CA Access Control Premium Edition

実装ガイド

r12.5

第 2 版

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

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On（CA 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）
- CA Enterprise Log Manager
- CA 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

形式	意味
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。

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。

マニュアルの変更点

第 2 版

本マニュアルの第 2 版は、r12.5 の GA 版の発表と同時にリリースされました。

この版では、以下のトピックが追加または更新されました。

- 実装計画 (19 ページ) - 概念を明確にするために、この章のトピックがいくつか更新されました。
- エンタープライズ管理サーバのインストール方法 (47 ページ) - ユーザの組織に合わせて CA Access Control エンタープライズ管理 をカスタマイズする新規手順を説明するトピックが更新されました。
- 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 (49 ページ) - このトピックから例が削除されました。
- CA Access Control エンタープライズ管理 のインストール (51 ページ) - CA Access Control エンタープライズ管理 のインストール後、コンピュータを再起動する新規要件でトピックが更新され、コンソールのインストールに関する記述が削除されました。
- SSL 通信用の CA Access Control エンタープライズ管理 の設定方法 (57 ページ) - この新規セクションでは、 Active Directory 使用時に、SSL を使用するように CA Access Control エンタープライズ管理 を設定する方法について説明します。
- CA Access Control エンタープライズ管理 の開始 (60 ページ) - この更新されたトピックでは、JBoss アプリケーション サーバが起動していることの検証方法について説明します。
- SQL Server データベース接続設定の変更 (64 ページ) - この新規トピックでは、CA Access Control エンタープライズ管理 と SQL Server との間の通信に関して、Windows 認証モードを有効にする方法について説明します。
- CA Access Control に対する CA Enterprise Log Manager の設定方法 (183 ページ) - この更新されたトピックでは、CA Enterprise Log Manager の設定方法に関する追加情報を提供します。
- SSL を使用した安全な通信 (189 ページ) - この更新されたトピックでは、提供する必要がある認証情報について説明します。
- レポート サービス サーバ コンポーネントの設定方法 (203 ページ) - この更新されたトピックでは、スナップショット定義作成の追加手順について説明します。

- UNAB ホストのインストールとカスタマイズ（213 ページ） - この更新された章では、UNAB エンドポイントのインストールに関して、理解しておくべき手順と概念について説明します。
- CA Access Control エンドポイント管理 の起動（258 ページ） - この新規の章は、インターフェースの変更を反映しています。
- Disaster Recovery Deployment のインストール（261 ページ） - Disaster Recovery Deployment のインストールに必要な手順と概念について説明する、新規の章です。
- CA Access Control r12.0 SP1 から CA Access Control r12.5 へのアップグレード（309 ページ） - この新規の章では、CA Access Control r12.0 SP1 を CA Access Control r12.5 にアップグレードする際に必要な手順と概念について説明します。

第 1 版

このマニュアルの第 1 版は、r12.5 でリリースされました。 本マニュアルのこの版では、r12.0 SP1 に対して以下の更新が加えられました。

- エンタープライズ デプロイ アーキテクチャ（22 ページ） - この更新されたトピックでは、CA Access Control エンタープライズ管理 の現在のデプロイ アーキテクチャについて説明します。
- CA Access Control の実装方法（25 ページ） - この新規トピックでは、組織への CA Access Control の実装手順について説明します。
- エンタープライズ管理サーバのインストール（43 ページ） - この更新された章では、CA Access Control エンタープライズ管理 の実装について説明します。
- Windows エンドポイントのインストールおよびカスタマイズ（69 ページ） - この更新された章では、CA Access Control Windows エンドポイントをインストールするために、理解しておく必要がある概念および手順について説明します。
- UNIX エンドポイントのインストールおよびカスタマイズ（107 ページ） - この更新された章では、CA Access Control UNIX エンドポイントをインストールするために、理解しておく必要がある概念および手順について説明します。
- CA Enterprise Log Manager との統合（179 ページ） - この更新された章では、CA Access Control エンタープライズ管理 を CA Enterprise Log Manager と統合するために、理解しておく必要がある概念および手順について説明します。
- エンタープライズ レポート機能の実装（201 ページ） - この更新された章では、CA Access Control エンタープライズ管理 にレポート機能を追加するために、理解しておく必要がある概念および手順について説明します。

- UNAB ホストのインストールとカスタマイズ（213 ページ） - この新しい章では、UNAB エンドポイントをインストールするために、理解しておく必要がある概念および手順について説明します。
- 拡張ポリシー管理環境への PMD の移行（295 ページ） - この更新された章では、簡略化された移行プロセスについて説明します。

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

本書では、CA Access Control Premium Edition のさまざまなコンポーネントを計画し、インストールし、さらにカスタマイズする方法について説明します。 対象となるコンポーネントは、Windows および UNIX 用の CA Access Control サーバおよびエンドポイント、CA Access Control エンドポイント管理 コンポーネントなどです。 エンタープライズ管理およびレポートのインストールに関する章は、CA Access Control Premium Edition にのみ該当します。

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: 実装計画

このセクションには、以下のトピックが含まれています。

セキュリティ システムの計画

セキュリティ システムの第一の目標は、組織の情報資産を保護することです。 効果的なセキュリティを実装するには、サイトに存在する脅威を認識する必要があります。 さらに、その脅威に対して最も効果的にサイトを保護できるように、CA Access Control の実装方法を決定する必要があります。

コンピュータ リソースの不正使用を防止するには、以下の 2 つの基本的な方法があります。

- 権限のないユーザによるシステムへのアクセスをブロックする
- アクセス権を持つユーザに対して特定の機密情報へのアクセスをブロックする

CA Access Control には、この両方の方法でシステムを保護するツールが用意されています。 ユーザのアクティビティをトレースして、コンピュータ システムの不正使用の試みを追跡する監査ツールもあります。

サイトに対する脅威に基づいてセキュリティ プロジェクトの目標を決定すれば、セキュリティ ポリシー ステートメントを作成して、実装チームを編成できます。 この実装チームは、セキュリティで保護する必要があるデータ、アプリケーション、およびユーザの決定に役立つ優先順位を確立する必要があります。

システム管理部門との連携

システム管理部門が CA Access Control の導入を決定しただけでは、サイトにおけるセキュリティが十分とは言えません。 セキュリティ プロジェクトの成功には、システム管理部門の積極的な関与が不可欠です。 システム管理部門は、セキュリティ ポリシー、手続き、セキュリティ機能に割り当てるリソース、およびコンピュータ システムのユーザの責任を決定する必要があります。 このようなシステム管理部門の支援がない場合、セキュリティの手続きは正しく使用されなくなり、単に管理上のわずらわしい作業となってセキュリティの効力が減少します。 このような状況は、セキュリティに関する誤解を生み、重大なセキュリティの脅威にさらされる危険を引き起こす原因となります。

セキュリティ管理者はシステム管理部門の協力を得て、明確で包括的なセキュリティ ポリシー ステートメントを準備する必要があります。 このステートメントには、以下の内容を含める必要があります。

- 正社員、パートタイマー、契約社員、およびコンサルタントに関する企業ポリシー
- システムを利用する外部ユーザに関する企業ポリシー
- システムを利用するすべてのユーザが求める動作
- 物理的な保護に関する考慮事項
- ユーザの各部門でのセキュリティ要件
- 監査上の要件

このような内容のセキュリティ ポリシーを作成することによって、CA Access Control の実装計画を、導入先のセキュリティ ポリシーに沿った現実的なものにすることができます。

実装計画の準備

実装計画の作成時に、計画の目標がセキュリティ ポリシーに沿っていることを繰り返し確認します。 新しいセキュリティ コントロールは、ユーザに適応期間を与えるために、段階的に導入する必要があります。

CA Access Control を実装するために、プロトタイプとしてユーザのパイロット グループを定義します。 テスト段階では、このパイロット グループに属しているビジネス データ、ジョブ、およびユーザが CA Access Control によって保護されます。 このパイロット グループでの CA Access Control のすべての機能をテストしてから、グループ以外のエンティティを保護します。 パイロット グループでのテストは、他の組織を保護する方法を理解するのに役立ちます。

実装チームは、保護する対象を決定するほか、現在の作業への影響を最小限に抑えながら新しいセキュリティ コントロールを導入する方法を考える必要があります。 実装計画では、さまざまなリソースやクラスに対するアクセスを制限せずにアクセスの監査のみを行う期間を考慮する必要があります。 この監査期間に作成される監査レコードによって、どのユーザがどのリソースにアクセスする必要があるか、傾向を確認できます。

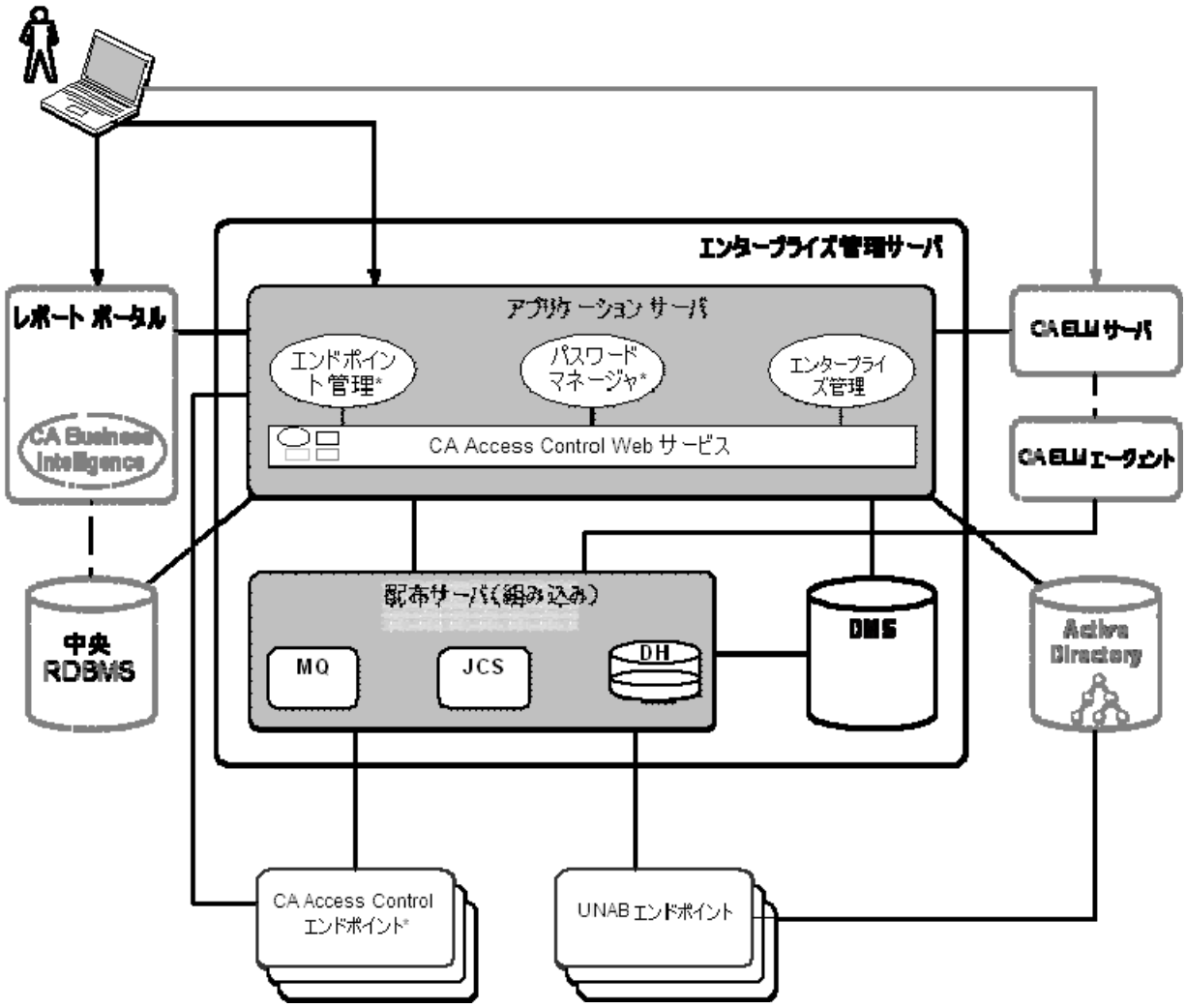
保護方法の決定

CA Access Control をインストールする前に、CA Access Control で使用する機能を決定する必要があります。 使用できるものは、以下のとおりです。

- CA Access Control を使用して、ネイティブ セキュリティを実装できます。 この場合は、CA Access Control エンドポイント管理 を使用して、すでに使い慣れているセキュリティ機能を実装できます。
- Policy Model データベース(PMDB)を使用し、ユーザ、グループ、およびアクセス ルールが定義されているセキュリティ データベースの情報をサブスクライバの集合に伝達できます。 PMDB は、受け取ったすべての更新情報を定期的にサブスクライバに伝達します。 このメカニズムによって、システム管理者の負担が大幅に軽減されます。
- 拡張ポリシー管理を使用し、企業に対して作成した複数ルールのポリシー(スクリプト ファイル)をデプロイできます。 このポリシー ベースの方法により、バージョン制御ポリシーの作成、エンタープライズ環境のホスト グループへのポリシーの割り当ておよび割り当て解除、デプロイ済みポリシーの直接デプロイおよび削除(デプロイ解除)、デプロイ ステータスおよびデプロイの偏差の確認などが可能になります。
- より高度な攻撃を防御するために CA Access Control を使用し、ネイティブ セキュリティを大幅に強化できます。 CA Access Control により、以下のことができます。
  - 特権アカウントの権限を制限する
  - 特別なユーザのユーザ パスワードを変更する機能など、特別な権限を一般ユーザに割り当てる
  - NTFS、FAT、および CDFS などの複数のファイル システムをサポートする
  - Windows および UNIX の両システムを含む異機種環境でセキュリティ ポリシーと監査を一元化する

エンタープライズ デプロイ アーキテクチャ

以下の図は、企業での CA Access Control のデプロイ方法について示したものです。



注: アスタリスク(*)の付いた CA Access Control コンポーネントは、CA Access Control および CA Access Control Premium Edition の両方で利用可能です。 その他のすべてのコンポーネントは CA Access Control Premium Edition においてのみ利用可能です。

エンタープライズ管理サーバ

エンタープライズ管理サーバは集中管理サーバで、エンドポイントへのポリシーのデプロイ、特権アカウントの管理、リソース、アクセサ、およびアクセス レベルの定義を行うためのコンポーネントやツールが含まれています。 エンタープライズ管理サーバには、エンタープライズ管理サーバ、エンドポイント、他のコンポーネント間の通信を管理するコンポーネントも含まれています。

エンタープライズ管理サーバをインストールすると、CA Access Control がサイレント インストールされます。 CA Access Control はエンタープライズ管理サーバを保護し、エンタープライズ管理サーバのアプリケーションをサポートするコア機能を提供します。

エンドポイント

CA Access Control を企業内で展開する場合、2 つのタイプのエンドポイントがあります。

- CA Access Control エンドポイント - CA Access Control をインストールしたエンドポイント。

  CA Access Control エンドポイントは、オプションで、PUPM エンドポイントとして設定することも可能です。

- UNAB エンドポイント - UNIX 認証ブローカ(UNAB)をインストールした UNIX エンドポイント。

  UNAB では、Active Directory データ ストアに格納されているクレデンシャルを使用して、ユーザを UNIX コンピュータにログインさせることができます。 これは、すべてのユーザに対して単一のデータ ストアを使用できることを意味します。ユーザは同じユーザ名とパスワードですべてのプラットフォームにログインできます。

レポート ポータル

レポート ポータルは CA Access Control レポートを表示します。

CA Access Control レポートは、各エンドポイントにある CA Access Control データベース内のデータに関する情報を提供します。データに関する情報とは、エンドポイントにデプロイしたルールやポリシー、およびそれらのルールやポリシーからの偏差です。CA Access Control レポートは CA Business Intelligence で表示します。

中央の RDBMS には、CA Access Control レポートで使用されるエンドポイント データが格納されています。

セントラル RDBMS

セントラル RDBMS には以下が格納されています。

- CA Access Control レポートで使用するエンドポイント データ
- Web ベース アプリケーションのセッション データ
- Web ベース アプリケーションのユーザ データ(ユーザ ストアとして Active Directory を使用しない場合)

注: Web ベースのアプリケーションは、CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、および CA Access Control パスワード マネージャです。

CA Enterprise Log Manager コンポーネント

各エンドポイントの CA Access Control 監査イベントを、収集およびレポート用に CA Enterprise Log Manager に送信できます。 以下のコンポーネントは、CA Access Control と CA Enterprise Log Manager の統合をサポートしています。

- CA Enterprise Log Manager エージェント - 配布サーバ上の監査キューから監査イベントを収集し、CA Enterprise Log Manager サーバに処理用に送信します。
- CA Enterprise Log Manager サーバ - 監査イベントを受信し、場合によっては抑制および集約ルールを適用後に、イベントを格納します。

注: CA Enterprise Log Manager コンポーネントの詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

Active Directory

Active Directory で定義されているグループとユーザを使用するように CA Access Control と CA Access Control Web ベース アプリケーションを設定できます。 これは、単一のデータ ストアをすべてのユーザに対して使用できることを意味します。

注: Web ベースのアプリケーションは、CA Access Control エンタープライズ管理、CA Access Control エンドポイント管理、および CA Access Control パスワード マネージャです。

CA Access Control の実装方法

組織に CA Access Control を実装する前に、インストールするコンポーネント、インストールの順序、インストール先について理解しておく必要があります。 CA Access Control を組織に展開する際は、以下のガイドラインに従ってください。

- 実装プロセスは、上位から下位へと進めてください。 最初に CA Access Control エンタープライズ管理 をインストールし、次に、CA Access Control エンドポイントをインストールします。
- 実装を開始する前に、使用するコンピュータが必要な仕様を満たし、前提条件となるソフトウェアがすべてインストールされていることを確認してください。

  注: ハードウェアとソフトウェアの要件の詳細については、リリース ノートを参照してください。

CA Access Control を実装するには、以下の手順を実行します。

1. CA Access Control のコンポーネント、各コンポーネントの機能、ほかの CA Access Control コンポーネントとの相互依存性を確認します。 インストール対象の CA Access Control コンポーネント、インストール先、インストールの順序を確認します。
2. エンタープライズ管理サーバを準備します。
3. エンタープライズ管理サーバ上に CA Access Control エンタープライズ管理 をインストールします。
4. CA Access Control エンタープライズ管理 を起動します。

   この手順で、CA Access Control エンタープライズ管理 が正常にインストールされたことを確認します。
5. （オプション） 別のサーバ上に、配布サーバの別のインスタンスをインストールします。

   CA Access Control 用にフェールオーバ ソリューションを実装するには、2 つ以上のサーバに配布サーバをインストールします。
6. エンドポイントをインストールします。

詳細情報:

エンタープライズ管理サーバの準備方法 (49 ページ)
CA Access Control エンタープライズ管理 のインストール (51 ページ)
CA Access Control エンタープライズ管理 を起動します。 (60 ページ)
CA Access Control エンタープライズ管理 を開く (61 ページ)

保護するポリシー オブジェクトの決定

以下のセクションでは、企業のアプリケーションおよびデータへのアクセスを許可するセキュリティ ポリシーによって使用される重要なオブジェクトについて説明します。

ユーザ

CA Access Control には、複数のユーザ タイプがあります。 ユーザ タイプごとに一定レベルの権限と一定の制限が設定されます。 組織のセキュリティ ポリシーを作成する作業には、特別な権限とそれを与えるユーザを決定する作業が含まれます。

CA Access Control では、ユーザがログオンできる回数や実行される監査の種類など、ユーザに関する情報を格納します。 ユーザに関する情報は、データベース レコードのプロパティに格納されます。

注: ユーザの詳細については、「エンドポイント管理ガイド」を参照してください。

ユーザ タイプ

CA Access Control は、以下のユーザ タイプをサポートしています。

一般ユーザ

社内のエンド ユーザ - 組織のビジネスを遂行する人たち。 システムに対する一般ユーザのアクセス権は、ネイティブ OS および CA Access Control の両方で制限できます。

特別な権限を持つユーザ(サブ管理者)

1 つ以上の特定の管理タスクを実行する権限が与えられた一般ユーザ。 一般ユーザに対して特定の管理機能の実行を許可すると、管理者の負荷を軽減できます。 CA Access Control では、これを「タスクの委任」といいます。

管理者

ネイティブ OS および CA Access Control 内で最上位の権限を持つユーザ。 管理者は、ユーザの追加、削除、および更新のほか、ほとんどすべての管理タスクを実行できます。 CA Access Control では、ネイティブ スーパーユーザの権限を制限できます。 そのアカウントが自動的に認識されない特定のユーザに管理タスクを割り当てることができます。 これは、どのユーザが管理タスクを実行するかが、侵入者にはただちに明らかにはならないことを意味します。

グループ管理者

ある特定のグループ内で、ユーザの追加、削除、更新など、ほとんどの管理者機能を実行できるユーザ。 制限された特定の権限を持つこのユーザ タイプは、ネイティブ Windows にはありません。

パスワード管理者

他のユーザのパスワード設定を変更する権限を持つユーザ。 パスワード管理者は、他のユーザの属性は変更できません。 このユーザ タイプは、ネイティブ OS にはありません。

グループ パスワード管理者

ある特定のグループ内で、他のユーザのパスワード設定を変更する権限を持つユーザ。 グループ パスワード管理者は、グループ内のユーザの、その他の設定を変更することはできません。 このユーザ タイプは、ネイティブ OS にはありません。

監査担当者

監査ログの読み取り権限を持つユーザ。 ログインやリソースへのアクセスが試みられたときに実行する監査の種類を決定する権限もあります。 このユーザ タイプは、ネイティブ OS にはありません。

グループ監査担当者

グループに関連する監査ログの読み取り権限を持つユーザ。 ある特定のグループ内で行う監査の種類を決定する権限もあります。 このユーザ タイプは、ネイティブ OS にはありません。

オペレータ

データベース内のすべての情報の表示（読み取り）、CA Access Control トレースの管理など、secons ユーティリティを使用したタスクの実行、および実行時統計情報の表示が可能なユーザ。 このユーザ タイプは、ネイティブ OS にはありません。

注: secons 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。

グループ オペレータ

データベースの、自分が定義されているグループに関するすべての情報を表示できるユーザ。 このユーザ タイプは、ネイティブ OS にはありません。

サーバ

実際にはプロセスである特別なタイプのユーザ。他のユーザの権限をリクエストすることが許可されています。

タイプの割り当て

CA Access Control 内では、1 つ以上の権限属性をユーザに割り当てることによって、特別なユーザを作成します。 これらの属性の名前は、システム レベルでは ADMIN、AUDITOR、PWMANAGER、OPERATOR、SERVER、グループ レベルでは GROUP-ADMIN、GROUP-AUDITOR、GROUP-PWMANAGER、GROUP-OPERATOR です。

詳細情報:

権限属性(31 ページ)

セキュリティ ポリシーとユーザ

組織のセキュリティ ポリシーを作成する際は、以下のことを決定する必要があります。

- 定義するユーザ
- 定義済みユーザに付与する特殊な権限(存在する場合)
- 定義済みユーザに許可する、グローバル権限属性およびグループ権限属性

  たとえば、システム管理者、グループ管理者、パスワード管理者、グループ パスワード管理者、監査担当者、オペレータとして定義するユーザを決定する必要があります。

グループ

グループは、通常、同一のアクセス権限を共有するユーザの集合です。 管理者は、グループへのユーザの追加、グループからのユーザの削除、およびシステム リソースへのアクセスをグループ単位で許可または拒否することができます。 このタイプのグループは、ネイティブ OS および CA Access Control の両方に存在します。

グループ レコードには、グループに関する情報が格納されます。 グループ レコードに格納される最も重要な情報は、グループのメンバであるユーザのリストです。

重要: グループ レコードのアクセス権限ルールは、グループの階層内の各ユーザに繰り返し適用されます。

たとえば、グループ A には、ユーザ X とグループ B という 2 つのメンバがあります。ユーザ Y はグループ B のメンバです。 ユーザがグループ A の権限ルールを変更する場合、CA Access Control は変更された権限ルールをグループ A 階層内のすべてのユーザおよびグループ、すなわち、ユーザ X、グループ B、ユーザ Y に適用します。

グループ レコードの情報はプロパティに格納されます。

CA Access Control では、グループ管理者は、グループ管理者が定義されている特定のグループのグループ機能を管理できます。 グループ パスワード管理者は、グループ メンバのパスワードを変更できます。

