CA Access Control Premium Edition

アップグレード ガイド

12.6.01

サードパーティに関する通知

CONTAINS IBM(R) 32-bit Runtime Environment for AIX(TM), Java(TM) 2 Technology Edition, Version 1.4 Modules

サンプル スクリプトおよびサンプル SDK コード

CA Access Control 製品に含まれているサンプル スクリプトおよびサンプル SDK コードは、情報提供のみを目的として現状有姿のまま提供されます。これらは特定の環境で調整が必要な場合があるため、テストや検証を実行せずに実稼働システムにデプロイしないでください。

CA Technologies では、これらのサンプルに対するサポートを提供していません。また、これらのスクリプトによって引き起こされるいかなるエラーにも責任を負わないものとします。

CA Technologies 製品リファレンス

このマニュアルが参照している CA Technologies の製品は以下のとおりです。

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On（eTrust SSO）
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM、旧 Unicenter NSM and Unicenter TNG）
- CA Software Delivery（旧 Unicenter Software Delivery）
- Unicenter Service Desk（旧 Unicenter Service Desk）
- CA User Activity Reporting Module（旧 CA Enterprise Log Manager）
- Identity Manager

ドキュメントの表記規則

CA Access Control のドキュメントには、以下の規則があります。

形式	意味
等幅フォント	コードまたはプログラムの出力
斜体	強調または新規用語
太字	表示されているとおりに入力する必要のある要素
スラッシュ（/）	UNIX および Windows のパスの記述で使用される、プラットフォームに依存しないディレクトリの区切り文字

また、本書では、コマンド構文およびユーザ入力の説明に（等幅フォントで）以下の特殊な規則を使用します。

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ（[]）で囲まれた文字列	オプションのオペランド
中かっこ（{}）で囲まれた文字列	必須のオペランド セット
パイプ（|）で区切られた選択項目	代替オペランド（1 つ選択）を区切ります。 たとえば、以下の例は「*ユーザ名*または*グループ名*のいずれか」を意味します。 {*username*|*groupname*}
…	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号（¥）	本書では、コマンドの記述が 1 行に収まらない場合があります。このような場合、行末の空白とそれに続く円記号（¥）は、そのコマンドが次の行に続くことを示します。 **注**：このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。これらの文字は、実際のコマンド構文の一部ではありません。

例：コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

```
ruler className [props({all|{propertyName1[,propertyName2]...})]
```

この例の内容

- 標準的な等幅フォントで表示されているコマンド名（ruler）は表示されているとおりに入力します。
- 斜体で表示されている *className* オプションは、クラス名（USER など）のプレースホルダです。
- 2 番目の角かっこで囲まれた部分を指定しなくても、コマンドは実行できます。この部分は、オプションのオペランドを示します。
- オプションのパラメータ（props）を使用する場合は、キーワード *all* を選択するか、またはカンマで区切られたプロパティ名を 1 つ以上指定します。

ファイル ロケーションに関する規則

CA Access Control のドキュメントには、ファイル ロケーションに関する以下の規則があります。

- *ACInstallDir* -- CA Access Control のデフォルトのインストール ディレクトリ。
  - Windows -- <インストール パス>
  - UNIX -- <インストール パス 2>
- *ACSharedDir* -- CA Access Control for UNIX で使用される、デフォルトのディレクトリ。
  - UNIX -- /opt/CA/AccessControlShared
- *ACServerInstallDir* -- CA Access Control エンタープライズ管理 のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir* -- デフォルトの配布サーバ インストール ディレクトリ。
  - /opt/CA/DistributionServer
- *JBoss_HOME* -- デフォルトの JBoss インストール ディレクトリ。
  - /opt/jboss-4.2.3.GA

CA への連絡先

テクニカル サポートの詳細については、弊社テクニカル サポートの Web サイト（http://www.ca.com/jp/support/）をご覧ください。

目次

第 1 章: 本書の内容

このガイドでは、CA Access Control Premium Edition サーバとエンドポイント コンポーネントをアップグレードする方法、および拡張ポリシー環境へ PMD を移行する方法について説明します。

用語を簡潔に示すために、本書の全体を通してこの製品を CA Access Control と呼びます。

第 2 章: サーバおよびエンドポイントのコンポーネントのアップグレード

このセクションには、以下のトピックが含まれています。

はじめに

アップグレード プロセスを開始する前に、以下のトピックを確認します。

既存の中央データベースの Microsoft SQL Server 2008 へのアップグレード

CA Access Control エンタープライズ管理 中央データベースが Microsoft SQL Server 2005 上で設定されており、Microsoft SQL Server 2008 にアップグレードする場合、新しいサーバで動作するようにエンタープライズ管理サーバを設定します。

以下の手順に従います。

1. エンタープライズ管理サーバ上の CA Access Control サービスをすべて停止します。
2. JBoss を停止します。以下の*いずれか*の手順を実行します。
   - JBoss がサービスとしてインストールされていない場合は、JBoss アプリケーション サーバ ウィンドウを中断します(Ctrl+C)。
   - JBoss がサービスとしてインストールされている場合は、サービス画面から JBoss サービスを停止します。
3. Microsoft SQL Server 2008 にアップグレードします。
4. Microsoft の Web サイトから Microsoft SQL Server JDBC ドライバ 2.0 をダウンロードします。
5. エンタープライズ管理サーバ上の一時ディレクトリにファイルを解凍します。

6. 以下の*いずれか*の手順を実行します。
   - JDK バージョン 1.5 を使用している場合は、sqljdbc.jar ファイルにアクセスします。
   - JDK バージョン 1.6 以降を使用している場合は、sqljdbc4.jar ファイルにアクセスし、名前を sqljdbc.jar に変更します。
7. エンタープライズ管理サーバ上の以下のディレクトリにファイルをコピーします。

   JBoss_HOME/server/default/lib

   注: このディレクトリ内の既存のファイルを上書きします。
8. Microsoft SQL Server 2008 サービスを開始します。
9. JBoss を起動します。
10. CA Access Control エンタープライズ管理 を起動します。

エンタープライズ管理用に CA Access Control エンドポイントを準備

CA Access Control エンドポイントにエンタープライズ管理サーバをインストールできます。エンドポイントには、エンタープライズ管理サーバに必要なすべてのコンポーネントは含まれていません。エンドポイントにエンタープライズ管理サーバをインストールする前に、エンドポイントを準備します。

以下の手順に従います。

1. エンドポイント上で CA Access Control サービス（Windows）またはデーモン（UNIX）をすべて停止します。
2. エンドポイントにエンタープライズ管理サーバをインストールします。

   Web ベース アプリケーションと配布サーバがインストールされます。まだインストールされていない場合、CA Access Control の最新のバージョンがインストールされます。
3. エンタープライズ管理サーバ上に DMS を作成します。

   エンタープライズ管理サーバ インストールはエンドポイント上で DMS を作成しません。dmsmgr ユーティリティを使用して、DMS を作成します。
4. エンタープライズ管理サーバ サービスまたはデーモンを開始します。

5. ADMIN、AUDITOR および論理認可属性を持つユーザ アカウントを作成します。

   CA Access Control エンタープライズ管理 に DMS 接続設定を定義する場合、論理ユーザ アカウントを使用します。

6. DMS 上にホスト グループを作成します。
7. dmsmgr ユーティリティを使用して、DMS にノードを追加します。
8. エンタープライズ管理サーバをインストールしたときに指定した、管理者ユーザ アカウントで CA Access Control エンタープライズ管理 にログインします。
9. CA Access Control エンタープライズ管理 で、DMS 接続設定を定義します。

   エンドポイント上で作成した DMS を指定します。

   エンタープライズ管理サーバをインストールして、作成した DMS を使用するように設定します。

注: dmsmgr ユーティリティの詳細については、「リファレンス ガイド」を参照してください。selang を使用したユーザの作成および設定方法については、「selang リファレンス ガイド」を参照してください。

エンタープライズ管理サーバをアップグレードするための準備

r12.5.x エンタープライズ管理サーバのインストールを r12.6.1 にアップグレードする前に、以下の情報を収集します。

- メッセージ キュー パスワード

  管理者ユーザ、レポートサーバ ユーザ、および +reportagent ユーザのパスワードを取得します。

- データベース接続情報

  ホスト名、ポート番号、データベース名、ユーザ名およびパスワードを取得します。

- Java 接続サーバのパスワード

  前回の CA Access Control エンタープライズ管理 インストール時に使用した通信パスワードを取得します。

- (オプション) Java 接続サーバ (JCS) SSL 証明書

  カスタムの SSL 証明書を使用した場合のみ、CA Access Control エンタープライズ管理 r12.5.x にアップグレードしてから、新しい SSL 証明書をインポートします。

アップグレード後の Java コネクタ サーバ SSL 証明書のインポート

CA Access Control r12.5 SP3 での Java コネクタ サーバ (JCS) SSL 証明書の変更により、CA Access Control r12.5.x からアップグレードした後、新しい SSL 証明書をインポートする必要があります。

重要: この手順は、カスタムの JCS SSL 証明書を使用した場合にのみ実行します。デフォルトの SSL 証明書を使用した場合、この手順を実行する必要はありません。

以下の手順に従います。

1. JBoss アプリケーション サーバを停止します。
2. 以下のディレクトリに移動します (*JBOSS_HOME* は、JBoss をインストールしたディレクトリです)。

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/trusttore/

3. ssl.keystore ファイルをバックアップします。

4. 移動したディレクトリで、コマンド プロンプト ウィンドウを開きます。
5. keytool ユーティリティを実行して、インポートするカスタムの SSL キーストアを指定します。*JAVA_HOME* は、JDK がインストールされているディレクトリを示します。以下に例を示します。

   ```
   JAVA_HOME¥bin¥keytool.exe -import -alias eta_client -file
   c:¥custom_certificate.der -keystore ssl.keystore
   ```

   パスワードの入力を促すメッセージが表示されます。
6. キーストアのパスワードを入力します。デフォルトのパスワードは、「*secret*」です。

   keytool により証明書の詳細と指紋が表示されます。
7. 「Yes」と入力して、その証明書をキーストアに追加します。

   keytool により、新規証明書が追加されます。
8. JBoss アプリケーション サーバを起動します。

   新しい JCS SSL 証明書ファイルが CA Access Control エンタープライズ管理にロードされました。

CA Access Control r5.3 からのアップグレード方法

コンポーネントの追加および展開の変更によって、CA Access Control r5.3 から CA Access Control r12.6.1 にはアップグレードできません。まず既存の CA Access Control r5.3 展開を CA Access Control r8.0 SP1 にアップグレードしてから、CA Access Control r12.6.1 にアップグレードします。

この手順に従って、既存の CA Access Control r5.3 展開をアップグレードします。

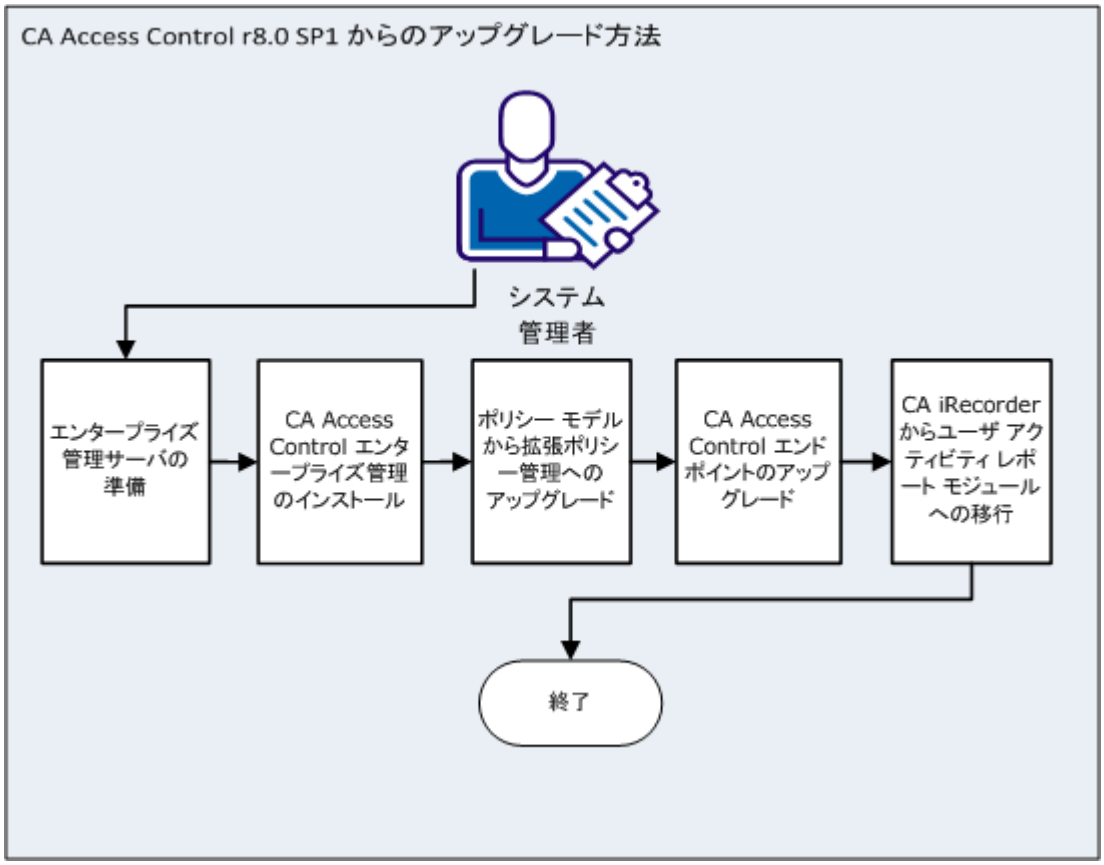
1. アップグレード プロセスを開始する前に、すべての CA Access Control コンポーネントをバックアップします。
2. CA Access Control r8.0 SP1 にアップグレードします。 (P. 17)
3. CA Access Control r12.6.1 にアップグレードします。

第 3 章: CA Access Control r8.0 SP1 からのアップグレード

このシナリオの目的は、CA Access Control r8.0 SP1 からアップグレードするための手順を説明することです。この章のアップグレード プロセスでは、CA Access Control r8.0 SP1 コンポーネントを別々のコンピュータにインストールしていることを前提にしています。

このセクションの情報は、CA Access Control の管理を行うシステム管理者または CA Access Control 管理者を対象としています。

以下の図は、CA Access Control r8.0 SP1 からのアップグレードを完了するための手順を示します。



重要: アップグレード プロセスを開始する前に、すべての CA Access Control コンポーネントをバックアップします。

以下の手順に従って、既存の CA Access Control r8.0 SP1 展開をアップグレードします。

1. エンタープライズ管理サーバを準備します。

   エンタープライズ管理サーバをインストールする前に、前提条件のインストールおよび設定によりコンピュータを準備します。

2. CA Access Control エンタープライズ管理 をインストールします (P. 21)。
3. Policy モデル環境から拡張ポリシー管理環境にアップグレードします (P. 71)。
4. CA Access Control エンドポイントをアップグレードします。
   - Windows -- Product Explorer を使用したインストール (P. 26)
   - UNIX -- install_base スクリプトを使用したインストール (P. 28)

