホストするデバイス（Web ブラウザなど）と Authentication Manager が、同一のトークン ファイルを同時に安全に生成できます。この場合は、トークン ファイルをメールで送信したり、USB ドライブなどの電子メディアに保存したりすることなく、ユーザーのデバイス上にトークン ファイルを配置できます。そのため、不正ユーザーによりトークン ファイルが傍受される危険性が大幅に軽減されます。 |
| **SNMP** | RSA SecurID Appliance 2.0 用の SNMP プラグ インをダウンロードしてインストールできます。 | SNMP は完全に統合されています。Web ベースの管理インタフェース（Security Console）を使用して、Authentication Manager ソフトウェア用に SNMP を構成できます。 |
| **NIC（ネットワーク インタフェース カード）** | すべてのネットワーク ポートはブリッジ接続されるため、使用する NIC を問いません。 | 1 つの仮想 NIC がサポートされます。 |

## Authentication Manager 8.0 のライセンス タイプ

各 Authentication Manager 導入環境には、ライセンスがインストールされている必要があります。このライセンスは、Authentication Manager アプライアンスを使用する権利を付与します。

次のライセンス タイプがあります。

**Base Server**：Authentication Manager の 1 つのプライマリ インスタンスと 1 つのレプリカ インスタンスを許可する永久ライセンス。

**Enterprise Server**：Authentication Manager の 1 つのプライマリ インスタンスと最大 15 個のレプリカ インスタンスを許可する永久ライセンス。Enterprise Server ライセンスには、トークンのプロビジョニング機能も含まれます。

各ライセンス タイプは、インストール可能な Authentication Manager のインスタンス数を制限します。ユーザー数の制限は、お客様のご使用要件に依存しています。

たとえば、従業員数 10,000 人のお客様の場合は、現在の従業員に加えて、将来的に雇用することになる従業員の数を考慮に入れて、11,000 ユーザー分のライセンスを購入されることが考えられます。

次の点を理解しておくことが重要です。

- 複数のライセンスをインストールできます。
- アカウント ID は、すべてのライセンスで同じである必要があります。
- ライセンス ID はスタック ID とも呼ばれ、各ライセンスで一意である必要があります。同じ ID のライセンスを 2 回インストールすることはできません。
- ライセンスの対象としてカウントされるのは、トークンが割り当てられているユーザーだけです。複数のトークンを割り当てられたユーザーは、1 回だけカウントされます。
- Security Console には、ユーザー数制限が近づくと警告メッセージが表示されます。メッセージが表示されるのは、ユーザー数制限が 85、95、100% を超えたときです。
- ユーザー カウントは毎時間システムによって更新されます。また、ユーザーが Security Console で［License Status（ライセンス ステータス）］ページを表示する度に更新されます。

次の表は、各ライセンス タイプの属性を示しています。

| ライセンス機能 | Base Server | Enterprise Server |
|---|---|---|
| トークンを割り当てるユーザー数 | 購入時にお客様が指定 | 購入時にお客様が指定 |
| インスタンス数 | 2[1] | 16（1 つのプライマリ インスタンスと 15 のレプリカ インスタンス） |

| ライセンス機能 | Base Server | Enterprise Server |
|---|---|---|
| RBA/ODA | オプション | オプション |
| 事業継続 | オプション | オプション |
| RADIUS | はい | はい |
| オフライン認証 | はい | はい |
| トークン | はい | はい |
| セルフ サービス | はい | はい |
| トークン プロビジョニング | いいえ | はい |

[1] インスタンス数が 2 までに制限されたライセンスでも、災害復旧用として 3 番目のインスタンスを使用できます。

事業継続オプションでは、ライセンスで通常許可されるユーザー数を超えるユーザーに一時的に RSA SecurID 認証を使用させることができます。RSA では、事業継続オプションを使用して作成したユーザーについては、トークンを割り当てて送付する必要が生じないように、On-Demand トークンコードの受信を有効にすることを推奨します。ただし、必要に応じて、RSA SecurID トークンをこれらのユーザーに割り当てることもできます。

特定の機能を追加したり、ユーザー数を追加する必要がある場合は、追加のライセンスを取得する必要があります。

## リスクベース認証

RBA（リスク ベース認証）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 認証および従来のパスワード ベースの認証を強化します。評価リスクが許容できない場合、ユーザーは次のいずれかの方法によってユーザー本人であることを証明するよう要求されます。

- ODA（On-Demand 認証）。ユーザーは、PIN、および、事前に設定した携帯電話番号またはメール アカウントに送信されたワンタイム トークンコードを正確に入力する必要があります。
- セキュリティ クエスチョン。ユーザーは、1 つ以上のセキュリティ クエスチョンに正しく回答する必要があります。質問の正解は、Self-Service Console で構成するか、またはサイレント収集期間に認証を行う時に構成します。

Authentication Manager には、各ユーザーのデバイスと行動パターンに関する情報をインテリジェントに収集して分析するリスクエンジンが含まれています。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。その後、リスクエンジンはユーザーの認証試行に高、中、低などの保証レベルを割り当てます。RBA は、この保証レベルを、あらかじめ構成された許容可能な最低保証レベルと比較します。保証レベルが最低保証レベルに満たない場合、このユーザーにはセキュリティ クエスチョンまたは ODA を使用したユーザー確認が求められます。

## Web Tier

Web Tier は、いくつかの AuthenticationManager サービスをネットワーク DMZ 内で安全にホストする軽量のアプリケーション サーバです。RBA（リスク ベース認証）、CT-KIP（Cryptographic Token Key Initialization Protocol）によるソフトウェア トークンの動的配布、Self-Service Console などのサービスは、企業ネットワークの外のユーザーからの利用が必要となる場合があります。ネットワークに DMZ がある場合、このようなサービスを DMZ に導入するために、Web Tier を使用します。

Web Tier を DMZ に導入するメリットは次のとおりです。

- Self-Service Console、CT-KIP サーバ、RBA のユーザーによって生じ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 サーバが、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し、管理します。
- RBA サービスや Web ベース アプリケーションのユーザー 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。

プライマリおよびレプリカ インスタンスはプライベート ネットワークのファイアウォールの内側に配置します。

## Authentication Manager 8.0 のアーキテクチャの変更

バージョン 6.1 では、プライマリ サーバが管理用サーバであり、正統なデータ ソースであるプライマリ データベースが配置されています。プライマリ サーバは次の処理を実行します。

- データベース管理
- レプリカ サーバへの変更のレプリケーション
- （オプション）ユーザーの認証

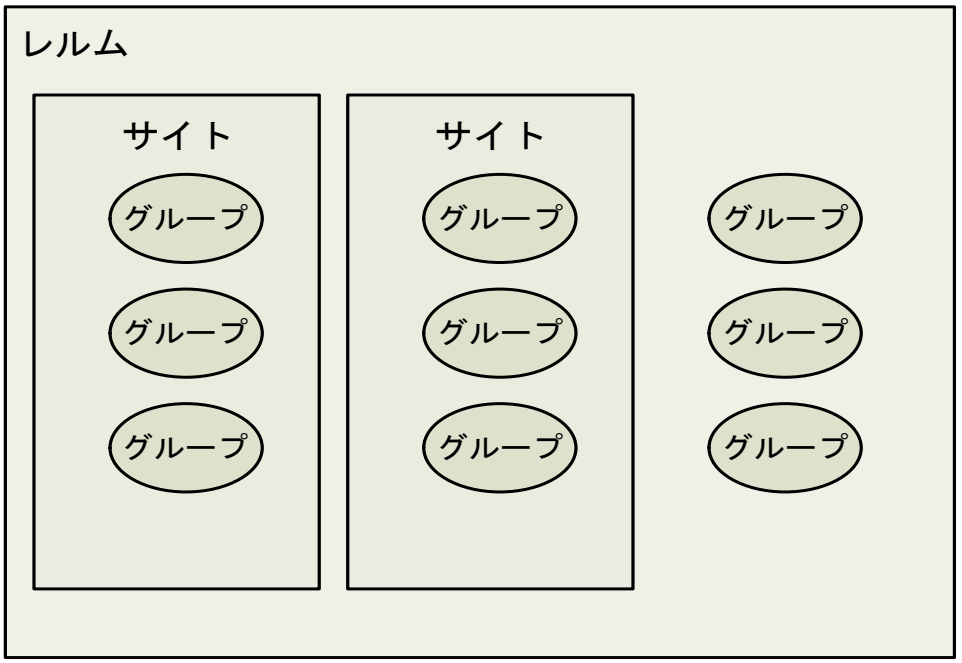
バージョン 8.0 では、プライマリ インスタンスがこれらの機能を実行できます。

Authentication Manager は、LDAP ディレクトリに保存されたユーザーやユーザー グループのデータはレプリケーションしません。LDAP の変更をレプリケーションする場合は、LDAP を構成する必要があります。

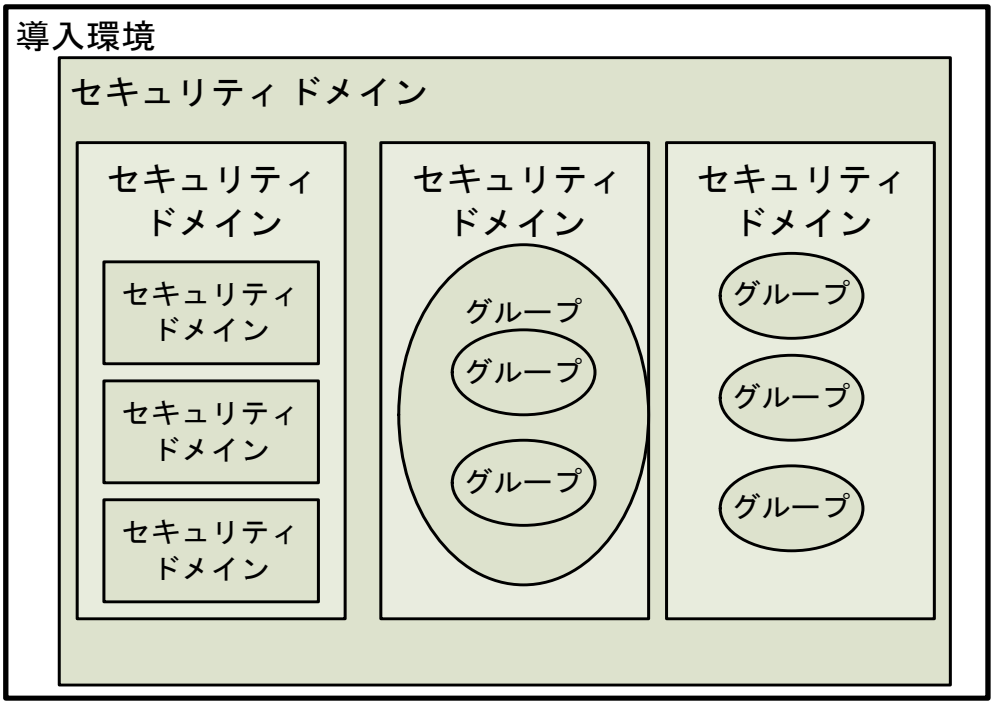
RSA Authentication Manager 6.1 の論理的アーキテクチャは、レルム、サイト、グループの階層構造に基づいています。レルムには、ユーザー、サイト、グループが含まれます。サイトにはユーザーとグループが、グループにはユーザーが含まれます。バージョン 8.0 では、この厳格な階層構造を拡張して、1 つの階層チェーンに複数のセキュリティ ドメインを配置できるようになりました。バージョン 6.1 では、1 つの導入環境で複数の仮想レルムがサポートされていました。バージョン 8.0 では 1 つのレルムだけがサポートされます。次の表に、階層内のオブジェクトと、オブジェクトに含めることのできるオブジェクトの名前を、バージョン 6.1 とバージョン 8.0 で比較します。

| オブジェクト | バージョン 6.1 | バージョン 8.0 |
|---|---|---|
| レルム（バージョン 6.1）/ 導入環境（バージョン 8.0） | サイト<br>グループ<br>ユーザー | セキュリティ ドメイン<br>ユーザー グループ<br>ユーザー |
| サイト（バージョン 6.1）/ セキュリティ ドメイン（バージョン 8.0） | グループ<br>ユーザー | セキュリティ ドメイン<br>ユーザー グループ<br>ユーザー |
| グループ | ユーザー | ユーザー グループ<br>ユーザー |

次の図に、RSA Authentication Manager 6.1 での階層を示します。




次の図に、RSA Authentication Manager 8.0 での階層を示します。



## サイトへの変更

バージョン 8.0 のセキュリティ ドメインは、バージョン 6.1 のサイトに相当します。ただし、セキュリティ ドメインは階層的にネストできます。さらに、セキュリティ ドメインは、管理者の権限適用範囲を特定のオブジェクトのグループに限定する唯一の方法です。管理者の権限適用範囲をグループに限定することはできません。

セキュリティ ドメインは、管理者が責任を負う領域を表し、通常はビジネス ユニット、部門、パートナーなどを表します。セキュリティ ドメインは導入環境内のオブジェクト（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。Authentication Manager のすべてのオブジェクトは、セキュリティ ドメインによって管理されます。セキュリティ ドメインを使用することで、次の操作が可能になります。

- ユーザーの編成と管理
- システム ポリシーの適用
- 管理の委譲
  セキュリティ ドメインへのアクセスを制限することにより、管理者の管理できる範囲を制限できます。

新しい導入環境をインストールしたときに、最上位のセキュリティ ドメインが自動的に作成されます。

デフォルトでは、外部 LDAP アイデンティティ ソース内のすべてのユーザーは、最上位のセキュリティ ドメインに追加されます。Security Console を使用してこれらのユーザーを手動で下位のセキュリティ ドメインに移動するか、ドメイン マッピングを構成してこれらのユーザーを特定のセキュリティ ドメインに追加できます。管理者が Security Console を使用して内部データベースに作成したユーザーは、その管理者がアクセス権を持つセキュリティ ドメインに追加されます。

たとえば、経理、R&D（研究開発）、HR（人事）などの部門別にセキュリティ ドメインを作成しておき、各部門のユーザーとユーザー グループを対応するセキュリティ ドメインに移動できます。

管理者が、特定のセキュリティ ドメイン内のユーザーを管理するためには、そのセキュリティ ドメインを管理する権限を持っている必要があります。次の点を理解しておくことが重要です。

- セキュリティ ドメインは、導入環境内に階層状に編成されます。
- 通常、セキュリティ ドメインは、組織の部門構造や地理的な位置に応じて作成されます。
- Authentication Manager バージョン 8.0 では、最大 1,000 個のセキュリティ ドメインがサポートされます。サポート数を超えるセキュリティ ドメインを使用する計画があるときは、RSA カスタマー サポートにお問い合わせください。

### ポリシーとセキュリティ ドメイン

セキュリティ ドメインでは、ユーザーと Authentication Manager とのやり取りのさまざまな側面（たとえば、RSA SecurID PIN の有効期間と形式、固定パスコードの有効期間と形式、パスワードの長さ、形式、変更の頻度など）を制御するシステム ポリシーが適用されます。

各セキュリティ ドメインには次のポリシーが割り当てられています。

- パスワード ポリシー
- トークン ポリシー
- ロックアウト ポリシー
- リスク ベース認証ポリシー
- セルフ サービス トラブルシューティング ポリシー
- オフライン認証ポリシー
- ワークフロー ポリシー
- リスク ベース認証メッセージ ポリシー

新しいセキュリティ ドメインを作成すると、デフォルト ポリシーが自動的に割り当てられます。カスタム ポリシーを割り当てることもできます。デフォルトとして使用するポリシーは選択可能で、必要に応じて変更できます。

下位のセキュリティ ドメインは、上位のセキュリティ ドメインからポリシーを継承しません。新しいセキュリティ ドメインには、階層内の上位のセキュリティ ドメインに割り当てられているポリシーにかかわらず、デフォルト ポリシーが適用されます。たとえば、最上位のセキュリティ ドメインにカスタム ポリシーを割り当てても、下位のセキュリティ ドメインではデフォルト ポリシーが引き続き使用されます。

## ユーザー グループへの変更

セキュリティ ドメインの階層を構築できるようになったため、バージョン 8.0 ではユーザー グループの必要性が小さくなりました。その結果、ユーザー グループはバージョン 6.1 のようには機能しなくなりました。

ユーザー グループの特徴は、次のとおりです。

- ユーザー グループには複数のユーザーおよびユーザー グループを含めることができます。
  外部アイデンティティ ソース内のユーザー グループには、同一のアイデンティティ ソースに属するユーザーとユーザー グループのみ含めることができます。内部データベース内のユーザー グループには、導入環境内の任意のアイデンティティ ソースのユーザーとユーザー グループを含めることができます。

- ユーザー グループには、異なるセキュリティ ドメインで管理されているユーザーやユーザー グループも含めることができます。つまり、セキュリティ ドメイン A に属するユーザーとセキュリティ ドメイン B に属するユーザーを同一のユーザー グループに追加し、同一の保護されたリソースへのアクセスを許可できます。
  導入環境内のあらゆるオブジェクト（ユーザー、ユーザー グループ、エージェントなど）は、1 つのセキュリティ ドメインにしか所属できないため、そのグループが所属するセキュリティ ドメインの管理者の権限では、バージョン 6.1 から移行されたグループに所属するすべてのメンバーを見ることができない場合があります。
- ユーザーは複数のユーザー グループに所属できます。

ユーザー グループは、Security Console で作成するか、Active Directory などの外部アイデンティティ ソースの場合はディレクトリのユーザー インタフェースを使用して作成できます。

バージョン 8.0 では、管理者の権限適用範囲をユーザー グループに制限できません。グループに対する権限を制御するには、そのグループが存在するセキュリティ ドメインを権限適用範囲として使用します。これは、管理者の権限適用範囲としてグループを使用するバージョン 6.1 とは異なります。

たとえば、サイトに属していないバージョン 6.1 グループは、スーパー管理者が管理する最上位のセキュリティ ドメインに移行されます。グループがサイトに属している場合は、グループは移行されたサイト用に作成された下位のセキュリティ ドメインに移行されます。サイト管理者、つまり下位のセキュリティ ドメインの管理者は、下位のセキュリティ ドメインを管理します。

### エージェントでのユーザーとユーザー グループのアクティブ化の移行

バージョン 8.0 では、制限付き認証エージェントでのグループのアクティブ化をサポートし、グループのアクセス時間を制限できますが、個々のユーザーのアクティブ化はサポートされていません。エージェントに対して個々のユーザーをアクティブ化することはできなくなったため、移行の際にはグループのアクティブ化を使用して同様の動作を維持します。

次の表では、エージェントでアクティブ化されたグループに対する移行の影響について説明します。

| 移行前 | 移行後 |
|---|---|
| 制限付きエージェントでアクセス時間制限付きでアクティブ化されたグループ | グループはアクセス時間制限付きで移行され、エージェントでアクティブ化される。グループ名の形式は次のようになる。<br>AM61_user*aceIDofUserGroup_FQDNofagent_ISname*<br>エージェントは制限付きエージェントのまま残る。 |
| 制限付きエージェントでアクセス時間制限なしでアクティブ化されたグループ | グループはアクセス時間制限なしで移行され、エージェントでアクティブ化される。グループ名の形式は次のようになる。<br>*Agent_Name*<br>エージェントは制限付きエージェントのまま残る。 |

| 移行前 | 移行後 |
| --- | --- |
| 制限なしエージェント上でアクセス時間制限付きでアクティブ化されたグループ | グループはアクセス時間制限付きで移行され、エージェントでアクティブ化される。グループ名の形式は次のようになる。<br>AM61_user*aceIDofUserGroup_FQDNofagent_ISname*<br>エージェントは制限付きエージェントとして移行される。<br>制限なしエージェントを制限付きエージェントに変換した結果、そのエージェントで（直接に、またはエージェントでアクティブ化されたグループのメンバーシップを通じて）アクティブ化されていないユーザーは、そのエージェントで認証を受けることができなくなる。 |
| 制限なしエージェントでアクセス時間制限なしでアクティブ化されたグループ | グループはアクセス時間制限なしで移行され、エージェントでアクティブ化される。グループ名の形式は次のようになる。<br>*Agent_Name*<br>エージェントは制限付きエージェントとして移行される。<br>制限なしエージェントを制限付きエージェントに変換した結果、そのエージェントで（直接に、またはエージェントでアクティブ化されたグループのメンバーシップを通じて）アクティブ化されていないユーザーは、そのエージェントを通じて認証を受けることができなくなる。 |

次の表では、エージェントでアクティブ化されたユーザーに対する移行の影響について説明します。

| 移行前 | 移行後 |
| --- | --- |
| 制限付きエージェントでアクセス時間制限付きでアクティブ化されたユーザー | 1 人のユーザーのみ含む内部グループが作成され、エージェントでアクティブ化される。<br>グループのアクセス時間は、ユーザーがバージョン 6.1 で割り当てられていたアクセス時間と同じ時間に制限される。<br>エージェントは制限付きエージェントのまま残る。 |
| 制限付きエージェントでアクセス時間制限なしでアクティブ化されたユーザー | 1 人のユーザーのみ含むグループが作成され、エージェントでアクティブ化される。<br>グループはアクセス時間が制限されない。<br>エージェントは制限付きエージェントのまま残る。 |

| 移行前 | 移行後 |
| --- | --- |
| 制限なしエージェントでアクセス時間制限付きでアクティブ化されたユーザー | 1 人のユーザーのみ含む内部グループが作成され、エージェントでアクティブ化される。<br>グループのアクセス時間は、ユーザーがバージョン 6.1 で割り当てられていたアクセス時間と同じ時間に制限される。<br>エージェントは制限付きエージェントとして移行される。<br>制限なしエージェントを制限付きエージェントに変換した結果、そのエージェントで（直接に、またはエージェントでアクティブ化されたグループのメンバーシップを通じて）アクティブ化されていないユーザーは、そのエージェントを通じて認証を受けることができなくなる。 |
| 制限なしエージェントでアクセス時間制限なしでアクティブ化されたユーザー | エージェントでアクティブ化されたすべてのユーザーを含む内部グループが作成され、そのグループがエージェントでアクティブ化される。<br>グループはアクセス時間が制限されない。<br>エージェントは制限付きエージェントとして移行される。 |