セキュリティ ポリシーとグループ

組織のセキュリティ ポリシーを作成する際は、以下のことを決定する必要があります。

- セキュリティ管理を目的として作成するグループ
- 各グループに追加するユーザ
- グループ管理者とグループ パスワード管理者を定義するかどうか、定義する場合はこれらの管理者の役割を割り当てるユーザ

事前定義されたユーザのグループ

CA Access Control には事前定義されたグループがあり、そのグループにユーザを追加することができます。 このようなグループの 1 つが、_restricted グループです。 _restricted グループのユーザのファイルとレジストリ キーは、すべて CA Access Control によって保護されます。 ファイルまたはレジストリ キーのアクセス ルールが明示的に定義されていない場合は、そのクラス(FILE または REGKEY)の _default レコードがアクセス権に適用されます。

_restricted グループにユーザを追加する方法は、他のグループにユーザを追加する場合と同じです。 たとえば、selang のコマンドを使用して pjones を _restricted グループに追加するには、プロンプトに以下のように入力します。

```
join pjones group(_restricted)
```

データベースで管理されていないファイルについては、このコマンドによって、FILE クラスの _default レコードで許可されているアクセス権(ある場合)のみが pjones に与えられます。

注: _restricted グループを使用する場合は、注意が必要です。 _restricted グループ内のユーザは、業務の遂行に必要な十分な権限を与えられていない場合があります。 このため、ユーザを _restricted グループに追加する場合は、最初に警告モードの使用を検討してください。 Warning モードでは、ユーザが業務を遂行するために必要なファイルおよびレジストリ キーを監査ログによって知ることができます。 監査ログの確認後、適切な権限を付与し、Warning モードをオフに切り替えます。

リソース アクセス用に事前定義されたグループ

CA Access Control に事前定義されている他のタイプのグループは、特定のリソースに対するアクセスの許可または禁止を定義します。 以下のグループが事前定義されています。

- _network

  _network グループは、ネットワークから特定のリソースへのアクセスを定義します。すべてのユーザは、このグループのメンバとして扱われます。つまり、ユーザをこのグループに明示的に追加する必要はありません。

  たとえば、特定のリソースの読み込みをネットワークからのみに限定できます。selang のコマンドを使用して、以下のように新規リソースを定義します。

  ```
  newres FILE ¥temp¥readonly
  ```

  次に、ネットワークから可能なアクセスを指定します。

  ```
  authorize FILE ¥temp¥readonly gid(_network) access(read)
  ```

  この指定は、CA Access Control エンドポイント管理 を使用して行うこともできます。

  ネットワークから ¥temp¥readonly にアクセスする場合、他の方法によるファイルへの明示的なアクセス権限がない限り、ユーザはこのファイルの読み込みのみを実行できます。

- _interactive

  _interactive グループは、特定のリソースが存在するコンピュータから、そのリソースに対するアクセス許可を定義します。 たとえば、ファイルに対する読み取りアクセス権を与える場合、このリソースに対してネットワークからのアクセスが許可されていない場合でも、ファイルが定義されているコンピュータからのアクセス権を与えることができます。

以下の点に注意してください。

- CA Access Control では、_network グループと _interactive グループの間に関係はありません。 これは、ネットワークから特定のリソースへのアクセスを定義するルールが、_network グループに存在し、 同時に、_interactive グループ内の他のルールで、同じリソースに対するアクセスを定義できる、ということを意味します。
- _network グループと _interactive グループにユーザを追加する必要はありません。
- これらのグループによって、データベースに定義されているすべての Windows リソースを保護できます。

リソース

セキュリティ ポリシーで最も重要なことは、保護を必要とするシステム リソースを決定し、リソースに設定する保護の種類を定義することです。

権限属性

権限属性は、データベース内のユーザ レコードに設定するプロパティです。権限属性によって、一般ユーザが実行できない操作をユーザに許可します。 権限属性には、グローバルとグループの 2 種類があります。 各グローバル権限属性によって、ユーザはデータベース内のレコードに対して特定の種類の機能を実行できます。 グループ権限属性によって、ユーザは指定した 1 つのグループ内で、特定の種類の機能を実行できます。 グローバル権限属性とグループ権限属性の機能と制限については、以下のセクションで説明します。

グローバル権限属性

自分のユーザ レコードにグローバル権限属性が設定されているユーザは、データベース内の関連するレコードに対して特別な機能を実行できます。 グローバル権限属性は、以下のとおりです。

- ADMIN
- AUDITOR
- OPERATOR
- PWMANAGER
- サーバ
- IGN_HOL

注: グローバル権限属性の詳細については、「エンドポイント管理ガイド」を参照してください。

グループ権限属性

自分のユーザ レコードにグループ権限属性が設定されているユーザは、指定されたグループ内で特別な機能を実行できます。 グループ権限属性は、以下のとおりです。

- GROUP-ADMIN
- GROUP-AUDITOR
- GROUP-OPERATOR
- GROUP-PWMANAGER

注: グローバル権限属性の詳細については、「エンドポイント管理ガイド」を参照してください。

B1 セキュリティ機能

Trusted Computer System Evaluation Criteria（TCSEC）は、米国政府によるコンピュータ セキュリティに関する基準です。 一般には、「Orange Book」と呼ばれています。 基準のレベル B1 では、ラベル付けセキュリティによる強制的保護セキュリティを規定しています。

CA Access Control は、以下に示す「Orange Book」の B1 機能を備えています。

- セキュリティ レベル
- セキュリティ カテゴリ
- セキュリティ ラベル

B1 セキュリティ機能を管理するには、selang または CA Access Control エンドポイント管理 を使用します。

セキュリティ レベル

セキュリティ レベルのチェックを有効にすると、CA Access Control は他の権限チェックに加えて、セキュリティ レベルのチェックを実行します。 セキュリティ レベルは、ユーザおよびリソースに割り当てることができる 1 から 255 までの正の整数です。 セキュリティ レベルが割り当てられているリソースに対してユーザがアクセスを要求すると、CA Access Control では、そのリソースのセキュリティ レベルとユーザのセキュリティ レベルが比較されます。 ユーザのセキュリティ レベルがリソースのセキュリティ レベルと同じか、それより上である場合、CA Access Control では他の権限チェックが続行されます。 リソースのセキュリティ レベルより下の場合、リソースへのユーザのアクセスは拒否されます。

SECLABEL クラスがアクティブな場合は、リソースとユーザのセキュリティ ラベルに関連付けられているセキュリティ レベルが使用され、リソース レコードおよびユーザ レコードに明示的に設定されているセキュリティ レベルは無視されます。

セキュリティ レベルのチェックを使用してリソースを保護するには、セキュリティ レベルをリソースのレコードに割り当てます。 newres コマンドまたは chres コマンドの level パラメータによって、セキュリティ レベルをリソースに割り当てます。

セキュリティ レベルのチェックで保護されているリソースに対してユーザのアクセスを許可するには、セキュリティ レベルをユーザのレコードに割り当てます。 newusr コマンドまたは chusr コマンドの level パラメータによって、セキュリティ レベルをユーザに割り当てます。

セキュリティ レベルのチェックの有効化および無効化

セキュリティ レベルのチェックを有効にするには、以下の setoptions コマンドを実行します。

```
setoptions class+ (SECLEVEL)
```

セキュリティ レベルのチェックを無効にするには、以下の setoptions コマンドを実行します。

```
setoptions class-(SECLEVEL)
```

セキュリティ カテゴリ

セキュリティ カテゴリ チェックを有効にすると、CA Access Control では、他の権限チェックに加えて、セキュリティ カテゴリ チェックが実行されます。 1 つ以上のセキュリティ カテゴリが割り当てられているリソースに対してユーザがアクセスを要求すると、CA Access Control では、そのリソース レコードのセキュリティ カテゴリのリストとユーザ レコードのセキュリティ カテゴリのリストが比較されます。 リソースに割り当てられたすべてのカテゴリがユーザのカテゴリ リストに含まれている場合は、他の権限チェックが続行されます。含まれていない場合は、リソースに対するユーザのアクセスは拒否されます。

SECLABEL クラスがアクティブな場合は、リソースとユーザのセキュリティ ラベルに関連付けられているセキュリティ カテゴリのリストが使用され、ユーザ レコードおよびリソース レコード内のカテゴリのリストは無視されます。

セキュリティ カテゴリのチェックによってリソースを保護するには、1 つ以上のセキュリティ カテゴリをリソースのレコードに割り当てます。 newres コマンドまたは chres コマンドの category パラメータによって、セキュリティ カテゴリをリソースに割り当てます。

セキュリティ カテゴリのチェックで保護されているリソースに対して、ユーザのアクセスを許可するには、1 つ以上のセキュリティ カテゴリをユーザのレコードに割り当てます。 newusr コマンドまたは chusr コマンドの category パラメータによって、セキュリティ カテゴリをユーザに割り当てます。

セキュリティ カテゴリ チェックの有効化および無効化

セキュリティ カテゴリのチェックを有効にするには、以下の setoptions コマンドを実行します。

```
setoptions class+ (CATEGORY)
```

セキュリティ カテゴリのチェックを無効にするには、以下の setoptions コマンドを実行します。

```
setoptions class-(CATEGORY)
```

セキュリティ カテゴリの定義

セキュリティ カテゴリは、CATEGORY クラスのリソースを設定することによって定義します。 セキュリティ カテゴリを定義するには、以下のように selang の newres コマンドを実行します。

```
newres CATEGORY name
```

name にはセキュリティ カテゴリの名前を指定します。

たとえば、Sales というセキュリティ カテゴリを定義するには、以下のコマンドを入力します。

```
newres CATEGORY Sales
```

Sales および Accounts というセキュリティ カテゴリを定義するには、以下のコマンドを入力します。

```
newres CATEGORY (Sales,Accounts)
```

セキュリティ カテゴリの一覧表示

データベースに定義されているすべてのセキュリティ カテゴリを一覧表示するには、以下のように find コマンドを実行します。

```
find class(CATEGORY)
```

セキュリティ カテゴリの削除

CATEGORY クラスからレコードを削除することによって、セキュリティ カテゴリを削除できます。 セキュリティ カテゴリを削除するには、以下の rmres コマンドを実行します。

```
rmres CATEGORY name
```

name にはセキュリティ カテゴリの名前を指定します。

たとえば、Sales というセキュリティ カテゴリを削除するには、以下のコマンドを入力します。

```
rmres CATEGORY Sales
```

セキュリティ ラベル

セキュリティ ラベルは、特定のセキュリティ レベルと 0 個以上のセキュリティ カテゴリとの関係を表します。

セキュリティ ラベル チェックを有効にすると、CA Access Control では他の権限チェックに加えて、セキュリティ ラベル チェックが実行されます。 セキュリティ ラベルが割り当てられているリソースへのアクセスをユーザが要求すると、CA Access Control では、そのリソース レコードのセキュリティ ラベルに指定されているセキュリティ カテゴリのリストと、ユーザ レコードのセキュリティ ラベルに指定されているセキュリティ カテゴリのリストが比較されます。 リソースのセキュリティ ラベルに割り当てられたすべてのカテゴリがユーザのセキュリティ ラベルに含まれている場合、CA Access Control では、セキュリティ レベルのチェックが続行されます。含まれていない場合は、リソースに対するユーザのアクセスは拒否されます。

その後、リソース レコードのセキュリティ ラベルに指定されているセキュリティ レベルと、ユーザ レコードのセキュリティ ラベルに指定されているセキュリティ レベルが比較されます。 ユーザのセキュリティ ラベルに割り当てられたセキュリティ レベルがリソースのセキュリティ ラベルに割り当てられたセキュリティ レベルと同じか、それより上である場合、CA Access Control では他の権限チェックが続行されます。リソースのセキュリティ レベルより下の場合は、リソースに対するユーザのアクセスは拒否されます。

セキュリティ ラベルのチェックが有効になっている場合、ユーザ レコードおよびリソース レコードに指定されているセキュリティ カテゴリとセキュリティ レベルは無視されます。セキュリティ ラベルの定義に指定されているセキュリティのレベルとカテゴリのみが使用されます。

セキュリティ ラベル チェックによってリソースを保護するには、セキュリティ ラベルをリソースのレコードに割り当てます。

セキュリティ ラベルのチェックで保護されているリソースに対して、ユーザのアクセスを許可するには、セキュリティ ラベルをユーザのレコードに割り当てます。

セキュリティ ラベル チェックの有効化および無効化

セキュリティ ラベルのチェックを有効にするには、以下の setoptions コマンドを実行します。

```
setoptions class+ (SECLABEL)
```

セキュリティ ラベルのチェックを無効にするには、以下の setoptions コマンドを実行します。

```
setoptions class-(SECLABEL)
```

セキュリティ ラベルの定義

セキュリティ ラベルは、SECLABEL クラスのリソースを設定することによって定義できます。 セキュリティ ラベルを定義するには、以下の newres コマンドを実行します。

```
newres SECLABEL name ¥
category(securityCategories) ¥
level(securityLevel)
```

各項目の説明:

name

セキュリティ ラベルの名前を指定します。

securityCategories

セキュリティ カテゴリのリストを指定します。 複数のセキュリティ カテゴリを指定する場合は、スペースまたはカンマを使用して各セキュリティ カテゴリの名前を区切ります。

注: セキュリティ ラベルを定義する前に、CATEGORY クラスのセキュリティ カテゴリを定義する必要があります。

securityLevel

セキュリティ レベルを指定します。 1 から 255 までの整数を指定します。

例: セキュリティ ラベルの定義

以下の例では、セキュリティ カテゴリ Sales と Accounts を含み、セキュリティ レベルが 95 の、Managers という名前のセキュリティ ラベルを定義します。

```
newres SECLABEL Manager category(Sales,Accounts) level(95)
```

セキュリティ ラベルの一覧表示

データベースで定義されているすべてのセキュリティ ラベルのリストを表示するには、以下のように find コマンドを実行します。

```
find class(SECLABEL)
```

セキュリティ ラベルの削除

SECLABEL クラスからレコードを削除することによって、セキュリティ ラベルを削除できます。 セキュリティ ラベルを削除するには、以下の rmres コマンドを実行します。

```
rmres SECLABEL name
```

name にはセキュリティ ラベルの名前を指定します。

たとえば、Managers というセキュリティ ラベルを削除するには、以下のコマンドを入力します。

```
rmres SECLABEL Managers
```

警告期間の使用方法

実装チームは、保護する対象を決定するほか、新しいセキュリティ コントロールを導入する方法を考える必要があります。 現在進行中の業務への影響を最小限に抑えるには、アクセス制約を適用するのでなく、リソースアクセスの監視のみを行う初期期間の実施を考慮する必要があります。

アクセスを監視するには、リソースを警告モードに設定します。 リソースまたはクラスに対する警告モードが有効になっていて、ユーザ アクセスがアクセス制約に違反したとき、CA Access Control では監査ログに警告メッセージが記録され、ユーザにリソースへのアクセスが許可されます。

注: 警告モードを使用する場合は、監査ログの最大サイズを増やすことを検討してください。 警告モードの詳細については、「エンドポイント管理ガイド」を参照してください。

スタッフの教育とトレーニング

セキュリティ管理者の仕事には、CA Access Control のインストール時に混乱なく作業を進めるために必要な知識をシステム ユーザに伝える仕事があります。

各ユーザが CA Access Control に関してどの程度詳しく理解する必要があるかは、そのユーザに使用を許可する機能によって異なります。 たとえば、システム ユーザのタイプによって、以下のような情報が必要になります。

- データベースで定義されているすべてのユーザ
  - ユーザ名とパスワードを使用してシステムにユーザ認証を求める方法、およびパスワードの変更方法を理解している必要があります。 システム セキュリティに対するパスワードの重要性を認識していることも必要です。
  - パスワード ポリシーのチェックを実装する場合は、パスワード マネージャについてもよく理解している必要があります。
  - 同時ログインを無効にする secons -d- および有効にする secons d+ コマンドを知っている必要があります。 同時ログインとは、1 人のユーザが複数の端末から同時に 1 つのシステムにログインして開始した複数のセッションのことです。
  - 一部のユーザは sesudo コマンドを実行する可能性があります。このコマンドを使用すると、事前定義されたアクセス ルール（パスワード チェックが含まれるかどうかは場合による）に基づいて代理ユーザになることができます。
- 技術サポート担当

  CA Access Control をインストールするユーザは、移行に関する考慮事項と、CA Access Control のインストールまたは再インストールに必要な手順をよく理解している必要があります。 データベースのメンテナンスを行うユーザは、データベース ユーティリティをよく理解しておく必要があります

  注: データベース ユーティリティの詳細については、「リファレンス ガイド」の「dbmgr」を参照してください。
- グループ管理者

  グループ権限のいずれかが割り当てられたユーザ、グループ属性（GROUPADMIN など）が割り当てられたユーザ、またはグループ レコードを所有するユーザには、グループ情報（28 ページ）が必要です。

  注: グループの詳細については、「selang リファレンス ガイド」の「group selang」コマンドの説明を参照してください。

- 監査担当者

  AUDITOR 属性が割り当てられたユーザは、監査ツール（CA Access Control エンドポイント管理 および seaudit ユーティリティ）をよく理解しておく必要があります。

  注: seaudit 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。

- 未承認アプリケーションを作成するプログラマ

  プログラマは、作成するアプリケーションで CA Access Control* 関数ライブラリを使用して、保護されているリソースへのアクセスの制御（SEOSROUTE_RequestAuth 関数を使用して）など、セキュリティに関連するサービスを要求できます。 また、インストール先では、インストール先定義のリソース クラスを作成できます。 導入先でこれらのリソース クラスのレコードを作成した場合、アプリケーションで SEOSROUTE_RequestAuth コマンドを発行して、アクションを完了するための十分な権限がユーザにあるかどうかをチェックできます。 特定のユーザ アクションに必要な権限のレベルは、そのアプリケーションが SEOSROUTE_RequestAuth 関数を呼び出す方法に従って決定されます。

  注: CA Access Control API の詳細については、「SDK 開発者ガイド」を参照してください。

- 承認済みアプリケーションを作成するプログラマ

  承認済みアプリケーション（SERVER 属性で実行するプログラム）を作成するプログラマは、CA Access Control* 関数ライブラリを使用して、セキュリティに関連する以下のサービスを要求できます。

  - ユーザの識別と検証
  - ユーザ ログアウト サービス
  - ユーザ認証要求

実装に関するヒント

このセクションでは、CA Access Control のインストール後に考慮すべき、実装に関するその他の情報を示します。

セキュリティの種類

サイトのセキュリティは、以下のアプローチのいずれかに従って処理できます。

- 明示的に許可されていないものはすべて禁止する。 これは理想的なアプローチですが、実装時に使用することは不可能です。 システムで行われることを許可するルールがないため、システムでは、アクセス ルールを定義しようとするすべての試みがブロックされます。 これは、イグニッションにキーを入れたまま、車から締め出されたような状態です。
- 明示的に禁止されていないものはすべて許可する。 このアプローチでは、セキュリティが低下する場合がありますが、セキュリティ システムを実装する上で、実用的な方法です。

CA Access Control では、第 2 のアプローチで開始し、アクセス ルールが定義された後に、第 1 のアプローチに切り替えます。 デフォルト アクセス(defaccess)ルールおよびユニバーサル アクセス(_default)ルールを使用すると、アプローチを定義し、いつでも保護ポリシーを切り替えることができます。

アクセサ

アクセサとは、リソースにアクセスできるエンティティのことです。 最も一般的なアクセサ タイプはユーザまたはグループです。つまり、アクセス権限の割り当ておよびチェックの対象となるユーザです。 プログラムがリソースにアクセスする際には、プログラムの所有者(ユーザまたはグループ)が「アクセサ」となります。 アクセサは、以下の 3 つのカテゴリに分類されます。

- 特定のユーザ名に関連付けられた要員
- アクセスする権限を持つグループのメンバである要員
- 特定のユーザ ID に関連付けられた運用プロセス

最も一般的なアクセサ タイプはユーザです。つまり、ログインを実行でき、アクセス権限の割り当ておよびアクセス権限のチェックを受ける要員です。 CA Access Control の最も重要な機能の 1 つは、アカウンタビリティです。 個々のアクションまたはアクセスの試みは、要求に対して責任を持つユーザの代わりに実行されます。

CA Access Control では、ユーザのグループを定義できます。 通常、ユーザは、プロジェクト、部、または課別にグループ化されます。 ユーザをグループ化することによって、セキュリティ管理に必要な作業量を大幅に削減することができます。

CA Access Control エンドポイント管理 または selang コマンドを使用して、ユーザやグループの新規定義、および既存のユーザやグループの変更を行うことができます。

リソース クラスとアクセス ルール

CA Access Control は、インストールされた直後に、システム イベントのインターセプト、およびリソースにアクセスするユーザ権限のチェックを開始します。 システム リソースに対するアクセスの制限方法と制限対象のリソースを CA Access Control に指示するまで、すべての権限チェックはアクセスを許可することになります。

保護対象のリソースのプロパティはリソース レコードに格納され、リソース レコードはクラスに分類されます。 リソース レコード内で最も重要な情報は、アクセス ルールです。アクセス ルールは、1 つ以上のリソースを操作する 1 つ以上のアクセサの権限を制御します。 アクセス ルールを定義するには、以下のいくつかの方法があります。

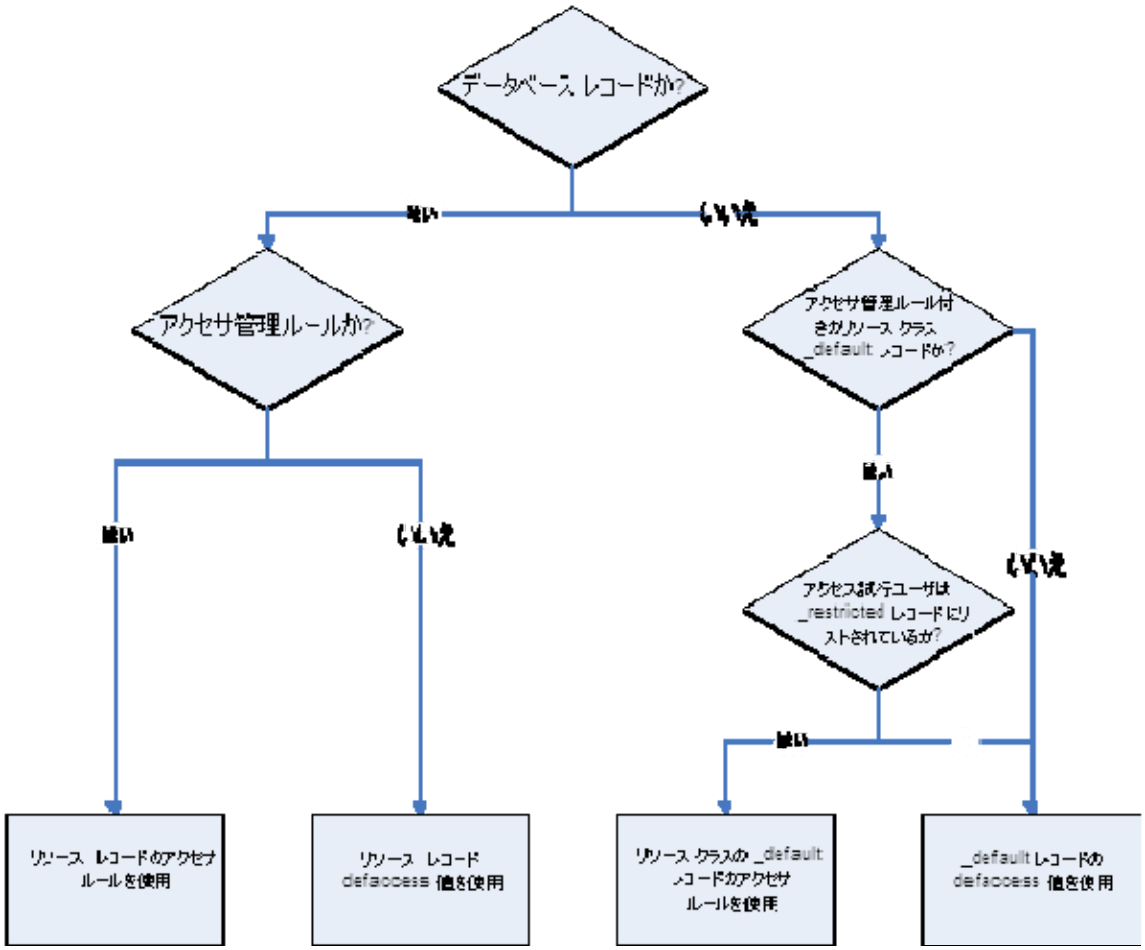
- Access Control List(リソースへのアクセス権を持つアクセサと、アクセサに実際に与えられるアクセス権を明示したリスト)。ACL ともいいます。
- Negative Access Control List(リソースへのアクセスが拒否されるアクセサを明示したリスト)。NACL ともいいます。
- リソースに対するデフォルト アクセス。ACL で明示的に定義されていないアクセサに対してアクセス ルールを指定します。
- ユニバーサル アクセス(クラスの _default レコード)。そのクラスの、特定のリソース レコードをまだ持たないリソースに対するアクセス権を指定します。
- プログラム アクセス制御リスト(PACL)。特定のプログラムを使用して、特定のアクセサに対するアクセス権を定義します。
- 条件付きアクセス制御リスト(CACL)。ある条件に基づいてアクセス権を与えます。たとえば、TCP レコードでは、特定のアクセサからの特定のリモート ホストに対するアクセス権を定義できます。
- Inet ACL。特定のポート経由の受信ネットワーク アクティビティに対するアクセス権を定義します。

defaccess と_default の使用方法

リソースへのアクセスが要求されると、その要求の処理方法を決定するために、以下の順序でデータベースが検索され、検出された最初のアクセス ルールが CA Access Control によって使用されます。 デフォルト アクセス(defaccess)と _default の違いに注意してください。