   注: このインストールによって、パスワード PMD もアップグレードされます。
5. (オプション) iRecorder product を CA User Activity Reporting Module へ移行します。

注: Policy Manager はアップグレードできません。CA Access Control エンドポイント管理 を使用して、エンドポイント上でポリシーを管理します。

エンタープライズ管理のための中央データベースの準備

CA Access Control エンタープライズ管理 には、リレーショナル データベース システム（RDBMS）が必要です。CA Access Control エンタープライズ管理 をインストールする前に、RDBMS をセットアップします。

CA Access Control エンタープライズ管理 で使用するデータベースのセット アップには以下の 2 つのオプションがあります。

- CA Access Control が提供するデプロイメント スクリプトを使用して、中央データベースに事前にデータを読み込みます。

  このオプションを使用した場合、データベースの準備と CA Access Control エンタープライズ管理 のインストールは別々に行われます。データベース管理者は、CA Access Control によって必要となったデータベースへの変更を確認および制御できます。

- CA Access Control エンタープライズ管理 によってインストール時に中央データベースが準備されます。

  このオプションを使用した場合、CA Access Control エンタープライズ管理 のインストール処理の一部としてデータベースにデータが読み込まれます。

以下の手順に従います。

1. まだ存在しない場合は、サポート対象の RDBMS を中央データベースとしてインストールします。

   注: サポート対象の RDBMS ソフトウェアの詳細については、「*リリース ノート*」を参照してください。

2. CA Access Control エンタープライズ管理 への RDBMS の設定:

   データベースにローカルで、またリモート クライアントからアクセス可能であることを確認します。

   - Oracle の場合、中央データベース用にユーザを作成します。

     このユーザには、以下の権限および設定が必要です。

     - CONNECT（次のシステム権限を付与: ALTER SESSION、CREATE CLUSTER、CREATE DATABASE LINK、CREATE SEQUENCE、CREATE SESSION、CREATE SYNONYM、CREATE TABLE、CREATE VIEW）
     - RESOURCE（次のシステム権限を付与: CREATE CLUSTER、CREATE INDEXTYPE、CREATE OPERATOR、CREATE PROCEDURE、CREATE SEQUENCE、CREATE TABLE、CREATE TRIGGER、CREATE TYPE）
     - CA Access Control エンタープライズ管理 サーバをホストする表領域に対する無制限の割り当て。

   - SQL Server の場合:

     - 大文字小文字を区別しない、新しいデータベースを作成します。

       このデータベースには、並べ替え順序として SQL_Latin1_General_CP1_CI_AS が必要です。

     - ユーザを作成し、新しいデータベースをそのユーザのデフォルト データベースにして、そのユーザに DBCREATOR および SYSADMIN 権限を割り当てます。

3. (オプション) CA Access Control が提供するデプロイメント スクリプトを使用して、中央データベースに事前にデータを読み込みます。

   a. デプロイメント スクリプトを展開する前にカスタマイズします。

      デプロイメント スクリプトは、CA Access Control エンタープライズ管理 で使用される 4 つのデフォルト ユーザ アカウント (superadmin、selfreguser、neteautoadmin、[default user]) を定義します。これらのデフォルト アカウントの名前およびパスワードは変更できます。

      重要: スクリプトのカスタマイズは、組み込みユーザ ストアを使用する場合のみ行います。Active Directory を使用する場合、CA Access Control エンタープライズ管理 ではアカウント情報を中央データベース内に格納しません。詳細については、「*実装ガイド*」を参照してください。

   b. デプロイメント スクリプトを展開します。

   c. CA Access Control エンタープライズ管理 のインストールに使用するデータベース ユーザを設定します。

      - Oracle の場合、作成したユーザの CONNECT ロールおよび RESOURCE ロールを保持します。
      - SQL Server の場合、ユーザを作成し、作成済みのデータベースをデフォルトとして選択し、データベースにユーザをマップして次の権限を設定します: CONNECT.SELECT、INSERT、DELETE、UPDATE、EXECUTE。

Windows での CA Access Control エンタープライズ管理 のインストール

CA Access Control エンタープライズ管理 をインストールすると、エンタープライズ管理のサーバ コンポーネントがすべてインストールされます。CA Access Control エンタープライズ管理 をインストールする前に、エンタープライズ管理サーバを準備します。

前提条件キットを使用して、CA Access Control エンタープライズ管理 のインストールを開始することをお勧めします。このインストーラでは、前提条件のサードパーティ ソフトウェアがインストールされてから、CA Access Control エンタープライズ管理 のインストールが開始されます。

以下の手順に従います。

1. JBoss アプリケーション サーバが実行中の場合は、これを終了させます。
2. CA Access Control がすでにインストールされているコンピュータに CA Access Control エンタープライズ管理 をインストールする場合は、CA Access Control サービスを停止します。

3. 光ディスクドライブに CA Access Control Premium Edition Server Components DVD for Windows を挿入します。
4. Product Explorer で[Components]フォルダを展開し、CA Access Control エンタープライズ管理 を選択し、[インストール]をクリックします。

   InstallAnywhere インストール プログラムが起動します。

   a. (オプション)カスタム FIPS キーのフルパス名を指定して、インストール中に使用します。

   b. コマンド プロンプト ウィンドウを開き、CA Access Control Premium Edition Server Components DVD for Windows 上の CA Access Control エンタープライズ管理 インストール実行可能ファイルに移動します。このファイルは以下の場所にあります。

      ```
      ¥EnterpriseMgmt¥Disk1¥InstData¥NoVM
      ```

   c. 以下の引数を指定して CA Access Control エンタープライズ管理 インストール実行可能ファイルを実行します。

      ```
      -DFIPS_KEY=full_pathname_to_FIPS_key
      ```

      たとえば、C:¥tmp¥FIPS.key にあるカスタム FIPS キーを使ってインストールするには、以下のように設定します。

      ```
      E:¥EnterpriseMgmt¥Dis1¥InstData¥NoVM¥install_EntM_r125.exe
      -DFIPS_KEY=C:¥tmp¥FIPSkey.dat
      ```

   重要: CA Access Control エンタープライズ管理 をインストールしてハイアベイラビリティを実現する場合、プライマリおよびセカンダリのエンタープライズ管理サーバ上に同じ FIPS キーを指定します。CA Access Control エンタープライズ管理 をインストールして FIPS サポートによるハイ アベイラビリティを実現する場合、カスタム FIPS キーを指定します。

   InstallAnywhere インストール プログラムが起動します。

5. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

   Java Development Kit(JDK)

   既存の JDK の場所を定義します。

   注: CA Access Control Premium Edition Third Party Component DVD を使用して必須ソフトウェアをインストールした直後に、CA Access Control エンタープライズ管理 のインストールを開始した場合、このウィザードは表示されません。インストール ユーティリティは、必須のソフトウェア インストール プロセスの際に指定した値を基に、このページのインストール設定を行います。

JBoss アプリケーション サーバ情報

アプリケーションをインストールする JBoss インスタンスを定義します。

これを行うには、以下を定義します。

- JBoss フォルダ（JBoss をインストールしているトップ ディレクトリ）。

  たとえば、Windows の場合は C:¥jboss-4.2.3.GA、Solaris の場合は /opt/jboss-4.2.3.GA です。
- URL（インストール先のコンピュータの IP アドレスまたはホスト名）。
- JBoss が使用するポート。
- JBoss が安全な通信のために使用するポート（HTTPS）。
- ネーミング ポート番号。

通信パスワード

（プライマリ エンタープライズ管理サーバのみ） CA Access Control エンタープライズ管理サーバのコンポーネント間通信に使用されるパスワードを定義します。

注: CA Access Control エンタープライズ管理 は通信パスワードを使用して Message Queue キーストアおよび管理者アカウントを管理し、CA Access Control エンタープライズ管理 とエンドポイントの間の通信を処理し、Java 接続サーバを管理します。

データベース情報

RDBMS への接続の詳細を定義します。

- **データベース タイプ** - サポートされている RDBMS を指定します。
- **ホスト名** - RDBMS をインストールしているホストの名前を定義します。
- **ポート番号** - 指定した RDBMS によって使用されるポートを定義します。インストール プログラムでは、RDBMS のデフォルト ポートが指定されます。
- **サービス名** - (Oracle) システムの RDBMS を識別する名前を定義します。たとえば、Oracle Database 10g の場合はデフォルトで *orcl* になります。
- **データベース名** - （MS SQL）作成したデータベースの名前を定義します。

- **ユーザ名** - データベースを準備した際に作成したユーザの名前を定義します。

  注: このユーザには、データベースを準備した際に適切なデータベース許可が与えられています。

- **パスワード** - データベースを準備した際に作成した RDBMS パスワードを定義します。

インストール プログラムは、続行する前にデータベースへの接続を確認します。

ユーザ ストア タイプ

CA Access Control エンタープライズ管理 が使用するユーザ ストア タイプ を定義します。以下の*いずれか*を選択します。

- **組み込みユーザ ストア** -- CA Access Control エンタープライズ管理 は RDBMS にユーザ情報を格納します。
- **Active Directory --** 次の 画面に接続情報の詳細を指定します。
- **他のユーザ ストア** -- CA Access Control エンタープライズ管理 のインストール完了後に、ユーザ ストアの構成情報を指定します。

注: UNAB にログイン許可ポリシーをデプロイするには、ユーザ ストアとして[Active Directory]または[他のユーザ スト]を選択する必要があります。ユーザ ストアとして[Active Directory]または[他のユーザ スト]を選択した場合、CA Access Control エンタープライズ管理 でユーザおよびグループを作成または削除できません。UNAB および Active Directory の制限事項の詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

Active Directory の設定

Active Directory ユーザ ストアの設定を定義します。

- **ホスト** -- Active Directory のドメイン コントローラ ホスト名を定義します。
- **ポート** -- Active Directory に対する LDAP クエリにデフォルトで使用されるポートを定義します(たとえば 389)。
- **検索ルート** - 検索ルートを、「ou=DomainName, DC=com」のように定義します。

  注: [検索ルート]には、ディレクトリツリーにおいて、[ユーザ DN]および[システムユーザ]として指定したユーザの識別名(DN)よりも高いノードを少なくとも 1 つ設定します。 そうしないと、エンタープライズ管理がタブをまったく表示せずに起動する場合があります。

- **ユーザ DN** -- CA Access Control エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウント名を定義します。例: CN=Administrator、cn=Users、DC=DomainName、DC=Com

  注: このユーザは、Active Directory に対する LDAP クエリを発行します。このパラメータ用の読み取り専用権限を持ったユーザを定義してもかまいません。ただし、読み取り専用権限を持ったユーザを定義する場合、CA Access Control エンタープライズ管理 内のユーザに管理ロールまたは特権アクセス ロールを割り当てることはできません。代わりに、Active Directory グループを指すように各ロールのメンバ ポリシーを変更します。

- **パスワード** -- CA Access Control エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウントのパスワードを定義します。

インストール プログラムは、続行前に Active Directory への接続を確認します。

注: ディレクトリ照会ユーティリティ DSQUERY を使用して、ユーザの識別名 (ユーザ DN) を検出することができます。このクエリは、Active Directory サーバ上で実行する必要があります。以下に例を示します。

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

システム ユーザ

(Active Directory のみ) CA Access Control エンタープライズ管理 で System Manager 管理ロールが割り当てられている Active Directory ユーザの DN を定義します。

例: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

注: デフォルトでは、System Manager 管理ロールを持ったユーザは、CA Access Control エンタープライズ管理 内のタスクをすべて実行、作成、および管理できます。システム マネージャ管理ロールの詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

管理者パスワード

（組み込みユーザ ストアのみ）CA Access Control エンタープライズ管理 管理者である superadmin のパスワードを定義します。インストール完了時に CA Access Control エンタープライズ管理 にログインできるように、パスワードをメモしておきます。

注: この手順で、組み込みユーザ ストアの superadmin ユーザを作成します。superadmin ユーザには、CA Access Control エンタープライズ管理 のシステム マネージャ管理ロールが割り当てられます。CA Access Control エンタープライズ管理 への初回ログイン時には、superadmin としてログインします。システム マネージャ管理ロールの詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

CA Access Control エンタープライズ管理 は、ウィザードの完了後にインストールされます。CA Access Control エンタープライズ管理 インストールを完了するために、コンピュータを再起動します。

6. [はい]を選択し、システムを再起動し、[完了]をクリックします。

これで、ご自分の環境に合わせて CA Access Control エンタープライズ管理 を設定できるようになりました。

Product Explorer を使用したインストール

CA Access Control Product Explorer では、CA Access Control の異なるアーキテクチャでのインストールと、ランタイム SDK のインストールが可能です。Product Explorer は、グラフィカル インターフェースを使用して CA Access Control のアンインストールを実行し、ユーザに対し、対話的にフィードバックを行います。

以下の手順に従います。

1. Windows の管理者権限を持つユーザ（すなわち、Windows Administrator または Windows Administrators グループのメンバ）として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA Access Control Endpoint Components for Windows DVD を光ディスクドライブに挿入します。

   autorun が有効になっている場合は、Product Explorer が自動的に表示されます。autorun が有効になっていない場合は、光ディスクドライブのディレクトリに移動し、PRODUCTEXPLORERX86.EXE ファイルをダブルクリックします。

4. Product Explorer のメイン メニューから、Components フォルダを展開し、CA Access Control for Windows（*my_architecture*）を選択し、［インストール］をクリックします。

   インストール先のコンピュータのアーキテクチャに適合するインストール オプションを選択する必要があります（32 ビット、64 ビット x 64、または 64 ビット Itanium）。

   ［セットアップ言語の選択］ウィンドウが表示されます。

5. CA Access Control をインストールする言語を選択し、［OK］をクリックします。

   CA Access Control インストール プログラムがローディングを開始し、しばらくして、概要画面が表示されます。

   注：CA Access Control の既存のインストールがインストール プログラムによって検出された場合、CA Access Control のアップグレードを実行するかどうかを選択するように促されます。

6. インストール画面の指示に従います。

   インストール中、ユーザは情報を入力するよう求められます。CA Access Control のインストール時にユーザが必要となる情報については、インストールワークシートを参照してください。

   インストール プログラムによって CA Access Control がインストールされます。インストールが完了したら、Windows をすぐに再起動するか、または後で再起動するかを選択します。