### LDAP ユーザーおよび非 LDAP ユーザーを含むグループの移行

バージョン 6.1 の管理では、LDAP ユーザーと非 LDAP ユーザー、つまり LDAP 同期ジョブによってデータベースに追加されたユーザーと、Database Administration アプリケーションで追加されたユーザーが混在するグループが許可されていました。バージョン 8.0 では、内部データベースに移行したユーザー グループに、導入環境内の任意のアイデンティティ ソースのユーザーとユーザー グループを含めることができます。次の表は、LDAP ユーザーと非 LDAP ユーザーが含まれるグループがどのように移行されるかを示しています。

| バージョン 6.1 | バージョン 8.0（移行後） |
| --- | --- |
| 外部グループ（EG1）に次のものが含まれる。<br>• LDAP グループにリンクされた LDAP ユーザー<br>• LDAP グループにリンクされていない LDAP ユーザー<br>• 非 LDAP ユーザー | LDAP ディレクトリ サーバの外部グループ（EG1）にリンクされたユーザーは、引き続き LDAP と外部グループ（EG1）に属する。<br>Authentication Manager は内部グループ（IG1）を作成し、ユーザーを次のように移行する。<br>• すべての非 LDAP ユーザーは、内部グループ（IG1）に追加される。<br>• 外部グループ（EG1）が LDAP ディレクトリ サーバに存在しない場合、リンクされた LDAP ユーザーは内部グループ（IG1）に追加される。<br>• 外部グループ（EG1）が LDAP ディレクトリ サーバに存在するが、ユーザーがリンクされていない場合、リンクされていない LDAP ユーザーは内部グループ（IG1）に追加される。 |
| 外部グループ（EG2）に非 LDAP ユーザーだけが含まれる。 | Authentication Manager は内部グループ（IG2）を作成し、すべての非 LDAP ユーザーを追加する。 |
| 外部グループ（EG3）に LDAP ユーザーだけが含まれる。 | • LDAP ディレクトリ サーバ内の外部グループ（EG3）にリンクされたユーザーは、引き続き LDAP と外部グループ（EG3）に属する。<br>• 外部グループ（EG3）が LDAP ディレクトリ サーバに存在しない場合、Authentication Manager は新しい内部グループ（IG3）を作成する。この存在しないグループにリンクされたユーザーは、内部グループ（IG3）に追加される。<br>• 外部グループ（EG3）が LDAP ディレクトリ サーバに存在するが、ユーザーがリンクされていない場合、Authentication Manager は新しい内部グループ（IG3）を作成する。リンクされていない LDAP ユーザーは、内部グループ（IG3）に追加される。 |
| 内部グループ（IS1）に LDAP ユーザーと非 LDAP ユーザーが含まれている。 | Authentication Manager は、LDAP ユーザーと非 LDAP ユーザーの両方を同じ内部グループ（IS1）に追加する。 |

## レプリケーション モデル

バージョン 8.0 のレプリケーション モデルには、次のような利点があります。

- ハードウェア障害発生時のデータ リカバリやデータ損失の最小化

  詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「災害復旧」の章を参照してください。
- レプリカ インスタンスの昇格による、管理のフェイルオーバー
- 認証のフェイルオーバー。プライマリ インスタンスがオフラインになった場合にも認証を継続できます。

レプリカ インスタンスで発生したすべての変更は、プライマリ インスタンスにコピーされます。その後、導入環境内の他のすべてのレプリカ インスタンスにその変更がコピーされます。

レプリケーションにより、内部データベースに対して次の 2 つのタイプの更新が反映されます。

**管理更新：**ユーザーの追加や削除など、管理に関するすべての変更は、プライマリ インスタンスで実行する必要があります。プライマリ インスタンスは、管理に関する変更をすべてのレプリカ インスタンスに反映します。

**ランタイム更新：**ユーザーの認証結果などのランタイム更新は、プライマリ インスタンスおよびすべてのレプリカ インスタンスで発生する可能性があります。レプリカ インスタンスでランタイム更新が発生すると、更新は最初にプライマリ インスタンスに反映されます。その後、更新はプライマリ インスタンスによって他のすべてのレプリカ インスタンスに反映されます。

## レプリカ インスタンスでのランタイム更新

次の表に、レプリカ インスタンスで発生する可能性のあるランタイム更新を示します。

| オブジェクト | レプリケーションされる変更 |
|---|---|
| ユーザー | ユーザーの固定パスコードまたは PIN の変更 |
| エージェント | • 自動登録によるエージェントの作成<br>• コンタクト リストへのエージェントの割り当て<br>• ノード シークレットの更新 |

| オブジェクト | レプリケーションされる変更 |
| --- | --- |
| トークン | 次の処理の結果として生じた変更<br>• 認証<br>• トークンの交換。既存のトークンの無効化、割り当て解除、削除や、交換トークンの割り当て、有効化など。実際の変更は、トークンの交換方法に関する Authentication Manager の構成内容により異なります。<br>• エマージェンシー パスコードの処理<br>• エージェントへのオフライン認証データの配布<br>• ソフトウェア トークンのシードの初期化 |

レプリカ インスタンスのログ データは、認証の結果生じる変更と同じ方法ではレプリケーションされません。ログ データは、プライマリ インスタンスのみに送信され、プライマリインスで一元的に保存されます。このログは導入環境内のすべてのインスタンスにはレプリケーションされません。

Authentication Manager は、LDAP ディレクトリ上のユーザーやユーザー グループのデータはレプリケーションしません。LDAP の変更をレプリケーションする場合は、LDAP を構成する必要があります。

## 管理機能

バージョン 8.0 では、バージョン 6.1 で Database Administration アプリケーションを使用したのと同様に、Security Console を使用して管理タスクを実行できます。リモート クライアント ソフトウェアを管理者用ハードウェアにインストールする必要はありません。Security Console はブラウザ ベースであるため、正しく構成されたサポート対象ブラウザからアクセスできます。

### ブラウザ ベースの管理の変更点

バージョン 8.0 は、導入環境の管理と構成のために次の管理ユーザー インタフェースを備えています。

- **Security Console**。RSA RADIUS の管理を含め、日常的な管理を行うブラウザ ベースのインタフェース。

  このコンソールから、日常的な管理タスクにアクセスできます。Security Console のインタフェースには、使用する管理者の管理者権限と権限適用範囲が反映されるため、その管理者に割り当てられたロールに対応するタスクとオブジェクトのみが表示されます。バージョン 6.1 の Database Administration アプリケーションで実行していたほとんどすべてのタスクは、Security Console から実行できます。

- **Operations Console**。Authentication Manager ユーティリティの実行、RSA RADIUS の構成、データ移行等を行うためのブラウザ ベースのインタフェース。このコンソールは、使用頻度の低いタスク（バージョン 6.1 レルムからのデータ移行や、RADIUS サーバの構成など）を行うために使用します。

- **Self-Service Console**。トークンのリクエスト（プロビジョニング機能が有効である場合）やセルフ サービス タスクを実行するためのユーザー向けのブラウザ ベースのインタフェース。このコンソールでは、トークンのアクティブ化、認証のテスト、アカウント登録、トークンのリクエスト、ユーザー グループ メンバーシップのリクエスト、トラブルシューティング タスクなどを行うことができます。

  Self-Service Console に表示される機能は、Authentication Manager にインストールされたライセンスによって変わります。

## 管理者の権限適用範囲の拡大

バージョン 8.0 の管理モデルは、ロール、権限、権限適用範囲という概念に基づいて構築されています。Authentication Manager には、事前定義された管理者ロールが存在しますが、カスタマイズしたロールを作成することもできます。詳細については、32 ページの「事前定義の管理者ロール」を参照してください。

次の表では、管理者を定義する要素について説明しています。

| 要素 | 説明 |
|---|---|
| ロール | 管理者が管理できる対象。たとえば、ユーザー アカウントなど。 |
| 権限 | 管理者が実行できる処理。たとえば、ユーザーにトークンを割り当てるなど。 |
| 権限適用範囲 | 管理者の権限が適用される境界範囲。権限適用範囲はセキュリティ ドメインによって決定します。 |

管理者ロールは、次の 2 つの要素で構成されています。

- 職務内容に基づいた権限の集合。
  権限はバージョン 6.1 でのタスク リストと同じです。
- 権限が適用される範囲。
  権限適用範囲は、バージョン 6.1 と同様に機能します。ただし、バージョン 8.0 では、管理者ロールの権限適用範囲をより柔軟に設定できるようになっています。権限適用範囲は、セキュリティ ドメインの階層に基づいて調整または拡張できます。バージョン 6.1 では、権限適用範囲はレルム、サイト、グループによって決定していました。

管理者ロールは、権限適用範囲内のいずれのユーザーにも割り当てることができます。ユーザーは、指定したセキュリティ ドメイン内で、割り当てられたロールに含まれる管理操作を実行できます。1 人の管理者に複数の管理者ロールを割り当てることもできます。

バージョン 8.0 の管理者ロールの詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「RSA Authentication Manager の管理の準備 」の章を参照してください。

### 事前定義の管理者ロール

バージョン 6.1 のロールは、タスク リスト（ロールを割り当てられた管理者がどのタスクを実行できるか）と権限適用範囲（管理者がどのオブジェクトを管理できるか）によって定義されます。事前定義のロールとして、レルム、サイト、グループの 3 つのロールが用意されています。各ロールを管理者に割り当てることにより、その管理者の権限適用範囲をレルム、レルム内の特定のサイト、レルム内の特定のグループのいずれかに設定できます。

次のセクションでは、バージョン 8.0 でのデフォルトの管理者ロールについて説明します。

- Super Admin（スーパー管理者）

  事前定義されたロールのうち、最も重要となるのがスーパー管理者ロールです。これは、導入環境内のすべてのセキュリティ ドメインに対するすべての管理者権限が付与されている唯一のロールです。このロールでは、他の管理者の作成や、セキュリティ ドメインの階層を作成できます。

  RSA では、スーパー管理者ロールを少なくとも 2 人の管理者に割り当てることを推奨します。このようにすることで、1 人のスーパー管理者が休暇を取ったり、長期間不在になった場合にも完全な管理制御を維持できます。

  RSA では、スーパー管理者ロールを最上位のセキュリティ ドメインに保存し、その他の管理者ロールは下位のセキュリティ ドメインに保存することを推奨します。これにより、たとえばヘルプ デスク 管理者ロールを持つ下位の管理者が、スーパー管理者のパスワードを変更し、そのパスワードを使用して Security Console にアクセスするといった事態を防止できます。

- Root Domain Administrator（ルート ドメイン管理者）このロールは、ポリシーや属性定義などの最上位のオブジェクトを含む、セキュリティ ドメインのすべての要素を管理する完全な管理責任を付与します。このロールにはスーパー管理者の一部の権限が含まれていません。

- Security Domain Administrator（セキュリティ ドメイン 管理者）

  このロールは、セキュリティ ドメインのツリー構造の、特定の分岐内のすべての要素を管理するための完全な管理責任を付与します。このロールの管理者は、ポリシーや属性定義などの最上位のオブジェクト管理を除いて、その分岐内に対するすべての権限を持ちます。デフォルトでは、このロールの権限適用範囲は導入環境全体となります。このロールの権限適用範囲を導入環境内の下位のセキュリティ ドメインに制限する場合は、このロールを編集するか、このロールを複製してから、複製したロールの権限適用範囲を編集します。このロールは、ロールが作成されたセキュリティ ドメインに制限されます。このロールの管理者は、自分のロールの一部の権限を委譲できます。

- User Administrator（ユーザー管理者）

  このロールは、ユーザーの管理、ユーザーへのトークンの割り当て、選択した認証エージェントへのアクセスの管理を行うための管理責任を付与します。このロールの管理者は、自分のロールの権限を委譲することはできません。

- Token Administrator（トークン管理者）

  この管理者ロールは、トークンのインポートと管理、ユーザーへのトークンの割り当てをするための完全な管理責任を付与します。このロールの管理者は、自分のロールの権限を委譲することはできません。

- Token Distributor（トークン配布者）

  このロールは、トークンのプロビジョニング要求を管理するための管理責任を付与します。トークン配布者は、ユーザーにトークンを割り当て、送付する方法も決定します。このロールの管理者は、自分のロールの権限を委譲することはできません。

- Request Approver（リクエスト承認者）

  このロールは、トークンのプロビジョニング要求を承認、更新、拒否するための管理責任を付与します。要求には、新しいユーザー アカウント、ユーザー グループ メンバーシップ、トークン、On-Demand トークンコード サービスなどが含まれます。このロールの管理者は、自分のロールの権限を委譲することはできません。

- Help Desk Administrator（ヘルプデスク管理者）

  このロールを割り当てられた管理者は、パスワードのリセット、アカウントのロック解除、アカウントの有効化などを行い、ユーザー のアクセスに関する問題を解決します。このロールの管理者は、自分のロールの権限を委譲することはできません。

- Agent Administrator（エージェント管理者）

  このロールは、認証エージェントの管理、認証エージェントへのアクセス権の付与を行うための管理責任を付与します。このロールの管理者は、自分のロールの権限を委譲することはできません。

これらのロールのデフォルトの権限の一覧など、詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「RSA Authentication Manager の管理の準備」の章を参照してください。

バージョン 8.0 のインストール時に、スーパー管理者ロールが割り当てられる初期スーパー管理者ユーザーを作成できます。次の表は、バージョン 6.1 のロールがどのように移行されるかを示しています。

| バージョン 6.1 | バージョン 8.0 |
|---|---|
| Realm Administrator | Root Domain Administrator |
| Site Administrator | Security Domain Administrator |
| Group Administrator | カスタム管理者ロールとして移行されるが、バージョン 6.1 のグループ管理者には割り当てられない。 |
| カスタム管理者 | カスタム管理者ロールとして移行される。 |

### グループ管理者

バージョン 8.0 では、管理者の権限適用範囲をグループに設定することができなくなりました。管理者の権限適用範囲はセキュリティ ドメインのみに設定できます。グループ管理者ロールは移行されますが、バージョン 6.1 におけるグループ管理者には割り当てられません。これは、移行した管理者の権限適用範囲がバージョン 6.1 での範囲よりも広くなることを防ぐためです。

たとえば、バージョン 6.1 のグループ管理者は、自分の権限適用範囲に含まれるグループ内のユーザーのみを表示および変更できます。グループ管理者を管理者として移行した場合、移行後の権限適用範囲はセキュリティ ドメインに設定されます。しかし、移行前には権限適用範囲に含まれていなかった他のユーザーやグループがセキュリティ ドメインに含まれる可能性があるため、権限適用範囲が広くなる可能性があります。移行プロセスでは、これらの管理者の権限をこのように拡張せずに制限するようにします。

移行後、以前のグループ管理者は管理者ではなくなります。このような以前のグループ管理者には、管理者ロールを明示的に割り当てるとともに、その権限の適用範囲を特定のセキュリティ ドメインに限定する必要があります。

## カスタム管理アプリケーション

バージョン 6.1 の API（Application Programming Interface）を使用して作成された管理者用ユーティリティは使用できなくなりました。これは、RSA Authentication Manager 8.0 ソフトウェアが Java を使用して完全に書き換えられたためです。バージョン 6.1 の管理用 API では、C および TCL の関数が提供され、管理用アプリケーションや TCL スクリプトを開発できました。バージョン 8.0 の API では、C#、Java、Jython のみが提供されます。カスタム管理アプリケーションは、新しい API を使用して書き換える必要があります。

## Authentication Manager のリアルタイム Activity Monitor

Activity Monitor では、Authentication Manager で発生したアクティビティのログ メッセージをリアルタイムで表示できます。それぞれの Activity Monitor には異なるタイプの情報が表示されます。

**Authentication Activity Monitor**：認証を受けているユーザー、認証リクエストの送信元などの情報を示します。

**System Activity Monitor**：アクティビティの時間、アクティビティの説明、アクティビティの処理が成功したかどうかを表示します。

**Administration Activity Monitor**：ユーザーがいつ追加または削除されたか、トークンがいつ割り当てられたかなど、Authentication Manager の導入環境への変更を表示します。

Activity Monitor を無期限に実行することはできなくなりました。バージョン 8.0 では、Activity Monitor は構成した時間の経過後に自動的にタイム アウトします。

Activity Monitor に表示するメッセージの種類を構成できます。たとえば、特定の管理者、ユーザー ID、認証エージェント、セキュリティ ドメインのアクティビティを表示するように Administration Activity Monitor を構成できます。

## レポート テンプレート

Authentication Manager に付属する事前定義されたレポート テンプレートを使用して、システム イベントやオブジェクト（ユーザーやトークンなど）についてのカスタマイズしたレポートを作成および実行できます。これらのレポートは、システム イベントの詳細情報を提供します。

各テンプレートには、定義済みの変数、列見出し、その他のレポート情報が含まれています。使用可能なレポート テンプレートの一覧については、「Authentication Manager 8.0 管理者ガイド」の「ログとレポート」の章を参照してください。

**重要：**バージョン 6.1 で作成したカスタム SQL クエリーや TCL スクリプトは、バージョン 8.0 には移行されません。既存のレポート テンプレートを確認して、カスタム クエリーの機能と、事前定義レポート テンプレートの機能とを照合してください。バージョン 8.0 でのカスタム クエリーの開発については、「Authentication Manager 8.0 Developer's Guide」を参照してください。

バージョン 8.0 では、Security Console でレポートを表示できます。またレポートは、カンマ区切り値、HTML、XML など、複数の形式で表示できます。

## RSA RADIUS

RSA RADIUS サーバは、Authentication Manager の管理インタフェースに完全に統合されました。RADIUS サーバを管理するには、Operations Console を使用します。次の操作を行えます。

- 導入環境内の RADIUS サーバの一覧、各 RADIUS サーバの IP アドレスとレプリケーション ステータスを表示します。
- RSA RADIUS が使用する証明書（RADIUS サーバ証明書と EAP（拡張認証プロトコル）認証用の信頼できるルート証明書を含む）を管理します。
- RADIUS ディクショナリ ファイル、構成ファイルなどの RADIUS サーバ ファイルを管理します。
- RADIUS サーバを再起動します。

RADIUS サーバのその他の管理には、Security Console を使用します。Security Console を使用して、RADIUS の日常的な管理タスクのほとんどを実行できます。これらの管理タスクは、RADIUS サーバ、クライアント、プロファイル、ユーザー属性に関するものです。

## レルム間認証とトラステッド レルムの比較

バージョン 8.0 のトラステッド レルムは、バージョン 6.1 のレルム間認証と同様に機能します。どちらの機能も、ビジターユーザーによるネットワークへのアクセスを許可します。2 つのレルム間で信頼関係を構築し、一方のレルムのユーザーがもお一方の信頼するレルムのエージェントで認証を受けられるようになります。

レルム間認証とトラステッド レルムには、4 つの大きな違いがあります。

- バージョン 8.0 のレルムは、信頼パッケージを交換する必要があります。
- バージョン 8.0 では、信頼は一方向と双方向のいずれも可能ですが、バージョン 6.1 のレルム間認証は常に双方向です。
- バージョン 8.0 では、管理者が、トラステッド レルムにアクセスできるユーザーをより詳細に制御できます。
- バージョン 8.0 のトラステッド レルムでは、他のバージョン 8.0 のトラステッド レルムからの RADIUS ユーザーの認証がサポートされますが、バージョン 6.1 レルムからの認証はサポートされません。バージョン 6.1 のレルム間認証では、相手がバージョン 6.1 のレルム、バージョン 8.0 のレルムのいずれであっても、RADIUS ユーザーの認証はサポートされません。

バージョン 8.0 では、「ホーム」レルムや「リモート」レルムという用語は使用されず、トラステッド レルムという用語だけが使用されます。

バージョン 6.1 でレルム間の関係を確立するときには、管理者は相手レルムの管理者にパスコードの数字のセットを提供する必要があります。レルム間の関係が確立し有効化されると、双方のレルムのユーザーが、相手レルムのオープン エージェントを通じて認証を受けられるようになります。

バージョン 8.0 では、管理者が自分のレルムに属するユーザーを他のレルム（トラステッド レルム）で認証できるようにする場合、信頼パッケージを使用してクレデンシャルを交換する必要があります。管理者が信頼パッケージをトラステッド レルムに送付した後、トラステッド レルムの管理者は信頼パッケージを自分のレルムにインポートします。