1. データベースにリソースのレコードがあり、そのレコードにアクセサを制御するルールが指定されている場合、CA Access Control はそのルールを使用します

2. データベースにレコードがあり、そのレコードにアクセサを制御するルールが指定されていない場合は、そのレコードのデフォルト アクセス ルール(defaccess 値)がアクセサに適用されます。
3. レコードが存在せず、リソース クラスの _default レコードにアクセサを制御するルールが指定されている場合、CA Access Control はそのルールを使用します。
4. レコードが存在せず、リソース クラスの _default レコードにアクセサを制御するルールが指定されていない場合、_default レコードのデフォルト アクセス ルール(defaccess 値)がアクセサに適用されます。 ファイルおよびレジストリ キーについては、この方法を _restricted ユーザ(29 ページ)のみに適用します。



注: リソース クラスおよびアクセス ルールの詳細については、「selang リファレンス ガイド」を参照してください。

第 3 章: エンタープライズ管理サーバのインストール

このセクションには、以下のトピックが含まれています。

環境アーキテクチャ

CA Access Control のエンタープライズ インストールでは、ポリシー、特権アカウント、UNAB エンドポイントの集中管理、各エンドポイントにデプロイされているポリシー情報の表示、および、エンドポイントのセキュリティ ステータスのレポートが可能です。 これらの機能は、Web ベース インターフェース、またはユーティリティによって管理できます。

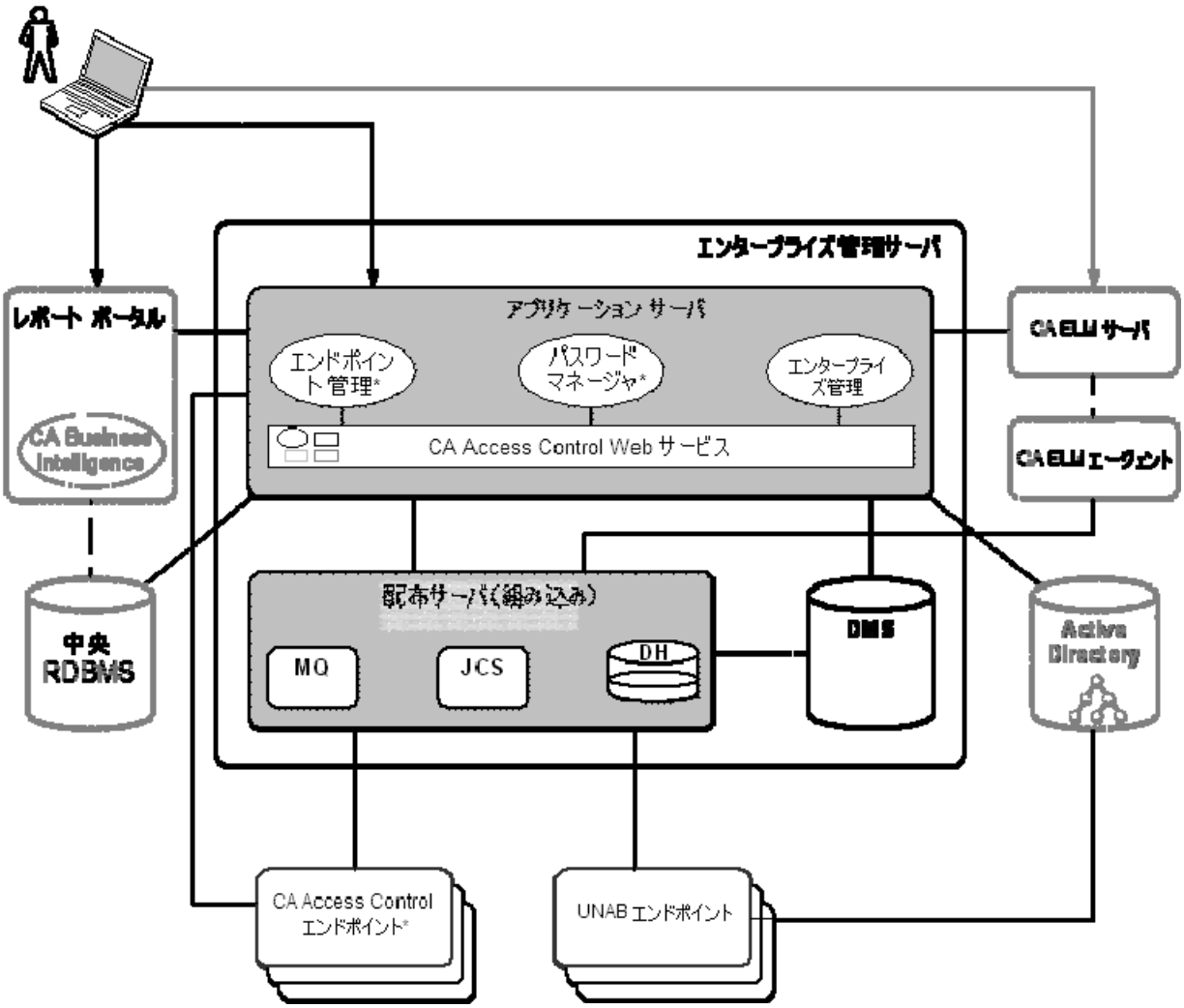
CA Access Control のエンタープライズ インストールを管理するには、中央コンピュータにエンタープライズ管理サーバをインストールし、組織に適合するように設定する必要があります。 エンタープライズ管理サーバには以下のコンポーネントが含まれています。

- デプロイ マップ サーバ (DMS)
- 配布サーバ
- Web ベースのアプリケーション

エンタープライズ管理サーバをインストールすると、CA Access Control がサイレント インストールされます。 CA Access Control はエンタープライズ管理サーバを保護し、エンタープライズ管理サーバのアプリケーションをサポートするコア機能を提供します。

エンタープライズ管理サーバをインストールした後、CA Access Control および UNAB エンドポイントをインストールし、設定する必要があります。 既存の CA Access Control エンドポイントがある場合、拡張ポリシー管理およびレポート用に、各エンドポイントを設定する必要があります。

次の図に、エンタープライズ管理サーバのアーキテクチャを示します。



デプロイ マップ サーバ(DMS)

DMS は、拡張ポリシー管理の中核となります。 DMS は、ポリシーに関する最新情報(ポリシーのバージョンおよびスクリプト)と、各コンピュータ上でのポリシー デプロイ ステータスを保持することを目的としています。 DMS には、ポリシーのバージョンが格納され、後から必要に応じてこれらのバージョンの割り当て、割り当て解除、デプロイ、およびデプロイ解除を行うことができます。

DMS は Policy Model ノードであり、データ リポジトリとして PMDB を使用します。 DMS は、 これが設定された各エンドポイントからの通知から受信したデータを収集し、これらのエンドポイントの各々のデプロイ情報を格納します。

配布サーバ

配布サーバは、アプリケーション サーバとエンドポイント間の通信を処理します。 配布サーバには次のコンポーネントが含まれています。

- 配布ホスト（DH）
- メッセージ キュー（MQ）
- Java 接続サーバ（JCS）

フェイルオーバのため、企業内で複数の配布サーバをインストールしたり、複数のコンピュータに配布サーバ コンポーネントをインストールしたりすることができます。 配布サーバは、デフォルトではエンタープライズ管理サーバ上にインストールされます。

分散ホスト（DH）

DH は、DMS で設定されたポリシー デプロイをエンドポイントに配布します。また、エンドポイントからでデプロイ ステータスを受信して、DMS に送信します。 このタスクを達成するために、DH は 2 つの Policy Model データベースを使用します。

- DH Writer - エンドポイントから受信したデータを DMS に書き込みます。

  この PMDB の名前は、DHNameWRITER です。ここで、DHName は DH の名前であり、デフォルトでは DH__ となります。

- DH Reader - DMS からデータを読み取り、エンドポイントがそのデータを取得できるようにします。

  この PMDB の名前は DHName です。ここで DHName は DH の名前であり、デフォルトでは、DH__ となります。

デフォルトでは、DH は 配布サーバと同じコンピュータにインストールされます。 ただし、複数の DH ノードをインストールし、各 DH に企業の 1 部門を管理させて、負荷を分散させることもできます。

メッセージ キュー

メッセージ キューは、エンタープライズ管理サーバと他のコンポーネント間で送受信されるメッセージを管理します。 メッセージ キューには、エンタープライズ管理サーバと通信する各クライアント コンポーネント専用の以下のキューがあります。

- レポート キュー - エンドポイント データベースのスケジュールされたスナップショットを受信します。

  レポート サービスは、スナップショットを使用して CA Access Control レポートを生成します。

- 監査キュー - エンドポイント上で発生した監査イベントを受信します。

  監査イベントを収集し、レポートするように CA Enterprise Log Manager を設定できます。

- サーバ - エンドポイント キュー - エンドポイントが収集した DMS からのデータを受信します。

  たとえば、UNAB 設定ポリシーをデプロイする場合、 DMS はこの設定ポリシーをサーバのこのキューに送信します。UNAB エージェントはこのキューからポリシーを収集し、UNAB エンドポイントにポリシーをデプロイします。

- エンドポイント - サーバ キュー - DMS が収集したエンドポイントの情報を受信します。

  たとえば、UNAB エンドポイントはハートビート通知をこのキューに送信し、DMS はこのキューからハートビート通知を収集してデータベース内のエンドポイントのステータスを更新します。

Java コネクタ サーバ（JCS）

Java コネクタ サーバ（JCS）は、Windows オペレーティング システムや SQL サーバのように、Java がサポートする管理デバイスと通信し、PUPM エンドポイントの特権アカウントを管理します。

Web ベースのアプリケーション

CA Access Control のエンタープライズ インストールを管理するために Web ベースのアプリケーションを使用します。 Web ベースのアプリケーションはアプリケーション サーバにインストールします。

アプリケーション サーバには次の Web ベース アプリケーションが含まれています。

- CA Access Control エンタープライズ管理 - 企業全体のポリシーを管理し、UNAB エンドポイントを設定します。 CA Access Control エンタープライズ管理 には、企業全体の特権アカウントを管理し、特権アカウントのパスワード ボールトとして機能する、特権ユーザ パスワード管理(PUPM)も含まれています。
- CA Access Control エンドポイント管理 - 各 CA Access Control エンドポイントを中央の管理サーバから管理および設定します。
- CA Access Control パスワード マネージャ - CA Access Control のユーザ パスワードを管理します。 CA Access Control ユーザのパスワードを変更したり、次回ログイン時にユーザに強制的にパスワードを変更させたりすることができます。

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方法

エンタープライズ管理サーバ コンポーネントによって、CA Access Control の企業への展開を一元的に管理できます。 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後、レポート サービスおよび、CA Access Control と UNAB のエンドポイントをインストールします。

実装を開始する前に、使用しているコンピュータが必要なハードウェアおよびソフトウェア要件を満たしていることを確認します。

注: ハードウェアとソフトウェアの要件の詳細については、リリース ノートを参照してください。

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するには、以下の手順を実行します。

1. エンタープライズ管理サーバを準備します。

   CA Access Control エンタープライズ管理 をインストールする前に、CA Access Control エンタープライズ管理 の必須ソフトウェアをインストールおよび設定して、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。

   Web ベースのすべてのアプリケーション、配布サーバ、DMS、および CA Access Control がインストールされます。

3. （オプション）SSL 通信用に JBoss を設定します。

   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。

4. （オプション）SSL 通信用に CA Access Control エンタープライズ管理 を設定します。

5. CA Access Control エンタープライズ管理 を起動します。

6. CA Access Control エンタープライズ管理 を開きます。

7. （オプション）詳細設定

   CA Identity Manager 管理コンソールを使用して、詳細な環境設定タスクを実行できます。こうしたタスクには、レポート データベースのプロパティの変更によるカスタム レポートの生成や、特定のイベント発生時の CA Access Control エンタープライズ管理 の設定による電子メール通知の送信などがあります。

8. （オプション）SQL Server のセキュリティ設定を Windows 認証モードに設定します。

   デフォルトでは、CA Access Control エンタープライズ管理 は SQL Server 認証モードでインストールされます。

9. （オプション）エンタープライズ レポート機能の実装

   CA Access Control エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ（CA Access Control レポート ポータル）を使用して、レポート機能を提供します。

10. （オプション） CA Enterprise Log Manager と統合します。

    これで、エンドポイントをインストールし設定できます。

詳細情報:

エンタープライズ レポート機能（201 ページ）
レポート サービス サーバ コンポーネントの設定方法（203 ページ）
CALM 統合アーキテクチャ（179 ページ）

エンタープライズ管理サーバの準備方法

エンタープライズ管理サーバは CA Access Control の組織への展開における、中央管理サーバです。 CA Access Control エンタープライズ管理 をインストールする前に、サーバを準備する必要があります。

注: CA Access Control エンタープライズ管理 のインストール時に、 CA Access Control エンドポイント管理 がまだインストールされていないことが検出されると、インストール プログラムによってそのインストールも行われます。 CA Access Control エンドポイント管理 がすでにインストールされている場合、該当する手順はすでに終了しているので、繰り返す必要はありません。

エンタープライズ管理サーバの準備を行うには、以下の手順を実行します。

1. エンタープライズ管理用のデータベースを準備します(49 ページ)。
2. 事前にインストールが必要なソフトウェアをインストールします(50 ページ)。

   CA Access Control は、Java Development Kit(JDK)および JBoss アプリケーション サーバをインストールするユーティリティを提供します。 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。

   注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA Access Control Premium EditionThird Party Components DVD に格納されています。 サポートされている JBoss バージョンの詳細については、「リリース ノート」を参照してください。

   これで、CA Access Control エンタープライズ管理 をエンタープライズ管理サーバにインストールする準備ができました。

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 をセットアップする必要があります。

CA Access Control エンタープライズ管理 用のデータベースを準備する方法

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アクセス可能、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:
     - 中央データベースに対して新しい管理ユーザを作成します。

       このユーザはテーブルを作成してデータを変更する権限を持っている必要があります。
     - データベースは 200 プロセス以上で設定します。
   - 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。
     - 新規ユーザを作成し、新しいデータベースはこれらユーザのデフォルトデータベースにし、ユーザには DB_owner 権限を与えます。

事前インストール ソフトウェアのインストール

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 EditionThird 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。

注: 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。 このソフトウェアがインストールされていない場合は、指定されたユーティリティを使用して、この手順でインストールすることをお勧めします。

事前インストール ソフトウェア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 サードパーティ 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. 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 診断ウィザード]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. (オプション)事前インストール ソフトウェアがインストールされた後に、CA Access Control エンタープライズ管理 のインストール プロセスを開始する場合、プロンプトが表示されたら、以下のいずれかを行います。

   - 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、[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。
   - CA Access Control エンタープライズ管理 インストーラが格納されているディレクトリの完全パスを指定します。

   [CA Access Control エンタープライズ管理 InstallAnywhere ウィザード]が開きます。

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。 このインストーラによって、必須のサードパーティ ソフトウェアをインストールし、次に、CA Access Control エンタープライズ管理 のインストール(以下の手順の手順 5)を開始します。

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. 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。

4. 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 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. 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。

   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

   CA Access Control エンタープライズ管理サーバ 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。

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) RDBMS に作成したデータベースの名前を定義します。
- ユーザ名 - RDBMS を準備した際に作成したユーザの名前を定義します。
- データベース ユーザ パスワード - 作成した管理ユーザ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。

[組み込みユーザ ストア]を選択すると、CA Access Control エンタープライズ管理 はユーザ情報を RDBMS に格納します。 Active Directory を選択する場合は、接続情報の詳細を指定します。

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 を選択する必要があります。 ユーザ ストアとして Active Directory を選択した場合、CA Access Control エンタープライズ管理 内の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 をインストールしたホストの名前を定義します。
- ポート - Active Directory が使用するポートを、「389」のように定義します。
- 検索ルート - 検索ルートを、「ou=DomainName, DC=com」のように定義します。
- ユーザ DN - Active Directory の管理者アカウント名を定義します。 このユーザ アカウントを使用して、CA Access Control エンタープライズ管理を管理します。 例: CN=Administrator、cn=Users、DC=DomainName、DC=Com
- パスワード - Active Directory の管理者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。

システム ユーザ

(Active Directory のみ)スーパーユーザ アカウントの完全 DNS 名を、「CN=SystemUser, ou=OrganizationalUnit, DC=DomainName, DC=Com」のように定義します。

注: この手順で、既存の Active Directory ユーザに superadmin アカウントを割り当てます。 superadmin アカウントには、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。 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

CA Access Control エンタープライズ管理 の管理者である 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。

重要: superadmin アカウントを使用するのは、組み込みユーザ ストアを使用する場合のみにしてください。 Active Directory を使用する場合は、管理者アカウントを使用する必要があります。

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する必要があります。

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。

コンピュータが再起動します。 次に、ご自分の組織に合わせて 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。

詳細情報:

エンタープライズ管理サーバの準備方法 (49 ページ)

SSL 通信用の JBoss の設定

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: SSL 通信用の JBoss の設定

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ユーザに表示します。

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。

SSL 通信用の JBoss の設定

1. JBoss が実行中の場合は、停止します。
2. コマンド プロンプト ウィンドウを開いて、JDK bin ディレクトリに移動します。
3. 以下のコマンドを入力します。

   ```
   keytool -genkey -alias entm -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。

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

   keytool ユーティリティは、キーストア用の新しいパスワードを入力するようにユーザに促します。

5. 新しいパスワードを入力します。

   .keystore ファイルが以下のフォルダに作成されます。

   ```
   ¥Documents and Settings¥username
   ```

6. ファイル名を entm.keystore に変更して、以下のフォルダに移動します。

   ```
   JBoss_directory¥server¥default¥conf
   ```

7. 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。

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

8. 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: このコネクタ ポート番号は、_the 前提条件または CA Access Control エンタープライズ管理 インストール処理中に指定した JBoss HTTPS ポート番号に対応します。

9. <Connector port> タグよりも上のコメント注釈「<!--」を削除してください。

   これで、このタグを編集できるようになりました。

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

    ```
    keystoreFile="${jboss.server.home.dir}/conf/entm.keystore"
    keystorePass="newPassword"
    ```

    keystoreFile

    キーストア ファイルの完全パス名を指定します。

    keystorePass

    キーストアのパスワードを入力します。

    <Connector port> タグが以下のように表示されます。

    ```
    <Connector port="18443" protocol="HTTP/1.1" SSLEnabled="true"
        maxThreads="150" scheme="https" secure="true"
        clientAuth="false" sslProtocol="TLS"
        keystoreFile="${jboss.server.home.dir}/conf/entm.keystore"
        keystorePass="newPassword" />
    ```

11. server.xml ファイルを保存して閉じます。

    ここで CA Access Control エンタープライズ管理 を起動します。

    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。

SSL 通信用に CA Access Control エンタープライズ管理 を設定する方法

デフォルトのインストールでは、CA Access Control エンタープライズ管理 は SSL をサポートしません。 これは、CA Access Control エンタープライズ管理 と Active Directory の間の通信が暗号化されないことを意味します。 Active Directory と連動する場合に、SSL を使用するように CA Access Control エンタープライズ管理 を設定できます。

1. DER、CRT または CERT 形式の Active Directory 証明書を取得します。
2. Active Directory 証明書をキーストアへ追加します。
3. SSL 通信を使用するように CA Access Control エンタープライズ管理 を設定します。

キーストアへの Active Directory 証明書の追加 - 例

CA Access Control エンタープライズ管理 を設定して SSL 通信を使用する前に、Active Directory 証明書をキーストアへ追加する必要があります。

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

例: キーストアへの Active Directory 証明書の追加

重要: この例では、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、Active Directory との安全な通信を行うために SSL の使用するように CA Access Control エンタープライズ管理 を設定する方法について説明します。 この手順を開始する前に、DER、CER または CERT にエンコードされたバイナリ形式の Active Directory 証明書を取得する必要があります。

1. JBoss が実行中の場合はそれを停止し、以下のいずれかの操作を実行します。
   - JBoss ジョブ ウィンドウから、プロセスを中断します(Ctrl+C)。
   - [サービス]パネルから JBoss アプリケーション サーバ サービスを停止します。
2. CA Access Control エンタープライズ管理 でコマンド プロンプト ウィンドウを開いて、以下のディレクトリに移動します。

   ```
   jboss_directory¥server¥default¥deploy¥IdentityMinder.ear¥custom¥ppm¥truststore
   ```
3. 以下のコマンドを入力します。

   ```
   keytool -import -keystore <ketstore> ssl.keystore -alias ad -file <activedirecoty.cert>
   ```

   パスワードの入力を促すメッセージが表示されます。

   -import

   ユーティリティが証明書を読み取り、それをキーストアにそ格納するように指定します。

   -keystore

   証明書がキーストア へインポートされるように指定します。

   -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指定します。

   -file

   Active Directory 証明書ファイルの完全パス名を指定します。

4. 「secret」というパスワードを入力します。
5. JBoss bin ディレクトリへ移動します。 デフォルトでは、このディレクトリは以下にあります。

   ```
   jboss_directory/bin
   ```

6. run.bat ファイルを編集可能な形式で開いて、trusted ユーザ ストア データで java_ops パラメータを設定します。 以下に例を示します。

   ```
   set JAVA_OPTS=%JAVA_OPTS% -Xms128m -Xmx512m
   -Djavax.net.ssl.trustStore=C:¥jboss-4.2.3.GA¥server¥default¥deploy¥IdentityMi
   nder.ear¥custom¥ppm¥truststore¥ssl.keystore
   -D-javax.net.ssl.trustStorePassword=secret
   ```

7. ファイルを保存して、JBoss を起動します。

SSL 通信用の CA Access Control エンタープライズ管理 の設定

Active Directory 証明書をキーストアへ追加した後に、SSL 通信が使用できるように CA Access Control エンタープライズ管理 を設定できます。

注: SSL 接続用に CA Access Control エンタープライズ管理 を設定するには、CA Identity Manager 管理コンソールを有効にする必要があります。 CA Identity Manager 管理コンソールの詳細については、CA Identity Manager 管理コンソールのオンラインヘルプをご覧ください。

SSL 通信用の JBoss の設定方法

1. CA Identity Manager 管理コンソールを開きます。
2. [ディレクトリ]を選択し、次に、ac-dir ディレクトリを選択します。

   ディレクトリ プロパティが表示されます。

3. [エクスポート]を選択して、ディレクトリ プロパティをエクスポートします。

   ダイアログ ボックスが表示されます。

4. 編集可能な形式でファイルを開きます。
5. <Provider userdirectory="ac-dir" type="LDAP"> タグを探します。
6. secure パラメータを true に変更します。 以下に例を示します。

   ```
   <LDAP searchroot="DC=abc,DC=company,DC=com" secure="true">
   ```

7. <Connection host="COMPUTER.abc.company.com" port=""> タグを探し、ポート番号を 636 に変更します。 以下に例を示します。

   ```
   <Connection host="COMPUTER.abc.company.com" port="636">
   ```

8. <Container objectclass="top,organizationalUnit" attribute="ou"/> タグをすべて検索して、各行の最後に value パラメータを入力します。 以下に例を示します。

   ```
   <Container objectclass="top,organizationalUnit" attribute="ou" value=""/>
   ```

9. ファイルを保存します。
10. CA Identity Manager 管理コンソールで、ディレクトリ プロパティ ページから[更新]を選択します。

    ダイアログ ボックスが表示されます。
11. インポートするファイルを参照して、探します。

    ディレクトリ環境設定ファイルが環境へインポートされます。
12. 環境を再起動します。

    これで、SSL を使用して CA Access Control エンタープライズ管理 が Active Directory と通信できるようになりました。

CA Access Control エンタープライズ管理 の起動

CA Access Control エンタープライズ管理 をインストールしたら、CA Access Control および Web アプリケーション サーバを起動する必要があります。

CA Access Control エンタープライズ管理 の起動方法

1. CA Access Control サービスが開始されていることを確認します。

   CA Access Control エンタープライズ管理 を使用するには、CA Access Control が実行中である必要があります。
2. JBoss アプリケーション サーバ サービスが開始されていることを確認します。
   JBoss アプリケーション サーバ サービスが開始されていない場合は、以下のいずれかの操作を実行します。

   - [スタート]-[プログラム]-[CA]-[Access Control]-[タスク エンジンの開始]をクリックします。

     注: タスク エンジンは、初回のロード時に多少時間がかかる場合があります。
   - [サービス]パネルから JBoss アプリケーション サーバ サービスを開始します。

   JBoss Application Server のロードが終了すると、CA Access Control エンタープライズ管理 の Web ベース インターフェースにログインできます。

CA Access Control エンタープライズ管理 を開く

CA Access Control エンタープライズ管理 をインストールして起動すると、CA Access Control エンタープライズ管理 の URL を使用してリモート コンピュータから Web ベースのインターフェースを起動することができます。

CA Access Control エンタープライズ管理 を開く方法

1. Web ブラウザを開き、使用しているホストに合わせて URL を入力します。

   http://enterprise_host:port/iam/ac

2. 自分のクレデンシャルを使用して、ログインします。

   CA Access Control エンタープライズ管理 のホームページが表示されます。

注: CA Access Control エンタープライズ管理 がインストールされている Windows コンピュータから CA Access Control エンタープライズ管理 を開くこともできます。それには、[スタート]-[プログラム]-[CA]-[Access Control]-[Enterprise Management]をクリックします。

例: CA Access Control エンタープライズ管理 を開く

ネットワーク上の任意のコンピュータから CA Access Control エンタープライズ管理 を開くには、Web ブラウザに次の URL を入力します。