7. ［はい、今すぐコンピュータを再起動します］を選択して［OK］をクリックします。

   システムの再起動後に、CA Access Control が正しくインストールされたことを確認できます。

   注：コンピュータを後で再起動するように選択した場合、コンピュータが再起動されるまでインストールが完了しないことを示す警告メッセージが表示されます。ログオン インターセプトなどの CA Access Control の一部の機能は、コンピュータを再起動するまで機能しません。

install_base スクリプトを使用したインストール

サポートされている OS には install_base スクリプトを使用して CA Access Control をインストールすることができます。これは対話形式のスクリプトですが、サイレント モードでの実行も可能です。

注: install_base スクリプトを実行する前に、インストールする機能を必ず決定し、install_base コマンドを確認します。これにより、決定した機能のインストールを開始する方法を把握することができます。また、install_base スクリプトのしくみを最初に学習することもできます。

以下の手順に従います。

1. CA Access Control がすでにインストールされていて実行中である場合は、管理者としてログインし、以下のコマンドを入力して、CA Access Control を停止します。

   ```
   ACInstallDir/bin/secons -sk
   ACInstallDir/bin/SEOS_load -u
   ```

2. *root* ユーザとしてログインします。

   CA Access Control をインストールするには、ルート権限が必要です。

3. 光ディスクドライブに CA Access Control Endpoint Components for UNIX DVD をセットします。

   重要: 光ディスクドライブから HP にインストールする場合は、DVD からファイル名が正しく読み込まれていることを確認する必要があります。ファイル名が強制的にすべて大文字の短い名前に変更されるのを防ぐために、*pfs_mountd &* および *pfsd &* コマンドを入力し、pfs_mountd、pfsd.rpc、pfs_mountd.rpc、および pfsd の 4 つのデーモンが呼び出されることを確認します。詳細については、該当する pfs* デーモンおよびコマンドのマニュアル ページを参照してください。

4. エンド ユーザ使用許諾契約の内容を読みます。

   install_base スクリプトを実行するには、エンド ユーザ使用許諾契約に同意する必要があります。エンド ユーザ使用許諾契約を読んだ後、インストールを続行するには、そのファイルの最後に記述されたコマンドを入力します。ライセンス ファイルの名前と場所を取得するには、install_base -h を実行します。

5. install_base スクリプトを実行します。

   install_base スクリプトが開始されると、選択内容に基づいて、インストールに関して該当する質問に答えるよう指示されます。

   注: インストール スクリプトによって適切な圧縮 tar ファイルが検出されるため、ご使用のプラットフォームに対する tar ファイル名の入力は省略できます。

   これで CA Access Control のインストールは完了しましたが、CA Access Control はまだ実行されていません。

例: サイレント インストールを使用した CA Access Control r12.6 SP1 for UNIX へのアップグレード

この例は、既存の CA Access Control r8.0 SP1 エンドポイントを CA Access Control r12.6 SP1 for UNIX にアップグレードする方法を示しています。この例では、エンドポイントへの新機能のインストールを可能にするパラメータ ファイルを使用して、CA Access Control をインストールします。

1. install_base スクリプト コマンドを確認します。

   この install_base スクリプトは、サイレント モードで CA Access Control r12.6 SP1 をインストールする場合に使用します。詳細については、「*実装ガイド*」を参照してください。

2. このパラメータ ファイルは、CA Access Control Endpoint Components for UNIX メディアにある tar 圧縮ファイルから抽出します。このファイルは以下のディレクトリにあります。

   ```
   ¥Unix¥Access-Control¥
   ```

3. install_base スクリプトを使用して、CA Access Control をインストールします。

   -autocfg コマンドを使用し、カスタマイズしたパラメータ ファイルを使用するように指定します。

   CA Access Control r12.6 SP1 は、指定したオプションでインストールされます。

例: パラメータ ファイル

パラメータ ファイルによって、エンドポイントに追加するソフトウェア コンポーネントを選択できます。ネイティブ インストール モードで CA Access Control をインストールする場合、インストールを開始する前に、ファイルをカスタマイズします。対話モードで CA Access Control をインストールする場合、インストール パラメータをファイルに抽出してから、インストール パラメータをカスタマイズできます。

以下は、パラメータ ファイルの一部分です。

```
#  Specifies whether you want to configure PUPM Agent
#  Values: "yes", "no"
#  Default: "no"
INSTALL_PUPM="yes"

# Specifies whether  enables KBL audit records management
# Values: yes, no
# Default: no
ENABLE_KBL=yes
```

この例では、PUPM 統合をインストールするように指定しました（INSTALL_PUPM=yes）。また、エンドポイント上でキーボード ロギングを有効にしました（ENABLE_KBL=yes）。

例: クライアントおよびサーバ パッケージおよびデフォルト機能をインストールする

以下のコマンドでは、対話形式の install_base スクリプトを開始し、すべてのデフォルト CA Access Control 機能でのクライアント パッケージおよびサーバ パッケージをインストールする方法を説明します。インストール中には、CA Access Control のクライアントおよびサーバ パッケージのインストールに関する質問に答えるように求められます。

```
/dvdrom/Unix/Access-Control/install_base
```

注: インストールするパッケージを指定していないので、install_base コマンドではクライアント パッケージとサーバ パッケージの両方がインストールされます。

例: STOP を有効にした状態でクライアント パッケージをカスタム ディレクトリにインストールする

以下のコマンドでは、対話形式の install_base スクリプトを開始してクライアント パッケージを /opt/CA/AC ディレクトリにインストールし、スタック オーバフロー防止機能オプションを有効にする方法を示します。

```
/dvdrom/Unix/Access-Control/install_base -client -stop  -d /opt/CA/AC
```

CA Access Control r12.0 SP1 からのアップグレード

このセクションでは、既存の CA Access Control r12.0 SP1 展開をアップグレードするために CA Access Control、またはシステム管理者が従う手順の詳細について説明します。この章のアップグレード処理では、管理者が CA Access Control r12.0 SP1 コンポーネントを別々のコンピュータ上にインストールしていると仮定します。

たとえば、エンタープライズ管理サーバは 1 台のコンピュータにインストールされており、DMS、DH、およびレポート サーバも個別のコンピュータにインストールされています。

この章で説明するアップグレード処理は、各コンポーネントを別々にアップグレードする方法です。

注: アップグレードは、CA Access Control エンタープライズ管理 r12.0 SP1 からのみ行うことができます。

はじめに

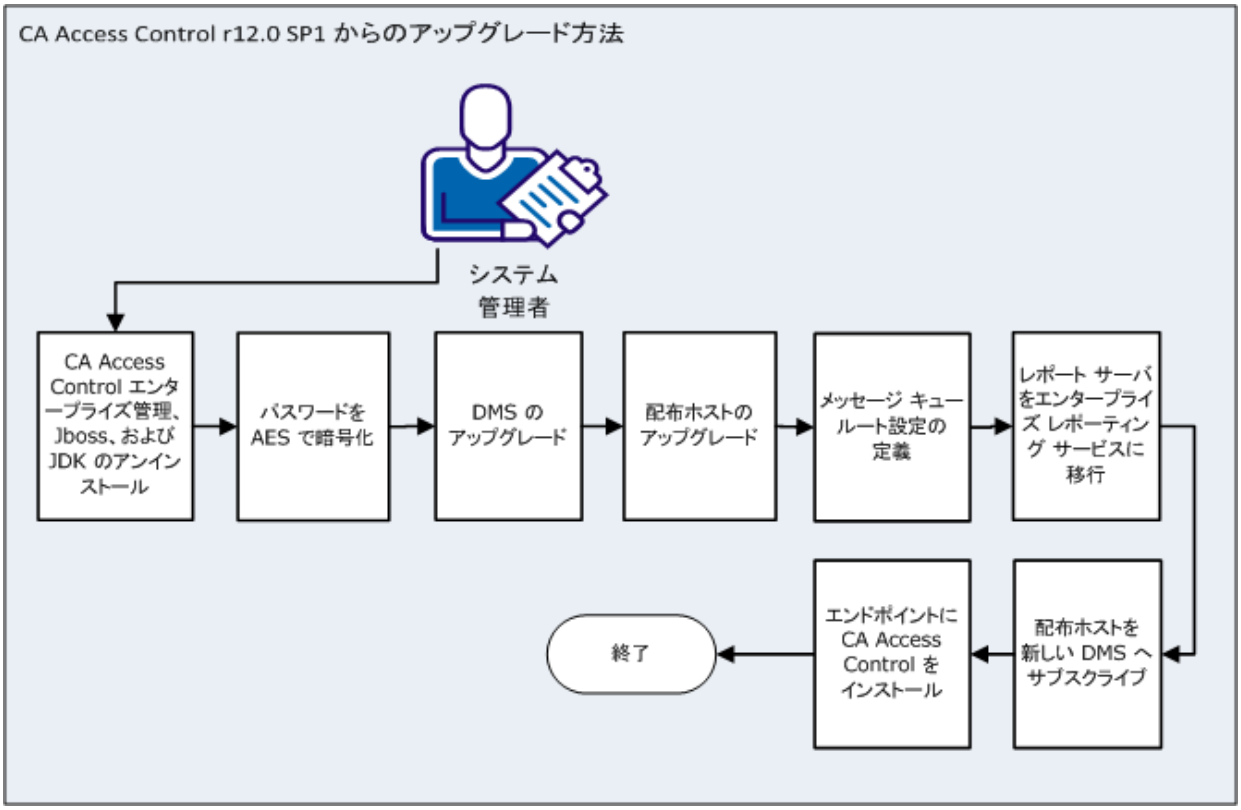
現在の CA Access Control インストールのアップグレード プロセスを開始する前に、以下の点について考慮する必要があります。

- アップグレード プロセスを開始する前に、CA Access Control コンポーネントをバックアップすることをお勧めします。アップグレード プロセスを開始する前に、すべてのデータベースを含め、システム ファイルをバックアップすることをお勧めします。
- CA Access Control エンタープライズ管理 がインストールするコンポーネントは、エンタープライズ管理サーバ、CA Access Control、配布サーバ、エンタープライズ レポート サービスです。
- アップグレード後は、以前の DMS は使用できなくなります。サーバを開始する前に、エンタープライズ管理サーバ、DMS、および DH をアップグレードする必要があります。
- エンタープライズ管理サーバをインストールするときに埋め込まれたユーザ ストアを使用することを指定します。

  重要: 組み込みユーザ ストアへのエンタープライズ管理サーバのインストール時に、UNAB レポートおよびログイン許可ポリシーを使用することはできません。UNAB レポートを生成し、ログイン許可ポリシーを設定するには、Active Directory をインストールする必要があります。

r12.0 SP1 からのアップグレード

以下の手順では、既存の CA Access Control r12.0 SP1 展開のアップグレード方法について説明します。



1. エンタープライズ管理サーバをアップグレードします。
    a. CA Access Control エンタープライズ管理 r12.0 SP1、JBoss および JDK をアンインストールします。
    b. 前提条件インストーラを使用して、JDK 1.5.0 および JBoss 4.2.3 をインストールします (P. 36)。
    c. CA Access Control エンタープライズ管理 をインストールします。
2. AES の既存のパスワードを暗号化します (P. 48)。

   CA Access Control エンタープライズ管理 r12.5 SP1 では、暗号化方式は RC2 から AES に変更されました。
3. DMS コンピュータをアップグレードします (P. 50)。

   注: DMS が CA Access Control エンタープライズ管理 と同じコンピュータにインストールされている場合、この手順を完了する必要はありません。
4. 配布ホスト(DH)をアップグレードします (P. 54)。

   注: 組織内のすべての DH をアップグレードします。DH がエンタープライズ管理サーバと同じコンピュータにインストールされている場合、この手順を完了する必要はありません。
5. メッセージ キュー(MQ)ルート設定を定義します (P. 56)。
6. レポート サーバをエンタープライズ レポーティング サービスへ移行します (P. 69)。
7. DH を新しい DMS へサブスクライブします (P. 70)。
8. (オプション) CA Access Control エンドポイントをアップグレードします (P. 70)。

エンタープライズ管理サーバのアップグレード

ここでは、エンタープライズ管理サーバをアップグレードするための手順、およびインストール後に実行する必要のある手順を説明します。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 r12.0 SP1 をアンインストールします。

   注: CA Access Control エンタープライズ管理 r12.0 SP1 のアンインストールの詳細については、このリリースの「*実装ガイド*」をご覧ください。
2. 既存の JDK および JBoss をアンインストールします。

3. 必須ソフトウェアをインストールします (P. 36)。
4. CA Access Control エンタープライズ管理 をインストールします (P. 21)。

   CA Access Control エンタープライズ管理 によって、以下もインストールされます。

   - エンタープライズ管理サーバ
   - CA Access Control
   - エンタープライズ レポーティング サービス。
   - 配布サーバ

   重要: CA Access Control エンタープライズ管理 のインストール時に、組み込みユーザ ストアを使用するように指定する必要があります。
5. レポーティング データベース スキーマが CA Access Control エンタープライズ管理 上のスキーマと同じでない場合、指定されたスクリプトを実行して、データベース スキーマを更新します。
6. (オプション) JBoss 用の安全な通信設定を行います (P. 43)。
7. CA Access Control エンタープライズ管理 上の DMS および DH を無効にします。以下のコマンドを実行します。

   ```
   dmsmgr -remove -auto
   ```

   重要: DMS が CA Access Control エンタープライズ管理 とは別のコンピュータにインストールされている場合のみ、この手順を完了します。

   注: アップグレード後は、既存の DMS は使用できなくなります。新しいエンタープライズ管理サーバをインストールした後に DMS をアップグレードしてください。dmsmgr ユーティリティの詳細については、「リファレンス ガイド」を参照してください。

これで、新しいエンタープライズ管理サーバがインストールされました。CA Access Control エンタープライズ管理 を開始する前に、DMS および配布ホストをアップグレードする必要があります。

必須ソフトウェア インストール ユーティリティの実行

Windows で有効

CA Access Control エンタープライズ管理 では、Java Development Kit (JDK) および JBoss アプリケーション サーバが実行されている必要があります。この事前インストールが必要なサードパーティ ソフトウェアの正しいバージョンは、CA Access Control Premium Edition Third Party Components DVD で提供されます。また、この DVD には、以下のような、事前インストール ソフトウェアをインストールするユーティリティもあります。

- JDK および JBoss を設定して、CA Access Control エンタープライズ管理 に適切な設定でインストールするようにします。
- JBoss をサービスとしてインストールします。
- あらかじめ設定された事前インストール ソフトウェアの設定で、CA Access Control エンタープライズ管理 のインストールを開始します。

これらのソフトウェアがすでにインストールされていれば、この手順をスキップできます。インストールされていない場合は、提供されているユーティリティを使用して、この手順に従ってインストールすることをお勧めします。

すでに JBoss がインストールされている場合、オープン ポートの問題を解決するために CA Access Control エンタープライズ管理 をインストールする前に、JBoss を一度だけ実行することをお勧めします。

以下の手順に従います。

1. 光ディスクドライブに CA Access Control Premium Edition Third-Party Components DVD for Windows を挿入します。
2. 光ディスクドライブ 上の PrereqInstaller ディレクトリに移動し、**install_PRK.exe** を実行します。