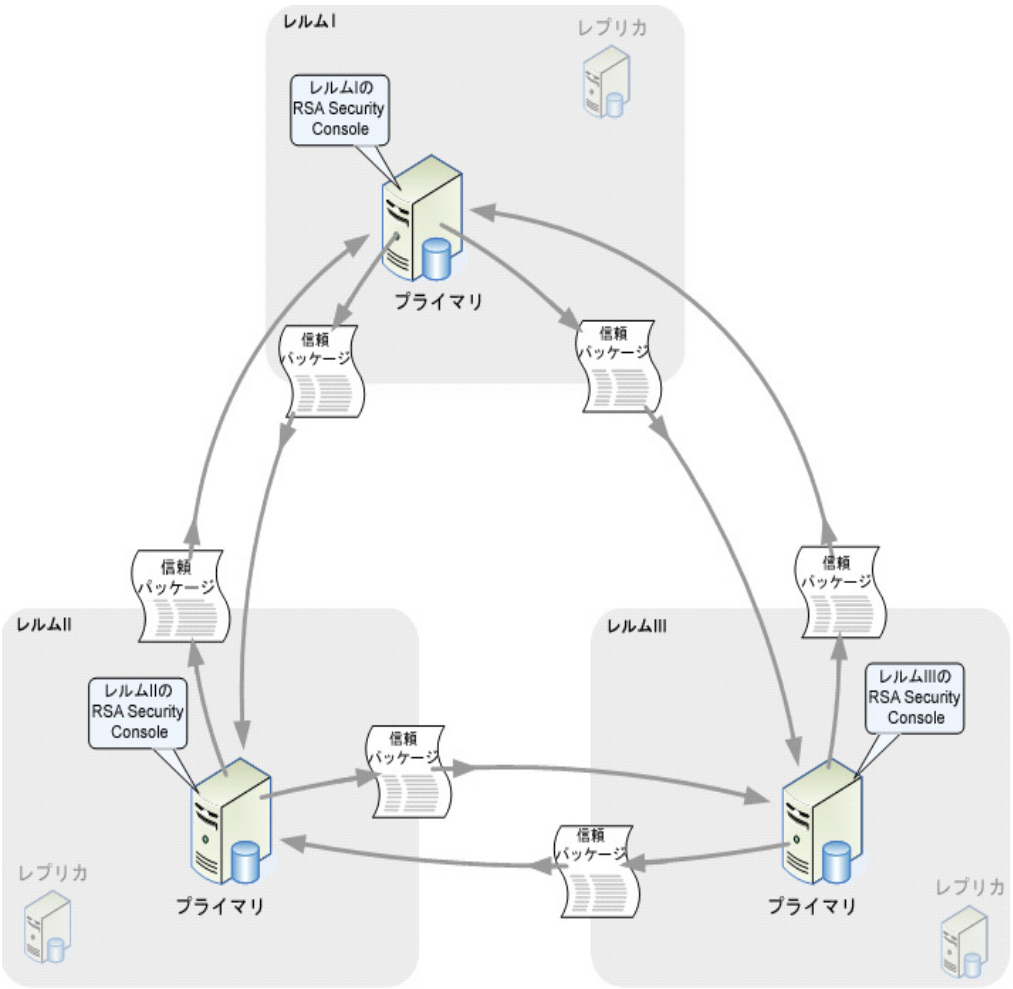
**注：**既存のすべてのレルム間の信頼関係を移行できます。バージョン 6.1 とバージョン 8.0 のレルム間で新たに信頼関係を確立することもできます。これは、Database Administration アプリケーションを使用して、バージョン 6.1 のレルムから実行する必要があります。詳細については、バージョン 6.1 のヘルプで「Setting Up Cross-Realm Authentication」のトピックを参照してください。

バージョン 8.0 のレルムでは、バージョン 6.1 レルムのユーザーを認証できます。ただし、バージョン 6.1 のトラステッド レルムをバージョン 8.0 に移行すると、移行後のバージョン 8.0 レルムと他のすべてのバージョン 8.0 レルムの間の信頼情報は無効になります。そのため、これらの信頼関係を再確立またはアップグレードする必要があります。移行後のバージョン 8.0 のレルムと、他のバージョン 6.1 のレルムとの間の信頼情報は維持されます。

### 一方向または双方向のトラステッド レルム

バージョン 6.1 でのレルム間認証の関係は常に双方向ですが、バージョン 8.0 のトラステッド レルムの関係は、一方向と双方向のいずれも可能です。一方向のトラステッド レルムでは、レルム A のユーザーはレルム B で認証を受けられますが、レルム B のユーザーはレルム A で認証を受けられません。双方向のトラステッド レルムでは、いずれのレルムのユーザーも他方のレルムで認証を受けられます。この機能により、レルムに対する管理制御が強化されて、他のレルムとの信頼関係の確立が、レルムの管理者の了解と承認のもとに計画的に実行されるようになります。

次の図では、3 つのレルム間での双方向のトラステッド レルム関係を示しています。




バージョン 8.0 では、管理者は次のタスクを実行することにより、トラステッドレルムにアクセスするユーザーを制御できます。

- レルム内に複製認証エージェント レコードを作成する。
- エージェントを制限付きエージェントにする。
- ユーザーをユーザー グループに追加する。
- エージェントに対してユーザー グループをアクティブ化する。

次の表では、バージョン 8.0 で確立できる信頼関係の 3 つのタイプについて説明します。

| 信頼関係のタイプ | 説明 | 信頼関係の確立方法 |
|---|---|---|
| バージョン 8.0 の 2 つのレルム間での一方向信頼 | レルム A のユーザーがレルム B で認証を受けることはできるが、逆のことはできない。 | 1. レルム B の管理者が、レルム A をトラステッド レルムとして追加する。<br>2. レルム B の管理者が、レルム A から受け取った信頼パッケージをインポートする。 |
| バージョン 8.0 の 2 つのレルム間での双方向信頼 | レルム A のユーザーがレルム B で認証を受けることができ、逆のこともできる。 | 1. レルム B の管理者が、レルム A をトラステッド レルムとして追加する。<br>2. レルム A の管理者がレルム B をトラステッド レルムとして追加する。<br>3. 双方の管理者が、信頼パッケージを作成、交換、インポートする。 |
| バージョン 6.1 とバージョン 8.0 のレルム間での双方向信頼 | バージョン 8.0 のユーザーがバージョン 6.1 のレルムで認証を受けることができ、逆のこともできる。 | 1. バージョン 6.1 のレルム管理者がバージョン 6.1 のデータベースにバージョン 8.0 のレルムを作成し、レルム シークレットをインポートする。<br>2. バージョン 8.0 のレルムで、バージョン 8.0 のレルムの代わりにバージョン 6.1 のレルムをトラステッド レルムとして追加する。 |

# 2 移行の計画

## 移行計画チェックリスト

移行プロセスを開始する前に、次のタスクを完了します。

- ❑ Authentication Manager 6.1 から 8.0 への移行アセスメントを実行します。42 ページの「Authentication Manager 6.1 から 8.0 への移行アセスメントの完了」を参照してください。
- ❑ 移行パスを決定する。
  - バージョン 6.1 と同じホスト名および IP アドレスを使用してバージョン 8.0 に移行する。
  - 新しいホスト名および IP アドレスを使用してバージョン 8.0 に移行する。
- ❑ 使用するアイデンティティ ソースを決定する。
  - 内部データベース
  - Microsoft Active Directory Server
  - Sun Java System Directory Server
  - Oracle Directory Server Enterprise Edition 11G
- ❑ 移行を担当する管理者が、バージョン 6.1 で次のタスクを実行するために必要なアクセス権と管理権限を持っていることを確認する。
  - データベースのダンプ
  - データベースをクリーンアップするために必要な管理タスクの実行

    データベースのクリーンアップが必要となる可能性のある問題の詳細については、101 ページの「移行レポート」を参照してください。
- ❑ 使用する Web ブラウザがサポートされるブラウザであり、RSA コンソールにアクセスできるように正しく構成されていることを確認する。サポートされている Web ブラウザのリストについては、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
- ❑ バージョン 6.1 のサーバで管理や認証などのサービスにカスタム ポートが使用されているかどうかを確認する。既存のサーバでカスタム ポートが使用されている場合は、移行後にバージョン 8.0 を構成して、同じポートを使用するように設定する必要があります。

- ❑ インストールされている認証エージェントがサポート対象であることを確認する。認証エージェントには次のタイプがあります。
  - RSA Authentication Agent
  - エージェント ソフトウェアが組み込まれた RSA Secured サード パーティ デバイス
  - バージョン 5 の認証 API を使用して作成されたカスタム エージェント

  バージョン 5 より前の認証 API を使用して開発したカスタム エージェントはサポートされていません。
- ❑ LDAP 同期ジョブをアイデンティティ ソースにマッピングする方法を決定する。
- ❑ バージョン 6.1 から移行するデータを決定する。
- ❑ 特定のセキュリティ ドメインへの移行が必要なデータがあるかどうかを判断する。

  特定のセキュリティ ドメインへ移行すると、一部の管理者の管理能力が影響を受ける可能性があります。
- ❑ NTLM 形式のユーザー ログオン名を UPN 形式に変換する必要があるかどうかを判断する。
- ❑ RSA Deployment Manager で未処理になっているトークン プロビジョニング要求をすべて解決する。
- ❑ RSA Authentication Manager バージョン 8.0 が導入されていることを確認する。導入の手順については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」を参照してください。
- ❑ バージョン 8.0 導入環境のスナップショットまたはバックアップを作成する。操作手順については、45 ページの「バージョン 8.0 導入環境のスナップショットまたはバックアップの作成」を参照してください。
- ❑ RADIUS サーバを移行するかどうかを決定する。プライマリ サーバを移行する前に、RADIUS を移行する必要があります。
- ❑ レプリカ インスタンスを追加する予定の場合は、プライマリ インスタンスの移行を完了してから、バージョン 8.0 レプリカ インスタンスを追加してください。

## Authentication Manager 6.1 から 8.0 への移行アセスメントの完了

RSA では、バージョン 8.0 に移行する前に、RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility を実行することを推奨しています。このユーティリティはデータベースを分析し、データの非互換性など移行の前に解決する必要がある問題や、期限切れトークンなどクリーンアップが必要な可能性がある領域があるかどうかを判別します。移行の前に、不要なデータや非互換データの問題を解決しておくと、バージョン 8.0 に正常に移行できます。

RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility および「RSA Authentication Manager 6.1 to 8.0 Migration Preparation Guide」は、SecurCare オンラインからダウンロードできます。
**https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9620** にアクセスしてください。

## 移行パスの選択

移行の際は、正しいアップグレード パスを選択することが最も重要なステップの 1 つとなります。次のいずれかの方法を選択します。

- 既存の 6.1 導入環境と同じホスト名と IP アドレスを使用して、バージョン 6.1 データをバージョン 8.0 導入環境に移行する。詳細については、43 ページの「同じホスト名および IP アドレスを使用した移行」を参照してください。
- 新しいホスト名と IP アドレスを使用して、バージョン 6.1 データをバージョン 8.0 導入環境に移行する。詳細については、44 ページの「新しいホスト名および IP アドレスを使用した移行」を参照してください。

バージョン 8.0 に移行する際、各インスタンスのホスト名と IP アドレスを移行後も維持するかどうかを決定する必要があります。どちらの方法にも、それぞれ長所と短所があります。

### 同じホスト名および IP アドレスを使用した移行

移行前と同じホスト名および IP アドレスを使用する場合は、新しい構成ファイル（**sdconf.rec**）を生成して各エージェントに配布する必要がないため、認証エージェントの更新に要する時間と労力を節約できます。

ただし、既存のバージョン 6.1 導入環境をネットワークから削除し、同じ名前と IP アドレスを使用して新しいバージョン 8.0 導入環境を追加するときに、Authentication Manager サーバは一時的に使用不可になります。バージョン 8.0 をテスト環境に導入すると、影響を最小限にとどめることができます。これにより、既存のバージョン 6.1 導入環境をシャットダウンした後、ただちにバージョン 8.0 導入環境をテスト環境から本番ネットワークに移動できます。バージョン 8.0 をテスト環境に導入すると、本番環境に移行する前に問題を検出して解決することが可能になります。

さらに、エージェントに新しいコンタクト リスト（導入環境内のすべてのサーバのリスト）が送信されるように、各 RSA Authentication Agent から **sdstatus.12** ファイルを削除する必要があります。

### 新しいホスト名および IP アドレスを使用した移行

バージョン 8.0 導入環境で新しいホスト名と IP アドレスを使用する場合は、新しい構成ファイルを生成して各認証エージェントに配布するための追加の時間が必要です。構成ファイルには、新しいホスト名と IP アドレスが含まれます。その操作を行うまで、認証エージェントはバージョン 8.0 インスタンスのホスト名と IP アドレスを認識できないため、認証リクエストを正しい Authentication Manager に送信することができません。したがって、ユーザーは認証できません。導入環境内のエージェントの数を調べ、それらをすべて更新するために必要となる時間を検討してください。

さらに、既存のレルム間の信頼関係がある場合は信頼を再確立する必要があります。

RSA Authentication Manager 6.1 または RSA SecurID Appliance 2.0 に戻す必要がある場合は、次の操作を実行します。

- バージョン 8.0 のインスタンスをシャットダウンして、バージョン 6.1 またはバージョン 2.0 サーバを再起動します。
- 構成ファイル（**sdconf.rec**）を各認証エージェントに再分配します。
- エージェントに新しいコンタクト リスト（導入環境内のすべてのサーバのリスト）が送信されるように、各 RSA Authentication Agent から **sdstatus.12** ファイルを削除します。

## 認証エージェントのサポート

移行後もユーザーが既存のエージェントおよび RSA Secured ハードウェアを通じて確実に認証を受けることができるように、既存のシステムにインストールされているすべての認証エージェントが Authentication Manager 8.0 でサポートされているエージェントであることを確認します。バージョン 5 以降のエージェントがサポートされています。

### 自動登録およびレガシー モード

バージョン 6.1 からバージョン 8.0 にアップグレードすると、自動登録は、レガシー モードに設定されます。レガシー モードは、自動登録エージェントを使用して IP アドレスの再割り当てを制御します。自動登録の詳細については、「RSA Authentication Manager 8.0 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。

### RSA Authentication Agent

サポートされている RSA Authentication Agent のリストは、RSA Web サイトの「RSA Authentication Agent Supported Platforms」からダウンロードできます。**http://japan.emc.com/security/rsa-securid/rsa-securid-authentication-agents.htm** にアクセスして、［**Resources**］をクリックします。

### サード パーティ製品の組み込みエージェント

RSA Secured Partner Solutions Directory 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。このディレクトリには、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実装ガイドおよびその他の情報が含まれています。

ネットワーク上にサード パーティ エージェントが存在する場合は、www.rsasecured.com にアクセスして、そのエージェント製品を検索し、バージョン 8.0 でサポートされているかどうかを確認します。

### 認証 API を使用して作成されたカスタム エージェント

バージョン 5 の認証 API を使用して開発されたカスタム認証エージェントがサポートされます。バージョン 5 より前の認証 API を使用して開発したカスタム エージェントはサポートされていません。

これらのエージェントのバージョンを確認するには、45 ページの「カスタム Windows エージェントの API バージョンの確認」を参照してください。

### カスタム Windows エージェントの API バージョンの確認

RSA Authentication Manager 8.0 への移行後も、ユーザーが既存のカスタム Windows エージェントを使用した認証を続行できることを確認するには、カスタム Windows エージェントの開発で使用された認証 API のバージョンを確認します。RSA Authentication Manager 8.0 では、バージョン 5 以降の認証 API がサポートされます。

**処理手順**

1. 各エージェントで **aceclnt.dll** ファイルを検索します。
2. ファイルを右クリックし、［**Properties**（プロパティ）］を選択します。
3. ［**Version**（バージョン）］タブをクリックします。

## バージョン 8.0 導入環境のスナップショットまたはバックアップの作成

移行するデータの形式が正しく安全であることを確認するために、RSA では、テスト システムで複数回の移行テストを実施することを推奨します。データの移行を再度実行する場合は、以前に移行したバージョン 6.1 のデータをすべてバージョン 8.0 のデータベースから削除する必要があります。そのためには、Authentication Manager 8.0 をインストールした直後に、次の操作のいずれかを実行する必要があります。

- バージョン 8.0 導入環境のスナップショットを作成します。

  Authentication Manager インスタンスのスナップショットを作成するときは、次の設定を指定する必要があります。

  – 仮想マシンのメモリは保存しないでください。

  – 静止ゲスト ファイル システムを選択します。このオプションでは、Authentication Manager インスタンスで実行中のプロセスが一時停止します。

  詳細については、VMware vSphere Client のドキュメントを参照してください。
- バージョン 8.0 データベースのバックアップを作成します。Operations Console ヘルプの「即時バックアップによるバックアップの作成」のトピックを参照してください。

## データ移行オプション

データ移行では、次の 3 つのモードの 1 つを選択する必要があります。

- 46 ページの「標準モード」
- 46 ページの「ローリング アップグレード モード」
- 47 ページの「カスタム モード」

### 標準モード

標準モードの移行では、次の操作が実行されます。

- テスト移行ではなく、本番の移行を実行する。
- データ競合が検出された場合に移行を停止せずに、ベスト エフォート方式でデータを移行する。
- 見つかったオブジェクトをすべて移行する。
- LDAP ユーザーを含め、ユーザーとユーザー グループをすべて内部データベースに移行する。
- すべてのオブジェクトを内部データベースに移行する。

### ローリング アップグレード モード

ローリング アップグレード モードでは、ダンプ ファイルに見つかったデルタ レコードのみ移行されます。デルタレコードは、プライマリ インスタンスの移行中にレプリカ インスタンス上に蓄積されたデータベースの変更をトラッキングしたものです。このモードは、レプリカ サーバの移行時に選択します。

## カスタム モード

カスタム モードでは、ダンプ ファイル内に見つかったオブジェクトのうち、特定のオブジェクトを移行の対象として選択できます。テスト移行を実行することもできます。カスタム モードでは、次のカスタマイズが可能です。


- 47 ページの「テスト移行」
- 47 ページの「LDAP ジョブとアイデンティティ ソースの同期」
- 49 ページの「移行中のデータ競合」
- 49 ページの「データのサブセットの移行」
- 49 ページの「特定のセキュリティ ドメインへのデータ移行」
- 50 ページの「NTLM から UPN へのログオン名の変換」
- 50 ページの「サポートされていない文字の置換」


### テスト移行

**カスタム モード** では、テスト移行を実行できます。

テスト移行では、次の操作が実行されます。

- 実際にデータを移行せずに（つまり、データベースに一切影響を与えずに）移行の結果を表示する。
- ダンプ ファイルのデータを処理する。ただし、変更をデータベースにコミットすることはない。
- 実際の移行を実行した際に発生する変更について詳細なレポートを生成する。

テスト移行は、実際の移行と同じ方法で実行するように構成できます。たとえば、ダンプ ファイル内のデータのすべてまたは一部を処理するか、またはデータ競合が検出されても処理を続行するように構成できます。テスト移行の完了後、生成された移行レポートを確認することで、データがどのように処理されるかを把握したり、競合の重大度を判別したり、データ移行後に競合を修正する方法を計画したりすることができます。

データの変換と移行レポートの詳細については、95 ページの付録 A、「移行データの変換」を参照してください。

### LDAP ジョブとアイデンティティ ソースの同期

**カスタム モード**では、LDAP ジョブをアイデンティティ ソースにマッピングできます。バージョン 8.0 では、LDAP ディレクトリ内のユーザー データおよびユーザー グループ データをリアルタイムに直接参照します。バージョン 6.1 では、データベースが LDAP ディレクトリと同期されます。大きな違いは、バージョン 6.1 ではデータベースに LDAP データのコピーが格納されるのに対し、バージョン 8.0 ではデータベースに LDAP ディレクトリ内のデータへの参照が格納される点です。LDAP ユーザーおよびユーザー グループを更新できるのは、LDAP 管理者のみです。

バージョン 6.1 のデータの移行中に LDAP 同期ジョブをアイデンティティ ソースにマッピングする方法を指定するよう Operations Console にプロンプトが表示されます。RSA では、移行を開始する前に、LDAP 同期ジョブをアイデンティティ ソースにマージする方法の計画を立てておくことを推奨します。

アイデンティティ ソースをマッピングするときに Operations Console に表示されるアイデンティティ ソースは、環境にリンクされているものに限られます。

バージョン 6.1 で複数の LDAP 同期ジョブを使用していた場合は、移行プロセスの中で、各ジョブに対して 1 つのアイデンティティソースを作成できます。ただし、複数の同期ジョブを 1 つのアイデンティティ ソースにマッピングすることにより、アイデンティティ ソースおよびユーザーの管理に伴う負荷を軽減できる場合があります。

バージョン 6.1 で LDAP 同期ジョブを構成するには、次の情報を指定する必要があります。

- LDAP ホスト
- ベース DN

  各同期ジョブについて、ベース DN をチェックし、1 つのアイデンティティ ソースにマージできる共通のベース DN が存在しないかどうかを確認します。
- 適用範囲

  ジョブの適用範囲では、ベース DN の下位でジョブの対象とする階層の数を指定します。ジョブの適用範囲がベース DN のみか、またはベース DN の 1 つ下位の階層のみの場合は、1 つのアイデンティティ ソースへの結合が可能なジョブがディレクトリ ツリーの下位に存在している可能性があります。
- クエリー フィルタ（オプション）

  クエリー フィルタは、特定の基準を満たすユーザーを選択するために指定します。ディレクトリ側で同時に更新できるレコード数の制限に対処するために Authentication Manager 側でユーザーにフィルタを適用していた場合は、フィルタをなくしてジョブをマージできます。たとえば、ユーザーを姓に基づいて選択するフィルタが複数のジョブに使用されていることがあります。あるジョブのフィルタでは姓が A ～ G で始まるユーザーを選択し、別のジョブのフィルタでは H ～ S で始まるユーザー、さらに別のジョブのフィルタでは T ～ Z で始まるユーザーを選択している、というケースが考えられます。このようなジョブが同じベース DN を持っている場合は、それらを 1 つのアイデンティティ ソースに結合します。

### 移行中のデータ競合

**カスタム モード**の移行では、次の方法でダンプ ファイル内のデータ競合を処理するように構成できます。

- データ競合が検出されたら、そのデータ競合を記録し、残りのデータの移行を続行する。
- データ競合を検出した場合、移行を停止する。
  競合が検出される前に行われた変更は、データベースに維持されます。