```
http://appserver123:8080/iam/ac
```

この URL からは、CA Access Control エンタープライズ管理 が appserver123 という名前のホストにインストールされ、デフォルトの JBoss ポート 8080 を使用しているのがわかります。

詳細な環境設定

CA Identity Manager 管理コンソールを使用して、詳細な環境設定タスクを実行できます。こうしたタスクには、レポート データベースのプロパティの変更によるカスタム レポートの生成や、特定のイベント発生時の CA Access Control エンタープライズ管理 の設定による電子メール通知の送信などがあります。

CA Identity Manager 管理コンソールによって、ディレクトリの管理およびグラフィカル表示を制御する環境を作成および管理できます。

注: 詳細については、CA Identity Manager 管理コンソールのオンライン ヘルプをご覧ください。オンライン ヘルプは、アプリケーションからアクセスできます。

CA Identity Manager 管理コンソールの有効化

CA Access Control エンタープライズ管理 の初回のインストール時には、CA Identity Manager 管理コンソール オプションは無効になっています CA Identity Manager 管理コンソールを有効にするには、デフォルト設定を変更します。

CA Identity Manager 管理コンソールの有効化

1. JBoss が実行されている場合は、停止します。 以下のいずれかの操作を実行します。
   - JBoss ジョブ ウィンドウから、プロセスを中断します(Ctrl+C)。
   - [スタート]-[設定]-[コントロール パネル]-[管理ツール]-[サービス]を選択し、JBoss アプリケーション サーバ サービスを停止します。
2. 以下のディレクトリに移動します。

   ```
   JBossInstallDir/server/default/deploy/
   IdentityMinder.ear/management_console.war/WEB-INF
   ```
3. 編集するために、web.xml ファイルを開きます。
4. 以下のセクションを探します。

   ```
   AccessFilter
   ```
5. <param-value> フィールドで、値を[True]に変更します。
6. ファイルを保存して閉じます。
7. JBoss を起動します。

   CA Identity Manager 管理コンソールが有効になります。

CA Identity Manager 管理コンソールの起動

CA Identity Manager 管理コンソールには Web ベースのインターフェースがあります。CA Identity Manager 管理コンソールを有効化して CA Access Control エンタープライズ管理 を起動すると、お使いのネットワーク上の任意のコンピュータから CA Identity Manager 管理コンソールを開くことができます。

CA Identity Manager 管理コンソールを開くには、ホストで Web ブラウザを起動し、次の URL 入力します。

```
http://enterprise_host:port/idmmanage
```

CA Identity Manager 管理コンソールが開きます。

例: CA Identity Manager 管理コンソールの起動

ネットワーク上の任意のコンピュータから CA Identity Manager 管理コンソール を開くには、Web ブラウザに次の URL を入力します。

```
http://appserver123:8080/idmmanage
```

この URL からは、CA Identity Manager 管理コンソールが appserver123 という名前のホストにインストールされ、デフォルトの JBoss ポート 8080 を使用しているのがわかります。

CA Identity Manager 管理コンソールでの作業

CA Identity Manager 管理コンソール を開いた場合、CA Identity Manager 環境で作業することになります。 CA Identity Manager 環境はユーザ ストアのビューです。 CA Identity Manager 環境では、ユーザ、グループ、組織、タスクおよびロールを管理します。さらに、電子メール通知オプションの設定、レポート データベース設定の定義も可能です。

注: 詳細については、CA Identity Manager 管理コンソールの CA Identity Manager 管理コンソール オンライン ヘルプを参照してください。

例: 電子メール通知の設定

次の例は、CA Identity Manager 管理コンソールで電子メール通知を設定する方法について示しています。 この例では、CA Identity Manager 管理コンソールが有効で、Web ブラウザを使用して、管理コンソールをアクセスしたと想定しています。

注: CA Identity Manager 管理コンソール オプションは PUPM およびレポート オプションについてのみ使用可能です。

重要: 環境の変更は、CA Access Control エンタープライズ管理 の安定性に影響を与える場合があります。詳細については、テクニカル サポート(http://ca.com/jp/support)にお問い合わせください。

電子メール通知の設定方法

1. [環境]を選択して設定する環境を選択し、[詳細設定]、[電子メール]の順に選択します。

   [電子メール]のプロパティ ウィンドウが表示されます。

2. 組織に該当するオプションを設定します。以下のオプションがあります。

   イベント電子メール有効化

   イベントに対する電子メール通知の送信を有効化します。

   タスク

   タスクに対する電子メール通知の送信を有効化します。

   テンプレート ディレクトリ

   CA Identity Manager が電子メール メッセージの作成に使用する、電子メール テンプレートの場所を指定します。

   注: 電子メール テンプレートは以下のディレクトリのサブディレクトリに格納されています。

   ```
   IdentityMinder.ear/custom/emailTemplates
   ```

   イベント

   電子メール通知を送信するイベントを指定します。

   以下のタスクの完了時またはワークフロー中に電子メールを送信

   電子メール通知を送信するタスクを指定します。

3. [保存]をクリックします。

   電子メール通知プロパティが保存されます。

SQL Server データベース接続性設定の変更

デフォルトでは、CA Access Control エンタープライズ管理 は、SQL Server 認証モードで、Microsoft SQL サーバ データベースにインストールされます。 Windows 認証モードで動作するように、CA Access Control エンタープライズ管理 のインストール後に、データベース認証モードを変更できます。

重要: SQL Server が Windows 認証モードで動作している場合、CA Access Control エンタープライズ管理 サーバは JBoss サービス アカウントを利用して SQL Server 上の CA Access Control データベースを管理します。 別の JBoss サービス アカウントの使用を選択した場合、SQL Server データベース インスタンス上のアカウントも変更する必要があります。

重要: Windows 認証モードで動作するように SQL サーバを設定するには、SQL Server JDBC 2.0 をインストールする必要があります。 SQL Server JDBC 2.0 ドライバは、Microsoft の Web サイトからダウンロードできます。

SQL Server データベース接続性設定の変更方法

1. まだこれを行っていない場合は、SQL Server JDBC 2.0 ドライバ ファイルをダウンロードし、一時フォルダに抽出してください。
2. JBoss が実行されている場合は、停止します。 以下のいずれかの操作を実行します。
   - JBoss アプリケーション サーバ ウィンドウを中断します(Ctrl+)。
   - [サービス]パネルから JBoss サービスを停止します。
3. JBoss lib ディレクトリへ移動します。 デフォルトでは、このディレクトリは以下にあります。

   ```
   JBoss-directory¥server¥default
   ```

4. ファイル sqljdbc.jar を一時ディレクトリから JBoss lib ディレクトリにコピーします。

   この名前のファイルが存在することを通知するメッセージが表示されます。
5. 新規ファイルで既存ファイルを上書きすることを選択します。

   新規ファイルがディレクトリに格納されます。
6. JBoss bin ディレクトリへ移動します。 デフォルトでは、このディレクトリは以下にあります。

   ```
   JBoss-directory¥bin
   ```

7. ファイル sqljdbc_auth.dll を一時ディレクトリから JBoss bin ディレクトリにコピーします。

   この名前のファイルが存在することを通知するメッセージが表示されます。
8. 新規ファイルで既存ファイルを上書きすることを選択します。

   新規ファイルがディレクトリに格納されます。
9. JBoss の deploy ディレクトリへ移動します。 デフォルトでは、このディレクトリは以下にあります。

   ```
   JBoss-directory¥server¥default¥deploy
   ```

10. 以下のファイルを開きます。
    - imauditdb-ds.xml
    - imtaskpersistencedb-ds.xml
    - imworkflowdb-ds.xml
    - objectstore-ds.xml
    - reportsnapshot-ds.xml
    - userstore-ds.xml
11. 各ファイルで <connection-url> タグを見つけて、DatabaseName= パラメータの後ろに以下を追加します。

    ;integratedSecurity=true
12. 各ファイルから、<security-domain> タグを削除します。
13. ファイルを保存して、JBoss を再起動します。

    これで、CA Access Control エンタープライズ管理 が Windows 認証モードで SQL サーバと連動するようになります。

例: JBoss 環境設定ファイルの変更による Windows 認証モードの有効化

以下の例は、SQL 認証モードから Windows 認証モードに切り替える JBoss 環境設定ファイルの 1 つを変更する方法を示します。 この例では、管理者はファイル objectstore-ds.xml を変更し、接続モードを Windows 認証(;integratedSecurity=true)に指定します。 次に、管理者はファイルから <security-domain> タグを削除します。 このタグが削除されるのは、その適用対象が SQL 認証モードのみであるためです。

以下の抜粋は、管理者が接続設定を変更した後の objectsstore-ds.xml ファイルを示しています。

```
<connection-url>jdbc:sqlserver://example.comp.com:1433;selectMethod=cursor;Database
seName=ACDB;integratedSecurity=true</connection-url>
```

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

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 システムにログオンしていることを確認してください。

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

1. JBoss が実行中の場合は、停止します。
2. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   [プログラムの追加と削除]ダイアログ ボックスが表示されます。
3. プログラム リストをスクロールして CA Access Control エンタープライズ管理 を選択します。
4. [変更と削除]をクリックします。

   CA Access Control エンタープライズ管理 のアンインストール ウィザードが表示されます。
5. ウィザードの手順に従って、CA Access Control エンタープライズ管理 をアンインストールします。

   アンインストールが完了し、コンピュータから CA Access Control エンタープライズ管理 が削除されます。
6. ウィザードを終了するには、[完了]をクリックしてください。

第 4 章: Windows エンドポイントのインストールおよびカスタマイズ

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

CA Access Control をインストールするには、事前に準備要件を満たし、必要な情報を揃えておく必要があります。

インストール方法

以下の方法で、CA Access Control Endpoint Components for Windows DVD を使用して CA Access Control for Windows をインストールできます。

- Product Explorer - CA Access Control をインストールするのに最も簡単な方法は、Product Explorer を使用することです。 Product Explorer は、グラフィカルなインストール プログラムで、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 では、インストールのプロセスが段階的に実行され、各段階で必要な情報を入力するように要求されます。

- コマンド ライン - インストール プログラムに対するコマンド ライン インターフェースを使用すれば、以下のことができます。
  - グラフィカル インストール プログラムを実行するためのカスタム デフォルトの設定

    コマンド ラインからグラフィカル インストール プログラムにデフォルト値を渡すことができます。 この方法を使用すれば、希望する事前設定済のデフォルトでインストール プログラムを開くだけでなく、インストールごとにオプションをカスタマイズすることも可能なバッチ ファイルを作成できます。
  - サイレント インストールの実行

    コマンド ラインでは、グラフィカル インストール プログラムにデフォルト値を単に渡すだけでなく、サイレント モードで CA Access Control をインストールすることも可能です。 リモート コンピュータにインストールする場合に、この方法を使用します。

新規インストール

CA Access Control の新しいインスタンスをインストールするときは、以下の点に注意してください。

- 「リリース ノート」をお読みください。

  このドキュメントでは、サポートされるプラットフォームに関する情報、既知の問題点、考慮事項、および CA Access Control をインストールする前に把握しておく必要のあるその他の重要な情報について説明しています。
- CA Access Control は、Windows の Administrator または Administrators グループのメンバがインストールする必要があります。
- CA Access Control は、ほかの製品のインストール ディレクトリとは別の固有のディレクトリにインストールします。
- Microsoft Internet Explorer 6.x または 7.x をインストールしておく必要があります。

- CA Access Control では、製品のインストールを完了するのに、Microsoft Visual C++ 2005 Redistributable Package が必要です。

  このパッケージが見つからない場合、インストール プログラムはこのパッケージをまずインストールします。

- CA のライセンス許可の使用

  CA のすべての製品およびオプションを使用するには、CA ソフトウェアが稼動するネットワーク内の各コンピュータでライセンス ファイルの CA.OLF が必要となります。CA Access Control の購入時に、この製品を正常にインストールおよび使用するために必要な情報が含まれるライセンス証明書を受け取ります。

  エンタープライズ ライセンス ファイルをインストールするには、CA.OLF ファイルを（CA Access Control という行を追加して）CA_license ディレクトリ（C:¥Program Files¥CA¥SharedComponents¥CA_LIC など）にコピーします。

アップグレードおよび再インストール

CA Access Control をアップグレードする場合は、以下の点に注意が必要です。

- 「リリース ノート」をお読みください。

  このドキュメントでは、サポートされるプラットフォームに関する情報、新しいリリースへのアップグレードが可能な CA Access Control のバージョン、既知の問題点、考慮事項、および CA Access Control をインストールする前に把握しておく必要のあるその他の重要な情報について説明しています。

- 実環境をアップグレードする前に、新しいリリースについて簡易的な内部テストを実施することをお勧めします。

- CA Access Control のアップグレード時には、インストールを完了させるために、コンピュータをリブートする必要があります。

  将来的にパッチは、リブートを必要としなくなる可能性があります。

- 対象となる環境が PMDB 階層で設定されている場合、またはそのような環境を設定する場合は、以下の作業を行うことをお勧めします。
  - 階層内の各コンピュータのインストールまたは各コンピュータのアップグレードを下から上の順(サブスクライバが最初)で行います。

    PMDB のアップグレード時に、旧バージョンを利用しているサブスクライバが存在する場合、誤ったコマンドが送信される場合があります。 この問題は、旧バージョンの PMDB に存在しないクラスやプロパティが新しい PMDB に含まれることが原因で発生します。

    注: 単一のコンピュータ上で動作する PMDB 階層については、同時にアップグレードすることができます。
  - PMDB またはポリシーの更新中にアップグレードを行わないでください。
  - サブスクライバおよび PMDB ポリシーをバックアップします。

  注: 旧バージョンの PMDB は、新しいバージョンのサブスクライバを保持できます。しかし、これと逆の状況は許可されていません。 旧バージョンのコマンドは最新バージョンでもサポートされているため、現在の CA Access Control のサブスクライバへの古い PMDB の伝播が可能です。
- アップグレードする前に使っていたのと同じ暗号化鍵を使用する必要があります。
- インストール プログラムは、前のインストールのレジストリ設定を自動的に保存およびアップグレードします。 旧バージョンのレジストリ キーが再配置された場合、アップグレード プロセスでは以前の設定が新しい場所にコピーされます。

  CA Access Control のレジストリ設定は、以下の場所に格納されています。

  ```
  HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl
  ```

- CA Access Control のバージョンがコンピュータにすでにインストールされている場合は、現在のデータベースのデータを引き続き使用するのか、データベースを削除して新しい空のデータベースを作成するのかを決める必要があります。

  インストールを続行するには、データの再使用を選択する必要があります。CA Access Control により、すべてのデータが新しいデータベースに転送されます。 新しい空のデータベースを作成する場合は、まず CA Access Control をアンインストールして既存のデータベースを削除し、CA Access Control を再度インストールします。

  重要: 現在のデータベースを削除するよう指定した場合は、すべての CA Access Control データが失われます。すなわち、データベースに定義したユーザ、グループ、およびリソース、リソースを保護するアクセス ルールが失われます。

- 完全監査は、 CA Access Control のアップグレード時に、デフォルトで有効になります。

  重要: データベースに保存されているルールによりますが、この機能の結果として、CA Access Control がログ ファイルに記録する監査イベントの数が大幅に増える可能性があります。 そのような場合、監査ログ ファイルのサイズとバックアップ設定を見直すことをお勧めします。

  注: 完全監査および監査ログ バックアップ用のレジストリ設定の使用および構成の詳細については、「Windows エンドポイント管理ガイド」を参照してください。

CA Unicenter の統合

CA Access Control と Unicenter セキュリティのコンポーネントを統合する場合は、以下の点に留意します。

- Unicenter の統合および移行インストールプロセスが正常に実行された後で、Unicenter TNG のログイン インターセプトが無効になっていることを確認する必要があります。

  Unicenter の統合および移行インストール プロセスの実行後に、Unicenter TNG のログイン インターセプトを実行しないことをお勧めします。

- Unicenter TNG のデータ スコーピング ルール(-DT サフィックスの付いた Unicenter TNG のアセット タイプを対象とするルール)は、移行プロセスでは無視されます。

  これらのルールは、CA Access Control 移行プロセスによってサポートされていません。

- Unicenter セキュリティは現在使用されていないため、以下の Unicenter セキュリティのアセット タイプ（CA-USER、CA-ACCESS、CA-USERGROUP、CA-ASSETGROUP、CA-ASSETTYPE、および CA-UPSNODE）に対して実装された Unicenter セキュリティ ルールはどれも使用されていません。

  このようなアセット タイプまたはそれらから派生したタイプを対象とするルールは、移行プロセスではすべて無視されます。

- Unicenter の統合プロセスの実行後に Unicenter TNG をアップグレードするか、または Unicenter TNG の修正プログラムを適用する場合、%CAIGLBL000%¥BIN ディレクトリにある CAUSECR.DLL ファイルが置き換えられていないこと、また CA Access Control のインストール パスの bin ディレクトリにある CAUSECR.DLL.EAC ファイルと同じであることを確認する必要があります。

- CA Access Control がアンインストールされた場合、Unicenter セキュリティ オプションの CA_ROUTER_CAUSECU が 1 にリセットされます。また、Unicenter セキュリティ オプションの SETLOCAL CAIACTSECSV が「yes」にリセットされ、%CAIGLBL000%¥BIN ディレクトリの CAUSECR.DLL ファイルが Unicenter のデフォルトのものに置き換えられます。 アンインストール プロセス後にこれらのオプションをカスタマイズする必要がある場合があります。

その他の製品との共存

CA Access Control をインストールする場合は、CA Access Control とその他のプログラムをコンピュータ上で共存させる場合の問題について検討してください。

CA Access Control は、たとえば、CA Antivirus などの他のプログラムと並行した環境で実行します。 これは、CA Access Control とローカル コンピュータ上で実行しているプログラムとの衝突を引き起こす可能性があります。 このため、共存ユーティリティ（eACoexist.exe）を CA Access Control のインストール中に実行して、衝突を引き起こす可能性のあるローカル コンピュータのプログラムを検出します。 ユーティリティは、CA Access Control がサポートする各共存プログラムにプラグイン（バイナリ モジュール）を使用します。 CA Access Control が検出するプログラムが trusted の場合は、CA Access Control は SPECIALPGM ルールを作成することによってプログラムを登録します。 この SPECIALPGM ルールはこのプログラムへのアクセスを決定し、アクセスを付与するときに CA Access Control がそれを確実に無視するようにします。

注: eACoexist ユーティリティおよびサポートされているプラグインに関する詳細については、「リファレンス ガイド」を参照してください。

例: Dr Watson の trusted プログラム ルール

この例では、共存ユーティリティが CA Access Control と同じコンピュータ上で Dr Watson アプリケーションを発見した場合に、作成できる trusted プログラム ルールを示します。 これらのルールは、デフォルトの Windows 2000 Server がインストールされているコンピュータでは、以下のようになります。

```
editres SPECIALPGM ('C:¥WINNT¥system32¥DRWTSN32.EXE') pgmtype(DCM)
editres PROGRAM ('C:¥WINNT¥system32¥DRWTSN32.EXE') owner(nobody) defacc(x) trust
```

通信の暗号化

CA Access Control をインストールする際は、CA Access Control コンポーネントと CA Access Control クライアント/サーバ間の通信の暗号化について考慮する必要があります。 次の方法で通信を暗号化することができます。

- 標準暗号化(対称鍵暗号化)
- SSL

SSL と対称鍵暗号化の両方の使用をお勧めします。

詳細情報:

コンポーネント間通信の暗号化(83 ページ)

標準暗号化

CA Access Control の標準暗号化は、ダイナミック リンク ライブラリ(DLL)によって実装されます。

CA Access Control のインストールでは、すべての暗号化 DLL が以下のディレクトリに格納されます。