   InstallAnywhere ウィザードが開きます。
3. 必要に応じてウィザードを完了します。

   注: 追加の JBoss ポート番号を設定するには、[JBoss ポート設定]ページの[詳細設定]を選択します。 ユーザがビジーな JBoss ポートを指定した場合、インストーラによって異なるポート番号の指定を促すメッセージが表示されます。

4. サマリ レポートで詳細を確認し、[インストール]をクリックします。

   事前インストール ソフトウェアがインストールされます。この処理には時間がかかる場合があります。

5. 以下の*いずれか*の操作を実行します。

   - 必須のソフトウェアをインストールした後、CA Access Control エンタープライズ管理 のインストールを開始する場合は、プロンプトが表示されたら光ディスクドライブにご使用のオペレーティング システム用の CA Access Control Premium Edition Server Components DVD を挿入し、[完了]を選択します。Product Explorer ウィンドウが表示されたら、閉じます。
   - 高可用性または障害復旧のために追加のエンタープライズ管理サーバをインストールする場合は、CA Access Control エンタープライズ管理 をインストールするカスタム FIPS キーを指定します。メッセージが表示されたら[完了]をクリックし、続いて[完了]をクリックして表示されたダイアログ ボックスを閉じます。
   - 必須のソフトウェアをインストールした後に CA Access Control エンタープライズ管理 のインストールを開始しない場合は、プロンプトが表示されたら[完了]をクリックし、[終了]をクリックして表示されたダイアログ ボックスを閉じます。

     必須のソフトウェアのインストール プロセスが完了しました。

Windows での CA Access Control エンタープライズ管理 のインストール

CA Access Control エンタープライズ管理 をインストールすると、エンタープライズ管理のサーバ コンポーネントがすべてインストールされます。CA Access Control エンタープライズ管理 をインストールする前に、エンタープライズ管理サーバを準備します。

前提条件キットを使用して、CA Access Control エンタープライズ管理 のインストールを開始することをお勧めします。このインストーラでは、前提条件のサードパーティ ソフトウェアがインストールされてから、CA Access Control エンタープライズ管理 のインストールが開始されます。

注: ネットワーク インストールによって CA Access Control エンタープライズ管理 をインストールすることはできません。CA Access Control Premium Edition Server Components DVD の Disk 1 ディレクトリの内容をすべてインストール ディレクトリにコピーするか、代わりにドライブを DVD にマッピングします。

Windows での CA Access Control エンタープライズ管理 のインストール方法

1. JBoss アプリケーション サーバが実行中の場合は、これを終了させます。
2. CA Access Control がすでにインストールされているコンピュータに CA Access Control エンタープライズ管理 をインストールする場合は、CA Access Control サービスを停止します。
3. 光ディスクドライブに CA Access Control Premium Edition Server Components DVD for Windows を挿入します。
4. Product Explorer で[Components]フォルダを展開し、CA Access Control エンタープライズ管理 を選択し、[インストール]をクリックします。

   InstallAnywhere インストール プログラムが起動します。
5. (オプション) カスタム FIPS キーのフルパス名を指定して、インストール中に使用します。

   a. コマンド プロンプト ウィンドウを開き、CA Access Control Premium Edition Server Components DVD for Windows の上の CA Access Control エンタープライズ管理 インストール実行可能ファイルに移動します。このファイルは以下の場所にあります。

   ```
   ¥EnterpriseMgmt¥Disk1¥InstData¥NoVM
   ```

   b. 以下の引数を指定して CA Access Control エンタープライズ管理 インストール実行可能ファイルを実行します。

   ```
   -DFIPS_KEY=full_pathname_to_FIPS_key
   ```

   たとえば、C:¥tmp¥FIPS.key にあるカスタム FIPS キーを使ってインストールするには、以下のように設定します。

   ```
   E:¥EnterpriseMgmt¥Disk1¥InstData¥NoVM¥install_EntM_r125.exe
   -DFIPS_KEY=C:¥tmp¥FIPSkey.dat
   ```

   重要: CA Access Control エンタープライズ管理 をインストールしてハイ アベイラビリティを実現する場合、プライマリおよびセカンダリのエンタープライズ管理サーバ上に同じ FIPS キーを指定します。CA Access Control エンタープライズ管理 をインストールして FIPS サポートによるハイ アベイラビリティを実現する場合、カスタム FIPS キーを指定します。

   InstallAnywhere インストール プログラムが起動します。

6. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

インストール フォルダの選択

インストール フォルダの完全パスを定義します。

デフォルト: ¥ProgramFiles¥CA¥AccessControlServer¥

注: 64 ビットのオペレーティング システムでのデフォルトのインストール フォルダは、以下のとおりです。

```
¥Program Files(x86)¥CA¥AccessControlServer¥
```

Java Development Kit（JDK）

既存の JDK の場所を定義します。

注: CA Access Control Premium Edition Third Party Component DVD を使用して必須ソフトウェアをインストールした直後に、CA Access Control エンタープライズ管理 のインストールを開始した場合、このウィザードは表示されません。インストール ユーティリティは、必須のソフトウェア インストール プロセスの際に指定した値を基に、このページのインストール設定を行います。

JBoss アプリケーション サーバ情報

アプリケーションをインストールする JBoss インスタンスを定義します。

これを行うには、以下を定義します。

- JBoss フォルダ（JBoss をインストールしているトップ ディレクトリ）。

  たとえば、Windows の場合は C:¥jboss-4.2.3.GA、Solaris の場合は /opt/jboss-4.2.3.GA です。
- URL（インストール先のコンピュータの IP アドレスまたはホスト名）。
- JBoss が使用するポート。
- JBoss が安全な通信のために使用するポート（HTTPS）。
- ネーミング ポート番号。

注: CA Access Control Premium Edition Third Party Component DVD を使用して必須ソフトウェアをインストールした直後に、CA Access Control エンタープライズ管理 のインストールを開始した場合、このウィザードは表示されません。インストール ユーティリティは、必須のソフトウェア インストール プロセスの際に指定した値を基に、このページのインストール設定を行います。

通信パスワード

（プライマリ エンタープライズ管理サーバのみ）CA Access Control エンタープライズ管理サーバのコンポーネント間通信に使用されるパスワードを定義します。

注: CA Access Control エンタープライズ管理 は通信パスワードを使用して Message Queue キーストアおよび管理者アカウントを管理し、CA Access Control エンタープライズ管理 とエンドポイントの間の通信を処理し、Java 接続サーバを管理します。

データベース情報

RDBMS への接続の詳細を定義します。

- **データベース タイプ** - サポートされている RDBMS を指定します。
- **ホスト名** - RDBMS をインストールしているホストの名前を定義します。
- **ポート番号** - 指定した RDBMS によって使用されるポートを定義します。インストール プログラムでは、RDBMS のデフォルト ポートが指定されます。
- **サービス名** - (Oracle) システムの RDBMS を識別する名前を定義します。たとえば、Oracle Database 10g の場合はデフォルトで *orcl* になります。
- **データベース名** - （MS SQL）作成したデータベースの名前を定義します。
- **ユーザ名** - データベースを準備した際に作成したユーザの名前を定義します。

  注: このユーザには、データベースを準備した際に適切なデータベース許可が与えられています。
- **パスワード** - データベースを準備した際に作成した RDBMS パスワードを定義します。

インストール プログラムは、続行する前にデータベースへの接続を確認します。

ユーザ ストア タイプ

CA Access Control エンタープライズ管理 が使用するユーザ ストア タイプ を定義します。以下の*いずれか*を選択します。

- **組み込みユーザ ストア** -- CA Access Control エンタープライズ管理 は RDBMS にユーザ情報を格納します。
- **Active Directory --** 次の 画面に接続情報の詳細を指定します。
- **他のユーザ ストア** -- CA Access Control エンタープライズ管理 のインストール完了後に、ユーザ ストアの構成情報を指定します。

注: UNAB にログイン許可ポリシーをデプロイするには、ユーザ ストアとして[Active Directory]または[他のユーザ スト]を選択する必要があります。ユーザ ストアとして[Active Directory]または[他のユーザ スト]を選択した場合、CA Access Control エンタープライズ管理 でユーザおよびグループを作成または削除できません。UNAB および Active Directory の制限事項の詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

Active Directory の設定

Active Directory ユーザ ストアの設定を定義します。

- **ホスト** -- Active Directory のドメイン コントローラ ホスト名を定義します。
- **ポート** -- Active Directory に対する LDAP クエリにデフォルトで使用されるポートを定義します(たとえば 389)。
- **検索ルート** - 検索ルートを、「ou=DomainName, DC=com」のように定義します。

  注: [検索ルート]には、ディレクトリツリーにおいて、[ユーザ DN]および[システムユーザ]として指定したユーザの識別名(DN)よりも高いノードを少なくとも 1 つ設定します。 そうしないと、エンタープライズ管理がタブをまったく表示せずに起動する場合があります。

- **ユーザ DN** -- CA Access Control エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウント名を定義します。例: CN=Administrator、cn=Users、DC=DomainName、DC=Com

  注: このユーザは、Active Directory に対する LDAP クエリを発行します。このパラメータ用の読み取り専用権限を持ったユーザを定義してもかまいません。ただし、読み取り専用権限を持ったユーザを定義する場合、CA Access Control エンタープライズ管理 内のユーザに管理ロールまたは特権アクセス ロールを割り当てることはできません。代わりに、Active Directory グループを指すように各ロールのメンバ ポリシーを変更します。

- **パスワード** -- CA Access Control エンタープライズ管理 を管理するために使用される Active Directory ユーザ アカウントのパスワードを定義します。

インストール プログラムは、続行前に Active Directory への接続を確認します。

注: ディレクトリ照会ユーティリティ DSQUERY を使用して、ユーザの識別名 (ユーザ DN) を検出することができます。このクエリは、Active Directory サーバ上で実行する必要があります。以下に例を示します。

```
dsquery user -name administrator
"CN=Administrator,CN=Users,DC=lab.DC=demo"
```

システム ユーザ

(Active Directory のみ) CA Access Control エンタープライズ管理 で System Manager 管理ロールが割り当てられている Active Directory ユーザの DN を定義します。

例: CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com

注: デフォルトでは、System Manager 管理ロールを持ったユーザは、CA Access Control エンタープライズ管理 内のタスクをすべて実行、作成、および管理できます。システム マネージャ管理ロールの詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

管理者パスワード

（組み込みユーザ ストアのみ）CA Access Control エンタープライズ管理 管理者である superadmin のパスワードを定義します。インストール完了時に CA Access Control エンタープライズ管理 にログインできるように、パスワードをメモしておきます。

注: この手順で、組み込みユーザ ストアの superadmin ユーザを作成します。superadmin ユーザには、CA Access Control エンタープライズ管理 のシステム マネージャ管理ロールが割り当てられます。CA Access Control エンタープライズ管理 への初回ログイン時には、superadmin としてログインします。システム マネージャ管理ロールの詳細については、「*エンタープライズ管理ガイド*」をご覧ください。

CA Access Control エンタープライズ管理 は、ウィザードの完了後にインストールされます。CA Access Control エンタープライズ管理 インストールを完了するために、コンピュータを再起動します。

7. [はい]を選択し、システムを再起動し、[完了]をクリックします。

   コンピュータが再起動します。これで、ご自分の環境に合わせて CA Access Control エンタープライズ管理 を設定できるようになりました。

JBoss の SSL 通信

デフォルトでは、JBoss のインストールで SSL はサポートされません。これは、CA Access Control エンタープライズ管理 と JBoss の間の一部の通信が暗号化されないことを意味します。安全に通信を行うために、SSL を使用するように JBoss を設定できます。

注: JBoss 用に SSL を設定する方法の詳細については、JBoss 製品のドキュメントを参照してください。

例: Windows で SSL 通信用に JBoss を設定する

この例では、安全に通信を行うために SSL を使用する JBoss アプリケーション サーバを設定する方法を示します。

重要: この手順では、JBoss バージョン 4.2.3 および JDK バージョン 1.5.0 を使用して、安全な通信を行うために SSL の使用するように JBoss アプリケーション サーバを設定する方法を説明します。

次の手順に従ってください:

1. JBoss が実行されている場合は、停止します。
2. コマンドプロンプト ウィンドウを開き、以下のディレクトリに移動します。

   JBoss_HOME¥server¥default¥deploy¥IdentityMinder.ear¥custom¥ppm¥truststore

3. 以下のコマンドを入力して、デフォルトの ssl.keystore パスワードを変更します。

   ```
   keytool -storepasswd -new password -keystore ssl.keystore -storepass secret
   ```

   -storepasswd

   キーストアのパスワード変更を指定します。パスワードは 6 文字以上である必要があります。

   -keystore

   証明書を追加するキーストアの名前を指定します。

   -keystore

   キーストアの名前を指定します。

   -storepass

   キーストアを保護するために使用するパスワードを定義します。

4. 以下のコマンドを入力して、エンタープライズ管理サーバ用のキーを作成します。

   ```
   keytool -genkey -alias entm -keystore ssl.keystore -keyalg RSA
   ```

   -genkey

   コマンドで鍵ペア（公開鍵と秘密鍵）が生成される必要があることを指定します。

   -alias

   キーストアへのエントリの追加で使用するエイリアスを定義します。

   -keyalg

   鍵ペアの生成に使用するアルゴリズムを指定します。

   keytool ユーティリティが起動します。

5. 「*secret*」というパスワードを入力します。

6. 必要に応じてプロンプトを完了し、Enter キーを押して、入力したパラメータを確認します。

   証明書がキーストアに追加されます。

   注: キーストアおよびキーの別名には、同一のパスワードを使用する必要があります。

7. 以下のコマンドを入力して、キーストア パスワードをファイルに暗号化します。

   ```
   java -cp JBoss_HOME/server/default/lib/jbossx.jar
   org.jboss.security.plugins.FilePassword welcometojboss 13 passowrd
   <kestore_password> keystore.password
   ```

   注: Salt と IterationCount は暗号化されたパスワードの強度を定義する変数です。この例では、welcometojboss は Salt で、13 は IterationCount です。

8. 以下のディレクトリで server.xml という名のファイルを検索し、編集可能な形式でそれを開きます。

   ```
   JBossInstallDir¥server¥default¥deploy¥jboss-web.deployer
   ```

9. 以下のセクションで <Connector Port> タグを探します。

   ```
   <!-- Define a SSL HTTP/1.1 Connector on port 8443
           This connector uses the JSSE configuration, when using APR, the
           connector should be using the OpenSSL style configuration
           described in the APR documentation -->
       <!--
       <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
                  maxThreads="150" scheme="https" secure="true"
                  clientAuth="false" sslProtocol="TLS" />
   ```

   注: コネクタ ポート番号は、必須ソフトウェアまたは CA Access Control エンタープライズ管理 のインストール時に指定した JBoss HTTPS ポート番号に対応します。