テスト移行を使用すると、データ競合に関する懸念を軽減でき、実際にデータベースに変更を加える前に移行による結果を確認できます。

### データのサブセットの移行

**カスタム モード**では、移行するデータを選択できます。バージョン 8.0 では、ダンプ ファイル内のデータにフィルタを適用できるため、特定のデータのみを移行して、他のデータを無視できます。ダンプ ファイルに対しては、次のデータ タイプに基づくフィルタを適用できます。

- システム設定
  たとえば、許可されている管理者認証方式、Windows パスワードの統合ステータス、PIN の長さの要件、パスワードの有効期限など。
- 管理者ロール
- レルム間の信頼関係
- RSA RADIUS プロファイル名と割り当て
- アクティブな LDAP 同期ジョブ

### 特定のセキュリティ ドメインへのデータ移行

**カスタム モード**では、特定のセキュリティ ドメインへのデータの移行を選択できます。たとえば、バージョン 6.1 の複数のレルムを 1 つのバージョン 8.0 の最上位セキュリティ ドメインに移行する場合、バージョン 6.1 の各レルムに対応する下位のセキュリティ ドメインを作成し、そのセキュリティ ドメインにデータを移行することによって、既存の構造の一部を維持することが可能です。

スーパー管理者は、導入環境内の任意のセキュリティ ドメインにデータを移行できます。下位の管理者がダンプ ファイル内のデータを移行する場合、移行先として選択できるセキュリティ ドメインは、その管理者の権限適用範囲に含まれているセキュリティ ドメインのみです。そのような場合、Operations Console にはそれらのセキュリティ ドメインのみ表示されます。

### NTLM から UPN へのログオン名の変換

バージョン 8.0 では、UPN（ユーザー プリンシパル名）形式のユーザー ログオン名の使用と格納が可能です。たとえば、**auser@domain.com** は UPN 形式の名前です。バージョン 6.1 では、ユーザー ログオン名を NTLM（Windows NT LAN Manager）形式で格納します（たとえば、**DOMAIN\auser**）。NTLM 形式の名前をそれに対応する UPN 形式の名前にマッピングすることができます。これにより、既存の認証エージェントからの認証リクエストを処理できるようになります。

マッピングを実行しないことを選択した場合は、既存のエージェントがユーザーを認証できない可能性があることに注意してください。

### サポートされていない文字の置換

バージョン 8.0 では、特定のデータベース レコードで、次の文字の使用がサポートされていません。

`< > & % '`

これらの文字の使用が許可されていない移行レコードとそのフィールドは、次のとおりです。

| レコード | フィールド |
|---|---|
| AgentAlternates | Net Address |
| Agent | Name、Net Address |
| EnabledUser | Login、Shell |
| Extension | Key、Value |
| Group | Login、Shell |
| Site | Name |
| TaskList | Name |
| User | Login、First Name、Last Name、Shell、Remote Alias |

6.1 データベースにこれらの文字を使用するレコードが含まれる場合、**カスタム移行**は、移行中に次のように文字を自動置換するオプションを提供します。

| サポートされていない文字 | 置換 |
|---|---|
| & | + |
| < | { |

| サポートされていない文字 | 置換 |
|---|---|
| ＞ | } |
| % | / |
| ` | ' |

RSA では、［**Replace Unsupported Characters（サポートされていない文字を置換）**］を選択してテスト移行を実行することを推奨しています。結果として出力される移行レポートを使用して、サポートされていない文字を使用しているレコードと、上記の置換により更新された値を識別します。バージョン 6.1 のレコードを手動で更新して、移行前に、サポートされていない文字を削除することもできます。

**重要：**実際の移行時に［**Replace Unsupported Characters（サポートされていない文字を置換）**］を選択すると、影響を受けるデータが変更されます。これには、ユーザー ID やユーザー拡張データが含まれます。実行する前に、このデータの変更の意味を考慮してください。たとえば、ユーザー ID を変更すると、認証の失敗や、外部のアイデンティティ ソースまたはトラステッド レルムへの接続障害が発生することがあります。

実際の移行時に［**Replace Unsupported Characters（サポートされていない文字を置換）**］オプションを使用する場合、結果として出力される移行レポートには、文字置換によって修正されたすべてのレコードが表示されます。

**重要：**サポートされていない文字を削除または置換せずに移行を進めても、それらの文字が含まれるレコードは移行されません。

## セルフ サービス データおよびプロビジョニング データの移行

旧バージョンの Authentication Manager で提供されていた、セルフ サービス / プロビジョニング ソリューションである RSA Deployment Manager は、廃止されました。トークン プロビジョニングは Security Console に統合され、ユーザー セルフ サービスは Self-Service Console に統合されました。

Deployment Manager データは、Self-Service Console に移行されません。このため、Deployment Manager のプロビジョニング機能を使用するライセンスを保持している場合は、バージョン 8.0 への移行を開始する前に、未処理のプロビジョニング要求がすべて処理されているか確認する必要があります。移行を行うと、未処理のすべてのリクエストが失われます。Self-Service Console を適切に構成した後、移行前にリクエストを送信していたユーザーに対して、リクエストを新たに送信する必要があることを通知する必要があります。

トークン プロビジョニング機能を使用するには、Enterprise Server ライセンスが必要です。

バージョン 8.0 には、アカウント登録要求とトークン要求の処理を担当する管理者に割り当てるため、事前定義のリクエスト承認者およびトークン配布者のロールが用意されています。

## SNMP のレポート

RSA Authentication Manager バージョン 8.0 に含まれる SNMP 機能を使用するためには、SNMP を構成する必要があります。以前の構成設定は移行されません。

RSA SecurID Appliance 2.0 以降では、RSA SecurID Appliance 2.0 用の SNMP プラグ インがサポートされていました。このオプションのソフトウェアでは、RSA Authentication Manager 6.1 以降のトラップが設定されます。Appliance 以外の RSA Authentication Manager 6.1 以降のサーバでは、サード パーティの SNMP ツールがサポートされていました。

RSA Authentication Manager バージョン 8.0 には、完全に統合された SNMP レポート機能が含まれます。Authentication Manager ソフトウェアの SNMP は、Security Console で構成できます。

詳細については、「管理ガイド」の「ログとレポート」の章の「高度なログとトラブルシューティング」を参照してください。

# 3 RADIUS の移行

## プライマリ インスタンスへの RADIUS データの移行

RADIUS データの移行では、バージョン 6.1 のデータをバージョン 8.0 のデータベースにインポートします。プライマリ サーバのデータを移行する前に RADIUS データを移行する必要があります。次の処理手順では、バージョン 6.1 のデータをバージョン 8.0 のプライマリ インスタンスに移行する方法を説明します。

### 開始する前に

45 ページの「バージョン 8.0 導入環境のスナップショットまたはバックアップの作成」を参照。

### 処理手順

1. 「RSA RADIUS エクスポート ユーティリティのインストール」
2. 「RADIUS 移行パッケージ ファイルの作成」
3. 「新しいプライマリ インスタンスへの RADIUS 移行パッケージ ファイルのコピー」
4. （オプション）「バージョン 8.0 へのカスタム RADIUS ディクショナリ属性の追加」
5. 「新しいプライマリ インスタンスでの RSA RADIUS 6.1 データ ファイルの移行」

## RSA RADIUS エクスポート ユーティリティのインストール

既存の RSA RADIUS 6.1 データをエクスポートするには、RSA RADIUS エクスポート ユーティリティをインストールする必要があります。このユーティリティは、RSA Authentication Manager 8.0 –Virtual Appliance DVD の中にある RSA Authentication Manager 6.x RADIUS Export Utility\app ディレクトリで提供されています。

### 開始する前に

RSA RADIUS エクスポート ユーティリティ ファイルを Database Administration アプリケーションを実行するシステムにコピーします。このシステムは、プライマリ サーバ、レプリカ サーバ、リモート管理マシンのいずれでもかまいません。

**処理手順**

1. 新しいコマンド シェルを開き、RSA Authentication Manager 6.x RADIUS Export Utility を展開したディレクトリに移動します。次を入力します。

   ```
   patchRemoteAdmin.bat
   ```

   Enter キーを押します。
2. 説明を読んでから、**y** と入力し、Enter キーを押します。
3. ベース インストール ディレクトリの絶対パス（例えば、**C:\Program Files\RSA Security\RSA Authentication Manager**）を入力し、Enter キーを押します。
   Authentication Manager をデフォルトのベース インストール ディレクトリにインストールした場合は、Enter キーを押します。

## RADIUS 移行パッケージ ファイルの作成

既存の RSA RADIUS 6.1 データをエクスポートするには、RADIUS エクスポート ユーティリティを使用して RADIUS 移行パッケージ ファイルを作成します。

**開始する前に**

「RSA RADIUS エクスポート ユーティリティのインストール」を参照。

**処理手順**

1. 以下のいずれかの操作を実行します。
   - Authentication Manager がローカル ホスト マシン上にある場合は、［**Start（スタート）**］＞［**Programs（すべてのプログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Host Mode**］をクリックして、RSA Authentication Manager 6.1 Administration クライアントを開きます。
   - Authentication Manager がリモート ホスト マシン上にある場合は、［**Start（スタート）**］＞［**Programs（すべてのプログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Remote Mode**］をクリックします。リモート ホスト マシンにログオンして、RSA Authentication Manager 6.1 Administration クライアントを開きます。
2. Authentication Manager Administration クライアントのツールバーで、［**RADIUS**］＞［**Manage RADIUS server（RADIUS サーバの管理）**］をクリックします。
   RADIUS エクスポート ユーティリティのダイアログ ボックスが開きます。
3. RADIUS エクスポート ユーティリティ ダイアログ ボックスで、［**Generate Package（パッケージの生成）**］をクリックします。

4. エクスポートが完了したら、RADIUS エクスポート ユーティリティのダイアログ ボックスに RADIUS 移行パッケージ ファイルの場所として、**RSA_AM_HOME/prog/radius/Admin/** が表示されます。
5. 「**Have you completed the export operation and are ready to restore the client to its original state（エクスポート操作を完了してクライアントを元の状態にリストアする準備ができましたか）**」というプロンプトが表示されたら、**y** と入力し、Enter キーを押します。
6. 「**Do you really want to remove this update（このアップデートを削除してもよろしいですか）**」というプロンプトが表示されたら、**y** と入力し、Enter キーを押します。
7. エクスポート パッチが正常に削除されたら、**exit** と入力し、Enter キーを押します。

## 新しいプライマリ インスタンスへの RADIUS 移行パッケージ ファイルのコピー

RSA Authentication Manager 6.1 プライマリ サーバをバージョン 8.0 のプライマリ インスタンスに移行しようとしている場合は、RSA Authentication Manager 6.1 プライマリ サーバ ホスト上の **RSA_AM_HOME/prog/radius/Admin/** ディレクトリから、RADIUS 移行パッケージ ファイルの **radiusMigration_*time_stamp*.pkg** をプライマリ インスタンスにコピーします。RSA では、RADIUS 移行パッケージ ファイルのコピーは、セキュア ネットワーク経由か、リムーバブル メディアを使用して行うことを推奨します。パッケージ ファイルをコピーしたディレクトリをメモしておきます。この場所は、Operations Console を使用して RADIUS データを移行するときに入力する必要があります。

**重要：**ファイル転送に FTP を使用する場合は、データの破損を防ぐためにバイナリ モードを使用してください。

RADIUS 移行パッケージには、RADIUS データベースのみのデータが含まれます。移行プロセスには、RADIUS ログ ファイルや構成ファイルは含まれません。ログ ファイルにアクセスするには、バージョン 6.1 Authentication Manager 導入環境から RADIUS インストール ディレクトリ全体をコピーして、バージョン 8.0 導入環境に貼り付けます。その後、「RSA RADIUS 6.1 Server 管理者ガイド」の「ログの記録」の章の情報を使って、ASCII テキスト ファイルであるバージョン 6.1 RADIUS ログにアクセスできます。

## バージョン 8.0 へのカスタム RADIUS ディクショナリ属性の追加

バージョン 6.1 環境でカスタム属性を持つ RADIUS ディクショナリが使用されている場合、RADIUS データをインポートする前にバージョン 8.0 RADIUS ディクショナリにこれらの属性を追加する必要があります。

**重要：**RADIUS データをインポートする前にバージョン 8.0 RADIUS ディクショナリにカスタム属性を追加しなかった場合、属性を追加した後に同じパッケージ ファイルから RADIUS データを再度移行する必要があります。

バージョン 6.1 のカスタム属性をバージョン 8.0 に追加するには、2 つのオプションがあります。

- 「バージョン 8.0 RADIUS ディクショナリの編集」。バージョン 6.1 RADIUS ディクショナリのカスタム属性を追加します。
- 「8.0 導入環境へのカスタム RADIUS ディクショナリの追加」

## バージョン 8.0 RADIUS ディクショナリの編集

バージョン 6.1 のカスタム属性を使えるように、バージョン 8.0 RADIUS ディクショナリを手動で編集します。RADIUS ディクショナリ ファイルは Operations Console で編集します。

変更は、編集を行った RADIUS サーバにのみ適用されます。

**重要：**構成ファイルの編集は慎重に行ってください。ユーザーが加えた変更は検証されることなく、既存ファイルが新しい内容で上書きされます。構成ファイルで使用する構文の詳細については、「RSA Authentication Manager 8.0 RADIUS リファレンス ガイド」を参照してください。

### 開始する前に

バージョン 8.0 導入環境の、スーパー管理者および Operations Console 管理者のクレデンシャルを持っている必要があります。

### 手順

1. RADIUS サーバをホストしている RSA Authentication Manager インスタンスの 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）**］の順にクリックします。
3. 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、［**OK**］をクリックします。
4. このインスタンスでホストされている RADIUS サーバを選択し、コンテキスト メニューから［**Manage Server Files（サーバ ファイルの管理）**］を選びます。

5. ［Manage Server Files（サーバ ファイルの管理）］ページで、次のいずれかを実行します。
   - ［**Configuration Files（構成ファイル）**］タブをクリックして、.conf、.aut、.ini などの構成ファイルを表示します。
   - ［**Dictionary Files（辞書ファイル）**］タブをクリックして、RADIUS 辞書ファイルを表示します。
6. 編集するファイルを選択して、コンテキスト メニューから［**Edit（編集）**］を選択します。
7. テキスト ファイルを編集して、［**Save（保存）**］をクリックします。
8. 変更を適用するには、［**Save & Restart RADIUS Server（保存して RADIUS サーバを再起動する）**］をクリックします。

**次のステップ**

編集内容を導入環境全体で同期する必要がある場合（.dct ファイルを編集した場合など）は、編集内容を他の RADIUS サーバにコピーする必要があります。編集内容を導入環境の他の RADIUS サーバにコピーするには、［Manage RADIUS Server（RADIUS サーバの管理）］ページから適切な RADIUS サーバを選択し、コピーまたは編集を行います。

## 8.0 導入環境へのカスタム RADIUS ディクショナリの追加

バージョン 6.1 のカスタム RADIUS ディクショナリをバージョン 8.0 に追加するには Operations Console を使います。

**開始する前に**

- スーパー管理者と Operations Console 管理者のクレデンシャルが必要です。
- カスタマイズした RADIUS ディクショナリ ファイルをバージョン 8.0 導入環境からアクセス可能な場所にコピーする必要があります。

**手順**

1. RADIUS サーバをホストしている RSA Authentication Manager インスタンスの 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）**］の順にクリックします。
3. 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、［**OK**］をクリックします。
4. 辞書を追加する RADIUS サーバを選択し、コンテキスト メニューから［**Manage Server Files（サーバ ファイルの管理）**］を選びます。
5. ［Manage Server Files（サーバ ファイルの管理）］ページで、［Dictionary Files（辞書ファイル）］タブをクリックします。
6. ［**Add New（新規追加）**］をクリックします。

7. ［**RADIUS Dictionary File（RADIUS 辞書ファイル）**］フィールドで、［**Browse（参照）**］をクリックします。
8. 追加する RADIUS 辞書を選択して、［**Open（開く）**］をクリックします。
9. ［**Submit（送信）**］をクリックします。
10. **vendor.ini** ファイルに辞書のエントリーを追加します。
    a. ［Manage Server Files（サーバ ファイルの管理）］ページで、［Configuration Files（構成ファイル）］タブをクリックします。
    b. **vendor.ini** ファイルをクリックして、コンテキスト メニューから［**Edit（編集）**］を選択します。
    c. 先ほど追加した辞書ファイルのエントリーを入力します。エントリーのフォーマットは、**vendor.ini** ファイルのコメントに説明されています。
    d. ［**Save（保存）**］をクリックします。
11. **dictiona.dcm** ファイルに辞書ファイルのエントリーを追加します。
    a. dictiona.dcm ファイルをクリックして、コンテキスト メニューから［**Edit（編集）**］を選択します。
    b. 先ほど追加した辞書ファイルのエントリーを入力します。［Specific Implementations］の下に、次のように入力します。
    ```
    @name
    ```
    ここで、*name* は辞書ファイル名です。
    c. ［**Save & Restart RADIUS Server（保存して RADIUS サーバを再起動する）**］をクリックします。
12. 導入環境にある各 RSA RADIUS サーバで、この手順を繰り返します。

## 新しいプライマリ インスタンスでの RSA RADIUS 6.1 データ ファイルの移行

新しいプライマリ インスタンスで RSA RADIUS 6.1 データ ファイルを移行するには、Operations Console を使います。

**開始する前に**

- プライマリ インスタンスをインストールする前に、RADIUS 移行パッケージ ファイルを生成します。詳細については、54 ページの「RADIUS 移行パッケージ ファイルの作成」を参照してください。
- 「新しいプライマリ インスタンスへの RADIUS 移行パッケージ ファイルのコピー」

**処理手順**

1. プライマリ インスタンス上で、Operations Console を起動し、ログオンします。
2. ［**Deployment Configuration（導入環境の構成）**］＞［**Migration（移行）**］＞［**From Version 6.1（バージョン 6.1 から）**］＞［**RADIUS Database（RADIUS データベース）**］の順にクリックします。
3. プロンプトに従って、現在の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。［**OK**］をクリックします。
4. ［RADIUS Server Migration（RADIUS サーバの移行）］ページで、RADIUS 移行パッケージ ファイルが保存してある場所を指定します。
5. ［**Start Migration（移行の開始）**］をクリックします。
6. ［**Done（終了）**］をクリックします。
7. Security Console を使用して、すべての RADIUS レプリカ サーバへのレプリケーションを開始します。
   a. プライマリ インスタンス上で、Security Console を起動し、ログオンします。
   b. ［**RADIUS**］＞［**RADIUS Servers（RADIUS サーバ）**］をクリックします。
   c. ［**Initiate Replication（レプリケーションの開始）**］をクリックします。

# 4 プライマリ サーバの移行

## プライマリ サーバの移行

既存の RSA Authentication Manager サーバ（RSA Authentication Manager 6.1 以降がインストールされている Appliance 以外のサーバ、またはバージョン 6.1 を含む RSA SecurID Appliance 2.0 以降）を、RSA Authentication Manager 8.0 に移行するには、次のステップを実行します。

### 開始する前に

- バージョン 8.0 データベースのバックアップを作成します。45 ページの「バージョン 8.0 導入環境のスナップショットまたはバックアップの作成」を参照してください。
- バージョン 6.1 RADIUS のデータをバージョン 8.0 導入環境に移行する予定の場合、RADIUS データを移行してからプライマリ インスタンス データを移行します。53 ページの「RADIUS の移行」を参照してください。

### 処理手順

1. バージョン 6.1 プライマリ サーバでデータベースとログをダンプし、その他のファイルとともに新しいデータベース サーバに転送します。62 ページの「RSA Authentication Manager 6.1 データベース ダンプ」を参照してください。
2. バージョン 6.1 のデータをバージョン 8.0 に移行します。70 ページの「標準モードの移行の実行」を参照してください。
3. 移行レポートを確認して、移行に関する問題が発生していないかどうかをチェックします。バージョン 6.1 のデータベースに問題があれば修正します。

4. 移行に失敗した場合は、バージョン 8.0 データベースを初期インストールの状態にリストアし、タスク 2、3、4 を繰り返します。

   バージョン 8.0 データベースを初期インストール状態に戻すには、バックアップを使ってリストアする必要があります。リストア後、スーパー管理者レコードとデフォルト ポリシーなどバージョン 8.0 のデフォルト値以外、データベースは事実上空白になります。データベースのリストアが完了した後、バージョン 6.1 のデータベース ダンプ ファイルの作成処理とバージョン 8.0 への移行処理を繰り返すことができます。データが正しくフォーマットされていることを確認した後、この章で説明している残りの処理手順を実行できます。

   バックアップからデータベースをリストアする手順については、「RSA Authentication Manager 8.0 管理者ガイド」の「災害復旧」の章にある「プライマリ インスタンスのデータ復旧」を参照してください。

5. バージョン 6.1 のログ ファイルを移行します。78 ページの「ログ ファイルの移行」を参照してください。

## RSA Authentication Manager 6.1 データベース ダンプ

すべてのデータとファイルを手動で収集してバージョン 8.0 のプライマリ インスタンスに転送する必要があります。必要なデータとファイルには、プライマリ データベースのダンプ ファイルとバージョン 6.1 のライセンス ファイルが含まれます。

これらのファイルを、Web ブラウザからアクセスできる場所にコピーします。Appliance から移行する場合は、これらのファイルを取得するために **backupCab1.cab** ファイルを展開する必要があります。