```
ACInstallDir¥bin
```

この場合、ACInstallDir は CA Access Control がインストールされているディレクトリです。

インストール中に CA Access Control が格納する DLL ファイルは以下のとおりです。

- defenc.dll(デフォルト暗号化、専用)
- aes128enc.dll(128 ビット AES 暗号化)
- aes192enc.dll(192 ビット AES 暗号化)
- aes256enc.dll(256 ビット AES 暗号化)

- desenc.dll（DES 暗号化）
- tripledesenc.dll（3DES 暗号化）

暗号化で使用される DLL の完全パスは、以下のレジストリ値として格納されています。

HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl¥Encryption Package

暗号化で使用する鍵を変更するには、対称モードで Sechkey ユーティリティを使用します。

詳細情報:

コンポーネント間通信の暗号化（83 ページ）

SSL、認証、および証明書

TLS などの Secure Sockets Layer（SSL）では、コンピュータ プログラム間の通信を実現できます。 このように行われる通信の特性は以下のとおりです。

- 通信への参加者の正体は、それ自身が表明したプログラムまたはユーザです。 これは認証と呼ばれています。
- データは安全に暗号化され、そのデータを読み取ることができるのは参加者だけです。

参加者は、X.509 証明書を使用して互いに認証します。 X.509 証明書は、証明書の所有者のアドレスを公開鍵とリンクさせる電子文書です。 この証明書は偽造することは不可能です。

SSL はクライアント サーバ モデルで動作します。 クライアントはサーバから X509 証明書を受け取ると、その証明書が有効かどうかをチェックします。 証明書が有効である場合、クライアントは、サーバの正体がそれ自身が主張するプログラムまたはユーザであることを認識するので、サーバは認証されます。 また、クライアントが証明書の公開鍵を使用してデータを暗号化した場合、サーバはそのデータしか復号化できません。したがって、データの安全性が守られます。 サーバ側では、クライアントから受信する X.509 を同様に使用します。

詳細情報:

コンポーネント間通信の暗号化（83 ページ）

証明書の内容

プログラムは X.509 証明書を送信して、その ID が公開鍵にバインドされていることを証明します。 これにより、他のプログラムは、証明書の所有者のみが暗号化されたメッセージを復号化できることを認識して、メッセージを暗号化します。

X.509 証明書の内容は以下のとおりです。

証明書データ

最も重要な証明書データ フィールドは、以下のとおりです。

- 証明書のサブジェクトの公開識別子（たとえば、Web アドレス）
- 証明書の有効期間（開始日および終了日）

証明書を認証する認証局（CA）の名前

証明書のリーダは、シグネチャが有効である場合、公開鍵がサブジェクトと関連付けられていることを CA が検証するものと確信できます。 つまり、証明書のリーダが CA を信頼している場合、そのリーダは公開鍵を使用して暗号化されたデータが所有者によってのみ読み取り可能であることを信用できます。

サブジェクトの公開鍵

証明書のリーダは、公開鍵を使用してデータを暗号化し、それを証明書のサブジェクトに送信します。

デジタル署名

デジタル署名は、CA の秘密鍵を使用して暗号化された、証明書内の他のすべてのデータをハッシュ方式でカプセル化したものです（暗号化の場合に反して、この場合は、送信者が公開鍵を使用してデータを暗号化します）。CA の公開鍵へのアクセス権を有する者は誰でも、シグネチャを読み取り、このシグネチャが証明書内の他のデータと一致するかどうかをチェックすることができます。 証明書内のいずれかのテキストが変更されている場合、シグネチャはもはや証明書のテキストとは一致しません。

サブジェクトの秘密鍵は証明書と関連付けられていますが、個別に管理され、安全性が保たれています。 サブジェクトは秘密鍵を使用して、プログラムが公開鍵を使用して暗号化したメッセージを復号化します。

証明書が証明すること

リーダは、認証局(CA)の公開鍵を使用して証明書シグネチャを検証することができます。復号化されたシグネチャが証明書の残りの内容と一致し、かつリーダが CA を信頼している場合、リーダは以下のことが当てはまることを認識しています。

- リーダが公開鍵を使用してデータを暗号化すると、そのデータを復号化し、読み取ることができるのは秘密鍵の所有者だけです。
- 証明書の秘密鍵の所有者は、証明書内で指定されたサブジェクトです。

証明書が有効であることを確信するために、リーダは CA を信頼し、さらに CA の公開鍵にアクセスする必要があります。 ほとんどの場合、CA はよく知られた会社であり、プログラム(およびすべての一般的な Web ブラウザ)は CA 公開鍵のコピーを保持しているので、リーダはオンラインで CA が本当に証明書を検証したかどうかをチェックする必要はありません。

発行者がまた所有者である場合、証明書は自己署名証明書と呼ばれます。この発行者を信頼することには、問題があります。

証明書を送信したプログラムが証明書の所有者であることを確認するには、リーダは他の方法を使用する必要があります。 通常、リーダは、証明書の送信者を探すのに使用したアドレスが証明書内にあるアドレスと同じであることをチェックします。

Product Explorer によるインストール

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。 さらに、インストールコンポーネントのシステム要件を表示できます。

注: autorun が有効になっている場合、CA Access Control Endpoint Components for Windows DVD を光ディスク ドライブに挿入すると、Product Explorer が自動的に表示されます。

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（80 ページ）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（101 ページ）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。

インストール ワークシート

インストール プログラムはユーザに CA Access Control の初期設定に必要な情報を入力するよう求めます。 以下のセクションでは、提供することが必要な情報を説明し、推奨事項を示します。

機能の選択

インストール プログラムの[機能の選択]画面では、CA Access Control をインストールする場所と、コンピュータにインストールする機能を定義することができます。 以下の機能が使用可能です。

機能	説明	推奨
タスクの委任	管理タスクを実行するのに必要な権限を一般ユーザに与えることができます。 **注**: デフォルトで選択されています。	この機能は、サブ管理権限をユーザに付与する場合に選択します。 インストール後に設定することもできます。
SDK	SDK と呼ばれるサブディレクトリを作成します。 このサブディレクトリには、CA Access Control SDK および API サンプルを使用するのに必要なライブラリおよびファイルが含まれています。	この機能は、CA Access Control のセキュリティ機能を使用して社内アプリケーションを開発する場合に選択します。
Stack Overflow Protection（STOP）	CA Access Control スタック オーバーフロー保護機能を有効にします。	この機能は、プログラムが不正に利用されるのを防ぐために選択します。

機能	説明	推奨
メインフレームのパスワード同期	ユーザ パスワードをメインフレーム コンピュータと同期させることができます。	この機能は、メインフレーム コンピュータとの同期を維持する場合に選択します。
Unicenter Integration	Unicenter NSM と CA Access Control を統合し、Unicenter NSM のデータを移行することができます。 CA Access Control により、Unicenter NSM の環境設定パラメータで指定されたホストまたは選択されたホストに監査データが送信されます。 **注**: この機能は、該当するコンピュータに Unicenter NSM がインストールされている場合にのみ利用できます。	
拡張ポリシー管理クライアント	ローカル コンピュータに拡張ポリシー管理を設定します。	この機能は、拡張ポリシー管理を使用したポリシーのデプロイ先とするすべてのエンドポイントに対して選択してください。
Policy Model サブスクライバ	親 PMDB から更新情報を受信するためにローカル コンピュータを設定します。	この機能は、親 PMDB からの更新対象とするすべてのエンドポイントに対して選択してください。 **注**: Policy Model サービスの詳細については、「エンドポイント管理ガイド」を参照してください。
PUPM エージェント	PUPM エージェントは、ローカル コンピュータを特権ユーザ パスワード管理(PUPM)用に設定し、このコンピュータから特権アカウントのパスワードを取得できるようにします。	この機能は、PUPM を使用して管理する特権アカウントがある、すべてのエンドポイントに対して選択してください。 **注**: PUPM 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。
レポート エージェント	データベースのスケジュールされたスナップショットを配布サーバに送信するように、コンピュータを設定することができます。 さらに、監査レコードを配布サーバに送信するように選択することができます。	レポート エージェント機能は、このエンドポイントをエンタープライズ レポートに含める場合に選択します。 CA Enterprise Log Manager を使用してエンタープライズ監査ログを管理する場合は、監査ルーティング サブ機能を選択します。

管理者とホストの情報

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
Administrators	CA Access Control データベースへの管理アクセス権限を有するユーザを定義することができます。	
管理端末	管理者が CA Access Control データベースを管理するために使用できるコンピュータを定義できます。	管理者が CA Access Control エンドポイント管理を使用して CA Access Control を管理する場合は、CA Access Control エンドポイント管理 がインストールされているコンピュータのみを定義する必要があります。 管理者によってブラウザが開かれるコンピュータを定義する必要はありません。
DNS ドメイン名	CA Access Control がホスト名に追加するネットワークのドメイン名を入力できます。	CA Access Control がホスト名に追加するドメイン名のうち少なくとも 1 つを入力する必要があります。

ユーザおよびグループ

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
主要なストアによるユーザおよびグループのサポート	既存の企業ユーザ ストアを使用できます。このため、CA Access Control データベース内でこれらのユーザを重複させる必要はありません。	企業ユーザ ストアをサポートするように、CA Access Control を設定することをお勧めします。企業ストアをサポートしない場合、保護対象のアクセサが CA Access Control データベース内で重複することになります。
Windows ユーザおよびグループのデータのインポート	保護対象のアクセサを作成するよう指定した場合は、既存の Windows ユーザおよびグループがデータベース内に自動的に作成されます。	Windows ユーザおよびグループをインポートするよう指定した場合は、以下のオプションのうちの 1 つ以上を選択します。 ■ ユーザのインポート - Windows ユーザをデータベースにインポートします。 ■ グループのインポート - Windows グループをデータベースにインポートします。 ■ ユーザのデフォルト グループへの接続 - インポートするユーザを、データベース内の適切なインポート済みグループに自動的に追加します。 ■ インポートされたデータの所有者の変更 - イ

情報	説明	推奨
		ンポートするデータの所有者として自分以外のユーザを定義します。 デフォルトでは、これらのレコードの所有者はインストール作業を実行している管理者に設定されます。 ■ ドメインからのインポート - 指定されたドメインからアクセサ データをインポートします。

Unicenter Integration

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
CA Access Control と Unicenter TNG の統合	Unicenter TNG の環境設定パラメータで指定されたホストまたは選択されたホストに監査データが送信されるように、CA Access Control を設定できます。	統合するには、監査データが Unicenter NSM に送信されるように指定し、CA Access Control が監査データを送信するホストを選択します。
CA Access Control と Unicenter カレンダの統合	Unicenter NSM カレンダとユーザおよびアクセス権限の統合がサポートされるよう設定できます。	デフォルトの設定 10 分前後の間隔で、Unicenter NSM カレンダから更新情報を取得するように CA Access Control を設定します。
Unicenter セキュリティのデータの移行	Unicenter セキュリティ データを CA Access Control に移行することができます。	このオプションを選択しない場合、Unicenter セキュリティから CA Access Control への移行は行われません。また、CA Access Control でのユーザ名は完全修飾されて表示されます（DOMAINNAME¥USERNAME）。 移行では、ユーザ名は修飾されません（USERNAME）。

コンポーネント間通信の暗号化

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

画面	説明	推奨
SSL 通信	コンポーネント間の通信に Secure Socket Layer（SSL）を使用するかどうかを指定できます。 SSL および対称鍵暗号化の両方を使用できます。	SSL（公開鍵を使用）および対称鍵暗号化を両方とも使用することをお勧めします。
証明書の設定	SSL を使用する場合は、使用す	確かな認証局（CA）が発行した証明書の使用をお

画面	説明	推奨
	る証明書を指定できます。	勧めします。
証明書の生成	ルート証明書として使用する、自己証明書と鍵のペアを作成できます。	自己証明書の使用も可能ですが、この方法はお勧めしません。 自己証明書を使用する場合は、自己証明書の使用をすべてのホストで許可する必要があります。
証明書の設定の変更	証明書の設定を変更できます。	証明書および鍵のペアの設定をデフォルト設定から変更することを強くお勧めします。
既存の証明書	インストールした証明書に関する情報が提供されます。	
暗号化の設定	暗号化の方法および対称暗号化の鍵を設定できます。	暗号化鍵の設定をデフォルト設定から変更することを強くお勧めします。

詳細情報:

標準暗号化(75 ページ)
SSL、認証、および証明書(76 ページ)

Policy Model のサブスクライバの設定

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
親 Policy Model データベースの指定	このデータベースがサブスクライブする 1 つ以上の親 PMDB を定義します。 ローカル データベースは、このリストで指定されていない PMDB からの更新情報を受け入れません。 親 PMDB は、pmdb@hostname.com の形式で定義します。	インストールの完了後、このデータベースを親 PMDB 上でサブスクライバとして定義する必要があります。 **注**: _NO_MASTER_ を親 PMDB として指定し、任意の PMDB から伝達される更新をローカル データベースが受け入れることを示します。
パスワード Policy Model	パスワードの変更を伝達する、親パスワード Policy Model を定義します。 パスワード PMDB は、pmdb@hostname.com の形式で定義します。	インストールの完了後、このデータベースをパスワード PMDB 上でサブスクライバとして定義する必要があります。

拡張ポリシー管理クライアント

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
拡張ポリシー管理サーバのホスト名の指定	拡張ポリシー管理サーバ コンポーネントがインストールされているサーバの名前を定義します。	dhName@hostName という形式でホスト名を定義します。たとえば、host123.comp.com という名前のホストに拡張ポリシー管理サーバ コンポーネントをインストールした場合は、DH__@host123.comp.com を使用する必要があります。 **注**: 拡張ポリシー管理およびレポー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。

レポート エージェントの設定

以下の表では、提供することが必要な情報を説明し、推奨事項を示します。

情報	説明	推奨
レポート スケジュールの選択	レポート エージェントが、いつ配布サーバ にデータベースのスナップショットを送信するかを指定します。	システム リソースの消費量が非常に大きい時間帯には、レポート エージェントによるスナップショットの送信をスケジュールしないことをお勧めします。
監査ルーティングの環境設定	監査ログ ファイルのタイムスタンプされたバックアップを保持するかどうかを指定します。 **注**: このオプションは、[機能の選択] ページで、監査ルーティングのインストールを選択している場合にのみ表示されます。	監査ログ ファイルのタイムスタンプされたバックアップを保持するように選択していることを確認してください。 これはデフォルトの設定で、すべての監査レコードがレポート エージェントによって確実に読み取ることができるようにするのに必要です。 CA Access Control は、50 ファイルに達すると、監査ログ ファイルを上書きします。 この数が企業に適さない場合は、logmgr レジストリ サブキーの audit_max_files トークンを適切な値に編集する必要があります。

配布サーバの設定

以下の表では、提供すべき情報について説明し、推奨事項を示します。

情報	説明	推奨
サーバ名	配布サーバがインストールされて	配布サーバがインストールされているホストの完全

情報	説明	推奨
	いるホストの名前を定義します。	修飾ホスト名を指定する必要があります。
セキュア接続の使用	配布サーバとレポート エージェント間および配布サーバと PUPM 間の通信に SSL を使用するかどうかを指定します。	SSL を使用することをお勧めします。 SSL を使用しない場合、配布サーバは、レポート エージェントおよび PUPM エージェントとの通信に TCP を使用します。
サーバ ポート	配布サーバとレポート エージェント間、および配布サーバと PUPM エージェント間の通信に使用するポート番号を定義します。	SSL 通信を使用する場合、デフォルトのサーバ ポートは 7243 です。 SSL 通信を使用しない場合、デフォルトのサーバ ポートは 7222 です。
通信キー	配布サーバとレポート エージェント間、および配布サーバと PUPM エージェント間の通信を認証するキーを新規に定義します。	配布サーバをインストールする場合は、必ず同じキーを使用してください。 **注**: SSL 通信を使用する場合、通信キーを指定する必要があります。 SSL 通信を使用しない場合、通信キーを指定しないことを選択できます。

コマンドラインによるインストール

コマンド ラインを使用すると、以下のことが可能です。

- グラフィカル インストール プログラムにデフォルト設定を渡します。
- CA Access Control をサイレント モードでインストールします。

インストール プログラムに対するカスタム デフォルトの設定

企業で使用するデフォルトを使用して CA Access Control インストール プログラムを設定するには、コマンド ラインを使用します。 グラフィカル インストール プログラムは、コマンド ラインから入力を受け取り、事前に選択されているオプションを確認します。

インストール プログラムに対してカスタム デフォルトを設定する方法

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、CA Access Control Product Explorer が表示されます。

4. CA Access Control Product Explorer が表示されたら、これを閉じます。
5. コマンド ラインを開き、光ディスク ドライブの以下のディレクトリに移動します。

   ```
   ¥architecture
   ```

   アーキテクチャ

   オペレーティング システムのアーキテクチャの省略形を定義します。

   X86、X64、および IA64 のいずれかとなります。
6. 以下のコマンドを入力します。

   ```
   setup [/s] /v"<insert_params_here>"
   ```

   <insert_params_here> 変数では、インストール プログラムに渡すインストール設定を指定します。

   インストール プログラムが表示されます。 インストール プログラムの画面には、プログラムに渡すように選択しているデフォルト オプションが表示されます。これらのオプションを変更して CA Access Control をインストールできます。

サイレント モードでのインストール

対話形式のフィードバックなしで CA Access Control をインストールするには、コマンドラインを使用して CA Access Control をサイレント モードでインストールすることができます。

CA Access Control をサイレント モードでインストールする方法

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、CA Access Control Product Explorer が表示されます。
4. CA Access Control Product Explorer が表示されたら、これを閉じます。

5. コマンド ラインを開き、光ディスク ドライブの以下のディレクトリに移動します。

   ¥architecture

   アーキテクチャ

   オペレーティング システムのアーキテクチャの省略形を定義します。

   X86、X64、および IA64 のいずれかとなります。

6. 以下のコマンドを入力します。

   setup /s /v"/qn COMMAND=keyword <insert_params_here>"

   <insert_params_here> 変数では、インストール プログラムに渡すインストール設定を指定します。

   注: サイレント インストールを実行するには、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への同意およびサイレント モードでの CA Access Control のインストールに必要な keyword は、インストール プログラムを実行したときに表示されるエンドユーザ使用許諾契約の下部にあります。

setup コマンド - CA Access Control for Windows のインストール

事前に設定されたカスタム デフォルト(86 ページ)を使用して CA Access Control for Windows をインストールする場合、または サイレント インストール(87 ページ)を実行する場合は、setup コマンドを使用します。

注: コマンド ラインの構文の詳細については、Microsoft Developer Network ライブラリで入手できる Windows インストーラ SDK を参照してください。

このコマンドの形式は以下のようになります。

```
setup [/s] [/L] [/v"<insert_params_here>"]
```

/s

setup の最初のダイアログ ボックスを非表示にします。

/L

CA Access Control インストール言語を定義します。

注: このリリースでサポートされている CA Access Control のインストール言語の詳細については、リリース ノートを参照してください。

/v "<insert_params_here>"

インストール プログラムに渡すパラメータを定義します。

注: パラメータはすべて二重引用符("")で囲みます。

以下のパラメータは、/v パラメータを介してインストール プログラムに渡されます。

/l[mask] log_file

インストール ログ ファイルの完全パスと名前を定義します。 利用可能な情報をすべてログに記録するには、マスク *v を使用します。

/forcerestart

インストールが完了した後でコンピュータが再起動されるよう指定します。

/norestart

インストールが完了した後でコンピュータが再起動されないよう指定します。

/qn

/s オプションとの組み合わせで、サイレント インストールを指定します。

重要: サイレント インストールを実行するには、COMMAND パラメータを使用する必要があります。

AC_API={1 | 0}

SDK ライブラリとサンプルをインストールする(1)かどうかを指定します。

デフォルト: 0(インストールしない)

ADMIN_USERS_LIST=¥"users¥"

CA Access Control データベースに対する管理アクセス権限を持つユーザのスペース区切りリストを定義します。

デフォルト: インストールを実行するユーザ

ADV_POLICY_MNGT_CLIENT={1 | 0}

ローカル コンピュータに拡張ポリシー管理を設定する(1)かどうかを指定します。

デフォルト: 0

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- APMS_HOST_NAME=¥"name¥"

  拡張ポリシー管理コンポーネントがインストールされているサーバの名前を定義します。

  注: このコンピュータに拡張ポリシー管理サーバ コンポーネントもインストールする場合、この情報を指定する必要はありません。

COMMAND=keyword

エンドユーザ使用許諾契約への同意およびサイレント モードでの CA Access Control のインストールに必要なコマンドを定義します。 実際に使用する必要がある keyword は、グラフィカル インストール プログラムを実行したときに表示されるエンドユーザ使用許諾契約の下部にあります。

デフォルト: none

DOMAIN_LIST=¥"domains¥"

ホスト名に追加する、CA Access Control 用のネットワーク DNS ドメインの名前のスペース区切りリストを定義します。

デフォルト: none

ENABLE_STOP={1 | 0}

スタック オーバーフロー保護(STOP)機能を有効にする(1)かどうかを指定します。

デフォルト: 0(無効)

注: STOP のサポートは、x86 と x64 のインストールにのみ適用できます。

HOSTS_LIST=¥"hosts¥"

管理者が CA Access Control データベースの管理に使用するコンピュータ(CA Access Control 端末)のスペース区切りリストを定義します。

デフォルト: 現在のコンピュータ

INSTALLDIR=¥"location¥"

CA Access Control がインストールされる場所を定義します。

デフォルト: C:¥Program Files¥CA¥AccessControl

MAINFRAME_PWD_SYNC={1 | 0}

メインフレームのパスワード同期機能をインストールする(1)かどうかを指定します。

デフォルト: 0(インストールしない)

PMDB_CLIENT={1 | 0}

ローカル CA Access Control データベースを親 Policy Model データベースにサブスクライブする必要があるかどうかを指定します。

デフォルト: 0(設定しない)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- PMDB_PARENTS_STR=¥"parents¥"

  ローカルの CA Access Control データベースがサブスクライブされる、親ポリシー モデル データベースのリストをカンマ区切りリストで定義します。任意の PMDB から伝達される更新をローカル データベースが受け入れるようにするには、_NO_MASTER_ を親 PMDB として指定します。

  デフォルト: none

- PWD_POLICY_NAME=¥"name¥"

  パスワード Policy Model の名前を定義します。

  デフォルト: none

PMDB_PARENT={1 | 0}

Policy Model 親データベースを作成する必要があるかどうかを指定します。このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- PMDB_NAME=¥"name¥"

  作成する PMDB の名前を定義します。

  デフォルト: pmdb

- PMDB_SUBSCRIBERS_STR=¥"subs¥"

  PMDB_NAME オプションで指定された PMDB が変更内容を伝達するサブスクライバ データベースのスペース区切りリストを定義します。これらは基本的にインストール済み親 PMDB のサブスクライバ データベースです。

REPORT_AGENT={1 | 0}

レポート エージェントをインストールする(1)かどうかを指定します。

デフォルト: 0(インストールしない)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- AUDIT_ROUTING={1 | 0}

  監査ルーティング機能がインストールする(1)かどうかを指定します。

  デフォルト: 0(インストールしない)

- NEW_KEY=¥"name¥"

  レポート サーバとレポート エージェント間の通信を認証する SSL キーを定義します。 また、USE_SECURE_COMM=1 とする必要があります。

- REPORT_DAYS_SCHEDULE=days

  レポート エージェントが動作する曜日のカンマ区切りリストを定義します。

  値: 日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日

  デフォルト: none

- REPORT_TIME_SCHEDULE={hh:mm}

  レポート エージェントが、指定された日に動作する時刻を定義します(たとえば、14:30)。

  制限: hh は 0～23 の範囲の数字で、mm は 0～59 の範囲の数字です。

  デフォルト: none

- REPORT_SERVER_NAME=¥"name¥"

  レポート エージェントの設定においてレポート サーバ ホストの名前を定義します(たとえば、test.company.com)。

  デフォルト: none

- REPORT_SERVER_PORT=¥"port¥"

  レポート エージェントの設定においてレポート サーバのポート番号を定義します。

  デフォルト: none

- USE_SECURE_COMM={1 | 0}

  レポート エージェントで安全な通信を使用する(1)かどうかを指定します。

  デフォルト: 0(設定しない)

PUPM_AGENT={1 | 0}

PUPM エージェントをインストールする(1)かどうかを指定します。

デフォルト: 0(インストールしない)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- DIST_SERVER_NAME=¥"name¥"

  レポート エージェントまたは PUPM エージェント設定用の配布サーバホストの名前を定義します(例: test.company.com)。

  デフォルト: none

- DIST_SERVER_PORT=¥"port¥"

  レポート エージェントまたは PUPM エージェント設定用の配布サーバのポート番号を定義します。

  デフォルト: 7243

- NEW_KEY=¥"name¥"

  配布サーバとレポート エージェント間、または配布サーバと PUPM エージェント間の通信を認証する SSL キーを定義します。

  また、USE_SECURE_COMM=1 とする必要があります。

- USE_SECURE_COMM={1 | 0}

  レポート エージェントまたは PUPM エージェントが安全な通信を使用する(1)かどうかを指定します。

  デフォルト: 1 (変更する)

TASK_DELEGATION={1 | 0}

タスクの委任機能を有効にするかどうかを指定します。

デフォルト: 1 (有効)

UNICENTER_INTEGRATION={1 | 0}

Unicenter の統合機能を有効にする(1)かどうかを指定します。 この機能は、該当するコンピュータに Unicenter NSM がインストールされている場合にのみ利用できます。

デフォルト: 0 (無効)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- SEND_DATA_TO_TNG={1 | 0}

  監査データを Unicenter NSM に送信する(1)かどうかを指定します。

  デフォルト: 1 (データを送信)

- OTHER_TNG_HOST_NAME=¥"name¥"

  監査データが送信されるホストを定義します。

  デフォルト: Unicenter NSM で指定されたホスト名

- SUPPORT_TNG_CALENDAR= {1 | 0}

  Unicenter NSM カレンダをサポートする(1)かどうかを指定します。

  デフォルト: 1 (サポートする)

- TNG_REFRESH_INTERVAL=¥"mm¥"

  更新間隔を分単位で定義します。 また、SUPPORT_TNG_CALENDAR=1 とする必要があります。

  デフォルト: 10

- UNICENTER_MIGRATION={1 | 0}

  Unicenter セキュリティ データを CA Access Control に移行する(1)かどうかを指定します。

  デフォルト: 1 (移行する)

USE_SSL={1 | 0}

通信の暗号化として SSL を設定するかどうかを指定します。

デフォルト: 0(設定しない)

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- CERT_OPTION={1 | 2}

  使用する認証オプションを指定します。

  値: 1 - CA Access Control 証明書を生成します。2 - インストールされた既存の証明書を使用します。

  デフォルト: 1

- GENERATE_OPTION={1| 2}

  CA Access Control 証明書の生成方法を指定します。 また、CERT_OPTION=1 とする必要もあります。

  値: 1 - デフォルトのルート証明書を使用します。2 - ルート証明書を指定します。

- GEN_ROOT_CERT=¥"file¥"

  ルート証明書ファイル(.pem)の完全修飾ファイル名を定義します。 また、CERT_OPTION=1 および GENERATE_OPTION=2 とする必要があります。

- GEN_ROOT_PRIVATE=¥"file¥"

  ルート秘密鍵ファイル(.key)の完全修飾ファイル名を定義します。 また、CERT_OPTION=1 および GENERATE_OPTION=2 とする必要があります。

- EXIST_ROOT_CERT=¥"file¥"

  ルート証明書ファイル(.pem)の完全修飾ファイル名を定義します。 また、CERT_OPTION=2 とする必要があります。

- EXIST_ROOT_PRIVATE=¥"file¥"

  ルート秘密鍵ファイル(.key)の完全修飾ファイル名を定義します。 また、CERT_OPTION=2 とする必要があります。

- EXIST_SERVER_CERT=¥"file¥"

  サーバ証明書ファイル(.pem)の完全修飾ファイル名を定義します。 また、CERT_OPTION=2 とする必要があります。

USE_SYMT_KEY={1 | 0}

通信に対して対称鍵暗号化を設定するかどうかを指定します。 USE_SSL=0 の場合、このパラメータは 1 に設定されます。

デフォルト: 1

このオプションを指定し、値を 1 に設定した場合は、以下のオプションも指定する必要があります。

- ENCRYPTION_METHOD={Default | DES | 3DES | ¥"256bit AES¥" | ¥"192bit AES¥" | ¥"128bit AES¥"}

  通信において使用する暗号化の方法を指定します。

  デフォルト: Default

- CHANGE_ENC_KEY={1 | 0}

  デフォルトの暗号化キーを変更する(1)かどうかを指定します。

  デフォルト: 1 (変更する)

- NEW_ENCRYPT_KEY=¥"key¥"

  デフォルトの暗号化キーの変更を指定した場合、暗号化キーを定義します。また、CHANGE_ENC_KEY=1 とする必要があります。

IMPORT_NT_DATA={Y | N}

プライマリ ユーザ ストアをサポートするかどうかを指定します。 N を指定すると、以下のオプションを 1 つ以上指定して、Windows ユーザと Windows グループを CA Access Control データベースにインポートできます。

- IMPORT_USERS={1 | 0}

  Windows ユーザをデータベースにインポートするかどうかを選択します。

- IMPORT_GROUPS={1 | 0}

  Windows グループをデータベースにインポートするかどうかを選択します。

- IMPORT_CONNECT_USERS={1 | 0}

  インポートしたユーザをデータベース内のインポートしたグループに自動的に追加するかどうかを指定します。

- IMPORT_CHANGE_OWNER={1 | 0} NEW_OWNER_NAME=name

  インポートしたデータの所有者として、自分以外のユーザを指定します。

- IMPORT_FROM_DOMAIN={1 | 0} IMPORT_DOMAIN_NAME=name

  定義したドメインからアクセサ データをインポートするかどうかを指定します。

注: デフォルトでは、これらのオプションのいずれも指定されていません(値 0 に相当する)。

例: setup コマンドを使用してインストール時のデフォルトを設定する

以下の例では、インストール ディレクトリを設定し、CA Access Control インストールのためにインストール ログ ファイルのデフォルトを定義し、グラフィカル インストール プログラムを開きます。