10. "<!--" above the <Connector port> タグのコメントを解除します。

    これで、このタグを編集できるようになりました。

11. <Connector port> タグへ以下のプロパティを追加します。

    ```
    securityDomain="java:/jaas/encrypt-keystore-password"
    SSLImplementation="org.jboss.net.ssl.JBossImplementation"
    ```

12. server.xml ファイルを保存して閉じます。
13. 以下のディレクトリに移動して、jboss-service.xml ファイルを見つけます。

    ```
    JBOss_HOME/server/default/deploy/jboss-web.deployer/META-INF
    ```

14. <server> および </server> タグの間に以下の mbean を追加します。

    ```
    <mbean code="org.jboss.security.plugins.JaasSecurityDomain"
    name="jboss.security:service=PBESecurityDomain">
          <constructor>
             <arg type="java.lang.String" value="encrypt-keystore-password"></arg>
          </constructor>
          <attribute
    name="KeyStoreURL">${jboss.server.home.dir}/deploy/IdentityMinder.ear/custom/
    ppm/truststore/ssl.keystore</attribute>
          <attribute
    name="KeyStorePass">{CLASS}org.jboss.security.plugins.FilePassword:${jboss.se
    rver.home.dir}/deploy/IdentityMinder.ear/custom/ppm/truststore/keystore.passw
    ord</attribute>
    <attribute name="Salt">welcometojboss</attribute>
    <attribute name="IterationCount">13</attribute>
     </mbean>
    ```

    注: 上の例では、welcometojboss は Salt で、13 は IterationCount です。

15. jboss-service.xml を保存して閉じます。
16. CA Access Control エンタープライズ管理 を起動して開きます。

    注: この手順を終えた後、JBoss および CA Access Control エンタープライズ管理 への接続には、SSL モードまたは SSL 以外のモードのいずれかを選択できます。

AES 暗号化方式でのパスワードの暗号化

CA Access Control r12.0 SP1 では、パスワードは RC2 暗号化方式を使用して暗号化されました。CA Access Control r12.5 SP1 では、パスワード暗号化方式が AES に変更されました。そのため、RC2 暗号化方式を使用して暗号化されたパスワードは CA Access Control の新しいバージョンでは機能しません。この問題を解決するには、CA Access Control r12.0SP1 からアップグレードした後、既存のパスワードを AES で暗号化します。

以下の手順に従います。

1. CA Access Control サービスをすべて停止します。
2. 以下の手順を実行します。
   a. 読み書きアクセス権を持つユーザとして、エンタープライズ管理サーバのデータベースに接続します。
   b. 以下のクエリを実行し、ユーザ ストアへ接続するために CA Access Control エンタープライズ管理 で使用されるパスワードを削除します。

      ```
      update IM_DIR_CONNECTION set password=null where
      connection_name='java:/userstore';
      ```
3. pwdtools ユーティリティを使用して、データベース内のすべてのパスワードを暗号化します。

   tlbusers テーブル内の各エントリのパスワードを、生成した暗号化されたパスワードに置き換えます。
4. 接続テーブルから DMS 設定を削除します。以下のクエリを実行します。

   ```
   DELETE FROM connection WHERE connection_name='con1';
   ```
5. すべての CA Access Control サービスを開始します。
6. CA Access Control エンタープライズ管理 で DMS 接続設定を設定します。

   注: DMS 接続設定の詳細については、オンライン ヘルプを参照してください。

例: pwdtools ユーティリティを使用したパスワードの暗号化

この例は、pwdtools ユーティリティを使用して、AES 暗号化モードでユーザのパスワードを暗号化する方法、および暗号化されたパスワードをエンタープライズ管理サーバ データベースに設定する方法を示しています。

1. pwdtool.bat を編集できる形で開きます。このファイルは以下のディレクトリにあります(*ACServerInstallDir* はエンタープライズ管理サーバがインストールされているディレクトリです)。

   ACServerInstallDir/IAM_Suite/Access_Control/tools/PasswordTool/

2. 「::SET JAVA_HOME=<enter valid java home here>」トークンに JAVA_HOME パスを入力します。以下に例を示します。

   ```
   SET JAVA_HOME=C:¥jdk1.5.0
   ```

3. コマンド ライン ウィンドウで、以下のコマンドを入力します。*password* はクリア テキスト パスワードで、*JBOSS_Home* は、JBoss がインストールされているディレクトリです。

   ```
   pwdtools -FIPS -p <"password"> -k
   JBOSS_HOME¥server¥default¥deploy¥IdentityMinder.ear¥config¥com¥
   netegrity¥config¥keys¥FIPSkey.dat
   ```

   暗号化されたパスワードが表示されます。パスワードをクリップボードにコピーします。

4. データベースに対する読み書きアクセス権と持つユーザとして、エンタープライズ管理サーバに接続します。

5. 以下のクエリを実行します。*encrypted password* は、クリップボードにコピーしておいた暗号化されたパスワードで、*username* はユーザ アカウントの名前です。

   ```
   update tblusers set password = '<encrypted password>' where
   loginid='<username>';
   ```

暗号化されたパスワードがアカウントのパスワードに設定されました。

DMS のアップグレード

新しい CA Access Control エンタープライズ管理 サーバのインストール後、既存の DMS をアップグレードする必要があります。アップグレード前に DMS の既存のインストールを削除する必要はありません。

重要: DMS が CA Access Control エンタープライズ管理 とは別のコンピュータにインストールされている場合のみ、この手順を完了します。

DMS をアップグレードするには、DMS コンピュータに CA Access Control をインストールします (P. 26)。

これで、CA Access Control エンタープライズ管理 を設定して DMS に接続できるようになりました (P. 52)。

Product Explorer を使用したインストール

CA Access Control Product Explorer では、CA Access Control の異なるアーキテクチャでのインストールと、ランタイム SDK のインストールが可能です。Product Explorer は、グラフィカル インターフェースを使用して CA Access Control のアンインストールを実行し、ユーザに対し、対話的にフィードバックを行います。

Product Explorer を使用したインストール方法

1. Windows の管理者権限を持つユーザ(すなわち、Windows Administrator または Windows Administrators グループのメンバ)として Windows システムにログインします。
2. 実行中のアプリケーションがあれば、すべて終了します。
3. CA Access Control Endpoint Components for Windows DVD を光ディスクドライブに挿入します。

   autorun が有効になっている場合は、Product Explorer が自動的に表示されます。autorun が有効になっていない場合は、光ディスクドライブのディレクトリに移動し、PRODUCTEXPLORERX86.EXE ファイルをダブルクリックします。
4. Product Explorer のメイン メニューから、Components フォルダを展開し、CA Access Control for Windows(*my_architecture*)を選択し、[インストール]をクリックします。

   インストール先のコンピュータのアーキテクチャに適合するインストール オプションを選択する必要があります(32 ビット、64 ビット x 64、または 64 ビット Itanium)。

   [セットアップ言語の選択]ウィンドウが表示されます。

5. CA Access Control をインストールする言語を選択し、[OK]をクリックします。

   CA Access Control インストール プログラムがローディングを開始し、しばらくして、概要画面が表示されます。

   注: CA Access Control の既存のインストールがインストール プログラムによって検出された場合、CA Access Control のアップグレードを実行するかどうかを選択するように促されます。

6. インストール画面の指示に従います。

   インストール中、ユーザは情報を入力するよう求められます。CA Access Control のインストール時にユーザが必要となる情報については、インストールワークシートを参照してください。

   インストール プログラムによって CA Access Control がインストールされます。インストールが完了したら、Windows をすぐに再起動するか、または後で再起動するかを選択します。

7. [はい、今すぐコンピュータを再起動します]を選択して[OK]をクリックします。

   システムの再起動後に、CA Access Control が正しくインストールされたことを確認できます。

   注: コンピュータを後で再起動するように選択した場合、コンピュータが再起動されるまでインストールが完了しないことを示す警告メッセージが表示されます。ログオン インターセプトなどの CA Access Control の一部の機能は、コンピュータを再起動するまで機能しません。

DMS との接続の設定

インストール時に、CA Access Control エンタープライズ管理 は、エンタープライズ サーバにインストールされているデプロイメント マップ サーバ（DMS）に対応して設定されます。別の DMS へのカスタム接続を作成するには、カスタム DMS への接続を設定して、環境に合わせて CA Access Control エンタープライズ管理 を設定する必要があります。

注: インストール時に、CA Access Control エンタープライズ管理 は、*ac_entm_pers* ユーザ アカウントを使用して、エンタープライズ管理サーバ上の DMS に対するデフォルト接続を作成します。

DMS への接続の設定方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
   a. ［システム］をクリックします。
   b. ［接続管理］サブタブをクリックします。
   c. 左側のタスク メニューで、DMS ツリーを展開します。

   ［接続の作成］タスクが使用可能なタスク リストに表示されます。
2. ［接続の作成］をクリックします。

   ［接続の作成］タスク ページが表示されます。
3. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

   接続名

   この接続に使用する名前を定義します。

   接続の種類

   作成する接続の種類を示します（AC）。

   説明

   （オプション）この接続に関する説明を定義します。

ホスト名

CA Access Control エンタープライズ管理 の動作対象となる DMS の名前を定義します。

形式: DMS*Name*@*hostName*

たとえば、ホスト host1.comp.com に CA Access Control エンタープライズ管理 をインストールする際にインストールされるデフォルト DMS を使用するには、DMS__@host1.comp.com と入力します。

ユーザ ID

DMS への管理権限を有するユーザの名前を定義します。

ログインされたユーザに代わって CA Access Control エンタープライズ管理 アクションを実行するには、デフォルトの管理ユーザを使用するのでなく、専用のプロキシ ユーザを使用することをお勧めします。

注: DMS 監査レコードに、CA Access Control エンタープライズ管理 にログインしたユーザの代わりに、定義されたプロキシ ユーザがデータベース コマンドを実行した旨が表示されます。

パスワード

DMS への管理権限を有するユーザのパスワードを定義します。

デフォルトの接続

この接続が、ユーザのログインの際に CA Access Control エンタープライズ管理 がデフォルトで使用する接続かどうかを指定します。

注: デフォルトの接続を指定する場合、ログアウトし、再度ログインしてから、接続を確立する必要があります。

[サブミット]をクリックします。

CA Access Control エンタープライズ管理 は、DMS へのログイン試行時に指定した情報を使用します。情報が正しい場合、接続が設定されます。これで、CA Access Control の企業展開を管理するために CA Access Control エンタープライズ管理 を使用できるようになりました。情報が不適切で、CA Access Control エンタープライズ管理 が DMS にログインできない場合、接続を確立できなかった理由を示すエラー メッセージが表示されます。

配布ホスト(DH)のアップグレード

DMS を正常にアップグレードした後、配布ホスト(DH)をアップグレードします。配布ホストを実行しているすべてのコンピュータ上に配布サーバをインストールして、DH をアップグレードします。

配布サーバのインストール後、メッセージ キュー ルーティング設定を構成して、配布サーバと CA Access Control エンタープライズ管理 の間のメッセージの送受信のルートを確立します。

重要: DH が CA Access Control エンタープライズ管理 とは別のコンピュータにインストールされている場合のみ、この手順を完了します。

配布ホストのアップグレード方法

1. DH コンピュータ上に配布サーバをインストールします (P. 54)。

   配布サーバは、Java コネクタ サーバ(JCS)、DH およびメッセージ キューをインストールします。

2. 配布サーバと CA Access Control エンタープライズ管理 間のメッセージ キュー ルーティング設定 (P. 56)を定義します。

   これで、配布サーバが設定されます。

配布サーバのインストール

ディザスタ リカバリ環境またはハイ アベイラビリティ環境で動作するように CA Access Control を設定する場合、配布サーバを別々のコンピュータにインストールし、その間でファイルが伝達されるように配布サーバを設定します。

配布サーバのインストール方法

1. お使いのオペレーティング システム用の適切な CA Access Control Premium Edition サーバ コンポーネント DVD を光ディスクドライブに挿入します。
2. 以下のいずれかの操作を行います。
   - Windows の場合

     autorun が有効になっている場合は、Product Explorer が自動的に表示されます。以下の手順を実行します。

     a. Product Explorer が表示されない場合は、光ディスクドライブのディレクトリに移動し、ProductExplorerx86.EXE ファイルをダブルクリックします。

     b. Product Explorer で[Components]フォルダを展開し、CA Access Control 配布サーバを選択して、[インストール]をクリックします。

     InstallAnywhere インストール プログラムが起動します。

   - UNIX の場合

     a. 光ディスクドライブをマウントします。

     b. ターミナル ウィンドウを開き、光ディスクドライブ上の以下のディレクトリに移動します。

     /DistServer/Disk1/InstData/NoVM

     c. 以下のコマンドを実行します。

     ```
     ./install_DistServer_r125.bin -i console
     ```

     InstallAnywhere インストール プログラムが起動します。

3. 必要に応じてウィザードを完了します。以下のインストール入力には、説明が必要です。

   メッセージ キュー設定

   メッセージ キュー サーバの管理者パスワード(通信パスワード)を定義します。

   制限: 最低 6 文字

   Java コネクタ サーバ - プロビジョニング ディレクトリ情報

   Java コネクタ サーバ用のパスワードを定義します。

   注: Java コネクタ サーバは、CA Access Control エンタープライズ管理 に特権アカウント管理機能を提供します。

   CA Access Control 配布サーバのインストールが完了します。

   注: ディザスタ リカバリの実装の一部として配布サーバをインストールする場合は、追加の手順を完了する必要があります。

メッセージ ルーティングの設定方法

エンタープライズ管理サーバと複数の配布サーバの単一のインスタンスから構成される環境で動作する場合、エンタープライズ管理サーバ上の MQ を指すように、MQ ルーティング設定をすべての配布サーバ上で設定する必要があります。これにより、CA Access Control エンドポイントから送信されるすべてのメッセージが、最終的に、エンタープライズ管理サーバ上に存在する単一の MQ に確実にルーティングされるようになります。

各配布サーバ上の MQ からエンタープライズ管理サーバにメッセージをルーティングするには、以下の手順に従います。

- 組織内の各配布サーバで、以下を行います。
  - メッセージ キュー サービスを停止します。
  - エンタープライズ管理サーバ メッセージ キューへのルーティングを変更します。
  - エンタープライズ管理サーバ メッセージ キューのパラメータを定義します。
  - 配布サーバ メッセージ キューの名前を設定します。
  - エンタープライズ管理サーバ メッセージ キューの場所を指定します。
  - メッセージ キュー サービスを開始します。

- エンタープライズ管理サーバで、以下の手順を実行します。
  - メッセージ キュー サービスを停止します。
  - 配布サーバ メッセージ キューへのルーティングを変更します。
  - 配布サーバ メッセージ キューのパラメータを定義します。
  - エンタープライズ管理サーバ メッセージ キューの名前を設定します。
  - エンタープライズ管理サーバ メッセージ キューの場所を指定します。
  - メッセージ キュー サービスを開始します。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