ファイルの転送に ftp を使用する場合は、ファイルの破損を防ぐためにバイナリ モードを使用してください。

次の表に、移行に必要なファイル、各ファイルが置かれている RSA Authentication Manager 6.1 アプリケーション ディレクトリ上の場所、各ファイルの用途に関する簡単な説明を示します。

| ファイル名 | アプリケーション ディレクトリ内での場所 | 説明 |
|---|---|---|
| **sdserv.dmp** | **data** | バージョン 6.1 のデータベースのデータ。 |
| **sdlog.dmp** | **data** | バージョン 6.1 のログ。詳細については、78 ページの「ログ ファイルの移行」を参照してください。 |

| ファイル名 | アプリケーション ディレクトリ内での場所 | 説明 |
|---|---|---|
| **license.rec** | **data** | バージョン 6.1 プライマリ サーバのライセンス ファイル。ライセンス ファイルは、移行時にバージョン 6.1 のデータベース内の暗号化された特定のフィールドを復号化するために必要になります。 |
| **startup.pf** | **rdbms32** | 起動パラメータ ファイルは、バージョン 6.1 を実行しているシステムが使用する言語を指定します。このファイルは、次のいずれかの言語を使用する場合に必要です。<br>• 中国語<br>• 日本語<br>• 韓国語<br>• スペイン語 |
| **active.map**<br>**sunone.map** | **utils/toolkit** | LDAP 同期ジョブ マップ ファイルは、LDAP ユーザーのユーザー情報が格納されている LDAP ディレクトリの場所を指定します。これらのファイルは、ユーザーおよびユーザー グループのデータを LDAP アイデンティティ ソースに移行する場合に必要です。内部データベースのみを使用してユーザーとユーザー グループのデータを格納している場合は、これらのファイルを転送する必要はありません。 |
| **cert7.db**<br>**key3.db** | **data** | LDAP ディレクトリ サーバへの SSL 接続の確立に必要な SSL セキュリティ証明書。<br>バージョン 8.0 への証明書のエクスポートの手順については、69 ページの「LDAP ディレクトリ証明書のエクスポート」を参照してください。内部データベースのみを使用してユーザーとユーザー グループのデータを格納している場合は、これらのファイルをエクスポートまたは転送する必要はありません。 |
| **sdtacplus.arg**<br>**sdtacplus.cfg** | **data** | TACACS+ 起動ファイルと構成ファイル。バージョン 6.1 Authentication Manager の導入環境で TACACS+ を使用している場合、これらのファイルを新しい TACACS+ ホストに移動する必要があります。詳細については、93 ページの「TACACS+ サポートの構成」の項を参照してください。 |

## Appliance 以外での RSA Authentication Manager 6.1 サービスの停止

Authentication Manager プロセスによってデータベースまたはログへの書き込みが一切行われないように、データベースまたはログをダンプする前に、RSA Authentication Manager 6.1 のサービスをすべて停止する必要があります。Appliance 以外の場合は、次の処理手順に従い RSA Authentication Manager 6.1 のサービスを停止します。

**処理手順**

以下のいずれかの操作を実行します。

- Windows の場合：
  - バージョン 6.1 のマシン上で［**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Control Panel**］の順にクリックします。
  - ［Control Panel（コントロール パネル）］メニューで、［**Start & Stop RSA Authentication Manager Services（RSA Authentication Manager サービスの起動と終了）**］をクリックします。
  - ［**Stop Services（サービスの停止）**］から［**Stop All（すべて停止）**］をクリックします。
- UNIX マシンの場合は、次のように入力します。

```
sdconnect stop
aceserver stop
```

## RSA SecurID Appliance 2.0 以降での RSA Authentication Manager 6.1 サービスの停止

Authentication Manager プロセスによってデータベースまたはログへの書き込みが一切行われないように、データベースまたはログをダンプする前に、RSA Authentication Manager 6.1 のサービスをすべて停止する必要があります。RSA SecurID Appliance 2.0 以降で RSA Authentication Manager 6.1 のサービスを停止するには、次の処理手順を実行します。

**処理手順**

1. コンピュータ上で、［**Start（スタート）**］＞［**All Programs（すべてのプログラム）**］＞［**Internet Explorer**］をクリックします。
2. Appliance Web UI にログオンします。

   Appliance Web UI を使用すると、Internet Explorer から Appliance 上の管理タスクを実行できます。［お気に入り］メニューのリンク（追加されている場合）をクリックするか、https://*ApplianceName*:8098/ または https://*ApplianceMachineIP*:8098/ などの URL を入力してアクセスします。
3. ［**Advanced（詳細）**］タブをクリックします。
4. ［**Remote Desktop（リモート デスクトップ）**］をクリックします。

5. Appliance のユーザー名とパスコード（PIN + トークンコード）を入力し、［**OK**］をクリックします。
6. Internet Explorer でスクロール ダウンして、Appliance の［**Start（スタート）**］ボタンを表示します。
7. Appliance で、［**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Control Panel**］の順にクリックします。
8. ［Control Panel（コントロール パネル）］メニューで、［**Start & Stop RSA Authentication Manager Services（RSA Authentication Manager サービスの起動と終了）**］をクリックします。
9. ［**Stop Services（サービスの停止）**］から［**Stop All（すべて停止）**］をクリックします。

## Appliance 以外のプライマリ サーバでのデータベースとログ ファイルのダンプ

バージョン 6.1 には、データベースのダンプ用に、GUI ベースのユーティリティ（Windows のみ）とコマンド ライン ユーティリティ（Windows、Linux、Solaris の各プラットフォーム）が用意されています。

このセクションで説明する処理手順のステップ 2 の後に［**Allow database connection in multiuser mode（マルチユーザー モードでデータベースの接続を許可）**］を選択すると、Authentication Manager をシャットダウンせずにデータベースをダンプできます。ただし、生成されるダンプ ファイルには最新の変更が含まれない場合があります。

### 開始する前に

- ログのサイズをチェックして、ダンプ ファイルを保存するために十分なディスク領域があることを確認します。
  ログ ファイルのサイズは、システム ログ パラメータで選択したログ条件と、既存のバージョン 6.1 のサーバでのアクティビティ量によって異なります。
- 64 ページの「Appliance 以外での RSA Authentication Manager 6.1 サービスの停止」

### 処理手順

1. ［**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Database Tools（RSA Authentication Manager データベース ツール）**］＞［**Dump（ダンプ）**］の順にクリックします。
2. ［**Select Databases to dump（ダンプするデータベースの選択）**］で［**Dump Server Database（サーバ データベースのダンプ）**］を選択し、ログ データを移行する場合は［**Dump Log Database（ログ データベースのダンプ）**］を選択します。

3. ［**Options（オプション）**］で［**Include delta tables in dump file（ダンプ ファイルにデルタ テーブルを含める）**］を選択して、レプリケーションされていない変更がすべて維持されるようにします。
4. ［**Selective Dump（選択ダンプ）**］では、どのボックスも選択しないでください。
5. ［**Disk Space Requirements（必要なディスク スペース）**］で、使用可能なディスク スペースが、必要なディスク スペースより大きいことを確認します。
6. ［**Output Directory（出力先ディレクトリ）**］フィールドでダンプ ファイルを作成するディレクトリ パスを指定します。
7. ［**OK**］をクリックします。
   ダンプ プロセスのステータスが表示されます。
8. 以下のいずれかの操作を実行します。
   - ダンプ プロセスのステータス レポートを保存する場合は、［**Save As（名前を付けて保存）**］をクリックしてファイル名とディレクトリを指定した後、［**Save（保存）**］をクリックし、［**Close（閉じる）**］をクリックします。
   - ダンプ プロセスが完了したら、［**Close（閉じる）**］をクリックします。

## RSA SecurID Appliance 2.0 でのデータベースとログ ファイルのダンプ

RSA SecurID Appliance 2.0 では、スクリプトを実行することによってデータベースとログ ファイルの両方をダンプできます。

RSA SecurID Appliance 2.0.1 以降では、Appliance Web UI を使用して迅速に処理手順を実行できます。68 ページの「RSA SecurID Appliance 2.0.1 以降でのデータベースとログ ファイルのダンプ」を参照してください。

### 開始する前に

64 ページの「RSA SecurID Appliance 2.0 以降での RSA Authentication Manager 6.1 サービスの停止」を参照。

### 処理手順

1. Internet Explorer を使用して、Appliance Web UI（ユーザー インタフェース）にログインします。
   Appliance Web UI を使用すると、Internet Explorer から Appliance 上の管理タスクを実行できます。［お気に入り］メニューのリンク（追加されている場合）をクリックするか、https://*ApplianceName*:8098/ または https://*ApplianceMachineIP*:8098/ などの URL を入力してアクセスします。
2. ［**Advanced（詳細）**］タブをクリックします。
3. ［**Remote Desktop（リモート デスクトップ）**］をクリックします。

4. Appliance のユーザー名とパスコード（PIN + トークンコード）を入力し、［**OK**］をクリックします。
5. Internet Explorer でスクロール ダウンして、Appliance の［**Start（スタート）**］ボタンを表示します。
6. Appliance で［**Start（スタート）**］＞［**Run（ファイル名を指定して実行）**］の順にクリックします。
7. ［**Browse（参照）**］をクリックします。
8. RSA SecurID Appliance 2.0 では、**C:￥authmgr￥scripts** ディレクトリに移動します。
9. **rotatebackup.bat** を選択し、［**Open（開く）**］をクリックします。
10. ［Run（ファイル名を指定して実行）］ダイアログ ボックスで、［**OK**］をクリックしてバックアップ ファイルを作成します。

    バックアップが完了してもメッセージは表示されません。このファイルに直接アクセスする必要はありません。

    バックアップ ファイル（**backupCab1.cab**）には、ユーザー データベースとログ データベース、ライセンス ファイル、構成ファイルのコピーが含まれます。
11. Appliance Web UI で、［**Maintenance（保守）**］タブをクリックします。
12. ［**Download Backup File（バックアップ ファイルのダウンロード）**］をクリックします。
13. ［**Download backupCab1.cab file（backupCab1.cab ファイルのダウンロード）**］をクリックします。［File Download - Security Warning（ファイルのダウンロード - セキュリティ警告）］ダイアログ ボックスが表示されます。
14. ［**Save（保存）**］をクリックします。
15. ［Save As（名前を付けて保存）］ダイアログ ボックスで、Appliance 以外の保護された場所を指定します。たとえば、管理者のみがアクセスできるネットワーク ディレクトリなどです。

    RSA では、Appliance 以外の場所にファイルをダウンロードすることを推奨します。信頼できる管理担当者のみが利用可能な保護された場所に、バックアップ ファイルを格納します。
16. ［**Save（保存）**］をクリックします。

    ダウンロードが完了すると、すべてのダイアログ ボックスが閉じます。
17. ［**Logout（ログアウト）**］をクリックします。
18. コンピュータ上の Internet Explorer を終了します。
19. **backupCab1.cab** ファイルがある場所に移動し、バックアップ ファイルの内容をフォルダに展開します。

    バージョン 8.0 に移行するために必要なファイルが取得できました。

## RSA SecurID Appliance 2.0.1 以降でのデータベースとログ ファイルのダンプ

RSA SecurID Appliance 2.0.1 以降では、Appliance Web UI からデータベースとログ ファイルの両方をダンプできます。

### 開始する前に

64 ページの「RSA SecurID Appliance 2.0 以降での RSA Authentication Manager 6.1 サービスの停止」を参照。

### 処理手順

1. Internet Explorer を使用して、Appliance Web UI（ユーザー インタフェース）にログインします。

   Appliance Web UI を使用すると、Internet Explorer から Appliance 上の管理タスクを実行できます。[お気に入り] メニューのリンク（追加されている場合）をクリックするか、https://*ApplianceName*:8098/ または https://*ApplianceMachineIP*:8098/ などの URL を入力してアクセスします。

2. [**Maintenance（保守）**] タブをクリックします。
3. [**Download Backup File（バックアップ ファイルのダウンロード）**] をクリックします。
4. [**Run Backup（バックアップの実行）**] をクリックします。

   数秒後に、[**Download backupCab1.cab（backupCab1.cab のダウンロード）**] リンクが表示され、その下にバックアップが完了した日時が表示されます。

   バックアップ ファイル（**backupCab1.cab**）には、ユーザー データベースとログ データベース、ライセンス ファイル、構成ファイルのコピーが含まれます。

5. [**Download backupCab1.cab file（backupCab1.cab ファイルのダウンロード）**] をクリックします。[File Download - Security Warning（ファイルのダウンロード - セキュリティ警告）] ダイアログ ボックスが表示されます。
6. [**Save（保存）**] をクリックします。
7. [Save As（名前を付けて保存）] ダイアログ ボックスで、Appliance 以外の保護された場所を指定します。たとえば、管理者のみがアクセスできるネットワーク ディレクトリなどです。

   RSA では、Appliance 以外の場所にファイルをダウンロードすることを推奨します。信頼できる管理担当者のみが利用可能な保護された場所に、バックアップ ファイルを格納します。

8. [**Save（保存）**] をクリックします。

   ダウンロードが完了すると、すべてのダイアログ ボックスが閉じます。

9. [**Logout（ログアウト）**] をクリックします。

10. コンピュータ上の Internet Explorer を終了します。
11. **backupCab1.cab** ファイルがある場所に移動し、バックアップ ファイルの内容をフォルダに展開します。
    バージョン 8.0 に移行するために必要なファイルが取得できました。

## LDAP ディレクトリ証明書のエクスポート

LDAP ディレクトリ証明書を使用すると、SSL（Secure Sockets Layer）プロトコルを使用して LDAP アイデンティティ ソースに接続できます。SSL では、Authentication Manager と LDAP ディレクトリとの通信が暗号化されます。各ディレクトリ サーバの証明書ファイルを入手できない場合は、既存のバージョン 6.1 導入環境から次の処理手順を使用して証明書をエクスポートできます。証明書を入手できる場合は、この処理手順を実行する必要はありません。

### 処理手順

1. ファイル内の証明書をリストします。バージョン 6.1 のプライマリ サーバのコマンド ライン プロンプトで ***ACEPROG*** ディレクトリに移動して次のように入力します。

   ```
   certutil -L -d ￥ACEDATA￥ldapjobs￥sslcerts￥cert7.db +
   key3.db
   ```

   ここで、*ACEDATA*￥ldapjobs￥sslcerts は、証明書ファイルが存在するバージョン 6.1 のディレクトリです。

2. リストに含まれる各証明書をエクスポートします。次を入力します。

   ```
   certutil -L -d -n 証明書名 -r > ファイル名 .cer
   ```

   各オプションの意味は以下のとおりです。

   - 証明書名は証明書の名前です。
   - ファイル名は証明書ファイル用に選択した名前です。

3. エクスポートした証明書ファイルをバージョン 8.0 のインスタンスにコピーし、移行後にインポートします。

### 次のステップ

証明書をバージョン 8.0 導入環境にインポートしてください。詳細については、「RSA Authentication Manager 8.0 管理者ガイド」の「LDAP ディレクトリの統合」の章にある「アイデンティティ ソースの SSL 証明書の追加」を参照してください。

## 標準モードの移行の実行

標準モードの移行では、管理者の関与を最小限にして、データを移行します。

**開始する前に**

- スーパー管理者である必要があります。
- 46 ページの「データ移行オプション」を参照して、移行するデータや使用するアイデンティティ ソースを計画し、そのセクションで説明されているその他の問題に対応してください。
- バージョン 8.0 データベースのバックアップを作成します。45 ページの「バージョン 8.0 導入環境のスナップショットまたはバックアップの作成」を参照してください。
- バージョン 6.1 のデータをダンプします。62 ページの「RSA Authentication Manager 6.1 データベース ダンプ」を参照してください。

**処理手順**

1. Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Migration（移行）**] > [**From Version 6.1（バージョン 6.1 から）**] > [**Server Database（サーバ データベース）**] 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. [Locate Files（ファイルの場所の指定）] 画面で、次のファイルの場所を指定します。
   - **sdserv.dmp** ファイル
   - バージョン 6.1 の **license.rec** ファイル
   - （オプション）日本語、中国語、韓国語、スペイン語のいずれかを使用している場合は、**startup.pf** ファイルの場所を指定します。
4. [**Scan Dump File（ダンプ ファイルのスキャン）**] をクリックします。
5. [Scan Results（スキャン結果）] 画面で、ダンプ ファイル内のデータが移行対象のデータであることを確認します。
6. [**Typical Mode（標準モード）**] を選択します。

7. （オプション）すでに移行したバージョン 6.1 サーバを移行しようとすると、［Scan Results（スキャン結果）］ページの［Migration Retry Cleanup（移行再試行クリーンアップ）］セクションが表示されます。チェックボックスをオンにすると、バージョン 8.0 インスタンスは、移行の再試行のための準備を整えます。先に進む前に、バージョン 8.0 インスタンスでバージョン 6.1 移行データが削除されていることを確認します。

   移行の再試行ではない場合、または次のシナリオに該当する場合は、このチェックボックスをオフにします。

   - 移行処理を、複数のバージョン 6.1 ダンプ ファイルを使用して実行する場合。たとえば、あるダンプ ファイルにはユーザーのみが含まれ、別のダンプ ファイルにはトークンのみが含まれる。
   - 移行を再試行する前に、以前移行したデータを削除していない。

8. ［**Next（次へ）**］をクリックします。
9. サマリー ページを確認してから、以下の 1 つを行います。
   - 内容が適切な場合は、［**Start Server Migration（サーバの移行を開始）**］をクリックします。
   - 前のページに戻るには、［**Back（戻る）**］をクリックします。
   - 内容をクリアしてホームに戻るには、［**Cancel（キャンセル）**］をクリックします。
10. 移行を開始すると［Migration Status（移行ステータス）］ページが表示され、実行中の移行タスク、開始時刻、タスクの完了率が表示されます。いつでも［**Cancel Migration（移行のキャンセル）**］をクリックすることができます。また、［**Refresh（更新）**］をクリックしてステータスを再表示することができます （移行タスクが表示されるページ セクションでは、自動更新も行われます）。

    移行が完了すると［Migration Results（移行結果）］ページが表示され、移行が成功したかどうかを示すメッセージが表示されます。移行が失敗した場合や、成功しても警告が出された場合は、エラー メッセージが表示されます。
11. ［Migration Results（移行結果）］ページの下部にあるリンクをクリックすると、**migration_summary.html** レポート、またはより詳細な **migration_detail.zip** ファイルを表示して、移行の結果について詳しく調べることができます （これらのファイルの両方、およびその他の移行情報は、［Migration Results（移行結果）］ページの下部に表示される結果ディレクトリに保存されています）。
12. ［Migration Results（移行結果）］ページを閉じるには、［**Done（終了）**］をクリックします。

インストール プロセスは、**/opt/rsa/am/utils/migration61** ディレクトリに **sdserv.dmp** ファイルを作成します。このファイルは、日付と時刻を示すフォルダに作成されます。たとえば、2008 年 9 月 2 日 1 時 02 分 44 秒に移行が完了した場合は、080902010244 となります。

## カスタム モードの移行の実行

カスタム モードの移行では、移行データのフィルタ処理、特定のデータの移行方法の構成、LDAP 同期ジョブをアイデンティティ ソースにマップする方法の指定を行うことができます。

**開始する前に**

- スーパー管理者である必要があります。
- 46 ページの「データ移行オプション」を参照して、移行するデータや使用するアイデンティティ ソースを計画し、そのセクションで説明されているその他の問題に対応してください。
- バージョン 8.0 データベースのバックアップを作成します。45 ページの「バージョン 8.0 導入環境のスナップショットまたはバックアップの作成」を参照してください。
- バージョン 6.1 のデータをダンプします。62 ページの「RSA Authentication Manager 6.1 データベース ダンプ」を参照してください。

**処理手順**

1. Operations Console で、［**Deployment Configuration（導入環境の構成）**］＞［**Migration（移行）**］＞［**From Version 6.1（バージョン 6.1 から）**］＞［**Server Database（サーバ データベース）**］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. ［Locate Files（ファイルの場所の指定）］画面で、次のファイルの場所を指定します。
   - **sdserv.dmp** ファイル
   - バージョン 6.1 の **license.rec** ファイル
   - （オプション）日本語、中国語、韓国語、スペイン語のいずれかを使用している場合は、**startup.pf** ファイルの場所を指定します。
4. ［**Scan Dump File（ダンプ ファイルのスキャン）**］をクリックします。
5. ［Scan Results（スキャン結果）］画面で、ダンプ ファイル内のデータが移行対象のデータであることを確認します。
6. ［**Custom Mode（カスタム モード）**］を選択します。

7. （オプション）すでに移行したバージョン 6.1 サーバを移行しようとすると、［Scan Results（スキャン結果）］ページの［Migration Retry Cleanup（移行再試行クリーンアップ）］セクションが表示されます。チェックボックスをオンにすると、バージョン 8.0 インスタンスは、移行の再試行のための準備を整えます。先に進む前に、バージョン 8.0 インスタンスでバージョン 6.1 移行データが削除されていることを確認します。

   移行の再試行ではない場合、または次のシナリオに該当する場合は、このチェックボックスをオフにします。

   - 移行処理を複数のバージョン 6.1 ダンプ ファイルを使用して実行する場合。たとえば、あるダンプ ファイルにはユーザーのみが含まれ、別のダンプ ファイルにはトークンのみが含まれる。
   - 移行を再試行する前に、以前移行したデータを削除していない。

8. ［**Next（次へ）**］をクリックします。
9. テスト移行を行うには、［**Create output report without performing actual migration（実際の移行を行わずにレポートを作成）**］を選択します。