```
setup.exe /s /v"INSTALLDIR="C:¥CA¥AC" /L*v %SystemRoot%¥eACInstall.log"
```

Unicenter ソフトウェア配信のインストール

Unicenter ソフトウェア配信から CA Access Control をインストールするには、以下の手順に従います。

注: CA Access Control Endpoint Components for Windows DVD には、REGINFO という名前のディレクトリが含まれています。 このディレクトリには、Unicenter ソフトウェア配信を使用して CA Access Control をインストールするために必要な複数のファイルが含まれています。

1. CA Access Control の Unicenter ソフトウェア配信パッケージをエクスポートするには、CA Access Control の Endpoint Components for Windows DVD を光ディスクドライブに挿入します。
2. Unicenter ソフトウェア配信のエクスプローラを起動します。
3. CA Access Control の Unicenter ソフトウェア配信パッケージを登録するには、CA Access Control をインストールする root ディレクトリを選択します。
4. CA Access Control パッケージを開きます。
5. サービスの開始、サービスの停止、アンインストール、およびアップグレードの各手順で、<admin> パラメータおよび <password> パラメータを CA Access Control の ADMIN ユーザのクレデンシャルと置き換えます。

   注: これらのクレデンシャルは、これらのプロセス中に CA Access Control を停止する際に使用されます。 ユーザを入力すると、そのユーザはこれらのクレデンシャルを使用してクライアント コンピュータにログオンできます。
6. パッケージを封印します。

Windows エンドポイントのアップグレード

いずれかのエンドポイントをアップグレードする場合、CA Access Control インストール プログラムは CA Access Control の主要機能、およびそのエンドポイントにすでにインストールされているすべての機能をアップグレードします。 CA Access Control の主要機能をアップグレードした後に、新機能をインストールできできます。

注: インストール完了後に、コンピュータの再起動が必要な場合があります。 アップグレード時に、CA Access Control のどのリリースで再起動が必要となるかについては、「リリース ノート」を参照ください。

エンドポイントのアップグレード方法

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。

   注: コンピュータのアーキテクチャと一致するインストール オプションは強調表示され、このコンピュータ上に CA Access Control がすでにインストールされていることがわかります。

   CA Access Control のアップグレードを実行するかどうか尋ねるダイアログ ボックスが表示されます。
5. [はい]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。
6. インストール画面の指示に従います。

   インストール プログラムによって CA Access Control がアップグレードされます。 アップグレードが完了すると、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. (オプション)「はい」を選択すると、コンピュータがすぐに再起動します。

   コンピュータが再起動して、アップグレードが完了します。

8. (オプション) 以下のように 追加の CA Access Control 機能をインストールします。

   a. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   b. プログラム リストをスクロールして CA Access Control を選択し、[変更]をクリックします。

      CA Access Control インストール プログラムのローディングが開始され、しばらくして、プログラムのメンテナンス画面が表示されます。

   c. [変更]を選択し、インストール画面の指示に従って、各機能をインストールします。

      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。 各機能のインストールで必要な情報については、インストール ワークシート(80 ページ)を参照してください。 インストール完了後に、コンピュータの再起動が必要な場合があります。

CA Access Control の起動および停止

デフォルトでは、Windows を開始する場合は常に、CA Access Control サービスが自動的に開始します。

CA Access Control の停止

secons ユーティリティを使用して、ローカル コンピュータおよびリモート コンピュータ上の CA Access Control を停止します。 CA Access Control の停止には特定の Windows 権限を必要としませんが、CA Access Control の ADMIN または OPERATOR 属性を持っている必要があります。

注: CA Access Control が Windows サービス マネージャから実行されている間は、その CA Access Control を停止できません。 secons ユーティリティを使用して CA Access Control を停止してから、Windows サービス マネージャ内で CA Access Control サービスを変更してください。

CA Access Control の停止方法

1. コマンド プロンプト ウィンドウを開き、CA Access Control バイナリがあるディレクトリに移動します。

   デフォルトでは、CA Access Control バイナリは C:¥Program Files¥CA¥AccessControl¥bin にあります。

2. 以下のコマンドを入力します。

   ```
   secons -s [hosts | ghosts]
   ```

   -s [hosts | ghosts]

   スペース区切りで定義された複数のリモート ホスト上の CA Access Control サービスを停止します。 ホストを指定しない場合、CA Access Control はローカル ホスト上のサービスを停止します。

   ghost レコードの名前を入力することで、ホスト グループを定義できます。 このオプションをリモート端末から使用する場合は、ユーティリティによってパスワードの検証が要求されます。 また、リモート コンピュータとローカル コンピュータの管理者権限、およびローカル コンピュータでのリモート ホスト データベースに対する書き込み権限も必要です。

   ユーザがローカル コンピュータ上の CA Access Control を停止する場合、以下のメッセージが表示されます。

   CA Access Control は現在停止中です。

   リモート ホスト上の CA Access Control を停止すると、リモート ホスト上の CA Access Control の停止が正常に行われたかどうかを報告するメッセージが表示されます。 1 台のリモート ホスト上の AC を正常に停止できなかった場合でも、そのホストの後に指定されているリモート ホスト上の AC の停止操作は続行されます。

CA Access Control の手動での起動

通常、Windows を起動することで、CA Access Control を起動します。

CA Access Control を停止した場合は、コマンド プロンプトからコマンドを発行することにより、CA Access Control を手動で再起動することができます。

CA Access Control を手動で起動するには、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 システムにログオンしていることを確認してください。
2. [コマンド プロンプト]ウィンドウで、CA Access Control のバイナリ ファイルがインストールされているディレクトリに移動します(デフォルトでは、バイナリ ファイルは、システム ディレクトリの C:¥Program Files¥CA¥AccessControl¥bin にインストールされています)。
3. 以下のコマンドを入力して、CA Access Control を起動します。

   ```
   seosd -start
   ```

インストールの確認

CA Access Control のインストールが正常に完了したら、以下の変更点に注目してください。

- 以下の Windows レジストリに新しいキーが追加されています。

  HKEY_LOCAL_MACHINE¥Software¥ComputerAssociates¥AccessControl

  CA Access Control が実行されている間、CA Access Control のキーおよびサブキーは保護されています。また、キーを変更できるのは、CA Access Control エンドポイント管理 を使用するか、selang コマンドの使用する場合のみです。 しかしながら、キーと値を読み取るために CA Access Control エンドポイント管理 または selang コマンドを使用する必要はありません。

- コンピュータを再起動すると、CA Access Control の複数の新しいサービスが自動的に開始されます。 これらのサービスには、Watchdog、Engine、および Agent が含まれます。この 3 つのサービスは必ずインストールされます。 タスクの委任などのその他のサービスは、インストール時に選択したオプションによってインストールされるかどうかが決まります。 CA Access Control サービスの表示名はすべて、「CA Access Control」で始まります。 Windows サービス マネージャを使用すれば、インストールされているサービスを確認し、それらのサービスが動作中であることを検証できます。

ログイン保護画面の表示

デフォルトでは、CA Access Control をインストールすると、サービスが実行されている場合に、ユーザが対話形式(GINA)でログインすると、常にログイン保護画面が表示され、このコンピュータが CA Access Control により保護されていることをユーザに通知します。

スプラッシュ画面が 4 秒間表示され、自動的に閉じます。

この保護メッセージを無効にするには、HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥AccessControl¥SplashEnable レジストリ キーの値を 1 から 0 に変更する必要があります。

エンドポイントへの拡張ポリシー管理の設定

拡張ポリシー管理サーバ コンポーネントをインストールしたら、拡張ポリシー管理を行うために企業内の各コンピュータを設定する必要があります。 その際、サーバ コンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: この手順では、拡張ポリシー管理を行うために CA Access Control の既存のインストールを設定する方法を示します。 エンドポイント上に CA Access Control をインストールした時にこの情報を指定している場合は、再びエンドポイントを設定する必要はありません。

エンドポイントを設定して拡張ポリシー管理を実行できるようにするには、コマンド ウィンドウを開き、次のコマンドを入力します。

```
dmsmgr -config -dhname dhName
```

dhName

エンドポイントが対応する分散ホスト(DH)名のカンマ区切り形式のリストを定義します。

例: DH__@centralhost.org.com

このコマンドでは、拡張ポリシー管理を行うためにエンドポイントが設定されます。また、定義された DH と動作するようにエンドポイントが設定されます。

注: 詳細については、「リファレンス ガイド」の「dmsmgr -config」コマンドの説明を参照してください。

レポート作成のための Windows エンドポイントの設定

CA Access Control エンドポイント管理 およびレポート ポータルのインストールおよび設定の完了後、配布サーバにデータを送信して処理するようにエンドポイントを設定できます。そのためには、レポート エージェントを有効にして設定します。

注: CA Access Control をインストールすると、レポート作成のためにエンドポイントを設定することが可能になります。 この手順では、インストール時にこのオプションを設定しなかった場合、レポートを送信するための既存のエンドポイントを設定する方法について説明します。

レポート作成のための Windows エンドポイントの設定方法

1. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   [プログラムの追加と削除]ダイアログ ボックスが表示されます。

2. プログラム リストをスクロールして CA Access Control を選択します。

3. ［変更］をクリックします。

   CA Access Control のインストール ウィザードが表示されます。

4. ウィザードのプロンプトに従って CA Access Control インストールを変更し、レポート エージェント機能を有効にします。

注: レポート エージェントを有効にしたら、CA Access Control 構成設定を変更してパフォーマンス関連の設定を変更できます。 レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

CA Access Control のクラスタ環境用へのカスタマイズ

クラスタ環境で CA Access Control を使用するには、クラスタの各ノードに CA Access Control をインストールする必要があります。 各ノードの共通リソース用に一連の同じルール（クォーラム ディスク、またはネットワーク インターセプトを使用している場合はネットワーク）を定義します。

CA Access Control では、CA Access Control がクラスタ環境で実行されているかどうかを検出できます。 CA Access Control により、クラスタに別のクラスタの内部通信用ネットワーク アダプタがあることが検出された場合、これらのネットワーク アダプタのネットワーク インターセプトは無効になります。 クラスタを企業内の他のネットワークに接続するネットワーク インターフェースについては、ネットワーク インターセプトは通常どおり機能します。

注: クラスタで、クラスタ内部通信用およびネットワークの他の部分との通信用の両方に同じネットワーク インターフェースが使用されている場合、この機能は有効になりません。

例

2 つのノードがあると仮定します。

- NODE1 は以下の 2 つの IP アドレスを保持しています。
  - 10.0.0.1 は、内部クラスタ ネットワーク IP アドレスです。
  - 192.168.0.1 は、外部ネットワーク接続用の IP アドレスです。
- NODE2 は以下の 2 つの IP アドレスを保持しています。
  - 10.0.0.2 は、内部クラスタ ネットワーク IP アドレスです。
  - 192.168.0.2 は、外部ネットワーク接続用の IP アドレスです。

  クラスタ自体は、これら以外の IP アドレス 192.168.0.3 を保持しています。

NODE1 と NODE2 の間の通信はクラスタ内部ネットワーク用の IP アドレスを使用して行われるため、ネットワーク インターセプトは、これらのノード間で接続が行われることを妨げません。

NODE1 または NODE2 で外部ネットワーク IP アドレスを使用して接続が行われる場合、ネットワーク インターセプトは CA Access Control のルールで定義したとおりに機能します。

さらに、クラスタの IP アドレス「192.168.0.3」に対して接続が行われた場合、ネットワーク インターセプトは CA Access Control で定義したとおりに機能します。

アンインストールの方法

以下の方法で Windows エンドポイントから CA Access Control をアンインストールすることができます。

- 標準アンインストール - この方法では、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。
- サイレント アンインストール - この方法では、コマンドラインを使用して、対話形式のフィードバックなしで CA Access Control をアンインストールします。

CA Access Control のアンインストール

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 システムにログオンしていることを確認してください。

CA Access Control のアンインストール方法

1. (オプション)CA Access Control のシャットダウン(99 ページ)を実行します。

   注: この操作をユーザが手動で実行しない場合、インストール プログラムが代わりに CA Access Control をシャットダウンします。

2. [スタート]-[設定]-[コントロール パネル]を選択します。

   Windows の[コントロール パネル]が表示されます。

3. [アプリケーションの追加と削除]をダブルクリックします。

   [プログラムの追加と削除]ダイアログ ボックスが表示されます。

4. インストールされているプログラムのリストから CA Access Control を選択し、[追加と削除]をクリックします。

5. CA Access Control の削除を確認するメッセージ ボックスで[はい]をクリックします。

6. アンインストールの完了後、[OK]をクリックします。
7. コンピュータを再起動すると、すべての CA Access Control コンポーネントが削除されます。

サイレント モードでの CA Access Control のアンインストール

対話形式のフィードバックなしで CA Access Control をアンインストールするには、コマンド ラインを使用して CA Access Control をサイレント モードでアンインストールすることができます。 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 システムにログオンしていることを確認してください。

CA Access Control r12.5 をサイレント モードでアンインストールするには、以下のコマンドを入力します。

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn insert_params_here
```

<insert_params_here> 変数では、インストール プログラムに渡すインストール設定を指定します。 たとえば、このコマンドは CA Access Control をアンインストールして、c:¥ac_uninst.log に以下のアンインストール ログを作成します。

```
Msiexec.exe /x{822BFADC-E040-4F5C-A00A-B8E558A2D616} /qn /l*v c:¥ac_uninst.log
```

注: この操作をユーザが手動で実行しない場合、インストール プログラムが代わりに CA Access Control をシャットダウンします。

第 5 章: UNIX エンドポイントのインストールおよびカスタマイズ

この章では、CA Access Control UNIX エンドポイントのインストール プロセスについて説明します。 この章の手順に従って CA Access Control のインストールを完了すると、CA Access Control エンドポイント ソフトウェアと CA Access Control の基本データベースがシステムにインストールされます。 次に、CA Access Control の起動方法、および関連するコマンドの使用方法について説明します。 起動後にデータベースを編集することにより、システムを保護するアクセス ルールを定義できます。

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

CA Access Control をインストールするには、事前に準備要件を満たし必要な情報をすべて揃えておく必要があります。

オペレーティング システムのサポートおよび要件

サポートされている UNIX オペレーティング システムのいずれか 1 つに CA Access Control をインストールすることができます。

注: 詳細については、「リリース ノート」を参照してください。

管理端末

CA Access Control ポリシーを管理するには、CA Access Control エンドポイント管理 および CA Access Control エンタープライズ管理 を使用して中央から管理するか、コマンド ライン(selang)を使用してコンピュータに接続し、コンピュータのアクセス ルールを直接更新します。

コンピュータのアクセス ルールを直接更新するには、管理用端末での書き込みアクセス権と、CA Access Control データベース内のコンピュータ ポリシーにおける admin 属性が必要です。

デフォルトでは、CA Access Control をインストールすると、ローカル コンピュータ端末に対してのみ端末許可が設定されます。 この設定は変更できます。それには、ローカル端末からこのオプションを無効にするか、リモートで管理可能な端末を追加します。

端末 my_terminal の管理オプションを、ユーザ my_user を使用してコンピュータ my_machine に追加するには、以下の selang ルールを作成します。

```
er terminal my_terminal owner(nobody) defaccess(r)
auth terminal my_terminal xuid(my_user) access(all)
```

これらのルールでは、すべてのユーザがこの端末にログインでき(CA Access Control 管理ではなく、通常のログイン)、企業ユーザ my_uid はコンピュータにログインし CA Access Control 管理ツール(selang や CA Access Control エンドポイント管理 など)を使用できます。

注: 管理者が CA Access Control エンドポイント管理 を使用して CA Access Control を管理する場合は、CA Access Control エンドポイント管理 がインストールされているコンピュータを定義するだけで済みます。 管理者によってブラウザが開かれるコンピュータを定義する必要はありません。

インストール上の注意事項

CA Access Control をインストールする際には、初回インストールまたはアップグレードの一環としてのインストールに関わらず、以下の点に注意してください。

- 「リリース ノート」をお読みください。

  このドキュメントでは、サポートされるプラットフォームに関する情報、既知の問題点、考慮事項、および CA Access Control をインストールする前に把握しておく必要のあるその他の重要な情報について説明しています。

- 対象となる環境が PMDB 階層で設定されている場合、またはそのような環境を設定する場合は、以下の作業を行うことをお勧めします。

  - Deployment Map Server(DMS)コンピュータをインストールまたはアップグレードします。

    これは拡張ポリシーベース管理を使用する場合にのみ必要な作業です。この作業により、各 Policy Model ノードおよびそのサブスクライバが DMS に確実に登録されます。

  - 階層内の各コンピュータのインストールまたは各コンピュータのアップグレードを下から上の順(サブスクライバが最初)で行います。

    PMDB のアップグレード時に、旧バージョンを利用しているサブスクライバが存在する場合、誤ったコマンドが送信される場合があります。 この問題は、旧バージョンの PMDB に存在しないクラスやプロパティが新しい PMDB に含まれることが原因で発生します。

    注: 単一のコンピュータ上で動作する PMDB 階層については、同時にアップグレードすることができます。

  - PMDB またはポリシーの更新中にアップグレードを行わないでください。
  - サブスクライバおよび PMDB ポリシーをバックアップします。

  注: 旧バージョンの PMDB は、新しいバージョンのサブスクライバを保持できます。しかし、これと逆の状況は許可されていません。 旧バージョンのコマンドは最新バージョンでもサポートされているため、CA Access Control r12.0 のサブスクライバへの古い PMDB の伝播が可能です。

- r12.0 より前のバージョンからアップグレードしている場合:

  - STOP によるバイパスが必要なプログラムは、データベース ルールとして定義されるようになります(stop タイプの SPECIALPGM レコード)。
  - SURROGATE によるバイパスが必要なプログラムは、データベース ルールとして定義されるようになります(surrogate タイプの SPECIALPGM レコード)。

  注: アップグレード プロセスでは、ファイル内に保存されている古い定義が新しいデータベース ルールに変換されます。 これらの新しいルールを既存の selang スクリプトに追加します。

- 既存の seos.ini ファイルおよび pmd.ini ファイルをアップグレードすることも、これらのファイルを新規作成することもできます。

  いずれの場合も、インストール スクリプトにより、古い seos.ini ファイルのコピーが seos_ini.back として保存され、各 pmd.ini ファイルのコピーが pmd_ini.back として保存されます。保存先は、該当する Policy Model ディレクトリです。

- アップグレード中には、CA Access Control によって、serevu.cfg、audit.cfg、trcfilter.init、および sereport.cfg という既存のファイルがバックアップされます。

  これらのファイルの変更内容を保持したい場合は、バックアップ ファイルを使用する必要があります。

- 既存のデータベースをアップグレードする場合は、以下の作業を行うことをお勧めします。

  - まず、データベースをバックアップします。

    データベースをバックアップするには、dbmgr -b を使用します。

  - sync モードのサブスクライバが存在していないことを確認します。

    サブスクライバのステータスを確認するには、sepmd -L を使用します。

- Unicenter セキュリティの統合および移行は、AIX、HP-UX PA-RISC、Solaris SPARC、および Linux x86 のプラットフォームでのみサポートされています。

- Unicenter TNG および CA Access Control for UNIX

  Unicenter NSM 3.0 より古いバージョンの Unicenter TNG がインストールされている場合は、以下の Unicenter TNG 修正プログラムをインストールして、CA Access Control でプロセス情報を取得できるようにしてください。

  - Unicenter TNG 2.4 運用の HP-UX ユーザの場合: 修正プログラム QO01182
  - Unicenter TNG 2.4 運用の Linux ユーザの場合: 修正プログラム PTF LO91335
  - Unicenter TNG 2.4 運用の Sun ユーザの場合: 修正プログラム QO00890

  注: Unicenter NSM 3.0 運用の AIX 5.x ユーザは、弊社 Unicenter テクニカルサポートにお問い合わせの上、互換性パッチを入手してください。 CA Access Control をホストにインストールする前に、この互換性パッチをインストールする必要があります。

- Linux s390 に Unicenter の関連オプション(install_base オプションは -uni、または -mfsd)をインストールする場合は、CA Access Control をインストールする前に、korn シェル(ksh)をインストールしておく必要があります。

  CCI Standalone (CCISA) のセットアップ スクリプトで ksh を使用しますが、これはデフォルトでは Linux にインストールされません。

- CA Access Control32 ビット バイナリを Linux x86 64 ビット上にインストールする場合は、_LINUX_xxx.tar.Z または CAeAC-xxxx-y.y.iiii.i386.rpm のいずれかのインストール パッケージを使用することをお勧めします。 これらのインストール パッケージは、32 ビットの CA Access Control バイナリを 64 ビットの Linux x86 システムにインストールします。 アップグレードの場合、これらのパッケージは以前の 32 ビット CA Access Control のインストールとの互換性を維持しています。 CA Access Control をインストールする前に、以下のオペレーティング システムの 32 ビット ライブラリがインストールされていることを確認する必要があります。

  ld-linux.so.2、libICE.so.6、libSM.so.6、libX11.so.6、libXext.so.6、libXp.so.6、libXt.so.6、libc.so.6、libcrypt.so.1、libdl.so.2、libgcc_s.so.1、libm.so.6、libncurses.so.5、libnsl.so.1、libpam.so.0、libpthread.so.0、libresolv.so.2、libstdc++.so.5、libaudit.so.0（RHEL5 および OEL 5 のみ）