配布サーバ上のメッセージ キュー設定の変更

デフォルトでは、すべての配布サーバは、そのサーバで実行されているメッセージ キューと連動するように設定されています。メッセージを別のメッセージ キューへルーティングするために、メッセージ キュー設定を再設定する必要があります。

この手順では、配布サーバ上でメッセージ キュー設定を変更して、CA Access Control エンタープライズ管理 メッセージ キューとの通信を有効にする方法について説明します。組織内の各配布サーバについて、この手順を完了します。

配布サーバ上のメッセージ キュー設定の変更方法

1. CA Access Control メッセージ キュー サービスを停止します。

   重要: CA Access Control メッセージ キュー サービスを停止させると、CA DSM r11Common Application Framework サービスも停止されます。

2. 配布サーバで、デフォルトでは以下のディレクトリ(ここで *DistServerInstallDir* は配布サーバをインストールしたディレクトリ)にあるファイル tibemsd.conf ファイルを開きます。

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

3. [サーバ]パラメータに、配布サーバの短いホスト名を入力します。
4. [ルーティング]パラメータ値を有効にします。
5. CA Access Control メッセージ キュー サービスを開始します。

   配布サーバ上のメッセージ キュー設定を変更しました。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

例: tibemsd.conf ファイル

以下の例は、DS_Example という名前の配布サーバのルーティング設定を変更した後の、tibemsd.conf ファイルの抜粋を示しています。

```
#######################
# サーバ識別情報
# サーバ:      一意のサーバ名
# パスワード:  ルーティングされた他のサーバへのログインに使用されるパスワード
#######################
server                  = DS_Example
password                =
#######################
…
#######################
# ルーティング  ルート設定は「routes.conf」にあります。 これにより
# このサーバのルーティング機能を有効または無効にします。
#######################
routing                 = enabled
#######################
```

エンタープライズ管理サーバでのメッセージ キュー設定の変更

この手順では、エンタープライズ管理サーバでメッセージ キュー設定を変更して、配布サーバとの通信を有効にする方法について説明します。

エンタープライズ管理サーバでのメッセージ キュー設定の変更方法

1. CA Access Control メッセージ キュー サービスを停止します。

   重要: CA Access Control メッセージ キュー サービスを停止させると、CA DSM r11Common Application Framework サービスも停止されます。

2. エンタープライズ管理サーバで、編集のため tibemsd.conf ファイルを開きます。このファイルは以下のディレクトリにあります。ここで *ACServerInstallDir* は、エンタープライズ管理サーバをインストールしたディレクトリです。

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

3. [サーバ]パラメータに、ドットで区切られない、エンタープライズ管理サーバの短縮ホスト名を入力します。

4. ［ルーティング］パラメータ値を有効にします。
5. CA Access Control メッセージ キュー サービスを開始します。

   エンタープライズ管理サーバでメッセージ キュー設定を変更しました。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

例: tibemsd.conf ファイル

以下の例は、ENTM_Example という名前の CA Access Control エンタープライズ管理 サーバのルーティング設定を変更した後の、tibemsd.conf ファイルの抜粋を示しています。

```
#######################
# サーバ識別情報
# サーバ:       一意のサーバ名
# パスワード:   ルーティングされた他のサーバへのログインに使用されるパスワード
#######################
server                  = ENTM_Example
password                =
#######################
…
#######################
# ルーティング  ルート設定は「routes.conf」にあります。 これにより
# このサーバのルーティング機能を有効または無効にします。
#######################
routing                 = enabled
#######################
```

メッセージ キューの接続設定

配布サーバ上のメッセージ キューからエンタープライズ管理サーバにメッセージを逆にルーティングするには、企業内の既存のメッセージ キュー設定を変更します。

例: 配布サーバ上のメッセージ キュー接続設定

この例では、配布サーバ上のメッセージ キュー サーバ設定を設定する方法を示します。エンタープライズ管理サーバにメッセージが送信されるようメッセージ キューを設定するには、エンタープライズ管理サーバ上で実行されているメッセージ キューのパラメータを定義します。

以下の手順に従います。

1. 配布サーバで、以下のいずれかを実行します。
   - (Windows 2003 Server) [スタート]-[プログラム]-[TIBCO-CA_AC]-[TIBCO EMS 5.1]-[EMS 管理ツールの開始]を選択します。
   - (UNIX) 以下を実行します。
     a. 以下のディレクトリに移動します(*DistServerInstallDir* は配布サーバをインストールしたディレクトリです)。

        ```
        DistServerInstallDir/MessageQueue/tibco/ems/5.1/bin
        ```

     b. 以下のコマンドを実行します。

        ```
        tibemsadmin
        ```

        [TIBCO EMS 管理ツール]コマンド プロンプト ウィンドウが開きます。
2. 以下のいずれかを使用して、メッセージ キューに接続します。
   - 以下のコマンドを入力して、SSL を使用して接続します。

     ```
     connect ssl://localhost:7243
     ```
   - 以下のコマンドを入力して、TCP を使用して接続します。

     ```
     connect tcp://localhost:7222
     ```

   ログイン名の入力を促すプロンプトが表示されます。
3. 「**admin**」と入力します。

   パスワードの入力を促すメッセージが表示されます。
4. 配布サーバのインストール時に指定したパスワードを入力します。
5. プロンプトが表示されたら、メッセージ キュー サーバ用の新しいパスワードを入力します。
6. メッセージ キューのパスワードを定義します。

   ```
   set server password=
   ```

   例: set server password=*<C0mp1ex>*
7. ENTM-NAME という名前のユーザを作成し、このユーザへパスワードを割り当てます。

   ```
   create user ENTM-NAME password=acserver_user-passwd
   ```

   例: create user EMS-SERVER password=*<acserver_user-passwd>*

   重要: エンタープライズ管理サーバ上の tibemsd.conf ファイルの[サーバ]パラメータに定義したものと同じ名前を指定します。

8. 以下の手順を実行します。
   a. 以下のコマンドを入力します。

      ```
      add member ac_server_users ENTM_NAME
      ```

      作成したユーザは ac_server_users グループに追加されます。
   b. 以下のコマンドを入力します。

      ```
      add member ac_endpoint_users ENTM_NAME
      ```

      作成したユーザは ac_endpoint_users グループに追加されます。
   c. 以下のコマンドを入力します。

      ```
      add member report_publishers ENTM_NAME
      ```

      作成したユーザには、メッセージを読み取り、CA Access Control キューへメッセージを発行する権限が付与されます。
9. 配布サーバを再起動します。

   加えた変更が適用されます。

例: エンドポイント管理サーバ上のメッセージ キュー接続設定の設定

この例では、エンタープライズ管理サーバ上のメッセージ キュー サーバ設定を設定する方法を示します。配布サーバにメッセージが送信されるようメッセージ キュー サーバを設定します。

この例では、DS-NAME という用語は配布サーバ コンピュータの名前に、ENTM-NAME という用語はエンタープライズ管理サーバの名前にそれぞれ関連付けられています。メッセージ キュー サーバ設定を定義する際は、これらの名前をサーバの実際の名前で置き換える必要があります。実際の名前は *tibemsd.conf* ファイルの「server」トークンで定義されています。

以下の手順に従います。

1. エンタープライズ管理サーバで、以下の手順を実行します。
   - (Windows 2003 Server) [スタート]-[プログラム]-[TIBCO-CA_AC]-[TIBCO EMS 5.1]-[EMS 管理ツールの開始]を選択します。
   - (UNIX) 以下を実行します。
     a. 以下のディレクトリに移動します。ここで *ACServerInstallDir* は、エンタープライズ管理サーバをインストールしたディレクトリです。

        ```
        ACServerInstallDir/MessageQueue/tibco/ems/5.1/bin
        ```

     b. 以下のコマンドを実行します。

        ```
        tibemsadmin
        ```

        [TIBCO EMS 管理ツール]コマンド プロンプト ウィンドウが開きます。
2. 以下のいずれかを使用して、メッセージ キューに接続します。
   - 以下のコマンドを入力して、SSL を使用して接続します。

     ```
     connect ssl://localhost:7243
     ```

   - 以下のコマンドを入力して、TCP を使用して接続します。

     ```
     connect tcp://localhost:7222
     ```

   ログイン名の入力を促すプロンプトが表示されます。
3. 「**admin**」と入力します。

   パスワードの入力を促すメッセージが表示されます。
4. エンタープライズ管理サーバのインストール時に指定したパスワードを入力します。

5. メッセージ キューのパスワードを定義します。

   `set server password=entm_server-passwd`

   例: set server password=*<ENTM_SERVER_NAME-passwd>*

6. 各配布サーバについて、DS-NAME という名のユーザを作成し、このユーザへパスワードを割り当てます。

   `create user DS-NAME password=dist_server_user`

   例: create user EMS-Server password=*<COmp1ex>*

   重要: エンタープライズ管理サーバ上の tibemsdf.conf ファイルの「server」パラメータに定義した名前と同じ名前を指定する必要があります。

7. 以下の手順を実行します。

   a. 以下のコマンドを入力します。

      `add member ac_server_users DS_NAME`

      作成したユーザは ac_server_users グループに追加されます。

   b. 以下のコマンドを入力します。

      `add member ac_endpoint_users DS_NAME`

      作成したユーザは ac_endpoint_users グループに追加されます。

   c. 以下のコマンドを入力します。

      `add member report_publishers DS_NAME`

      作成したユーザには、メッセージを読み取り、CA Access Control キューへメッセージを発行する権限が付与されます。

8. 変更を有効にするために、配布サーバを再起動します。

   これで、エンタープライズ管理サーバでメッセージ キュー接続設定を変更しました。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

配布サーバ上のメッセージ キューの名前の設定

配布サーバからエンタープライズ管理サーバへメッセージを転送するには、各メッセージ ルートを設定して、配布サーバ上のメッセージ キューからエンタープライズ管理サーバ上のメッセージ キューへメッセージを転送します。

この手順では、配布サーバ上のメッセージ キュー設定を定義します。エンタープライズ管理サーバでメッセージ キューの設定を提供するように、メッセージ キュー設定ファイルを変更します。

配布サーバ上のメッセージ キューの名前の設定方法

1. 配布サーバで、ファイル queues.conf を開きます。このファイルはデフォルトで以下のディレクトリにあります(*DistServerInstallDir* は、配布サーバをインストールしたディレクトリです)。

   DistServerInstallDir/ACMQ/tibco/cfgmgmt/ems/data

2. 「queue/snapshots」という名前のキューを探し、このキュー名の後ろに、@ 記号、続いて、ENTM-NAME 値を追加します。

   queue/snapshots@*ENTM-NAME*

   ENTM-NAME

   エンタープライズ管理サーバの短縮名を定義します。

   重要: エンタープライズ管理サーバ上の tibemsd.conf ファイルの[サーバ]パラメータに定義したものと同じ名前を指定します。

3. 「queue/audit」という名前のキューを探し、このキュー名の後ろに、@ 記号、続いて、ENTM-NAME 値を追加します。

   queue/audit@*ENTM-NAME*

4. 「ac_endpoint_to_server」という名前のキューを探し、このキュー名の後ろに、@ 記号、続いて、ENTM-NAME 値を追加します。

   ac_endpoint_to_server@*ENTM-NAME*

5. 「ac_server_to_endpoint」という名前のキューを探し、このキュー名の後ろに、@ 記号、続いて、ENTM-NAME 値を追加します。

   ac_server_to_endpoint@*ENTM-NAME*

6. ファイルを保存して閉じます。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

エンタープライズ管理サーバでのメッセージ キューの名前の設定

この手順では、エンタープライズ管理サーバでメッセージ ルーティング設定を定義します。このメッセージ キューをプライマリ サーバとして認識するように、エンタープライズ管理サーバでメッセージ キュー設定を設定します。

エンタープライズ管理サーバでのメッセージ キューの名前の設定方法

1. エンタープライズ管理サーバで、編集可能な形式でファイル queues.conf を開きます。このファイルは以下のディレクトリにあります。ここで *ACServerInstallDir* はエンタープライズ管理サーバをインストールしたディレクトリです。

   ```
   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data
   ```

2. 「queue/snapshots」という名前のキューを見つけ、このキュー名の後ろに、「secure」、「global」という単語を追加します。

   ```
   queue/snapshot secure, global
   ```

3. 「queue/audit」という名前のキューを見つけ、このキュー名の後ろに、「secure」、「global」という単語を追加します。

   ```
   queue/audit secure, global
   ```

4. 「ac_endpoint_to_server」という名前のキューを見つけ、このキュー名の後ろに、「secure」、「global」という単語を追加します。

   ```
   ac_endpoint_to_server secure, global
   ```

5. 「ac_server_to_endpoint」という名前のキューを見つけ、このキュー名の後ろに、「secure」、「global」という単語を追加します。

   ```
   ac_server_to_endpoint secure, global
   ```

6. ファイルを保存して閉じます。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

メッセージのルーティング設定

メッセージ キュー設定を設定済みで、配布サーバとエンタープライズ管理サーバでメッセージ キュー ルーティング設定を設定した後、配布サーバとエンタープライズ管理サーバ上でメッセージ ルートをセットアップします。

例: 配布サーバ上でのメッセージ ルートのセットアップ

この例では、配布サーバ上でのメッセージ ルート設定のセットアップ方法について説明します。CA Access Control エンドポイントから到着するメッセージをエンタープライズ管理サーバのメッセージ キューにルーティングするように、配布サーバとエンタープライズ管理サーバの間にルートをセットアップします。組織内の配布サーバごとに、この手順を完了します。

1. 配布サーバで、routes.conf ファイルを編集できる形で開きます。このファイルはデフォルトで以下のディレクトリにあります(*DistServerInstallDir* は、配布サーバをインストールしたディレクトリです)。

   DistServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 以下のエントリを追加します。

   ```
   [ENTM-NAME]
   url          = ENTM-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   ENTM-NAME

   エンタープライズ管理サーバの短縮名を定義します。

   ENTM_URL

   エンタープライズ管理サーバ URL を定義します。

3. ファイルを保存します。
4. CA Access Control メッセージ キュー サービスを再起動します。

例: エンタープライズ管理サーバ上でのメッセージ ルートのセットアップ

この例では、エンタープライズ管理サーバでのメッセージ ルート設定のセットアップ方法について説明されています。エンタープライズ管理サーバから配布サーバに、さらにそこからエンドポイントにメッセージを送信するように、エンタープライズ管理サーバと配布サーバの間にルートをセットアップします。

1. エンタープライズ管理サーバで、ファイル routes.conf を開きます。このファイルはデフォルトでは以下のディレクトリにあります(*ACServerInstallDir* は、エンタープライズ管理サーバをインストールしたディレクトリです)。

   ACServerInstallDir/MessageQueue/tibco/cfgmgmt/ems/data

2. 以下のエントリを追加します。

   ```
   [DS-NAME]
   url          = DS-URL
   ssl_verify_host = disabled
   ssl_verify_hostname = disabled
   ```

   DS_NAME

   配布サーバの短縮名を定義します。

   DS_URL

   配布サーバの URL を定義します。

3. ファイルを保存します。
4. CA Access Control メッセージ キュー サービスを再起動します。

注: メッセージ ルーティングの詳細については、「*TIBCO Enterprise Message Service User's Guide*」を参照してください。Tibco ドキュメントはメッセージ キューの一部としてインストールされ、*ACServerInstallDir*/MessageQueue/tibco/ems/5.1/doc に保存されます。

レポート サーバをエンタープライズ レポーティング サービスへ移行します。

エンタープライズ レポーティング サービスは、レポート サーバ機能を単一のエンタープライズ規模のレポート サービスにバンドルします。 設計上の変更により、レポート サーバは現在 CA Access Control エンタープライズ管理 の一部になっていて、もはや個別のコンポーネントではありません。配布サーバをレポート サーバにインストールし、メッセージ キュー設定を再設定して、レポート サーバを移行します。

注: この移行プロセスでは、既存のエンドポイントが継続して、レポート サーバ コンピュータ上のメッセージ キューを使用します。この手順の完了後、エンドポイント上のレポート エンドポイント設定を再設定する必要はありません。

重要: レポート サーバが CA Access Control エンタープライズ管理 とは別のコンピュータにインストールされている場合のみ、この手順を完了します。

以下の手順に従います。

1. 配布サーバをレポート サーバ コンピュータにインストールします (P. 54)。
2. JBoss サービスを無効にします。
3. 配布サーバと CA Access Control エンタープライズ管理 間のメッセージ キュー ルート設定 (P. 56)を定義します。

   エンタープライズ レポーティング サービス(レポート サーバを含む)がインストールされます。これで、エンタープライズ レポーティング サーバ コンポーネントを設定できます。

   注: エンタープライズ レポーティング サーバのコンポーネントの詳細については、「エンタープライズ管理ガイド」を参照してください。
4. DH を新しい DMS へサブスクライブします (P. 70)。

DMS への DH のサブスクライブ

CA Access Control エンタープライズ管理 コンポーネントのアップグレードを完了したら、以前の DMS を使用できなくなります。そのため、CA Access Control エンタープライズ管理 を開始する前に、新しい DMS で機能する、アップグレードされた DH を設定してください。

重要: この手順を完了するのは、レポート サーバ コンピュータに配布サーバをインストールした場合のみです。

以下の手順に従います。

1. 配布サーバでコマンド プロンプト ウィンドウを開きます。
2. 配布ホストに新しい DMS をサブスクライブします。

   ```
   sepmd -s DH__WRITER DMS__@<entm>
   ```

3. 親配布ホストとして新しい DMS を追加します。

   ```
   sepmd -s DMS__ DH__@<host_name>
   ```

4. エンタープライズ管理サーバ上でコマンド プロンプト ウィンドウを開き、新規サブスクライバを作成します。

   ```
   sepmd -n DH__@<host_name>
   ```

注: sepmd ユーティリティの詳細については「*リファレンス ガイド*」を参照してください。

CA Access Control エンドポイントのアップグレード

CA Access Control エンタープライズ管理、DMS、配布ホスト、およびレポート サーバをアップグレードした後に、既存の CA Access Control r12.0 SP1 エンドポイントをアップグレードできるようになりました。

CA Access Control のエンドポイントをアップグレードするには、CA Access Control をエンドポイントにインストールします (P. 26)。

第 4 章: 詳細ポリシー管理環境への PMD の移行

このセクションには、以下のトピックが含まれています。

詳細ポリシー管理環境への移行

Policy Model (PMD) 環境から詳細ポリシー管理環境に移行する場合は、エンドポイントにルールをデプロイする方法を変更します。

- PMD 環境では、中央データベース (PMDB) で定義する正規のルールは自動的に設定された階層のデータベースに伝搬されます。
- 詳細ポリシー管理環境では、ポリシー (ルールのグループ) を 1 つ以上のホストまたはホスト グループに割り当てます。また、ポリシーのデプロイ解除 (削除)、デプロイのステータスやデプロイの偏差の表示を行うこともできます。

PMD 環境から詳細ポリシー管理環境に移行する場合は、以下を行います。

- 追加のコンポーネントをインストールする
- PMDB のルールからポリシーを作成する
- エンドポイントをアップグレードする
- PMD 構造をフラット化する

詳細ポリシー管理では、階層ホスト グループをサポートしていません。PMD アーキテクチャに階層 PMDB が含まれている場合は、PMD 階層をフラット化する必要があります。

注: 拡張ポリシー管理は、パスワード管理コマンドによるポリシーをサポートしません。エンドポイント間でパスワードを同期し、パスワード管理ルールを配布するには、パスワード PMD を使用する必要があります。パスワード PMD を拡張ポリシー管理環境に移行することはできません。代わりに、パスワード ルールをサブスクライバにのみ送信するように、パスワード PMD にフィルタ ファイルを適用します。

移行プロセスのしくみ

詳細ポリシー管理環境に移行すると、ポリシーのデプロイ/デプロイ解除を行ったり、ポリシーのデプロイおよび偏差のステータスを確認したりすることができます。移行タスクのほとんどは CA Access Control が実行しますが、ユーザ自身が実行するタスクもあります。移行プロセスのしくみを理解しておけば、問題が発生した場合のトラブルシューティングに役立ちます。

以下の手順では、移行プロセスの各段階の概要を示します。

1. エンタープライズ管理サーバ コンポーネントをインストールします。

   拡張ポリシー管理環境は、エンタープライズ管理インストール プロセスの一部として設定されます。

2. PMD を CA Access Control r12.5 以降にアップグレードします。
3. PMD にサブスクライブしているエンドポイントを拡張ポリシー管理環境に移行します。
4. CA Access Control エンタープライズ管理 で、PMDB のルールをポリシー ファイルにエクスポートします。
5. CA Access Control エンタープライズ管理 は、DMS に以下を作成します。
   - 移行した PMDB に対応するホスト グループ (GHNODE オブジェクト)
   - PMDB のエンドポイント サブスクライバに対応するホスト (HNODE オブジェクト)
   - ポリシー ファイルにルールを含む POLICY オブジェクト

6. CA Access Control エンタープライズ管理 で、ホスト グループにホストを追加します。CA Access Control は、POLICY オブジェクトをホスト グループに割り当て、PMDB のエンドポイント サブスクライバに対応するホストに展開します。
7. CA Access Control エンタープライズ管理 で、以下の*いずれか*を実行します。
   - PMD がパスワード PMD である場合、PMD にフィルタ ファイルを適用します。
   - PMD がパスワード PMD でない場合、PMD を削除します。

注: policydeploy ユーティリティを使用して、移行タスクを実行することもできます。

詳細情報:

詳細ポリシー管理への移行方法 (P. 76)

ポリシーの作成と割り当て方法

PMD 環境から拡張ポリシー管理環境に移行する場合は、CA Access Control を使用して PMDB 内のルールからポリシーを作成し、それらのポリシーを DMS 内のホスト グループに割り当てます。

以下に、CA Access Control がポリシーを作成し、割り当てるプロセスについて示します。

1. CA Access Control は、PMDB 内のルールをポリシー ファイルにエクスポートします。

   注: CA Access Control が特定クラスのリソースを変更するルールのみをエクスポートするように指定できます。

2. CA Access Control は、新しいリソースまたはアクセサを作成する各ルールを、リソースまたはアクセサを変更するルールに変更します。たとえば、CA Access Control はすべての newres ルールを editres ルールに変更します。

   このステップにより、リソースまたはアクセサを新規作成するルールを、同じエンドポイントに 2 回以上デプロイした場合に発生するエラーが防止されます。

3. CA Access Control は、DMS 上の PMD に対応するホスト グループ (GHNODE オブジェクト) を作成します。

4. PMDB にリストされた各エンドポイント サブスクライバに対し、CA Access Control は、対応するホスト（HNODE オブジェクト）が DMS 内にすでに作成されているかどうかを確認します。

   - PMDB にリストされた、DMS 内に対応するホストを持つ各サブスクライバに対し、CA Access Control はステップ 3 で作成したホスト グループにホストを追加します。
   - PMDB にリストされた、DMS 内に対応するホストを持たない各サブスクライバに対し、CA Access Control は、エンドポイントに対応するホストを作成し、ステップ 3 で作成したホスト グループにそのホストを追加します。

   注: CA Access Control は、サブスクライバ PMDB に対応するホストは作成しません。

5. CA Access Control はエクスポートされたポリシー ファイルのルールを使用して、DMS 内に POLICY オブジェクトを作成します。

   注: CA Access Control は、POLICY オブジェクト用のデプロイ解除スクリプトは作成しません。

6. CA Access Control は、POLICY オブジェクトをステップ 3 で作成したホスト グループに割り当てます。

詳細情報:

PMDB の移行 (P. 78)

ポリシーが移行されたエンドポイントに最初に送信されるしくみ

PMD 環境から拡張ポリシー管理環境に移行する場合、CA Access Control は PMDB のルールからポリシーを作成し、移行されたエンドポイントにそれらを送信します。CA Access Control がポリシーを移行したエンドポイントに最初に送信する方法を理解することは、移行プロセス中に発生するエラーを解決するのに役立ちます。

以下のプロセスは、エンドポイントで CA Access Control を開始した後で、ポリシーが移行されたエンドポイントに最初に送信される方法について説明します。

1. CA Access Control は、開始して DMS にハートビート通知を送信する policyfetcher を呼び出します。
2. DMS は、ハートビート通知を受信して対応するホスト（HNODE）オブジェクトが、DMS に存在するかどうかを確認します。

3. 以下の*いずれか*のイベントが発生します。
   - 対応するホストが DMS に存在し、そのホストが、移行した PMD に対応するホスト グループの一部である場合:
     a. CA Access Control はエンドポイントとホストを関連付けます。
     b. CA Access Control は、ホスト グループに割り当てられるポリシーをエンドポイントにデプロイします。
   - 対応するホストが DMS に存在しない場合:
     a. CA Access Control はホストを作成します。
     b. ポリシーを作成して割り当てると、CA Access Control は、移行した PMD に対応するホスト グループにそのホストを追加します。
     c. CA Access Control は、ホスト グループに割り当てられるポリシーをエンドポイントにデプロイします。
4. CA Access Control は、ポリシーに一覧表示された各リソースの[更新時間]プロパティを、ポリシーがデプロイされた時間に変更します。

   注: CA Access Control によって、オブジェクトの作成コマンドがオブジェクトの変更コマンドに変更されたため、ポリシーに対するデプロイのエラーは表示されないはずです。

注: ポリシーとホスト グループの詳細については、「*エンタープライズ管理ガイド*」を参照してください。

CA Access Control が、パスワード PMD にフィルタ ファイルを適用するしくみ

拡張ポリシー管理は、パスワード管理コマンドによるポリシーをサポートしません。エンドポイント間でパスワードを同期し、パスワード管理ルールを配布するには、パスワード PMD を使用します。パスワード PMD を拡張ポリシー管理環境に移行する場合は、パスワード ルールをサブスクライバにのみデプロイするように、パスワード PMD にフィルタ ファイルを適用します。

以下に、CA Access Control がパスワード PMD にフィルタ ファイルを適用するプロセスについて示します。

1. CA Access Control は、filter.flt という名前のテキスト ファイルを作成し、以下の行を追加します。