   移行レポートをレビューして、選択した設定で実際の移行を行うとどうなるかを見ることができます。
10. データ競合がある場合、移行プロセスでどのように処理するかを次のいずれかから指定します。
    - 移行を続行して移行レポートで競合について説明するには、［**Best Effort（ベスト エフォート）**］を選択します。
    - 移行を停止して移行レポートで競合について説明するには、［**No Conflict（競合なし）**］を選択します。
11. RSA Authentication Manager 6.1 ダンプ ファイルの［**Select objects to migrate（移行するオブジェクトを選択）**］セクションの項目をレビューします。移行したいオブジェクトが選択されていることを確認します。移行したくないオブジェクトは選択をクリアします。

    RADIUS 6.1 データの移行の場合に、RADIUS 設定（ポリシー設定など）と RADIUS データ（プロファイル名、ユーザー プロファイル割り当て、RADIUS エージェント ホスト）の両方を移行する場合は、［**Select objects to migrate（移行するオブジェクトを選択）**］セクションで［**Migrate System Settings（システム設定を移行）**］および［**Migrate RADIUS（RADIUS を移行）**］の両方を選択する必要があります。

    ダンプ ファイルに自動登録されたエージェントが見つかった場合にのみ、移行するオブジェクトのリストに［Migrate Agents（エージェントを移行）］が表示されます。自動登録されたエージェントの既存のエージェント IP アドレスをそのまま使うには、［Migrate Agents（エージェントを移行）］の下にある［**Protect all IP addresses（すべての IP アドレスを保護）**］チェックボックスをオンにします。

12. ユーザーの移行先となるアイデンティティ ソースを選択します（導入環境に LDAP 同期ジョブがない場合、[**Selectively migrate users to appropriate identity sources（適切なアイデンティティ ソースを選択してユーザーを移行）**] オプションは使用できません）。

    - [**Migrate all users to the internal database（すべてのユーザーを内部データベースに移行）**]。すべてのユーザーを Authentication Manager 内部データベースに移行するには、このオプションを選択します。
    - [**Migrate all users to the Identity Source（すべてのユーザーを単一のアイデンティティ ソースに移行）**]。ドロップダウン リストには、構成されたすべての外部アイデンティティ ソースが表示されます。すべてのユーザーの移行先となる単一のアイデンティティ ソースを選択します。

      外部アイデンティティ ソースを選択する際、[**Migrate all users to the Identity Source（すべてのユーザーを単一のアイデンティティ ソースに移行）**] フィールドの下に、チェックボックスとテキストが表示されます。ダンプ ファイルに含まれるユーザーが移行先のアイデンティティ ソースに存在しない場合に、そのユーザーを Authentication Manager 内部データベースに移動するには、チェックボックスをオンにします。チェックボックスをオンにしなかった場合、これらのユーザーは削除されます。
    - [**Selectively migrate users to appropriate identity sources（適切なアイデンティティ ソースを選択してユーザーを移行）**]。LDAP 同期ジョブをアイデンティティ ソースにマップするには、このオプションを選択します。このオプションは、導入環境に LDAP 同期ジョブがある場合にのみ使用できます（LDAP 同期ジョブのマッピングは、[Customize Migration（移行のカスタマイズ）] ページを完了して、[**Next**（次へ）] をクリックした後に行います）。

      このオプションを選択すると、[**Selectively migrate users to appropriate identity sources（適切なアイデンティティ ソースを選択してユーザーを移行）**] フィールドの下に、チェックボックスとテキストが表示されます。ダンプ ファイルに含まれるユーザーが移行先のアイデンティティ ソースに存在しない場合に、そのユーザーを Authentication Manager 内部データベースに移動するには、チェックボックスをオンにします。チェックボックスをオンにしなかった場合、これらのユーザーは削除されます。

13. ［**User ID Format (Internal Database):（ユーザー ID 形式（内部データベース）:)**］フィールドをレビューして、必要に応じて変更します。

    ダンプ ファイルに NTLM 形式のユーザー ID が含まれる場合、［**User ID Format (Internal Database):（ユーザー ID 形式（内部データベース）:)**］が表示され、デフォルトで選択されます。ユーザー ID は、フィールドの下にある［**Domain Name Mapping（ドメイン名マッピング)**］セクションにリストされます。

    移行時に、ユーザー ID を NTLM 形式から UPN 形式にマッピングする場合は、フィールドを選択したままにします。マッピングにより、Authentication Manager データベース上に保存するユーザー ID の形式が変更されます。移行時にマッピングを行わない場合は、［**User ID Format (Internal Database):（ユーザー ID フォーマット（内部データベース）:)**］フィールドの選択をクリアします。

    移行時にユーザー ID を NTLM 形式から UPN 形式にマッピングするには、［**Domain Name Mapping（ドメイン名マッピング)**］セクションのリストにある NTLM 形式のユーザー ID をクリックします。［NTLM Name（NTLM 名）］フィールドに NTLM 形式のユーザー ID が表示されます。Windows 2000 の FQDN（完全修飾ドメイン名）UPN 形式を使って、対応するユーザー ID を［**UPN Name（UPN 名)**］フィールドに入力して、［**Update（更新)**］をクリックします。マッピングするユーザー ID ごとにこの処理手順を繰り返します。

    移行後に、Security Console を使用して NTLM 形式から UPN 形式へのマッピングを有効にできますが、この処理では Authentication Manager データベース上のユーザー ID は変更されません。ランタイムに Authentication Manager が NTLM 形式の認証リクエストを受け付けた場合に、UPN 形式にマッピングできるようになるだけです。移行後に NTLM から UPN へのマッピングを行う方法については、「Security Console Help」で「エージェント設定の構成」のトピックを参照してください。

14. ユーザーの移行先となるセキュリティ ドメインを選択します。

15. 移行レポートの形式を選択します。次の形式のいずれかまたは両方を選択するか、どれも選択しなくてもかまいません。レポートは［Server Migration Results（サーバ移行結果)］ページに表示されるサーバ上の移行結果ディレクトリに格納されます。

    - 移行出力ファイルが大きいことが予想される場合は、［**GZIP Output (GZIP 出力)**］を選択します。このオプションでは、サマリー レポートや詳細移行レポートだけでなく、すべての出力ファイルに対して zip 圧縮が行われます。相当数の移行出力ファイルが移行結果ディレクトリに格納されます。
    - すべての移行データの詳細を出力したい場合は、［**Verbose Report (詳細レポート)**］を選択します。**migration_detail.zip** ファイルに出力されます （このオプションはデフォルトで選択されています)。

16. ［Customize Migration（移行のカスタマイズ）］ページを完了した後、［**Next（次へ）**］をクリックします。
    続くステップは、ステップ 10 で選択した項目によって異なります。
    - ［Migrate all users to the internal database（すべてのユーザーを内部データベースに移行）］を選択した場合、ステップ 19 に進みます。
    - ［Migrate all users to the Identity Source（すべてのユーザーを単一のアイデンティティ ソースに移行）］を選択した場合、ステップ 17 を完了してからステップ 19 に進みます。
    - ［Selectively migrate users to appropriate identity sources（適切なアイデンティティ ソースを選択してユーザーを移行）］を選択した場合、以降のすべてのステップを完了します。
17. ［Upload LDAP Files（LDAP ファイルをアップロード）］ページで、Active Directory の **active.map** ファイルと Sun ONE の **sunone.map** ファイルの場所を選択します。
18. ［Map LDAP to Identity Source（LDAP をアイデンティティ ソースにマップ）］ページで、次のように選択します （このステップは LDAP 同期ジョブを移行する場合のみ必要です。このページは、適切なアイデンティティ ソースを選択してユーザを移行するよう選択した場合にのみ表示されます）。
    - LDAP 同期ジョブに含まれないユーザーをどのように処理するかオプションを選択します。
    - ［**Identity Source（アイデンティティ ソース）**］ドロップダウン リストから、各 LDAP 同期ジョブのマップ先となるアイデンティティ ソースを選択します。必要なすべてのアイデンティティ ソースを選択すると、［Summary（サマリー）］ページが表示されるため、選択をレビューしてから移行を開始できます。ステップ 19 に進んでください。
    - 希望するアイデンティティ ソースがまだ定義されていないためリストにない場合、リストで［**Add Identity Source（アイデンティティ ソースの追加）**］を選択します。Operations Console の［Add New Identity Source（新しいアイデンティティ ソースの追加）］ページが表示され、マッピングする LDAP 同期ジョブの情報があらかじめ入力されています。新しいアイデンティティ ソースを作成した後（または、作成しないで［**Cancel（キャンセル）**］をクリックした場合）、［Map LDAP to Identity Source（LDAP をアイデンティティ ソースにマップ）］ページに戻ります。ドロップダウン リストに新しいアイデンティティ ソースが表示されます。これで、LDAP 同期ジョブを新規作成されたアイデンティティ ソースにマップできます。
      環境が複雑で多くのアイデンティティ ソースを作成する必要がある場合、移行を中断し、Operations Console からアイデンティティ ソースを作成します （Operations Console ホーム ページで、［**Deployment Configuration（導入環境の構成）**］＞［**Identity Sources（アイデンティティ ソース）**］＞［**Add New（新規追加）**］の順にクリックします）。アイデンティティ ソースの作成が完了した後、移行処理を再開し、LDAP 同期ジョブを既存のアイデンティティ ソースにマップします。

19. ［Summary（サマリー）］ページをレビューします。以下のいずれかの操作を実行します。
    - ［Summary（サマリー）］ページに表示されている項目と設定に問題がない場合は、［**Start Server Migration（サーバの移行を開始）**］をクリックします（ステップ 6 でテスト移行のオプションを選択した場合、［**Start Test Server Migration（サーバのテスト移行を開始）**］をクリックしてテスト移行を実行します）。
    - 前のページに戻るには、［**Back（戻る）**］をクリックします。
    - 内容をクリアしてホームに戻るには、［**Cancel（キャンセル）**］をクリックします。

    移行を開始すると［Migration Status（移行ステータス）］ページが表示され、実行中の移行タスク、開始時刻、タスクの完了率が表示されます。いつでも［**Cancel Migration（移行をキャンセル）**］をクリックすることができます。また、［**Refresh（更新）**］をクリックしてステータスを再表示できます（移行タスクが表示されるページ セクションでは、自動更新も行われます）。

    移行が完了すると［Migration Results（移行結果）］ページが表示され、移行が成功したかどうかを示すメッセージが表示されます。移行が失敗した場合や、成功しても警告が出された場合は、エラー メッセージが表示されます。
20. ［Migration Results（移行結果）］ページの下部にあるリンクをクリックすると、**migration_summary.html** レポート、またはオプションを選択していた場合はより詳細な **migration_detail.zip** ファイルを表示して、移行の結果について詳しく調べることができます（これらのファイルの両方、およびその他の移行情報は、［Migration Results（移行結果）］ページの下部に表示される、結果ディレクトリに保存されています）。移行結果を確認したら、［**Done（終了）**］をクリックし、［Migration Results（移行結果）］ページを閉じます。

    テスト移行を実施すると、同じ移行レポートが作成されますが、実際の移行は行われず、システムに影響はありません。テスト移行の結果ページで、［**Start Server Migration（サーバの移行を開始）**］をクリックすると先ほど実行したテストの実際の移行が行われます。［**Cancel（キャンセル）**］をクリックすると、Operations Console ホーム ページに戻ります。

移行プロセスは、**/opt/rsa/am/utils/migration61** ディレクトリに **sdserv.dmp** ファイルを作成します。このファイルは、日付と時刻を示すフォルダに作成されます。たとえば、2008 年 9 月 2 日 1 時 02 分 44 秒に移行が完了した場合は、080902010244 となります。

### 次のステップ

バージョン 6.1 の Database Administration アプリケーションを使用して、移行レポートで明らかになった問題を解決してください。問題解決の詳細については、95 ページの付録 A、「移行データの変換」を参照してください。

## ログ ファイルの移行

ログは、バージョン 6.1 のサーバからバージョン 8.0 のデータベースに移行できます。この 1 回の処理手順で、すべてのログ データを 1 つの場所に格納できます。

バージョン 6.1 のログ メッセージの一部は、バージョン 8.0 の同等のログ メッセージに移行されます。バージョン 6.1 のイベントおよび対応するバージョン 8.0 のイベントのリストについては、79 ページの「ログ移行のイベント マッピング」を参照してください。残りのバージョン 6.1 のログ メッセージは汎用ログ メッセージとして認証ログ イベントに移行され、メッセージのテキストは正確に汎用メッセージの詳細フィールドに格納されます。次の標準マッピングが使用されます。

Activity Key = *Authentication_Manager_6.1_migrated_log_message*

Description = "*Authentication_Manager_6.1_migrated_log_message*. Original message:*Authentication_Manager_6.1_migrated_log_event_name"*

たとえば、バージョン 6.1 イベント「Changed user admin level」には対応するバージョン 8.0 イベントがありません。そのため、移行後の汎用ログ メッセージは次のようになります。

Activity Key = AM61 Migrated log message

Description = AM61 Migrated log message Original message:"Changed user admin level"

バージョン 6.1 のログ メッセージをバージョン 8.0 にインポートするには、次の処理手順を実行します。

ログ メッセージを複数回インポートすると、重複したログ エントリーが作成されます。

### 開始する前に

- バージョン 6.1 のログ ファイルをダンプします。詳細については、65 ページの「Appliance 以外のプライマリ サーバでのデータベースとログ ファイルのダンプ」を参照してください。
- バージョン 6.1 のログ ダンプ ファイルをバージョン 8.0 のプライマリ インスタンスに転送します。

### 処理手順

1. Operations Console で、[**Deployment Configuration（導入環境の構成）**] > [**Migration（移行）**] > [**From Version 6.1（バージョン 6.1 から）**] > [**Log Migration（ログの移行）**] 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. [Locate Files（ファイルの場所の指定）] ページでログ ダンプ ファイル（**sdlog.dmp**）を参照します。

4. ［Summary - Log Migration（サマリー - ログの移行）］ページを確認します。
5. ［**Start Log Migration（ログの移行を開始）**］をクリックします。
   移行タスクが開始すると［Log Migration Status（ログ移行ステータス）］ページに各移行タスクが表示されます。ページを更新するには、［**Refresh（更新）**］をクリックします。いつでも［**Cancel Migration（移行をキャンセル）**］をクリックすることができます。また、［Refresh（更新）］をクリックしてステータスを再表示できます
   ログの移行が完了すると、［Log Migration Results（ログの移行結果）］ページが表示されます。
6. Web ブラウザでログ移行レポートを表示するには、**migration_summary.html** をクリックします。［**Done（終了）**］をクリックするとページが終了します。

## ログ移行のイベント マッピング

ログ ファイルの移行後、バージョン 6.1 サーバの認証イベントは、次の表に示すようにバージョン 8.0 のイベントにマッピングされてデータベースに保存されます。

| バージョン 6.1 の認証イベント | 対応するバージョン 8.0 のイベント |
|---|---|
| Agent host not found | Lookup Authentication agent |
| User not on agent host | Authentication agent access check |
| • New PIN received<br>• PIN created by user<br>• ACCESS DENIED<br>• PIN rejected | PIN change attempted |
| • Passcode accepted<br>• New PIN required | New pin mode activated for token |
| Next tokencode On | Next tokencode mode activated for token |

| バージョン 6.1 の認証イベント | 対応するバージョン 8.0 のイベント |
|---|---|
| • Token disabled, too many failures<br>• PASSCODE REUSE ATTACK detected<br>• ACCESS DENIED, next tokencode bad<br>• ACCESS DENIED, previous tokencode<br>• ACCESS DENIED, token disabled<br>• ACCESS DENIED, passcode incorrect<br>• Passcode accepted<br>• Next tokencode accepted<br>• ACCESS DENIED, bad user password<br>• Password authentication<br>• Administrator sign on | Principal authentication |
| • ACCESS DENIED, syntax error | Authentication log request |
| • Unassigned replacement token<br>• Unassigned as replacement token<br>• Unassigned replaced token | Token replaced, original token unassigned |
| Deleted replaced token | Token replaced, original token deleted |
| Node secret sent to agent host | Node secret sent |
| User not in database | Resolve principal by userid/alias |
| • XR PASSCODE accepted,<br>• XR ACCESS DENIED, next code bad<br>• XR ACCESS DENIED, bad passcode | Trusted Realm Authentication |
| XR new PIN created by user | Trusted Realm new PIN created by user |
| XR next tokencode On | Trusted Realm Authentication Request activated next tokencode mode for token |
| XR next tokencode accepted | Trusted realm next token code accepted |
| • Administrator sign off<br>• Administrator sign on failed | Principal session logout<br><br>Principal session logout |

| バージョン 6.1 の認証イベント | 対応するバージョン 8.0 のイベント |
|---|---|
| Offline-Auth Download Requested | Offline Authentication Data Download |
| Offline-Auth Download Timed-Out | Offline Authentication Data Download Failed |
| Offline-Auth Download Failed | Offline Authentication Data Download Failed |

ログ ファイルの移行後、バージョン 6.1 サーバの管理イベントは、次の表に示すようにバージョン 8.0 のイベントにマッピングされてデータベースに保存されます。

| Version 6.1 Administrative Event | 対応するバージョン 8.0 のイベント |
|---|---|
| Disabled token | Disable Token |
| Enabled token | Enable Token |
| • Assigned token<br>• Assigned replacement token<br>• Assigned as replacement token | Link Token with Principal |
| Unassigned token | Unlink Token with Principal |
| PIN cleared | Clear Token Pin |
| Added user | Create principal |
| Edited user | Update principal |
| Deleted user | Delete principal |
| Edited token | Update Token |
| Deleted SID token | Delete Token |
| Deleted AES token | Delete Token |
| Added group | Create group |
| Edited group | Update group |
| Deleted group | Delete group |
| Added member to group | Associate group with principal |

| Version 6.1 Administrative Event | 対応するバージョン 8.0 のイベント |
|---|---|
| Deleted member from group | Disassociate Group from Principal |
| Added group to agent host | Link Agent with Group |
| Deleted group from agent host | UnLink Agent with Group |
| Added realm | Create Realm |
| Enabled auto agent reg | Enable Agent Auto-registration |
| Disabled auto agent reg | Disable Agent Auto-registration |
| Resynchronized token | Resynchronize Token |
| Synchronized token | Sync Token |
| Enabled emergency code punct | Token marked as lost.Enabled emergency access fixed token code. |
| Disabled emergency code punct | Disabled emergency access |

# 5 レプリカ サーバの移行

## レプリカ サーバの移行

プライマリ サーバを移行してバージョン 6.1 プライマリ サーバをシャットダウンした後、レプリカ サーバを移行するまでは、レプリカ サーバのデータベースに対する変更（デルタ レコード）をプライマリ インスタンスに送信できません。レプリカ サーバがプライマリ サーバと通信できない状態になっている間に認証が行われると、変更（つまりデルタ レコード）がデータベース内に蓄積されます。レプリカ データベースから移行する必要がある重要なデータは、これらのデルタ レコードのみです。たとえば、デルタ レコードには、PIN の変更、無効化されたトークン、トークンや認証エージェントに関するその他の重要な情報が含まれます。

**開始する前に**

バージョン 8.0 レプリカ インスタンスを導入します。「RSA Authentication Manager 8.0 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。

**処理手順**

1. 「レプリカ サーバ データベースのダンプ」（83 ページ）。
2. 「8.0 プライマリ インスタンスへのレプリカ デルタ レコードの移行」（84 ページ）。
3. 導入環境に新しいホスト名と IP アドレスのインスタンスが追加された場合は、コンタクト リストを更新する必要があります。手順については、86 ページの「コンタクト リストの更新」を参照してください。

## レプリカ サーバ データベースのダンプ

レプリカ データベースをダンプすると、データベース ダンプ ファイルが作成されます。このファイルを使用して、バージョン 6.1 のレプリカ データベースをバージョン 8.0 データベースに移行します。バージョン 6.1 には、データベースのダンプ用に、GUI ベースのユーティリティ（Windows のみ）とコマンド ライン ユーティリティ（Windows、Linux、Solaris の各プラットフォーム）が用意されています。

**開始する前に**

以下のいずれかの操作を実行します。

- 「Appliance 以外での RSA Authentication Manager 6.1 サービスの停止」
- 「RSA SecurID Appliance 2.0 以降での RSA Authentication Manager 6.1 サービスの停止」

**処理手順**

1. バージョン 6.1 のマシン上で［**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Database Tools**］＞［**Dump（ダンプ）**］の順にクリックします。
   ［Authentication Manager Database Dump（Authentication Manager データベースのダンプ）］ダイアログ ボックスが開きます。
2. ［**Select Databases to dump（ダンプするデータベースの選択）**］で［**Dump Server Database（サーバ データベースのダンプ）**］を選択します。
3. ［**Options（オプション）**］で［**Include delta tables in dump file（ダンプ ファイルにデルタ テーブルを含める）**］を選択して、関連するすべてのデルタ情報をダンプの対象に含めます。
4. ［**Disk Space Requirements（必要なディスク スペース）**］で、使用可能なディスク スペースが、必要なディスク スペースより大きいことを確認します。［**Output Directory（出力ディレクトリ）**］ボックスで、ダンプ ファイルの作成先となるディレクトリ パスを指定します。
5. ［**OK**］をクリックします。
   ダンプ プロセスのステータスが表示されます。
6. 以下のいずれかの操作を実行します。
   - ダンプ プロセスが完了したら、［**Close（閉じる）**］をクリックします。
   - ダンプ プロセスのステータス レポートを保存する場合は、［**Save As（名前を付けて保存）**］をクリックしてファイル名とディレクトリを指定した後、［**Save（保存）**］をクリックし、［**Close（閉じる）**］をクリックします。

## 8.0 プライマリ インスタンスへのレプリカ デルタ レコードの移行

レプリカ サーバがプライマリ サーバと通信できない状況下で、レプリカ サーバ上で認証が行われると、デルタ レコードと呼ばれるデータベース変更が蓄積されます。バージョン 6.1 の各レプリカ サーバのデルタ レコードを、バージョン 8.0 プライマリ インスタンスに移行する必要があります。