  以下に、必要な関連 RPM パッケージを示します。

  - SLES 10： compat-libstdc++、glibc-32bit、libgcc、ncurses-32bit、pam-32bit、xorg-x11-libs-32bit
  - SLES 9： glibc-32bit、libgcc、libstdc++、ncurses-32bit、pam-32bit、XFree86-libs-32bit
  - RHEL 5 および OEL 5： audit-libs、compat-libstdc++、glibc、libgcc、libICE、libSM、libXext、libXp、libXt、ncurses、pam
  - RHEL 4 および OEL 4： compat-libstdc++、glibc、libgcc、ncurses、pam、xorg-x11-deprecated-libs、xorg-x11-libs
  - RHEL 3： glibc、libgcc、libstdc++、ncurses、pam、XFree86-libs

- CA Access Control 64 ビット バイナリを Linux x86 64 上にインストールするには、_LINUX_X64_xxx.tar.Z または CAeAC-xxxx-y.y.iiii.x86_64.rpm のいずれかのインストール パッケージを使用します。 これらのインストール パッケージを使用している場合は、その他に RPM パッケージをインストールする必要はありません。

  64 ビットの CA Access Control バイナリを 64 ビットの Linux x86 にインストールまたはアップグレードする前に、以下の点に注意が必要です。

  - 64 ビットのインストール パッケージは、selock や selogo などの CA Access Control GUI ユーティリティをサポートしていません。
  - install_base スクリプトが 32 ビットと 64 ビットの両方の tar ファイルにアクセスできる場合、install_base スクリプトはデフォルトで 32 ビットの tar ファイルを使用します。 この動作を変更するには、install_base コマンドの実行時に使用する tar ファイルを指定します。 64 ビットの RPM パッケージをインストールする場合は、64 ビットのバイナリとライブラリのみがインストールされます。
  - 構築されて API にリンクされているアプリケーションは、64 ビットのインストール用に再構築する必要があります。 64 ビットの API サンプルを構築するには、LINUX64 系のターゲットを使用します。 このターゲットは、D64BIT および -D64BITALL（-m32 を削除）を使用します。 ライブラリを構築するには、-melf_x86_64 が必要です。

- install_base スクリプトを使用して 32 ビットの CA Access Control インストールから 64 ビットのインストールにアップグレードするには、インストールの前に -force_install フラグを設定する必要があります。 このフラグを設定していない場合、インストールは失敗します。
- CA Access Control をアンインストールしてから cawin を完全にアンインストールするには、アンインストール プロセスで 32 ビットと 64 ビットの両バージョンの cawin が削除されるように rpm -e --allmatches を使用してください。

- CA Access Control を 64 ビット Linux s390 にインストールする場合は、以下のオペレーティング システムの 32 ビット ライブラリがインストールされていることを必ず確認してください。

  ld.so.1、libcrypt.so.1、libc.so.6、libdl.so.2、libICE.so.6、liblaus.so.1（SLES 8、RHEL 3）、libaudit.so.0（RHEL 4、RHEL 5）、libm.so.6、libnsl.so.1、libpam.so.0、libresolv.so.2、libSM.so.6、libX11.so.6、libXext.so.6、libXp.so.6、libXt.so.6

  以下に、必要な関連 RPM パッケージを示します。

  - SLES 10： glibc-32bit、pam-32bit、xorg-x11-libs-32bit
  - SLES 9： XFree86-libs-32bit、glibc-32bit、pam-32bit
  - RHEL 5： audit-libs、libXp、glibc、libICE、libSM、libX11、libXext、libXt、pam
  - RHEL 4： audit-libs、glibc、pam、xorg-x11-deprecated-libs、xorg-x11-libs
  - RHEL 3： glibc、laus-libs、pam
- -all オプションを使用して、CA Access Control を Linux および Linux-IA64 プラットフォームにインストールする場合、mfsd はインストールされません。
- 32 ビットまたは 64 ビットの Linux コンピュータに CA Access Control 32 ビットバイナリをインストールする場合、事前に、libstdc++.so.5 32 ビット ライブラリがインストールされていることを確認する必要があります。 このライブラリをインストールしないと、CA Access Control のインストール後に ReportAgent デーモンが開始されません。

ネイティブ インストール

CA Access Control に用意されているネイティブ パッケージ形式を使用すると、サポートされているオペレーティング システム上で、CA Access Control をネイティブにインストールおよび管理できます。 ネイティブ パッケージでは、ネイティブ パッケージ管理ツールを使用して、インストールされた CA Access Control を管理できます。

ネイティブ パッケージ

CA Access Control には、サポートする各ネイティブ インストール形式について、ネイティブ パッケージがあります。 これらのパッケージでは、ネイティブ パッケージ機能を使用して、CA Access Control コンポーネントのインストール、更新、および削除を管理できます。 ネイティブ パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

以下は、パッケージとその説明です。

ca-lic

(Linux のみ)他のすべてのパッケージの前提条件となる CA ライセンス プログラムをインストールします。

注: Linux の場合は RPM 形式でのみ提供されます。

ca-cs-cawin

(Linux のみ)CA Access Control パッケージのインストール前にインストールする必要がある、 CAWIN 共有コンポーネントをインストールします。

注: Linux の場合は RPM 形式でのみ提供されます。

CAeAC

中心となる CA Access Control コンポーネントをインストールします。 これは、メインの CA Access Control インストール パッケージです。サーバ、クライアント、ドキュメント、TNG 統合、API、および mfsd の各パッケージの組み合わせです。これらのパッケージは、従来は別々に提供されていました。

一部のネイティブ コマンド(RPM でのパッケージの削除など)を実行するには、パッケージの名前を知る必要があります。 パッケージ ファイルを使用してパッケージの名前を確認するには、適切なネイティブ パッケージ コマンドを入力します。 たとえば、RPM パッケージの場合は、以下のように入力します。

```
rpm -q -p RPMPackage_filename
```

ネイティブ インストールの際に考慮するその他の事項

ネイティブ パッケージングを使用して CA Access Control をインストールするときは、以下の点に注意してください。

- CA Access Control RPM パッケージをインストールするには、事前に以下のパッケージをインストールしておく必要があります。
  - ライセンス プログラム パッケージ ca-lic-01.0080 以上
  - CAWIN パッケージ ca-cs-cawin-11.0.6 以上

- カスタム CA Access Control RPM ネイティブ インストール パッケージ (customize_eac_rpm)を作成するには、ご使用のコンピュータで rpmbuild ユーティリティが使用可能である必要があります。
- カスタム CA Access Control AIX ネイティブ インストール パッケージ (customize_eac_bff)を作成するには、コンピュータに bos.adt.insttools をインストールする必要があります。

  AIX 5.2 の場合、bos.adt.insttools のバージョンは 5.2.0.75 以降である必要があります。
- AIX ネイティブ パッケージは、bos.rte.install 5.2.0.75 で作成されます。 したがって、ネイティブ パッケージングをエラーなしに操作するには、bos.rte.install 5.2.0.75 以降を使用することをお勧めします。
- HP-UX ネイティブ パッケージは、インストール時に Perl を使用します。
- Solaris ネイティブ パッケージは、グループおよび全員に対する読み取りアクセス権が設定された公開場所(/var/spool/pkg など)に配置される必要があります。
- Solaris ネイティブ パッケージ コマンド pkgadd -R は、CA Access Control パッケージではサポートされていません。

  インストール ディレクトリを変更するには、CA Access Control パッケージ カスタマイズ スクリプトを使用します(customize_eac_pkg -i install_loc)。
- HP-UX ネイティブ パッケージのローカライズされたバージョンをインストールする場合は、必ず、カスタマイズされたパッケージに使用するパラメータ ファイル内の LANG 設定の値を設定してください。

  注: パラメータ ファイルには、すでに LANG 設定が含まれています。 設定するには、先頭のコメント文字(#)およびスペースを削除し、値を入力します。 locale -a コマンドを使用すると、OS がサポートしているエンコーディング値を見ることができます。

詳細情報:

インストール上の注意事項(109 ページ)

RPM Package Manager のインストール

RPM Package Manager（RPM）は、個々のソフトウェア パッケージを作成、インストール、クエリ、確認、更新、および消去することができるコマンドライン ユーティリティです。RPM は、UNIX プラットフォームで使用するためのものです。

注: 詳細については、RPM Package Manager の Web サイト（http://www.rpm.org）および RPM に関する UNIX のマニュアル ページを参照してください。

通常のインストールの代わりに、CA Access Control に用意されている RPM パッケージを使用することができます。 これにより、インストールした CA Access Control を、RPM を使用してインストールされた他のソフトウェアと同様に管理できます。

RPM データベースからの既存の RPM パッケージの削除

自分で作成した CA Access Control RPM パッケージがすでにインストールされている場合は、そのパッケージを RPM データベースから削除する必要があります。これにより、新たにインストールされたパッケージがデータベースに反映されます。 既存のパッケージを削除することなく新しいパッケージをインストールした場合、RPM データベースでは古いパッケージと新しいパッケージの両方がインストールされていると示されますが、ファイル システムでは、既存のファイルが新しいパッケージのファイルによって上書きされます。 RPM でパッケージをアップグレードする場合、パッケージの名前は現在インストールされているパッケージと同じ名前にする必要があります。

注: パッケージを削除しても CA Access Control ファイルは削除されません。ネイティブ パッケージをインストールすると、アップグレードされます。

RPM データベースからパッケージを削除するには、以下のコマンドを使用します。

```
rpm -e --justdb your_ACPackageName
```

CA Access Control RPM パッケージのカスタマイズ

ネイティブ パッケージを使用して CA Access Control をインストールする前に、CA Access Control パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。 パラメータ ファイルを変更しなくても済むように、カスタマイズ スクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、CA Access Control パッケージをカスタマイズしてください。

サポートされた各 Linux オペレーティング システムに対する RPM パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages/RPMPackages ディレクトリにあります。

CA Access Control RPM パッケージのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所にコピーします。

   OS は、オペレーティング システム上の適切なサブディレクトリ名です。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

2. customize_eac_rpm スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA Access Control のエンド ユーザ使用許諾契約が含まれています。

   注: customize_eac_rpm スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

   ```
   customize_eac_rpm -a [-d pkg_location] pkg_filename
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA Access Control パッケージをカスタマイズします。

   ```
   customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
   ```

6. (オプション)インストール パラメータ ファイルの言語を指定します。

   ```
   customize_eac_rpm -r -l lang [-d pkg_location] pkg_filename
   ```

7. (オプション)eTrust Access Control r8 SP1 パッケージからアップグレードします。

   ```
   customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
   ```

8. (オプション)デフォルトの暗号化ファイルを変更します。

   ```
   customize_eac_rpm -s -c certfile -k keyfile [-d pkg_location] pkg_filename
   ```

9. (オプション)インストール パラメータ ファイルを取得します。

   ```
   customize_eac_rpm -g -f tmp_params [-d pkg_location] pkg_filename
   ```

10. (オプション)インストール要件に合わせて、インストール パラメータ ファイルを編集します。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。 たとえば、POSTEXIT 設定(前の # 文字を削除します)をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション)カスタマイズしたパッケージのインストール パラメータを設定します。

    ```
    customize_eac_rpm -s -f tmp_params [-d pkg_location] pkg_filename
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA Access Control をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。 以下の例では、CA Access Control Endpoint Components for UNIX DVD(/mnt/AC_DVD にマウント)にある x86 CA Access Control RPM パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/RPMPackages/LINUX/CAeAC*i386.rpm /tmp
cp /mnt/AC_DVD/NativePackages/RPMPackages/pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
/mnt/AC_DVD/NativePackages/RPMPackages/customize_eac_rpm -w keyword -d /tmp
CAeAC*i386.rpm
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA Access Control をインストールできるようになりました。

詳細情報:

customize_eac_rpm コマンド - RPM パッケージのカスタマイズ(120 ページ)

CA Access Control RPM パッケージのインストール

インストールした CA Access Control を、インストールされた他のソフトウェアと同様に管理するには、CA Access Control RPM パッケージをカスタマイズしてインストールします。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

注: 実際に使用するコマンドは、アップグレードなのか初回インストールなのか、またはデフォルトのディレクトリへのインストールなのかなど、さまざまな要因によって異なります。コマンドの例は、このトピックに記述されています。

CA Access Control RPM パッケージをインストールする方法

1. rpm コマンドを使用して、ca-lic パッケージをインストールします。

   ライセンス プログラムがインストールされます。

2. rpm コマンドを使用して、ca-cs-cawin RPM パッケージをインストールします。

   CAWIN がインストールされます。

   注: ライセンス プログラムをカスタム ディレクトリにインストールした場合、同じカスタム ディレクトリを CAWIN パッケージに対しても指定してください。

3. CAeAC パッケージのカスタマイズ (116 ページ)

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

4. rpm コマンドを使用して、CAeAC パッケージをインストールします。

   CA Access Control がインストールされます。

   重要: 既存の CA Access Control パッケージをアップグレードする場合は、SEOS syscall をアンロードしてから、新しいパッケージのインストールを試みます。 そうしない場合は、インストールに失敗します。

例: Red Hat Linux に CA Access Control をインストールする、または Red Hat Linux 上の CA Access Control をアップグレードする

以下の例では、CA Access Control Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント)にある CA Access Control パッケージを Red Hat Linux x86 ES 4.0 コンピュータにインストールする方法を示します。 この方法により、CA Access Control の新規インストールを行ったり、現在インストールされている CA Access Control RPM パッケージのアップグレード(インストールされているパッケージを最初に削除する必要はなし)を行ったりすることが可能です。 これを行うには、ライセンス プログラム パッケージ、CAWIN パッケージをこの順番でインストールし、次に、CA Access Control パッケージをカスタマイズして使用許諾契約に同意し、以下のようにインストールします。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX
rpm -U ca-lic*i386.rpm ca-cs-cawin*i386.rpm
cp CAeAC*i386.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*i386.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*i386.rpm
rpm -U /tmp/CAeAC*i386.rpm
```

例: eTrust Access Control r8 SP1 パッケージのインストールからのアップグレード

/opt/CA/eTrustAccessControl にインストールされている eTrust Access Control r8 SP1 パッケージを、Linux s390 SLES 9 コンピュータの CA Access Control Endpoint Components for UNIX DVD (/mnt/AC_DVD に搭載)にある CA Access Control パッケージにアップグレードする方法について、以下に例を示します。 これを行うには、以下の手順を使用して、ライセンス プログラム パッケージ、CAWIN パッケージ、およびカスタマイズされた CA Access Control パッケージをこの順番でインストールします。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX390
rpm -U ca-lic*rpm ca-cs-cawin*rpm
cp -R CAeAC*s390.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /opt/CA -d /tmp CAeAC*s390.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*s390.rpm
rpm -U /tmp/CAeAC*s390.rpm
```

例: カスタム ディレクトリに CA Access Control および必須パッケージをインストールする

以下の例では、CA Access Control Endpoint Components for UNIX DVD (/mnt/AC_DVD にマウント)にあるデフォルトの CA Access Control および必須パッケージを、Red Hat Linux Itanium IA64 ES 4.0 のカスタム ディレクトリにインストールする方法を示します。 これを行うには、以下のコマンドを使用します。

```
cd /mnt/AC_DVD/NativePackages/RPMPackages/LINUX_IA64
rpm -U --prefix /usr/CA/shared ca-lic*ia64.rpm
rpm -U --prefix /usr/CA/shared ca-cs-cawin*ia64.rpm
cp -R CAeAC*ia64.rpm /tmp
cp ../pre.tar /tmp
chmod 777 /tmp/CAeAC*s390.rpm
../customize_eac_rpm -u /usr/CA -d /tmp CAeAC*ia64.rpm
../customize_eac_rpm -w keyword -d /tmp CAeAC*ia64.rpm
rpm -U --prefix /usr/CA /tmp/CAeAC*ia64.rpm
```

CA Access Control は、指定したカスタム ディレクトリと製品の名前(Access Control)を連結した /usr/CA/AccessControl のカスタム ディレクトリにインストールされます。

注: ご使用の環境に $CASHCOMP 変数が定義されていない場合(/etc/profile.CA に定義可能)、ライセンス プログラムは指定されたディレクトリにのみインストールされます。 定義されている場合、ライセンス プログラムは $CASHCOMP にインストールされます。 $CASHCOMP が定義されていない場合に、-lic_dir を指定しないと、ライセンス プログラムは /opt/CA/SharedComponents ディレクトリにインストールされます。 ライセンス プログラムおよび CAWIN は、同じカスタム ディレクトリにインストールする必要があります。

詳細情報:

ネイティブ インストールの際に考慮するその他の事項(113 ページ)
CA Access Control RPM パッケージのカスタマイズ(116 ページ)
customize_eac_rpm コマンド - RPM パッケージのカスタマイズ(120 ページ)

customize_eac_rpm コマンド - RPM パッケージのカスタマイズ

customize_eac_rpm コマンドは、CA Access Control RPM パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、CA Access Control RPM パッケージでのみ機能します。

  注: このスクリプトは、CAWIN およびライセンス プログラム パッケージで使用するためのものではありません。

- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_rpm -h [-l]
customize_eac_rpm -a [-d pkg_location] pkg_filename
customize_eac_rpm -w keyword [-d pkg_location] pkg_filename
customize_eac_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_eac_rpm -s [-f tmp_params] | -c certfile | -k keyfile} [-d pkg_location]
pkg_filename
customize_eac_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_eac_rpm -u install_prefix [-d pkg_location] pkg_filename
customize_eac_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

カスタマイズする CA Access Control パッケージのファイル名を定義します。

注: -d オプションを指定しない場合は、パッケージ ファイルの完全パス名を定義する必要があります。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはパッケージ ファイルへの完全パス名が pkg_filename であるとみなします。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作用の一時ディレクトリを設定します。

-u install_prefix

eTrust Access Control r8 SP1 パッケージをインストールしている場所のプレフィクスを定義します。 実際のインストール場所は、このプレフィクスと製品の名前を連結したものになります。 r8 SP1 パッケージは製品の名前に eTrust があるため、eTrustAccessControl サブディレクトリにインストールされました。 新しいバージョンは、AccessControl サブディレクトリにインストールされます。

たとえば、r8 SP1 が /opt/CA/eTrustAccessControl にインストールされており、r12.0 SP1 にアップグレードする場合は、rpm コマンドを使ってパッケージをインストールする前に以下を入力します。

```
./customize_eac_rpm -u /opt/CA -d . CAeAC-1200-0.1106.i386.rpm
```

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [ ]内）。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

RPM パッケージのアンインストール

インストールされている CA Access Control RPM パッケージをアンインストールするには、インストール時とは逆の手順で、CA Access Control パッケージをアンインストールする必要があります。

RPM パッケージのアンインストール方法

1. メインの CA Access Control パッケージをアンインストールします。

   ```
   rpm -e CAeACPackage_name
   ```

2. CAWIN パッケージをアンインストールします。

   ```
   rpm -e ca-cs-cawinPackage_name
   ```

Solaris ネイティブ パッケージングのインストール

Solaris のネイティブ パッケージングは、コマンドライン ユーティリティとして提供されます。このため、各パッケージを個別に作成、インストール、削除、およびレポートすることができます。

注: Solaris ネイティブ パッケージングの詳細については、Sun Microsystems の Web サイトならびに pkgadd、pkgrm、pkginfo、および pkgchk に関するマニュアル ページを参照してください。

通常のインストールの代わりに、CA Access Control に用意されている Solaris ネイティブ パッケージを使用することができます。 このため、インストールした CA Access Control を、Solaris ネイティブ パッケージングを使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、CA Access Control をアンインストールするには、pkgrm コマンドを使用する必要があります。 uninstall_AC スクリプトは使用しないでください。

Solaris ネイティブ パッケージのカスタマイズ

ネイティブ パッケージを使用して CA Access Control をインストールする前に、CA Access Control パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。 パラメータ ファイルを変更しなくても済むように、カスタマイズ スクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、CA Access Control パッケージをカスタマイズしてください。

サポートされている各 Solaris オペレーティング システムに対する Solaris ネイティブ パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

Solaris ネイティブ パッケージのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

   重要: パッケージを展開するときは、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうでないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

2. customize_eac_pkg スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA Access Control のエンド ユーザ使用許諾契約が含まれています。

   注: customize_eac_pkg スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

   ```
   customize_eac_pkg -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内のキーワードをメモします。

   以下の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA Access Control パッケージをカスタマイズします。

   ```
   customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
   ```

6. (オプション)インストール パラメータ ファイルの言語を指定します。

   ```
   customize_eac_pkg -r -l lang [-d pkg_location] [pkg_name]
   ```

7. (オプション) インストール ディレクトリを変更します。

   ```
   customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
   ```

8. (オプション)デフォルトの暗号化ファイルを変更します。

   ```
   customize_eac_pkg -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. (オプション)インストール パラメータ ファイルを取得します。

   ```
   customize_eac_pkg -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. (オプション)インストール要件に合わせて、インストール パラメータ ファイルを編集します。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。 たとえば、POSTEXIT 設定(前の # 文字を削除します)をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション)カスタマイズしたパッケージのインストール パラメータを設定します。

    ```
    customize_eac_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA Access Control をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。 以下の例では、CA Access Control Endpoint Components for UNIX DVD(/mnt/AC_DVD にマウント)にある x86 CA Access Control Solaris パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/_SOLARIS_X86_PKG*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _SOLARIS_X86_PKG*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_pkg -w keyword -d /tmp CAeAC
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA Access Control をインストールできるようになりました。

詳細情報:

customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ(129 ページ)

Solaris ネイティブ パッケージのインストール

インストールした CA Access Control を、インストールされたほかのソフトウェアと同様に管理するには、CA Access Control Solaris ネイティブ パッケージをカスタマイズしてインストールします。 CA Access Control Solaris のネイティブ パッケージを使用すると、Solaris 上で CA Access Control を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

CA Access Control Solaris ネイティブ パッケージのインストール方法

1. (オプション) Solaris ネイティブ インストール時のデフォルトを設定します。
   a. インストール管理ファイルを現在の場所にコピーします。

      ```
      convert_eac_pkg -p
      ```

      インストール管理ファイルを現在の場所に myadmin という名前でコピーします。

      インストール管理ファイルを編集して、pkgadd のインストール時のデフォルトを変更できます。 pkgadd -a オプションを使用すれば、CA Access Control など、特定のインストール用に変更されたファイルを使用できます。 ただし、このファイルは CA Access Control に固有のものではありません。

      重要: インストールされている既存の Solaris パッケージを以前の CA Access Control リリースからアップグレードするには、この手順を実行する必要があります。

   b. インストール管理ファイル (myadmin) を必要に応じて編集し、そのファイルを保存します。

      これで、他のインストールに影響を及ぼすことなく、変更したインストール設定を CA Access Control ネイティブ インストールのために使用できます。

   注: Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。 インストール管理ファイルおよびこのファイルの使い方の詳細については、pkgadd (1M) および admin (4) に関する Solaris のマニュアルページを参照してください。

2. CAeAC パッケージのカスタマイズ (123 ページ)

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のようにパッケージをインストールします。

   ```
   pkgadd [-a dir/myadmin] -d pkg_location CAeAC
   ```

   -a dir/myadmin

   手順 1 で作成した myadmin インストール管理ファイルの場所を定義します。

このオプションを指定しない場合、pkgadd ではデフォルトのインストール管理ファイルが使用されます。

pkg_location

CA Access Control パッケージ(CAeAC)が配置されている場所を定義します。

重要: パッケージは、公開場所(つまり、グループおよび全員に対する読み取りアクセス権が設定された場所)に配置する必要があります。 たとえば、/var/spool/pkg です。

注: Solaris ネイティブ パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

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

詳細情報:

ネイティブ インストールの際に考慮するその他の事項(113 ページ)
選択したゾーンへの Solaris ネイティブ パッケージのインストール(128 ページ)
Solaris ネイティブ パッケージのカスタマイズ(123 ページ)
customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ(129 ページ)
convert_eac_pkg - Solaris ネイティブ インストールの設定(131 ページ)

選択したゾーンへの Solaris ネイティブ パッケージのインストール

Solaris のネイティブ パッケージングを使用し、選択したゾーンに CA Access Control をインストールすることができます。 それには、CA Access Control をグローバル ゾーンにインストールする必要があります。