```
#-------------------------------------------------------------------------
--
# access    env     class   objects properties              pass/nopass
#-------------------------------------------------------------------------
--
  *         *       USER    *       OLD_PASSWD;CLR_PASSWD   PASS
  *         *       *       *       *                       NOPASS
#-------------------------------------------------------------------------
--
```

2. CA Access Control はパスワード PMD ディレクトリに filter.flt を保存します。
3. CA Access Control は次の場所の「フィルタ」環境設定に filter.flt のフル パスを追加します。
   - （UNIX）pmd.ini ファイルの［pmd］セクション
   - （Windows）以下のレジストリ キー

     HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Pmd¥*PMDB_Name*

詳細ポリシー管理への移行方法

詳細ポリシー管理環境に移行すると、ポリシーのデプロイ/デプロイ解除を行ったり、ポリシーのデプロイおよび偏差のステータスを確認したりすることができます。

注: 拡張ポリシー管理は、パスワード管理コマンドによるポリシーをサポートしません。エンドポイント間でパスワードを同期し、パスワード管理ルールを配布するには、パスワード PMD を使用する必要があります。パスワード PMD を拡張ポリシー管理環境に移行することはできません。

移行処理を開始する前に、以下を確認します。

- すべてのサブスクライバが利用可能である
- サブスクライバが PMDB からすべての更新をすべて受信している
- PMDB と同期しているサブスクライバが存在しない

重要: 移行プロセスを開始する前に PMDB をバックアップしておくことを強くお勧めします。

PMD 環境から詳細ポリシー管理環境に移行するには、以下のようにします。

1. エンタープライズ管理サーバ コンポーネントをインストールします。

   拡張ポリシー管理環境は、エンタープライズ管理インストール プロセスの一部として設定されます。

2. PMD ホストを CA Access Control r12.5 以降にアップグレードします。
3. エンドポイントを移行 (P. 78)します。
4. PMDB を移行 (78P.)します。

詳細情報:

移行プロセスのしくみ (P. 72)

エンドポイントの移行

エンドポイントの移動は、PMD 環境から拡張ポリシー管理環境に移行するプロセスの 3 番目の手順です。前の手順では以下を行いました。

- エンタープライズ管理サーバ コンポーネントのインストール
- PMD ホストの CA Access Control r12.5 以降へのアップグレード

この手順では、移行した PMDB にサブスクライブするエンドポイントを移行します。

エンドポイントを移行する方法

1. エンドポイントを CA Access Control r12 以降にアップグレードします。
2. 拡張ポリシー管理クライアント コンポーネントを設定するために、エンドポイント上で以下のコマンドを実行します。

   ```
   dmsmgr -config -endpoint
   dmsmgr -config -dh dh_name@host_name
   ```

   エンドポイントは詳細ポリシー管理環境に更新されます。

PMDB の移行

PMDB を移行する前に、移行プロセス全体の各ステージで実行する必要がある手順について理解しておくことをお勧めします。PMDB の移行は、企業に展開された CA Access Control を拡張ポリシー管理環境へ移行するプロセスの手順の 1 つでしかありません。

PMDB の移行は、PMD 環境から拡張ポリシー管理環境へ移行するプロセスの最終手順です。前の手順では以下を行いました。

- エンタープライズ管理サーバのインストール
- PMD ホストの CA Access Control r12.5 以降へのアップグレード
- エンドポイント(エンドポイントの CA Access Controlr12.0 以降へのアップグレード、および拡張ポリシー管理クライアント コンポーネントの設定)の移行

この手順では、CA Access Control エンタープライズ管理 を使用して、PMDB 内にあるルールからのポリシーの作成、移行された PMDB 用のホスト グループの作成、PMDB サブスクライバに対応するホストのこのホスト グループへの追加を行います。また、新規ポリシーのホスト グループへの割り当ても選択できます。

重要: [次へ]ボタンをクリックするたびに、CA Access Control エンタープライズ管理 は DMS または PMDB 内でのアクションを完了します。これらのアクションの結果を元に戻すのは、困難な場合があります。

PMDB の移行方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]タブ、[ポリシー]サブタブの順にクリックし、ポリシー ツリーを展開して、[PMDB 移行]をクリックします。

   [PMDB ホスト ログオン]ページが表示されます。

2. PMDB へのアクセスが許可されているユーザのユーザ名とパスワード、および移行する PMDB の名前を入力し、[ログイン]をクリックします。

   注: PMDB 名は、*PMDBname@host*(例: master_pmdb@example)の形式で指定します。

   [PMDB 移行プロセス]ページは、[全般]タスク ステージで表示されます。

3. 以下のフィールドに入力し、[次へ]をクリックします。

   名前

   ポリシーの名前を定義します。この名前は、DMS で一意(強制)、および企業内で一意(強制ではないが、同じ名前のポリシーが存在する場合はポリシーをホストにデプロイできなくなる)にする必要があります。

   説明

   (オプション)ポリシーの役割説明(形式自由)を定義します。このフィールドを使用して、このポリシーの目的と、ポリシーの識別に役立つ情報を記録します。

ポリシー クラス

そのルールをエクスポートしてポリシーに含めるクラスを指定します。[選択リスト]列でクラスを指定しない場合、すべてのクラスがエクスポートされ、ポリシーに含められます。

依存クラスのエクスポート

[選択リスト]列で指定するクラスに依存するすべてのクラスのエクスポートを指定します。このオプションを選択しない場合、CA Access Control は[選択リスト]列で指定したクラスのみをエクスポートします。

[ポリシー スクリプト]タスク ステージが表示されます。

4. エクスポート済みルールを確認し、必要があれば変更して、[次へ]をクリックします。

   CA Access Control エンタープライズ管理 は、ルールからポリシーを作成します。[ホスト グループ]タスク ステージが表示されます。

5. 以下のようにして、ダイアログ ボックスを完了し、[次へ]をクリックします。

   ホスト グループ

   ホストの追加先のホスト グループの名前を指定します。既存のホスト グループを指定するか、または新しいホスト グループを作成できます。

   注: 既存のホスト グループにホストを追加する場合、CA Access Control はホスト グループに割り当てられた任意のポリシーを、自動的にホストにデプロイします。

   ポリシーの割り当て

   (オプション)ポリシーのホスト グループへの割り当てを指定します。

   割り当てられたホスト

   ホスト グループに追加するホストを指定します。

   注: デフォルトで、このテーブルには、アクセス権限がある移行済み PMDB のすべてのサブスクライバが含まれています。[割り当てられたホスト]リストからホストの追加および削除を行うことができます。しかし、ホストにアクセスする権限がなければ、ホストをホスト グループに追加できません。

   CA Access Control エンタープライズ管理 はホストをホスト グループに追加し、指定されている場合、ポリシーをホスト グループに割り当てます。[PMD オプション]タスク ステージが表示されます。

6. 移行した PMDB に適用するオプションを以下から選択します。

   手順 3 (ホスト グループ手順) で指定したホストの登録を取り消します。

   前のタスク ステージで、移行済み PMDB から選択したエンドポイントの登録解除を指定します。

   すべての PMDB サブスクライバをサブスクライブ解除

   移行した PMDB のすべてのサブスクライバがサブスクライブ解除されます。

   PMD の削除

   移行した PMDB が削除されます。

   重要: ユーザ パスワード コマンドを伝達するために PMDB 使用する場合は、削除しないでください。

   PMD フィルタ ファイルの追加

   PMDB がサブスクライバのみにユーザ パスワード コマンドを伝達するように、移行した PMDB にフィルタ ファイルを追加します。このオプションを選択すると、移行した PMDB はパスワード PMDB となります。

7. [次へ]をクリックします。

   CA Access Control は、指定したアクションを実行します。[移行アクション サマリ]タスク ステージが表示され、移行プロセスが完了します。

詳細情報:

ポリシーの作成と割り当て方法 (P. 73)

クラスの依存関係

PMDB から指定されたクラス用のルールをエクスポートする場合、依存クラス用のルールをエクスポートすることも選択できます。CA Access Control で依存クラスをエクスポートする必要があることを指定すれば、CA Access Control は以下をエクスポートします。

- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに対応するリソース グループが含まれる場合、CA Access Control はそのリソース グループに存在するリソースを変更するルールもエクスポートします。

  たとえば、FILE クラス ルールのエクスポートを指定した場合、CA Access Control は FILE クラスと GFILE クラスのリソースを変更するルールをエクスポートします。

- 特定のリソース グループのリソースを変更するルールをエクスポートする場合、CA Access Control はそのリソース グループのメンバ リソースを変更するルールもエクスポートします。

  たとえば、GFILE クラス ルールのエクスポートを指定した場合、CA Access Control は GFILE クラスと FILE クラスのリソースを変更するルールをエクスポートします。

- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに PACL が含まれる場合、CA Access Control は PROGRAM クラスに存在するリソースを変更するルールもエクスポートします。

- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスに CALACL が含まれる場合、CA Access Control は CALENDAR クラスに存在するリソースを変更するルールもエクスポートします。

- 特定のクラスのリソースを変更するルールをエクスポートし、そのクラスのリソースの 1 つが CONTAINER リソースグループのメンバである場合、CA Access Control は CONTAINER クラスのリソースを変更するルール、および各 CONTAINER リソース ループのメンバとなっているリソースを変更するルールをエクスポートします。

  たとえば、CONTAINER クラス ルールのエクスポートを指定し、CONTAINER オブジェクトが FILE オブジェクトを保持している場合、CA Access Control は、CONTAINER クラスと FILE クラスのリソースを変更するルールをエクスポートします。

重複した HNODE が DMS に表示される

症状:

拡張ポリシー管理環境に PMD を移行した後、同じエンドポイントを表わす 2 つの HNODE が DMS に作成される。

解決方法:

エンドポイントの完全修飾ホスト名は DMS 上とエンドポイント上で同じではありません。この問題を解決するためには、DMS で HNODE オブジェクトのうちの 1 つを削除します。

注: HNODE オブジェクトおよび DMS の詳細については、*「エンタープライズ管理ガイド」*を参照してください。

階層 PMDB の移行

詳細ポリシー管理では、階層ホスト グループをサポートしていません。PMD アーキテクチャに階層 PMDB が含まれている場合は、移行プロセス中に PMD 階層をフラット化する必要があります。

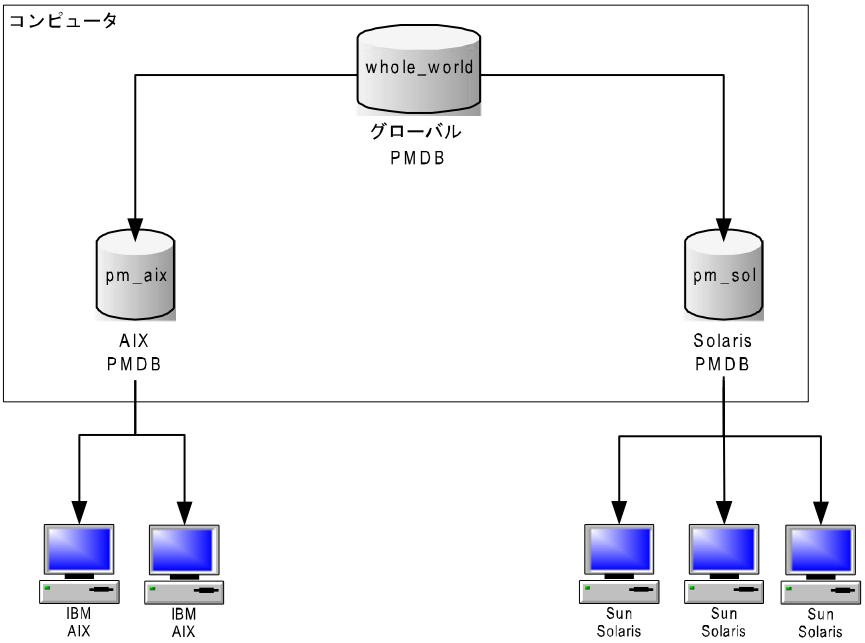
PMD 階層をフラット化した場合、各 PMDB を個別に移行します。移行中、CA Access Control は階層環境にある各 PMDB に対応するホスト グループを作成します。各エンドポイントは、サブスクライブしていた PMDB に対応するすべてのホスト グループに追加されます。

階層 PMDB の移行方法

1. マスタ PMDB を移行します。
2. 各サブスクライバ PMDB を移行します。

例: 階層 PMDB の移行

以下の図では、階層 PMDB の PMD 環境の例を示します。



この例では、pm_aix および pm_solaris という PMDB は、whole_world という PMDB のサブスクライバです。すべての IBM AIX エンドポイントは、pm_aix のサブスクライバです。すべての Sun Solaris エンドポイントは、pm_sol のサブスクライバです。事実上、すべてのエンドポイントは、whole_world のサブスクライバです

この PMD 環境を拡張ポリシー管理環境に移行する場合は、以下の手順を実行します。

1. whole_world PMDB を移行します。

   CA Access Control が whole_world ホスト グループを作成します。すべてのエンドポイントは、このホスト グループのメンバです。

2. サブスクライバ PMDB を移行します。

   - pm_aix PMDB を移行します。

     CA Access Control が pm_aix ホスト グループを作成します。IBM AIX エンドポイントは、このホスト グループのメンバです。

   - pm_sol PMDB を移行します。

     CA Access Control が pm_sol ホスト グループを作成します。Sun Solaris エンドポイントは、このホスト グループのメンバです。

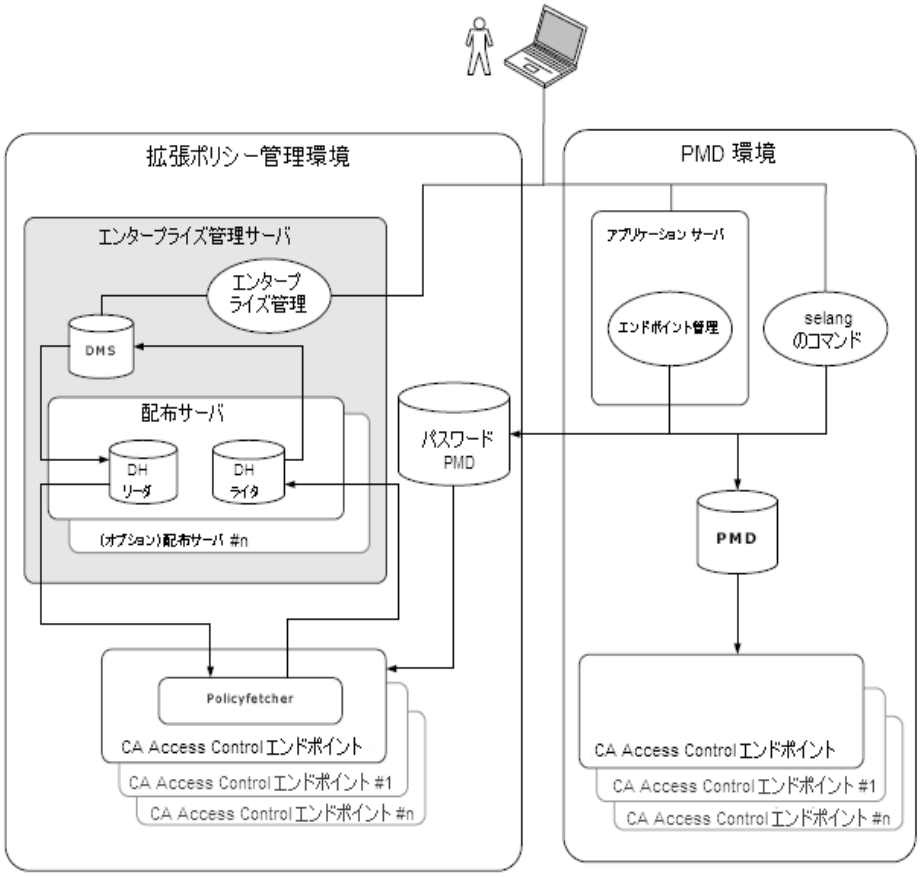
注: PMD 環境では、pm_aix PMDB にフィルタ ファイルを適用すると、whole_world PMDB からデプロイされたルールを IBM AIX エンドポイントで受信できなくなる場合があります。拡張ポリシー管理環境では、IBM AIX エンドポイントは whole_world ホスト グループのメンバです。whole_world ホスト グループにデプロイするすべてのルールは、フィルタされずにすべてのエンドポイントにデプロイされます。拡張ポリシー管理環境でルールをデプロイする場合、この動作の変更に注意する必要があります。

混合ポリシー管理環境

混合ポリシー管理環境とは、いくつかのエンドポイントは PMD に登録されていて、いくつかのエンドポイントは拡張ポリシー管理環境に定義されてる CA Access Control デプロイメントです。

以下の図では、混合ポリシー管理環境での CA Access Control デプロイメントの例を示します。

注: この図には表示されていませんが、エンドポイントは PMD に登録して、拡張ポリシー管理環境で定義することもできます。たとえば、拡張ポリシー管理環境のエンドポイントにポリシーをデプロイして、PMD から同じエンドポイントに selang ルールを伝達することもできます。



混合ポリシー管理環境のエンドポイントの更新

混合ポリシー管理環境でエンドポイントを更新する場合は、各環境のエンドポイントを別々に更新します。

注: エンドポイントは、CA Access Control の後のバージョンで導入されたクラスを変更するルールは、受け入れることができません。たとえば、r12.5 の PMD または DMS のルールをデプロイしていても、r8 のエンドポイントが受け入れられるのは、r8 の機能を変更するルールのみです。

混合ポリシー管理環境でエンドポイントを更新する方法

1. エンドポイントにデプロイする selang デプロイ コマンドを使用してスクリプト ファイルを作成します。
2. CA Access Control エンタープライズ管理 で、以下を実行します。
   a. ポリシーのバージョンを DMS に保存します。
   b. 保存したポリシーのバージョンを更新するホスト グループに割り当てます。

   CA Access Control は、ホスト グループのエンドポイントにポリシーをデプロイします。
3. スクリプト ファイルの selang コマンドを使用して PMDB を更新します。

   PMDB は、エンドポイントにコマンドを伝播します。

注: ポリシーのバージョンを保存して割り当てる方法については、「*エンタープライズ管理ガイド*」を参照してください。PMDB を更新する方法については、お使いの OS に対応する「*エンドポイント管理ガイド*」を参照してください。