**開始する前に**

- 83 ページの「レプリカ サーバ データベースのダンプ」の処理手順を実行して、**sdserv.dmp** ファイルを作成する必要があります。
- Operations Console 管理者およびスーパー管理者のクレデンシャルが必要です。

**処理手順**

1. バージョン 8.0 のプライマリ インスタンスで Operations Console を開き、Operations Console 管理者のユーザー ID とパスワードを使用してログオンします。
2. ［**Deployment Configuration（導入環境の構成）**］＞［**Migration（移行）**］＞［**From Version 6.1（バージョン 6.1 から）**］＞［**Server Database（サーバ データベース）**］の順にクリックし、スーパー管理者のユーザー ID とパスワードを使用してログオンします。
3. ［Locate Files（ファイルの場所の指定）］画面で、次のファイルの場所を指定します。
   - **sdserv.dmp** ファイル
   - バージョン 6.1 の **license.rec** ファイル
   - （オプション）日本語、中国語、韓国語、スペイン語のいずれかを使用している場合は、**startup.pf** ファイルの場所を指定します。
4. ［Scan Results（スキャン結果）］画面で、ダンプ ファイル内のデータが移行対象のデータであることを確認します。
5. デルタ レコードのみを移行するには［**Rolling Upgrade Mode（ローリング アップグレード モード）**］を選択します。
6. ［**Next（次へ）**］をクリックすると、サマリー ページが表示されます。
7. Summary page（サマリー ページ）を確認します。内容が適切な場合は、［**Start Server Migration（サーバの移行を開始）**］をクリックします。前のページに戻るには、［**Back（戻る）**］をクリックします。内容をクリアしてホームに戻るには、［**Cancel（キャンセル）**］をクリックします。

   移行を開始すると［Migration Status（移行ステータス）］ページが表示され、実行中の移行タスク、開始時刻、タスクの完了率が表示されます。いつでも［**Cancel Migration（移行のキャンセル）**］をクリックしてキャンセルすることができます。また、［**Refresh（更新）**］をクリックしてステータスを再表示することができます。移行タスクを示すページのセクションは、自動的に更新されます。

   移行が完了すると［Migration Results（移行結果）］ページが表示され、移行が成功したかどうかを示すメッセージが表示されます。移行が失敗した場合や、成功しても警告が出された場合は、エラー メッセージが表示されます。

8. ［Migration Results（移行結果）］ページの下部にあるリンクをクリックすると、**migration_summary.html** レポート、またはより詳細な **migration_detail.zip** ファイルを表示して、移行の結果について詳しく調べることができます（これらのファイルの両方、およびその他の移行情報は、［Migration Results（移行結果）］ページの下部に表示される結果ディレクトリに保存されています）。移行結果を確認したら、［**Done（終了）**］をクリックし、［Migration Results（移行結果）］ページを閉じます。

## コンタクト リストの更新

仮想アプライアンスで新しいホスト名と IP アドレスを使用する場合は、プライマリ インスタンスの Security Console でコンタクト リストを更新する必要があります。この更新によって、新しいレプリカ インスタンスへの参照情報が追加されます。同じホスト名および IP アドレスを使用して移行を実行した場合は、コンタクト リストを更新する必要はありません。

サーバを再起動した場合は、新しいレプリカ インスタンスへの参照は自動的に更新されます。

**処理手順**

1. Security Console で、［**Access（アクセス）**］＞［**Authentication Agents（認証エージェント）**］＞［**Authentication Manager Contact List（Authentication Manager コンタクト リスト）**］＞［**Automatic Rebalance（自動更新）**］の順にクリックします。
2. ［**Rebalance（更新）**］をクリックします。
3. 認証を実行します。

# 6 移行後タスクの実行

## 移行後のタスク

移行が完了した後、導入環境ごとに該当する特定の移行後タスクを完了する必要があります。

| タスク | 説明 | リファレンス |
|---|---|---|
| カスタム ポートの構成 | RSA Authentication Manager 6.1 サーバで、デフォルト ポートではなくカスタム ポートを使用していた場合は、次のサービスで、引き続きそれらのカスタム ポートを使用できます。<br>• Agent 認証<br>• Agent 自動登録<br>• オフライン認証ダウンロード | 90 ページの「カスタム ポートの構成」 |
| トークン ポリシーの構成 | バージョン 8.0 では、ユーザーがシステム生成 PIN またはユーザー作成 PIN のどちらかを選択することはできなくなりました。システム生成 PIN またはユーザー作成 PIN のどちらかか一方を要求するようにトークン ポリシーを構成する必要があります。 | Security Console ヘルプで「トークンポリシーの編集」トピックを参照してください。 |

| タスク | 説明 | リファレンス |
| --- | --- | --- |
| インスタンス IP アドレスの変更 | インスタンスの初期 IP アドレスは、Quick Setup の実行中に指定します。インスタンス IP アドレスを変更した場合は、次の操作を実行する必要があります。<br>• 新しい URL を入力して、各 RSA Console にアクセスします。詳細については、「RSA Authentication Manager 8.0 セットアップと構成ガイド」の「プライマリ インスタンスの導入」の章の「コンソールのログオン」を参照してください。<br>• プライマリ インスタンスの IP アドレスを変更する場合は、導入環境内の各レプリカ インスタンスにプライマリ インスタンスの新しい IP アドレスを設定する必要があります。レプリカ インスタンスでは、プライマリ インスタンスに接続するために新しい IP アドレスが必要です。 | Operations Console ヘルプで「プライマリ インスタンス IPv4 ネットワーク設定の変更」トピックを参照してください。 |
| 新しい Authentication Manager 構成ファイルの生成と導入 | スタンドアロン プライマリ インスタンスの IP アドレスを変更した場合、または一部の認証エージェントが、新しい IP アドレスを持つインスタンスとのみ通信するようにしたい場合、新しい Authentication Manager 構成ファイル（**sdconf.rec**）を生成して、影響を受けるすべての認証エージェントに導入する必要があります。 | 92 ページの「Authentication Manager 構成ファイルの生成」を参照してください。 |

| タスク | 説明 | リファレンス |
| --- | --- | --- |
| 変更をレプリケーションするように RSA RADIUS を構成します。 | RADIUS レプリケーションでは、RADIUS レプリカ サーバ上のデータが、RADIUS プライマリ サーバ上のデータと同期されます。管理者が Security Console を使用して RADIUS データを変更すると、プライマリ サーバはそれを検出し、レプリケーション可能なすべての RADIUS データをレプリカ サーバに送信します。変更がなかった場合、プライマリ サーバはいずれのデータもレプリケーションしません。<br>定期レプリケーションと呼ばれる自動レプリケーションを構成するか、変更を手動でレプリケーションすることができます。 | 「RSA Authentication Manager 8.0 管理者ガイド」の「RSA RADIUS」の章の「RADIUS データのレプリケーション」セクションを参照してください。 |
| RADIUS サーバ用クライアントの編集 | 移行では、以下の条件が当てはまる場合、導入環境内の RSA RADIUS サーバの IP アドレスが変更になります。<br>• バージョン 6.1 の RSA RADIUS サーバがリモート RADIUS サーバであった<br>• バージョン 6.1 の RADIUS サーバがローカル RADIUS サーバで、新しい IP アドレスとホスト名を使用してバージョン 6.1 を移行した<br>RADIUS サーバの IP アドレスが変更された場合、新しい IP アドレスを使用するようにすべての RADIUS クライアントを更新する必要があります。その操作には、RADIUS クライアント デバイスのネイティブ ツールを使用します。 | RADIUS クライアント デバイスのドキュメントを参照してください。 |

| タスク | 説明 | リファレンス |
|---|---|---|
| デフォルトの RADIUS プロファイルの構成 | バージョン 6.1 でデフォルトの RADIUS プロファイルを設定していた場合、そのプロファイルはバージョン 8.0 に移行されますが、デフォルトのプロファイルには設定されません。移行後にこのプロファイル、または他のいずれかのプロファイルをデフォルトとして指定するには、Security Console を使用します。 | 詳細については、Security Console ヘルプで「RADIUS プロファイルの構成」のトピックを参照してください。 |
| RSA RADIUS の動作テスト | RSA RADIUS が正常に動作することを確認します。 | 93 ページの「RSA RADIUS の動作テスト」を参照してください。 |
| TACACS+ サポートの構成 | バージョン 8.0 では、プライマリ インスタンスと同じマシンでは TACACS+ はサポートされていません。バージョン 6.1 で同じマシン上で TACACS+ を使用していた場合は、個別の TACACS+ ホストを構成し、それを、1 つのエージェントとしてバージョン 8.0 導入環境に追加する必要があります。 | 93 ページの「TACACS+ サポートの構成」を参照してください。 |

## カスタム ポートの構成

RSA Authentication Manager 6.1 サーバで、デフォルト ポートではなくカスタム ポートを使用していた場合は、次のサービスで、引き続きそれらのカスタム ポートを使用できます。

- Agent 認証
- Agent 自動登録
- オフライン認証ダウンロード

**処理手順**

1. Security Console でのカスタム ポートの構成
2. Authentication Manager サービスの再起動
3. Authentication Manager 構成ファイルの生成

## Security Console でのカスタム ポートの構成

Security Console を使用して、バージョン 8.0 導入環境のカスタム ポートを構成します。

### 処理手順

1. 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。
2. [Authentication Settings（認証設定）] で、[**Agents（エージェント）**] をクリックします。
3. [**Authentication Service（認証サービス）**] の [**Port（ポート）**] フィールドに、エージェントが認証サービスとの通信に使用するポート番号を入力します。デフォルトでは、ポート番号は 5500 です。
4. [**Agent Auto-Registration Service（エージェント自動登録サービス）**] の [**Port（ポート）**] フィールドに、エージェントがエージェント自動登録サービスとの通信に使用するポート番号を入力します。デフォルトでは、ポート番号は 5550 です。
5. [**Offline Authentication Download Service（オフライン認証ダウンロードサービス）**] の [**Port（ポート）**] フィールドで、オフライン認証データ、およびオフライン認証データのリクエストを送信するために使用するポート番号を入力します。デフォルトでは、ポート番号は 5580 です。
6. [**Save（保存）**] をクリックします。

## Authentication Manager サービスの再起動

Operations Console を使用してシステムをリブートすると、Authentication Manager サービスは自動的に開始されます。

リブート処理は約 10 分かかります。リブートが完了すると、Operations Console のログオン ページにリダイレクトされます。

### 開始する前に

Operations Console 管理者である必要があります。

### 手順

1. リブートするアプライアンスで、RSA Operations Console にログオンします。
2. [**Maintenance（保守）**] > [**Reboot Appliance（アプライアンスのリブート）**] の順にクリックします。
3. [Reboot Appliance Confirmation（アプライアンスリブートの確認）] ページで、[**Yes, reboot the appliance（はい、アプライアンスをリブートします）**] を選択し、[**Reboot（リブート）**] をクリックします。
4. [Reboot Appliance Progress（アプライアンスのリブート中）] ページで、リブートが完了するまで待機します。

## Authentication Manager 構成ファイルの生成

認証エージェントと RSA Authentication Manager の間の通信を構成する必要があります。これを行うには、Security Console を使用して、RSA Authentication Manager 構成ファイル **sdconf.rec** を含む zip ファイル（**AM_Config.zip**）を生成します。通信を構成するには、**sdconf.rec** を各エージェント ホストにコピーします。**sdconf.rec** ファイルには、ファイル生成時のサーバ トポロジーのスナップショットが含まれています。エージェントは **sdconf.rec** ファイル内のデータをバックアップとして使用します。

生成された zip ファイルには、エージェント上で構成可能な failover.dat ファイルも含まれています。プライマリ インスタンスが使用不可になったり、NAT（ネットワーク アドレス変換）を使用するファイアウォールによってエージェント ホストから分離されたりした場合に、failover.dat ファイルを使用してエージェントの自動登録を完了できます。このファイルには、プライマリ インスタンス、レプリカ インスタンス、それぞれのエイリアス IP アドレスのリストが含まれています。

### 開始する前に

- エージェントが Authentication Manager に接続できることを確認します。
- 構成設定を確認します。Security Console ヘルプ トピックの「エージェント設定の構成」を参照してください。

### 手順

1. Security Console で、[**Access（アクセス）**] > [**Authentication Agents（認証エージェント）**] > [**Generate Configuration File（構成ファイルの生成）**] の順にクリックします。
2. [**Maximum Retries（最大リトライ回数）**] ドロップダウン メニューで、認証エージェントが Authentication Manager との通信を確立する際の試行回数を選択します。この回数に達すると、「Cannot initialize agent - server communications（エージェントとサーバの通信を初期化できません）」というメッセージが返されます。
3. [**Maximum Time Between Each Retry（最大リトライ間隔）**] ドロップダウン メニューで、認証エージェントが Authentication Manager との通信を確立する際の試行間隔（秒単位）を選択します。
4. [**Generate Config File（構成ファイルの生成）**] をクリックします。
5. [**Download Now（今すぐダウンロード）**] をクリックし、**AM_Config.zip** をローカル マシンに保存します。

### 次のステップ

- **AM_Config.zip**（**sdconf.rec** ファイルと **failover.dat** ファイルが含まれる）を各エージェント ホストにコピーします。
- 新しい **sdconf.rec** ファイルでエージェントを構成します（必要に応じて **failover.dat** ファイルも使用します）。手順については、エージェントのマニュアルを参照してください。

## RSA RADIUS の動作テスト

RSA RADIUS の動作をテストするには、次の 2 通りの方法があります。

- RSA RADIUS サーバと Authentication Manager の間で RSA SecurID 認証が正しく行われるかどうかをテストする。さまざまなサードパーティ RADIUS テスト認証ツールのいずれかを利用してテストを容易に行うことができます （これらのツールの多くはインターネット上で検索可能です）。
- エンド ツー エンドの認証をテストし、RADIUS クライアントが RSA RADIUS および Authentication Manager を使用して認証に成功することを確認する。

次の手順でテストを実施し、ユーザーが RSA RADIUS および Authentication Manager を使用して認証に成功することを確認します。

**処理手順**

1. RADIUS クライアントが RSA RADIUS サーバと通信するように RADIUS クライアントを構成します。詳細については、RSA Security Console ヘルプで「RADIUS クライアントの追加」のトピックを参照してください。
2. テスト ユーザーに RSA SecurID トークンと必要なソフトウェアを支給します。
3. 1 つの特定の RADIUS サーバをテストする場合は、クライアント デバイスにログインしてその管理プログラムを起動し、RADIUS 構成インタフェースから RADIUS サーバの IP アドレスを入力します。
4. ユーザーに SecurID トークンを使用して保護リソースへのアクセスを試行してもらいます。
   ユーザーが認証に成功すれば、RADIUS が適切に構成されています。

## TACACS+ サポートの構成

Authentication Manager バージョン 8.0 では、Authentication Manager と同じサーバに TACACS+ を導入することはサポートされていません。
Authentication Manager バージョン 6.1 と同じマシンで TACACS+ を使用していた場合、移行後も TACACS+ を継続して使用するには、次のタスクを実行する必要があります。

1. サポート対象の別サーバに TACACS+ をインストールします。詳細については、TACACS+ のドキュメントを参照してください。
2. **sdtacplus.arg** および **sdtacplus.cfg** ファイルを、Authentication Manager 6.1 サーバから TACACS+ ホストにコピーします。

3. バージョン 8.0 プライマリ インスタンスの Security Console で、新しいエージェントとして TACACS+ ホストを追加します。作業手順については、Security Console ヘルプで「認証エージェントの追加」トピックを参照してください。
4. Authentication Manager 構成ファイル **sdconf.rec** を生成し、TACACS+ ホストに配布します。操作手順については、92 ページの「Authentication Manager 構成ファイルの生成」を参照してください。

# A 移行データの変換

## 移行データの変換

次の表では、さまざまなタイプのデータがどのように移行されるかを説明しています。

| データ | 移行の結果 |
|---|---|
| LDAP 同期ジョブ | ユーザーやグループのように LDAP に直接関連づけられているレコードは、アイデンティティ ソースに存在しているかどうか検証される。オプションを指定した場合、LDAP 上に存在しないレコードは内部データベースに作成される。 |
| ユーザー データ | ユーザー データは、次の情報を含めて移行される。<br>• RADIUS プロファイル名（割り当てられている場合）。<br>• レルム間認証の割り当て（ある場合）。<br>• ドメイン名でのログオン。ログオン名は NTLM 形式から UPN 形式に変換可能。<br>ユーザーのセキュリティ ブロックが空の場合はユーザーの属性は移行されない。セキュリティ ブロックには Windows のログオン パスワードとエマージェンシー アクセス パスワードが保存され、いずれも SecurID for Windows で使用される。 |
| PIN データ | PIN は移行される。<br>PIN の有効期限は移行されない。移行した PIN の有効期限を設定する場合は、Security Console ヘルプで「トークンポリシーの編集」トピックを参照してください。 |
| サイト データ | サイトはセキュリティ ドメインに移行される。 |

| データ | 移行の結果 |
| --- | --- |
| グループ データ | グループはユーザー グループに移行される。バージョン 6.1 では、グループに LDAP ユーザーと非 LDAP ユーザーの両方が含まれる場合がある。移行すると、LDAP ユーザー用と非 LDAP ユーザー用に別々のグループが作成される。グループ アクセス制限も移行される。<br>バージョン 6.1 では、管理者の権限適用範囲を特定のグループに設定することができるが、管理者とグループの関連づけは移行されない。 |
| ユーザーからグループへのメンバーシップ データ | グループ メンバーシップは、ユーザー グループ メンバーシップに移行される。他のグループ メンバーシップ データ（グループ エイリアスやシェル データなど）も移行される。 |
| グループのアクティブ化を行うエージェントのデータ | 認証エージェントでのグループのアクティブ化設定は移行される。バージョン 8.0 でのグループのアクティブ化の実装方法変更に伴い、グループが関連づけられているエージェントはすべて制限付きエージェントとして移行される。 |
| ユーザーのアクティブ化を行うエージェントのデータ | エージェントがすべてのユーザーに対してオープン（制限なし）である場合、ユーザーとエージェント間の既存の関連づけは移行されない。このような場合は移行レポートに記載される。<br>エージェントが制限付きの場合、新しいグループを作成してユーザーをグループに追加し、エージェントでグループをアクティブ化し、アクセス時間を制限することで、移行後もユーザーのアクティブ化設定（およびアクセス時間制限）が保持される。同じ制限付きエージェントでアクティブ化されたユーザーが複数いる場合は、アクセス時間制限に基づいて複数のグループが作成される。<br>たとえば、エージェントでアクティブ化されたユーザーが 3 名いて、そのうち 2 名のユーザーのアクセス時間が午前 8 時から午後 5 時の間、その他のユーザーのアクセス時間が午後 3 時から午後 11 時の間の場合、次の 2 つのグループが作成される。1 つはアクセス時間が午前 8 時から午後 5 時の間のグループ、もう 1 つは午後 3 時から午後 11 時のグループである。この後、該当するユーザーがグループに追加され、それらのグループがエージェントでアクティブ化される。どちらの場合も、エージェントは制限付きエージェントとして移行される。 |

| データ | 移行の結果 |
| --- | --- |
| エージェント データ | エージェント データは、エージェント名、IP アドレス、グループのアクティブ化設定、セカンダリ ノードを含めて移行される。エージェントでの個々のユーザーのアクティブ化設定は、新しい内部ユーザーグループのアクティブ化設定に移行される。<br>エージェントの自動登録設定は移行される。RSA SecurID for Windows Authentication Agent 6.1.2 の場合は、自動登録エージェントのプライマリ IP アドレスの更新の可否についても移行される。バージョン 6.1.2 より前の RSA SecurID for Windows Authentication Agent の場合は、移行処理の詳細オプションの構成時に、自動登録エージェントの IP アドレスを保護するかどうかを選択できる。<br>エージェント レコードに保存されている RADIUS 接続パラメータは移行されない。 |
| トークン データ | トークン レコードとユーザーの割り当ては移行される。 |
| セカンダリ ノード データ | 認証エージェントのセカンダリ ノードは移行される。 |
| ワンタイム パスワード データ | ワンタイム パスワード データ（紛失したトークンの代わりに使用する固定パスワードとワン タイム トークンコード セットの両方）は移行される。 |
| クライアント タイプ データ | エージェント タイプは移行されない。バージョン 8.0 で認識されるエージェントは、標準エージェントと Web エージェントの 2 種類のみ。バージョン 6.1 のエージェント タイプは、バージョン 8.0 のネクスト トークンコード モードでのランタイム動作には影響しない。また、バージョン 8.0 では、シングル トランザクション エージェントはサポートされない。 |
| システム設定データ | PIN の生成設定を除くすべてのシステム設定を移行するように選択できる。<br>システム生成 PIN とユーザー作成 PIN のどちらかをユーザーが選択できるようにする機能は廃止。PIN ポリシーでシステム生成 PIN かユーザー作成 PIN のどちらかに設定する必要がある。 |

| データ | 移行の結果 |
| --- | --- |
| 管理者データ | • サイト管理者は移行される。ただし、バージョン 8.0 では、管理者の権限適用範囲はグループではなくセキュリティ ドメインのみであるため、グループに割り当てられた管理者は管理者として移行されない。<br>• 割り当てられたタスク リストにシステム パラメータを編集する権限のみが含まれている管理者は、管理者として移行されない。システム パラメータは移行されないため、システム パラメータを編集する権限のみを持つ管理者は、バージョン 8.0 でこれに対応するタスクを実行することはできない。<br>• 割り当てられたタスク リストにトラステッド レルムを構成する権限が含まれていない管理者は、トラステッド レルム（バージョン 8.0 の場合。バージョン 6.1 のレルム間認証の関係に相当）を表示できない。たとえば、バージョン 6.1 のグループ タスク リストまたはサイト タスク リストが割り当てられている管理者は、トラステッド レルムを表示することができない。バージョン 8.0 でトラステッド レルムを表示するには、トラステッド レルムを構成するための権限が必要。 |
| 管理者ロール データ | サイト管理者ロールは移行される。グループ管理者ロールは移行されるが、どの管理者にも割り当てられない。カスタマイズしたロールは同等のカスタム ロールに移行される。<br>RSA では、移行された各管理者ロールの権限とそれらの適用範囲を検証して、割り当てられた管理者が十分な権限を保持しているか確認することを推奨。 |

| データ | 移行の結果 |
| --- | --- |
| タスク リスト データ | 同等の権限がない場合を除き、タスク リスト データはバージョン 8.0 の権限に移行される。たとえば、管理者にシステム パラメータの編集を許可するタスク、LDAP 同期ジョブに関連するタスク、グループ管理に関連するタスクのデータは移行されない。<br>バージョン 8.0 には対応する権限がないため、ログの構成に関連する次のタスクは移行されない。<br>• Automate log maintenance（ログ メンテナンスを自動化）<br>• Configure logged events（ログ済みイベントを構成）<br>• Delete log entries（ログ エントリーを削除）<br>• Edit system log parameters（システム ログ パラメータを編集）<br>• Enable/disable system logging（システム ログを有効化 / 無効化）<br>• Restore filter configuration（フィルタ構成をリストア）<br>• Save filter configuration（フィルタ構成を保存）<br>• Log statistics（統計をログ）<br>ポリシーに関連する次のタスクにはスーパー管理者ロールが必要となる。バージョン 6.1 の管理者でタスク リストにこれらのタスクが含まれている場合は、スーパー管理者ロールを割り当てられない限り、これらのタスクを実行できない。<br>• Add/edit/delete offline auth configuration（オフライン認証構成を追加 / 編集 / 削除）<br>• Add/edit/delete RADIUS policy（RADIUS ポリシーを追加 / 編集 / 削除）<br>• Add/edit/delete EAP protected OTP policies（EAP 保護 OTP ポリシーを追加 / 編集 / 削除）<br>• Add/edit/delete token policies（トークン ポリシーを追加 / 編集 / 削除）<br>**注：**タスク リストにシステム パラメータを編集する権限のみが含まれる管理者は、管理者として移行されない。システム パラメータは移行されないため、システム パラメータを編集する権限のみを持つ管理者は、バージョン 8.0 でこれに対応するタスクを実行することはできない。 |
| ユーザー拡張データ | ユーザー拡張データはユーザーのユーザー属性フィールドに移行され、移行出力ディレクトリでコンマ区切りの（.csv）ファイルにエクスポートされる。 |

| データ | 移行の結果 |
|---|---|
| トークン拡張データ | トークン拡張データはトークンのトークン属性フィールドに移行され、移行出力ディレクトリでコンマ区切りの（.csv）ファイルにエクスポートされる。 |
| グループ拡張データ | グループ拡張データはグループのノート フィールドに移行され、移行出力ディレクトリでコンマ区切りの（.csv）ファイルにエクスポートされる。 |
| エージェント拡張データ | エージェント拡張データはエージェントのノート フィールドに移行され、移行出力ディレクトリでコンマ区切りの（.csv）ファイルにエクスポートされる。 |
| サイト拡張データ | サイト拡張データはセキュリティ ドメインのノート フィールドに移行され、移行出力ディレクトリでコンマ区切りの（.csv）ファイルにエクスポートされる。 |
| RADIUS プロファイル データ | RADIUS プロファイル名およびユーザーへのプロファイル割り当ては移行される。プロファイルの属性および属性値が RSA RADIUS サーバ データベースに保存され、Authentication Manager データとは別に移行される。 |
| レプリカ データ | レプリカ サーバに関するデータは移行されない。ただし、レプリカ サーバ自体は移行可能。移行後のプライマリ インスタンスは、従来のレプリカ サーバとは通信を試みない。 |
| レルム間データ | レルム間認証の関係は移行される。バージョン 8.0 では、従来のレルム間モデルとは異なる新しいトラステッド レルム モデルを実装。詳細については、36 ページの「レルム間認証とトラステッド レルムの比較」を参照してください。 |
| エージェント デルタ データ | レプリカ サーバで行われた認証エージェントの変更は、移行および処理される。 |
| ユーザー デルタ データ | レプリカ サーバで行われたユーザーの変更は、移行および処理される。 |
| トークン デルタ データ | レプリカ サーバで行われたトークンの変更は、移行および処理される。これにはトークンの削除およびトークンの交換処理が含まれる。 |
| ワンタイム パスワード デルタ データ | レプリカ サーバで行われたワンタイム パスワードの変更は、移行される。これには認証に使用されたワンタイム パスワードの削除が含まれる。 |
| ログ レコード | ログ レコードは手動での移行が必要。詳細については、78 ページの「ログ ファイルの移行」を参照してください。 |

## 移行レポート

移行が完了すると、移行レポートが生成されます。レポートには、正常に移行されたデータ、移行に失敗したデータ、RSA Authentication Manager 8.0 で使用される新しい論理モデルに適合させるためにデータに加えられた変更がリストされています。

- 移行のために選択したパラメータおよびオプション。
- ダンプ ファイルの解析結果のサマリー（ダンプ ファイルにどのタイプのデータが存在したかなど）。
- 移行されたオブジェクト（ユーザー、ユーザー グループ、トークン、エージェント、ポリシー、管理者ロール、拡張データなど）のリスト。
- 移行した Authentication Manager が正しく安全に機能するために解決する必要のあるデータ形式に関する問題。

  バージョン 6.1 の Database Administration アプリケーションを使用して、移行レポートで明らかになった形式に関する問題を解決してください。

以降のセクションでは、移行レポートに表示される可能性がある問題の一部について概説します。また、バージョン 6.1 のデータベースでこれらの問題をクリーンアップする方法について説明します。クリーンアップ処理を実施した後に、リストアしたバージョン 8.0 のデータベースに対して再び移行を実施してください。


- 101 ページの「複数値拡張データ」
- 102 ページの「異なるサイトの複数グループのユーザー」
- 103 ページの「LDAP 同期ジョブにグループ データが含まれない場合の制限付きエージェントのアクティブ化」
- 103 ページの「LDAP 同期ジョブにグループ データが含まれない場合の制限付きエージェントのアクティブ化」
- 103 ページの「エマージェンシー コードの PIN オプション」
- 104 ページの「管理者の認証方式としての SecurID_Native の追加」


### 複数値拡張データ

RSA Authentication Manager 6.1 では、個々のオブジェクト（個々のユーザー、ユーザー グループ、エージェント、トークンなど）に対してのみ拡張データを定義できますが、システム全体で共通の拡張データを定義することはできません（そのため、全ユーザー、全グループ、全エージェント、全トークンに対して共通の拡張データセットを定義することはできません）。結果として、同じタイプのデータ（ユーザーの電話番号など）が格納された複数の拡張フィールドがデータベースに含まれることがありますが、一貫性のないフィールド名が設定され、同様に一貫性のない値の形式が設定される場合があります。各拡張フィールドはそれぞれ個別のフィールドとして移行され、データベース内の各関連オブジェクトに追加されます。

たとえば、ユーザーの電話番号の拡張フィールドがあり、それらの拡張フィールドの名前がユーザーごとに異なる（Phone Num.、Phone Number、Ph. Num.）場合があります。移行後、すべての移行済みユーザーには電話番号として複数の拡張属性が設定されます。この例では、全ユーザーに Phone Num.、Phone Number、Ph. Num. という名前の拡張属性が設定されます。3 つの属性のうち 2 つは空です。移行前にそのユーザーの拡張フィールドとして指定されていた属性にのみ、電話番号のデータが格納されます。

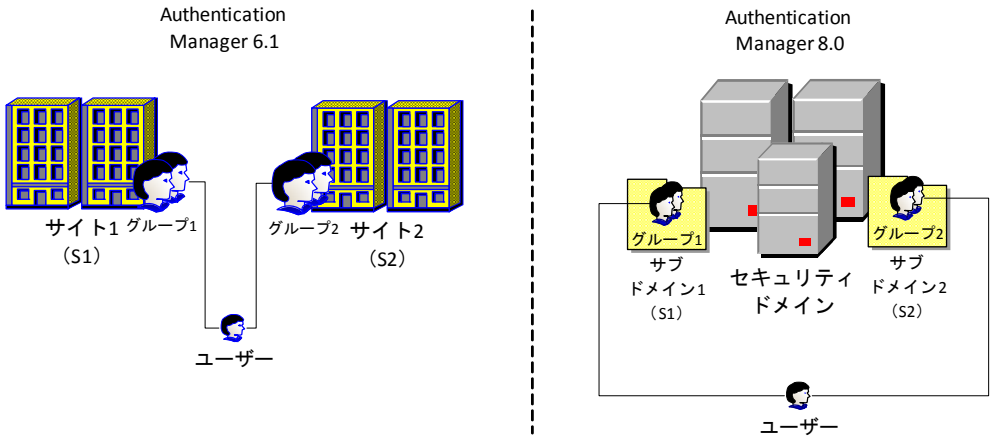
移行レポートを参照して使用されている拡張データに一貫性がない場合は、使用するフィールド名を決定します。それに適合しないユーザーの拡張データを編集し、拡張フィールド名を決定したものに合わせます。

## 異なるサイトの複数グループのユーザー

RSA Authentication Manager 6.1 では、1 人のユーザーが、異なるサイトに属する複数のグループへのグループ メンバーシップを持つことができます。バージョン 8.0 では、ユーザーまたはユーザー グループが存在できる外部アイデンティティ ソースは 1 つのみです。そのため、ある外部アイデンティティ ソースのユーザーが異なる外部アイデンティティ ソースのユーザー グループのメンバーになることはできません。

バージョン 8.0 への移行後、サイトはセキュリティ ドメイン内のサブドメインに変換されます。バージョン 6.1 のグループはこれらのサブドメインに移行され、ユーザーは同一セキュリティ ドメイン内にあるこれら 2 つのユーザー グループのメンバーとなります。

次の図で、それぞれサイト 1 およびサイト 2 にあるグループ 1 とグループ 2 に属するユーザーは、バージョン 8.0 の同じセキュリティ ドメイン内にあるサブドメイン 1 とサブドメイン 2 に移行されます。



## LDAP 同期ジョブにグループ データが含まれない場合の制限付きエージェントのアクティブ化

移行前に次の状況に該当する場合、移行後一部のエージェントで LDAP ユーザーが認証を受けることができません。

- ユーザーを同期する LDAP 同期ジョブが、ユーザーが属する LDAP グループを同期するように構成されていない。
- LDAP 同期ジョブでアクセスするディレクトリ サーバが読み取り専用である。
- ユーザーが、RSA Authentication Manager 6.1 のデータベースにのみ存在するグループに属している
  (管理者がバージョン 6.1 の Database Administration アプリケーションを使用して作成したグループに LDAP ユーザーを追加した場合など)。
- ユーザーが認証エージェントでアクティブ化されていた場合、移行時に、そのユーザーがメンバーとして属するユーザー グループの新規作成と、認証エージェントでのユーザー グループのアクティブ化が試行される。

バージョン 6.1 では、LDAP グループを同期することなく LDAP ユーザーを同期できます。このようなジョブで同期されたユーザーはグループのメンバーになることはできますが、このグループは内部データベースに存在するグループのみです。つまり、グループ関係が分かるのは Authentication Manager のみということです。ディレクトリ サーバで定義されたグループ メンバーシップは、Authentication Manager では分かりません。

この問題を解決するには、ディレクトリ サーバを担当する管理者に連絡し、LDAP 同期ジョブにグループ データを追加できるよう依頼します。

## エマージェンシー コードの PIN オプション

バージョン 6.1 では、トークンの紛失または破損が発生した場合、ユーザーは固定パスワードまたはワンタイム パスワード セットのいずれかを使用できます。固定パスワードまたはワンタイム パスワード セットを生成する際は、管理者が固定パスワードまたはワンタイム パスワード セットの PIN オプションを選択します。バージョン 6.1 では、PIN オプションにシステム全体で有効なパラメータはありません。

バージョン 8.0 では、これらのエマージェンシー アクセス方法をオンライン エマージェンシー トークンコードと呼びます。バージョン 8.0 では、オフライン エマージェンシー認証と同じ PIN オプションがオンライン認証にも適用されます。

移行後は、オフライン エマージェンシー コードの生成用に構成された PIN オプションが、オンライン エマージェンシー コードにも適用されます。バージョン 6.1 で生成された既存の固定パスワードおよびワンタイム パスワード セットは移行され、移行後のバージョン 8.0 の導入環境で引き続き機能しますが、新しく生成する固定パスワード（バージョン 8.0 では固定パスコード）およびワンタイム パスワード セット（バージョン 8.0 ではエマージェンシー コード）はいずれもバージョン 6.1 のオフライン エマージェンシー コード用に構成された PIN オプションに準拠します。

## RSA Authentication Manager 6.1 のオフライン エマージェンシー設定の表示

バージョン 8.0 への移行後は、Authentication Manager によって、新しく生成された固定パスワードとワンタイム パスワード セットに、バージョン 6.1 のオフライン エマージェンシー コードの PIN オプションが適用されます。Authentication Manager がこれらのパスワードに適用するバージョン 6.1 の設定は参照可能です。

### 処理手順

1. RSA Authentication Manager 6.1 Database Administration アプリケーションを開きます。
2. ［System（システム）］メニューから、［**System Configuration（システム構成）**］＞［**Edit Offline Auth Config（オフライン認証構成の編集）**］の順にクリックします。
3. ［**Codes Contain（使用可能な文字）**］で、設定を参照します。

## 管理者の認証方式としての SecurID_Native の追加

移行レポートに次のメッセージが含まれる場合、SecurID_Native 認証方式を使用するよう、Security Console の構成が必要です。

```
SecurId_Native authentication is allowed in the dump file.As
system settings were not migrated, an admin may not be able
to log into admin console using SecurID as an authentication
method.
```

次の場合に、前述のメッセージが移行レポートに表示されます。

- バージョン 6.1 の Authentication Manager のシステム パラメータに、管理者の認証方式として SecurID カード、フォブ、USB が含まれている。
- システム パラメータを移行しなかった。

その結果、バージョン 6.1 の Database Administration アプリケーションの認証方式として、SecurID カード、フォブ、USB トークンのいずれかのみ使用可能な Authentication Manager 管理者は、Security Console にログオンできなくなります。システム パラメータを移行するか、またはコンソール認証方式として **SecurID_Native** を有効にすることで、この問題を解決できます。

**処理手順**

1. 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。
2. ［**Security Console Authentication Methods（Security Console の認証方式）**］をクリックします。
3. ［**Console Authentication**］フィールドで、認証方式として［**SecurID_Native**］を追加します。
4. ［**Save（保存）**］をクリックします。
5. ［**Yes, update authentication methods configuration（はい、認証方式の構成を更新します）**］を選択します。
6. ［**Update Authentication Methods Configuration（認証方式の構成を更新）**］をクリックします。

# B RSA Authentication Manager 8.0 からバージョン 6.1 への復元

## 移行からの復元

バージョン 8.0 への移行後、バージョン 6.1 に必要なデータとアプリケーション ファイルはすべて元の Authentication Manager ハードウェアに残っています。ただし、単にバージョン 8.0 を停止してバージョン 6.1 を再起動しても、バージョン 6.1 へは戻りません。復元する前に、次の 4 つの重要な問題について考慮する必要があります。

- データ消失
  バージョン 8.0 の管理や認証アクティビティに関するデータはすべて消失し、バージョン 6.1 で使用するためにリカバリすることはできません。バージョン 6.1 のサーバは、移行時と同じ状態のままになります。
- 認証のダウンタイムと認証エージェントの更新
  復元する際は必ずバージョン 8.0 の停止とバージョン 6.1 の再起動が必要になりますが、管理機能のダウンタイムは最小限に抑えられます。ただし、認証機能のダウンタイムは、すべての認証エージェントの更新に要する時間によって影響を受けます。
- 認証エージェント
  認証エージェントが復元したバージョン 6.1 のサーバと通信できるようにするには、移行のタイプに応じて、すべての認証エージェントに新しい構成ファイルを作成するか、またはすべての認証エージェントから **sdstatus.12** ファイルを削除する必要があります。
- レプリケーション トラフィック
  復元したバージョン 6.1 のレプリカ データベースには、レプリカ サーバの起動時にプライマリ サーバにレプリケーションされるデルタ レコードが含まれたままです。このため、プライマリ サーバとネットワーク上のレプリカ サーバ間に多数のアクティビティが発生する可能性があります。

## 別のホスト名と IP アドレスを使用した移行からの復元

新しいホスト名または IP アドレスを使用して移行した場合、バージョン 6.1 への復元手順の中で、バージョン 8.0 のインスタンスで認証していたすべての認証エージェント用に、バージョン 6.1 の新しい構成ファイルを生成する必要があります。

**処理手順**

1. バージョン 8.0 のプライマリ インスタンスで Authentication Manager サービスをすべて停止します。手順については、「RSA Authentication Manager 8.0 管理者ガイド」の「高度な管理」の章の「RSA Authentication Manager サービスの手動管理」を参照してください。
2. バージョン 6.1 のプライマリ サーバを起動します。

   Windows の場合：

   a. バージョン 6.1 のプライマリ サーバ上で［[**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Control Panel（RSA Authentication Manager コントロール パネル）**］の順にクリックします。

   b. 左側のメニューで、［**Start & Stop RSA Authentication Manager Services（RSA Authentication Manager サービスの起動と終了）**］をクリックします。

   c. ［Start Services（サービスの起動）］で［**Start All（すべてを起動）**］をクリックします。

   Solaris および Linux の場合：

   バージョン 6.1 のプライマリ サーバ上でコマンド ラインに次のコマンドを入力します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

3. Database Administration アプリケーションで、すべての認証エージェントに対して新しい構成ファイルを生成します。

   a. ［**Agent Host（エージェント ホスト）**］＞［**Generate Configuration Files（構成ファイルの生成）**］の順にクリックします。

   b. ［**All Agent Hosts（すべてのエージェント ホスト）**］をクリックします。

   c. ［**OK**］をクリックします。

   **sdconf.rec** ファイルが ***ACEDATA*/config_files** ディレクトリ内のディレクトリに作成されます。ディレクトリには、割り当てられたアクティング マスター（またはアクティング マスター / スレーブのペア）と割り当てられたアクティング サーバの IP アドレスを組み合わせた名前が付きます。
4. バージョン 8.0 の各レプリカ インスタンスで Authentication Manager サービスをすべて停止します。
5. バージョン 6.1 のレプリカ サーバを再起動します。
6. 新しい **sdconf.rec** ファイルをバージョン 8.0 のインスタンスで認証されていたすべてのエージェントに配布します。

## 同じホスト名と IP アドレスを使用した移行からの復元

同じホスト名または IP アドレスを使用して移行した場合、バージョン 6.1 への復元プロセスでは、バージョン 8.0 プライマリ インスタンスをネットワークから削除し、バージョン 6.1 のプライマリ インスタンスを開始し、各 RSA Authentication Agent から **sdstatus12** ファイルを削除する必要があります。これにより、各エージェントは、バージョン 6.1 サーバが含まれる新しいサーバ リストを受信します。

### 処理手順

1. バージョン 8.0 のプライマリ インスタンスで Authentication Manager サービスをすべて停止します。手順については、「RSA Authentication Manager 8.0 管理者ガイド」の「高度な管理」の章の「RSA Authentication Manager サービスの手動管理」を参照してください。
2. ネットワークからバージョン 8.0 のプライマリ インスタンスを削除します。
3. バージョン 8.0 のプライマリ インスタンスと同じホスト名と IP アドレスを使用してネットワークにバージョン 6.1 のプライマリ サーバを追加します。
4. バージョン 6.1 のプライマリ サーバを起動します。

   Windows の場合：

   a. バージョン 6.1 のプライマリ サーバ上で［**Start（スタート）**］＞［**Programs（プログラム）**］＞［**RSA Security**］＞［**RSA Authentication Manager Control Panel（RSA Authentication Manager コントロール パネル）**］の順にクリックします。

   b. 左側のメニューで、［**Start & Stop RSA Authentication Manager Services（RSA Authentication Manager サービスの起動と終了）**］をクリックします。

   Solaris および Linux の場合：

   バージョン 6.1 のプライマリ サーバ上でコマンド ラインに次のコマンドを入力します。

   ```
   ACEPROG/sdconnect start
   ACEPROG/aceserver start
   ```

5. バージョン 8.0 のレプリカ インスタンスをすべて停止します。
6. 各 RSA Authentication Agent の **sdstatus12** ファイルを削除します。

   このファイルを削除すると、各エージェントが **sdconf.rec** ファイルを読み取ります。このファイルには、プライマリ サーバとレプリカ サーバの名前が含まれています。エージェントがこれらのサーバの 1 つに接続すると、新しいバージョン 6.1 のサーバのリストがサーバからエージェントに送信されます。エージェントは新しいサーバ リストを受け取るまで、**sdeconf.rec** ファイルに含まれているサーバとのみ通信できます。
7. ネットワークからバージョン 8.0 のレプリカ インスタンスをすべて削除します。
8. バージョン 8.0 のレプリカ インスタンスと同じホスト名と IP アドレスを使用してネットワークにバージョン 6.1 のレプリカ サーバを追加します。

# C 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

## れ



## ろ