注: Solaris ネイティブ パッケージを使用して、CA Access Control をすべてのゾーンにインストールすることをお勧めします。

選択したゾーンに CA Access Control をインストールする方法

重要: すべてのゾーンで必ず同じ CA Access Control バージョンを使用するようにしてください。

1. グローバル ゾーンから以下のコマンドを発行して、CA Access Control をインストールします。

   ```
   pkgadd -G -d pkg_location CAeAC
   ```

   pkg_location

   カスタマイズした CA Access Control パッケージ(CAeAC)が配置されている場所を定義します。

   重要: パッケージは、公開場所(つまり、グループおよび全員に対する読み取りアクセス権が設定された場所)に配置する必要があります。 たとえば、/var/spool/pkg です。

   このコマンドによって、CA Access Control がグローバル ゾーンにのみインストールされます。

2. グローバル ゾーン内で SEOS_load コマンドを入力して、CA Access Control カーネル モジュールをロードします。

   注: CA Access Control カーネルはロードされますが、CA Access Control はグローバル ゾーン内のイベントをインターセプトしません。

3. CA Access Control をインストールするそれぞれの非グローバル ゾーンで以下の操作を行います。

   a. 非グローバル ゾーンの一時的な保存場所に CAeAC パッケージをコピーします。

   b. 非グローバル ゾーンから以下のコマンドを発行します。

      ```
      pkgadd -G -d pkg_location CAeAC
      ```

      このコマンドは、作業元である非グローバル ゾーンに CA Access Control をインストールします(前の手順でコピーしたパッケージを使用)。

   これで、内部ゾーンで CA Access Control を開始できるようになります。

注: CA Access Control をグローバル ゾーンから削除する前に、すべての非グローバル ゾーンからアンインストールする必要があります。

customize_eac_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ

customize_eac_pkg コマンドは、CA Access Control Solaris ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な CA Access Control Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_pkg -h [-l]
customize_eac_pkg -a [-d pkg_location] [pkg_name]
customize_eac_pkg -w keyword [-d pkg_location] [pkg_name]
customize_eac_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_pkg -i install_loc [-d pkg_location] [pkg_name]
customize_eac_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_pkg -g -f tmp_params -d pkg_location pkg_name
customize_eac_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

(オプション)カスタマイズする CA Access Control パッケージの名前です。 パッケージを指定しない場合、スクリプトはデフォルトでメインの CA Access Control パッケージ (CAeAC)を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作用の一時ディレクトリを設定します。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

convert_eac_pkg - Solaris ネイティブ インストールの設定

Solaris pkgadd のデフォルト動作は、インストール管理ファイルによって決定されます。デフォルトの設定を変更するには、インストール管理ファイル(デフォルトでは、/var/sadm/install/admin/default)を変更する必要があります。 たとえば、CA Access Control パッケージによって setuid 実行可能ファイルがインストールされたら、必要に応じて、インストール後スクリプト(root として実行)を実行できます。 デフォルトの Solaris pkgadd 動作では、これらの操作の確認がユーザに求められます。

注: インストール管理ファイルを編集して、pkgadd のインストール時のデフォルトを変更できます。 pkgadd -a オプションを使用すれば、CA Access Control など、特定のインストール用に変更されたファイルを使用できます。 ただし、このファイルは CA Access Control に固有のものではありません。

このコマンドの形式は以下のようになります。

```
convert_eac_pkg -c [-d pkg_location] [pkg_name]

convert_eac_pkg -p [-f file]
```

-c

古い形式のパッケージを新しい形式のパッケージに変換します。

注: 古い形式のパッケージは、CA Access Control r8 SP1 で使用されていました。アップグレードを行う前に、これらを変換する必要があります。

インストールされた CA Access Control パッケージまたはスプールされたパッケージの情報は、変換できます。 スプールされたパッケージについては、-d オプションを使用してパッケージがどこに配置されているかを示します。

-d pkg_location

ファイル システム上でパッケージを配置するディレクトリを定義します。

pkg_name

パッケージの名前を定義します(デフォルトでは CAeAC)。

-p

名前が付けられたカスタム パッケージ構成ファイルを用意します。

-f file

CA Access Control インストール管理ファイルを作成する場所を定義します。

これを指定しないと、現在のディレクトリに[「myadmin」という名前のファイルが作成されます。

例: サイレント インストールを行うために Solaris ネイティブ インストールを設定する

以下の手順では、setuid 実行可能ファイルのインストールについての確認、またはインストール後スクリプトの実行についての確認をユーザが求められないように Solaris ネイティブ インストールを設定する方法について説明します。

1. インストール管理ファイルを現在の場所にコピーします。

   ```
   convert_eac_pkg -p
   ```

   これによって、他のインストールに影響することなく、CA Access Control ネイティブ インストールの構成設定を変更できます。

2. パッケージ構成ファイル(myadmin)内の以下の設定を、以下のように編集します。

   ```
   setuid=nocheck
   action=nocheck
   ```

   ファイルを保存します。

3. パッケージをカスタマイズします。

   最小要件として、使用許諾契約への同意を指定する必要があります。

4. 以下のコマンドを実行して、カスタマイズされた CA Access Control パッケージをサイレント インストールします。

   ```
   pkgadd -n -a config_path¥myadmin -d pkg_path CAeAC
   ```

例: 古い形式を使用する Solaris ネイティブ インストールをアップグレードする

以下の手順では、既存の CA Access Control ネイティブ パッケージ インストールを新しいリリースにアップグレードする前にその変換を行う方法について説明します。 これを行うには、以下のコマンドを実行します。

```
convert_eac_pkg -c CAeAC
```

HP-UX ネイティブ パッケージのインストール

HP-UX のネイティブ パッケージは、GUI とコマンドライン ユーティリティのセットとして提供されます。これにより、個々のソフトウェア パッケージの作成、インストール、削除、およびレポート作成を行うことができます。 HP-UX ネイティブ パッケージでは、リモート コンピュータにソフトウェア パッケージをインストールすることもできます。

注: HP-UX のネイティブ パッケージである、Software Distributor-UX (SD-UX)の詳細については、HP の Web サイト(http://www.hp.com)を参照してください。 swreg、swinstall、swpackage、および swverify については、man ページも参照できます。

通常のインストールの代わりに、CA Access Control に用意されている SD-UX ネイティブ パッケージを使用することができます。 これにより、インストールした CA Access Control を、SD-UX を使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、CA Access Control をアンインストールするには、swremove コマンドを使用する必要があります。 uninstall_AC スクリプトは、使用しないでください。

SD-UX 形式パッケージのカスタマイズ

ネイティブ パッケージを使用して CA Access Control をインストールする前に、CA Access Control パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。 パラメータ ファイルを変更しなくても済むように、カスタマイズ スクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、CA Access Control パッケージをカスタマイズしてください。

サポートされた各 HP-UX オペレーティング システムに対する Software Distributor-UX (SD-UX)形式パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリに格納されています。

SD-UX 形式パッケージのカスタマイズ

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

   重要: パッケージを展開するときは、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうでないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

2. customize_eac_depot スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA Access Control のエンド ユーザ使用許諾契約が含まれています。

   注: customize_eac_depot スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

   ```
   customize_eac_depot -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA Access Control パッケージをカスタマイズします。

   ```
   customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
   ```

6. (オプション)インストール パラメータ ファイルの言語を指定します。

   ```
   customize_eac_depot -r -l lang [-d pkg_location] [pkg_name]
   ```

7. (オプション) インストール ディレクトリを変更します。

   ```
   customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
   ```

8. (オプション)デフォルトの暗号化ファイルを変更します。

   ```
   customize_eac_depot -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. (オプション)インストール パラメータ ファイルを取得します。

   ```
   customize_eac_depot -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. (オプション)インストール要件に合わせて、インストール パラメータ ファイルを編集します。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。 たとえば、POSTEXIT 設定(前の # 文字を削除します)をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション)カスタマイズしたパッケージのインストール パラメータを設定します。

    ```
    customize_eac_depot -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA Access Control をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。 以下の例では、CA Access Control Endpoint Components for UNIX DVD(/mnt/AC_DVD にマウント)にある x86 CA Access Control SD-UX パッケージをカスタマイズして使用許諾契約に同意する方法を示します。

```
cp /mnt/AC_DVD/NativePackages/_HPUX11_PKG_*.tar.Z /tmp
cp /mnt/AC_DVD/NativePackages/pre.tar /tmp
cd /tmp
zcat _HPUX11_PKG_*.tar.Z | tar -xvf -
/mnt/AC_DVD/NativePackages/customize_eac_depot -w keyword -d /tmp CAeAC
```

/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、CA Access Control をインストールできるようになりました。

詳細情報:

customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ(136 ページ)

HP-UX ネイティブ パッケージのインストール

インストールした CA Access Control を、インストールされたほかのソフトウェアと同様に管理するには、CA Access Control SD-UX 形式パッケージをカスタマイズしてインストールします。 CA Access Control SD-UX 形式パッケージを使用すると、HP-UX に CA Access Control を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

CA Access Control HP-UX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

   HP-UX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. CAeAC パッケージのカスタマイズ(133 ページ)

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを使用して、カスタマイズされたパッケージを SD-UX に登録します。

   ```
   swreg -l depot pkg_location
   ```

   pkg_location

   CA Access Control パッケージ(CAeAC)が配置されている場所を定義します。

4. 以下のコマンドを使用して、CA Access Control パッケージをインストールします。

   ```
   swinstall -s pkg_location CAeAC
   ```

   SD-UX は、pkg_location ディレクトリから、CAeAC パッケージのインストールを開始します。

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

詳細情報:

ネイティブ インストールの際に考慮するその他の事項(113 ページ)
SD-UX 形式パッケージのカスタマイズ(133 ページ)

customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ

customize_eac_depot コマンドは、SD-UX 形式パッケージ用の CA Access Control ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な CA Access Control Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_depot -h [-l]
customize_eac_depot -a [-d pkg_location] [pkg_name]
customize_eac_depot -w keyword [-d pkg_location] [pkg_name]
customize_eac_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_eac_depot -i install_loc [-d pkg_location] [pkg_name]
customize_eac_depot -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_eac_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(オプション)カスタマイズする CA Access Control パッケージの名前です。 パッケージを指定しない場合、スクリプトはデフォルトでメインの CA Access Control パッケージ (CAeAC)を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

HP-UX パッケージのアンインストール

インストールされている CA Access Control HP-UX パッケージをアンインストールするには、インストール時とは逆の手順で、CA Access Control パッケージをアンインストールする必要があります。

CA Access Control パッケージをアンインストールするには、メインの CA Access Control パッケージをアンインストールします。

```
swremove CAeAC
```

AIX ネイティブ パッケージのインストール

AIX ネイティブ パッケージは、GUI およびコマンドライン ユーティリティのセットとして提供されます。これを使用して、個別のソフトウェア パッケージを管理できます。

通常のインストールの代わりに、CA Access Control に用意されている AIX ネイティブ パッケージを使用することができます。 これにより、インストールした CA Access Control を、AIX installp を使用してインストールされた他のソフトウェアと同様に管理できます。

注: 一部の AIX バージョンはいくつかのパッケージ形式(installp、SysV、RPM)をサポートしていますが、CA Access Control では AIX のネイティブ パッケージ形式(installp)のみが提供されます。

重要: パッケージのインストール後、CA Access Control をアンインストールするには、installp コマンドを使用する必要があります。 uninstall_AC スクリプトは、使用しないでください。

bff ネイティブ パッケージ ファイルのカスタマイズ

ネイティブ パッケージを使用して CA Access Control をインストールする前に、CA Access Control パッケージをカスタマイズして、使用許諾契約への同意を指定する必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

パッケージをカスタマイズするには、パッケージからインストール パラメータ ファイルをデプロイし、必要に応じて変更し、パッケージに再度ロードします。 パラメータ ファイルを変更しなくても済むように、カスタマイズ スクリプトとして提供されているコマンドもあります。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、CA Access Control パッケージをカスタマイズしてください。

サポートされた各 AIX オペレーティング システムに対する installp 形式ネイティブ パッケージ(bff ファイル)は、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

bff ネイティブ パッケージ ファイルのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージ(bff ファイル)を必要に応じてカスタマイズできます。

   重要: この領域のディスク容量は、再パッケージングの一時的なファイルを格納できるように、少なくともパッケージの 2 倍のサイズである必要があります。

2. customize_eac_bff スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび CA Access Control のエンド ユーザ使用許諾契約が含まれています。

   注: customize_eac_bff スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 使用許諾契約を表示します。

   ```
   customize_eac_bff -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 使用許諾契約に同意することを示すために、CA Access Control パッケージをカスタマイズします。

   ```
   customize_eac_bff -w keyword [-d pkg_location] pkg_name
   ```

6. (オプション)インストール パラメータ ファイルの言語を指定します。

   ```
   customize_eac_bff -r -l lang [-d pkg_location] pkg_name
   ```

7. (オプション) インストール ディレクトリを変更します。

   ```
   customize_eac_bff -i install_loc [-d pkg_location] [pkg_name]
   ```

8. (オプション)デフォルトの暗号化ファイルを変更します。

   ```
   customize_eac_bff -s -c certfile -k keyfile [-d pkg_location] pkg_name
   ```

9. インストール パラメータ ファイルを取得します。

   ```
   customize_eac_bff -g -f tmp_params [-d pkg_location] pkg_name
   ```

10. (オプション)インストール要件に合わせて、インストール パラメータ ファイルを編集します。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。 たとえば、POSTEXIT 設定(前の # 文字を削除します)をアクティブにして、実行するインストール後スクリプトをポイントするようにします。

11. (オプション)カスタマイズしたパッケージのインストール パラメータを設定します。

    ```
    customize_eac_bff -s -f tmp_params [-d pkg_location] pkg_name
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で CA Access Control をインストールできるようになりました。

詳細情報:

customize_eac_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ(142 ページ)

AIX ネイティブ パッケージのインストール

インストールした CA Access Control を、インストールされたほかのソフトウェアと同様に管理するには、CA Access Control AIX ネイティブ パッケージをカスタマイズしてインストールします。 CA Access Control AIX のネイティブ パッケージ(bff ファイル)を使用すると、AIX に CA Access Control を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

CA Access Control AIX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

   AIX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. CAeAC パッケージのカスタマイズ(139 ページ)

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. (オプション)インストールするパッケージのレベル(バージョン)を記録します。

   ```
   installp -l -d pkg_location
   ```

   pkg_location

   CA Access Control パッケージ(CAeAC)が配置されている場所を定義します。

   pkg_location 内の各パッケージについて、AIX ではパッケージ レベルの一覧が作成されます。

   注: AIX ネイティブ パッケージのインストール オプションの詳細については、installp の man ページを参照してください。

4. 以下のコマンドを使用して、CA Access Control パッケージをインストールします。

   ```
   installp -ac -d pkg_location CAeAC [pkg_level]
   ```

   pkg_level

   前に記録したパッケージのレベル番号を定義します。

   AIX は、pkg_location ディレクトリから、CAeAC パッケージのインストールを開始します。

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

詳細情報:

bff ネイティブ パッケージ ファイルのカスタマイズ(139 ページ)
ネイティブ インストールの際に考慮するその他の事項(113 ページ)

customize_eac_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ

customize_eac_bff コマンドによって、bff ネイティブ パッケージ ファイル用の、CA Access Control ネイティブ パッケージ カスタマイズ スクリプトが実行されます。

このパッケージは、AIX で使用可能な CA Access Control ネイティブ パッケージのいずれでも機能します。 パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

重要: パッケージの抽出場所には、再パッケージの中間ファイルを保存するために、少なくともパッケージの 2 倍のサイズが必要です。

注: ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_eac_bff -h [-l]
customize_eac_bff -a [-d pkg_location] pkg_name
customize_eac_bff -w keyword [-d pkg_location] pkg_name
customize_eac_bff -r [-d pkg_location] [-l lang] [pkg_name]
customize_eac_bff -i install_loc [-d pkg_location] [pkg_name]
customize_eac_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location] pkg_name
customize_eac_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

カスタマイズする CA Access Control パッケージ(bff ファイル)の名前です。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

AIX パッケージのアンインストール

インストールされている CA Access Control AIX パッケージをアンインストールするには、インストール時とは逆の手順で、CA Access Control パッケージをアンインストールする必要があります。

CA Access Control パッケージをアンインストールするには、メインの CA Access Control パッケージをアンインストールします。

```
installp -u CAeAC
```

通常のスクリプト インストール

CA Access Control では、UNIX 上に CA Access Control を対話形式またはサイレント モードでインストールする install_base スクリプトを提供しています。

通常のスクリプト インストール(ネイティブ インストールでなく)を使用する場合は、CA Access Control インストール メディアに含まれる 3 つのファイルが必要になります。

- install_base - tar ファイルから CA Access Control をインストールするスクリプトです。
- _opSystemVersion_ACVersion.tar.Z - すべての CA Access Control ファイルが含まれている圧縮 tar ファイルです。 たとえば、CA Access Control r12.0 を IBM AIX バージョン 5 にインストールする場合、使用する tar ファイルは _AIX5_120.tar.Z となります。

- pre.tar - 圧縮された tar ファイルであり、インストールに関するメッセージおよびエンド ユーザ使用許諾契約が含まれています。

  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で検出されるコマンドを入力します。

  - サイレント インストール(install_base -autocfg を使用)を実行する場合は、-command オプションと、エンド ユーザ使用許諾契約ファイルの最後で検出されるコマンドを使用します。
  - 応答ファイル(-autocfg file_name)を使用する場合、-command オプションは必要ありません。

  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。間違ったコマンドを入力した場合も、ファイルの名前と場所が得られます。

これらのファイルは、CA Access Control Endpoint Components for UNIX DVD の /Unix/Access-Control ディレクトリにあります。

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(147 ページ)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(153 ページ)を最初に学習することもできます。

CA Access Control をインストールする方法

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 を装着します。

   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: 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
```

install_base コマンド - インストール スクリプトの実行

install_base コマンドでは、インストール スクリプトを実行し、1 つ以上のインストール オプションが選択された 1 つ以上の CA Access Control パッケージをインストールします。

このコマンドの形式は以下のようになります。

```
install_base [tar_file] [packages] [options]
```

tar_file

(オプション)ご使用のプラットフォームに対応する CA Access Control インストール ファイルが含まれている tar ファイルの名前を定義します。 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、tar ファイル名の入力は省略できます。

packages

(オプション)インストールする CA Access Control パッケージを定義します。 パッケージを何も指定しない場合は、インストール スクリプトによりクライアント 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。ただし、CA Access Control のアップグレードしている場合は例外で、すでにインストールされているパッケージと同じパッケージがインストールされます。

注: クライアント パッケージについては、その他のパッケージをインストールする前に、インストールする必要があります。 ただし、クライアント パッケージと一緒に他のパッケージもインストールするように指定することは可能です。

インストールできる CA Access Control パッケージを以下に示します。

-all

すべての CA Access Control パッケージをインストールします。 クライアント パッケージ、サーバ パッケージ、API パッケージ、MFSD パッケージがあります。 また STOP(-stop オプション)が有効になります。

-api

API ライブラリおよびサンプル プログラムが含まれている API パッケージをインストールします。

-client

CA Access Control コア機能が含まれているクライアント パッケージをスタンドアロン コンピュータにインストールします。

-mfsd

メインフレーム同期デーモンが含まれている MFSD パッケージをインストールします。

注: MFSD パッケージをインストールするには、事前にサーバ パッケージをインストールしておく必要があります。

-server

サーバ パッケージをインストールします。サーバ パッケージには、より多くのバイナリおよびスクリプト(selogrcd、sepmd、sepmdd、sepmdadm、secrepsw)が含まれています。 これらは、クライアント パッケージを補完するものです。 たとえば、sepmdd では、コンピュータに Policy Model を設定できます。

-uni

Unicenter セキュリティ統合および移行パッケージをインストールします。このパッケージは、CA Access Control と、Unicenter の CAUTIL、負荷管理、およびイベント管理の各コンポーネント、ならびに Unicenter EMSec API との統合をサポートします。

オプション

(オプション)追加で設定するインストール オプションを定義します。

注: CA Access Control の機能に影響するインストール オプション(たとえば、-stop) を指定できるのは、クライアント パッケージをインストールするときのみです。インストール プロセスに影響するインストール オプション(たとえば、-verbose)は、どのパッケージでも指定できます。

指定できるオプションを以下に示します。

-autocfg [response_file]

インストールをサイレント モード(対話モードをオフ)で実行します。 応答ファイルが指定されている場合、インストールではそのファイル内に格納された環境設定を使用して、対話形式のインストール プロセスに自動的に応答します。応答ファイルが指定されていない場合、または応答ファイルにオプションが指定されていない場合、インストールでは事前設定済のデフォルトが使用されます。

応答ファイルの作成方法

- -savecfg オプションを使用します。
- parameters.tar にあるインストール パラメータ ファイルを編集します。

重要: 応答ファイルを指定しない場合は、-autocfg オプションを使用するときに、-command オプションを使用する必要があります。

サイレント インストールを実行する場合は、以下の点に留意してください。

- 暗号化鍵は変更できません。
- デフォルトでは、クライアント パッケージとサーバ パッケージのみがインストールされます。

  他のパッケージまたは機能をインストールするには、通常のインストールの場合と同様に適切なオプションを指定する必要があります。
- install_base コマンドでは、インストールに関する詳細がインストール中に画面に出力されません。

  インストール中にインストールに関するメッセージを画面に表示させるには、-verbose オプションを使用します。
- セキュリティ上の理由により、サポート エージェントとレポート サーバ間の SSL 通信を保護する共有秘密キーをサイレント インストールで指定することはできません。 共有秘密キーを指定するには、インストール後にレポート エージェント ユーザ(+reportagent)を設定する必要があります。

-command keyword

エンド ユーザ使用許諾契約にユーザが同意していることを指定するコマンドを定義します。 このコマンドは使用許諾契約(角かっこ[ ]内)の最後にあり、-autocfg オプションを使用する際は、このコマンドを使用する必要があります。エンド ユーザ使用許諾契約ファイルの場所を特定するには、install_base -h を実行します。

注: エンド ユーザ使用許諾契約が利用できるのは、ヘルプが表示されている間だけです。 ヘルプを読み終えると、エンド ユーザ使用許諾契約は削除されます。

-d target_dir

カスタム インストール ディレクトリを定義します。 デフォルトのインストール ディレクトリは、/opt/CA/AccessControl です。

重要: マウントしたネットワーク ファイル システム(NFS)に CA Access Control データベースを配置することはできません。

-dns | -nodns

DNS ホストの有無に関係なく、lookaside データベースを作成します。 -nodns オプションは、インストール中に CA Access Control が DNS 内の任意のホストで nslookup を実行しないことを指定します。

-fips

FIPS 専用の公開鍵(非対称)の暗号化を有効にするよう指定します。

-force

インストール時に、新たにアクティブになったサブスクライバ更新（sepmd -n および subs <pmdb> newsubs(sub_name)）を無視して、インストールを続行するようにします。 デフォルトでは、インストールが停止し、サブスクライバの更新をまず終了させるよう求められます。

注：このオプションを使用した場合、新しいサブスクライバ更新は失敗します。

-force_encrypt

インストール時に、警告を表示せずにデフォルト以外の暗号化鍵を使用するようにします。

重要：アップグレードが完了すると、暗号化鍵はデフォルトに設定されます。

注：CA Access Control には、SSL、AES（128 ビット、192 ビット、および 256 ビット）、DES、および 3 DES も用意されており、この中から選択できます。

-force_install

すでにインストールされているバージョンを強制的に上書きインストールします。同じバージョンを上書きインストールする場合、このオプションを使用します。

-force_kernel

古いカーネルのアンロードが不可能なことを警告することなく、インストールが続行されるようにします。

注：インストール完了後に、コンピュータの再起動が必要な場合があります。

-g groupname

CA Access Control ファイルのグループ所有者の名前を定義します。 デフォルト値は 0 です。

-h | -help

このコマンドのヘルプを表示します。

-ignore_dep

アンインストール手順で、他の製品との依存関係をチェックしないように指定します。

-key encryption_key

アップグレード時に暗号化鍵を復元します。

注：アップグレード時には、アップグレードの前に使用していたのと同じ暗号化鍵を使用する必要があります。

-lang lang

CA Access Control をどの言語でインストールするかを定義します。 サポート対象の言語および文字セットについては、ヘルプを表示（install_base -h）する際にこのオプションの説明を確認してください。

-lic_dir license_dir

ライセンス プログラムがまだインストールされていない場合、ライセンス プログラムのインストール ディレクトリを定義します。

注: コンピュータ環境に $CASHCOMP 変数が定義されていない場合 (/etc/profile.CA に定義可能)、ライセンス プログラムは指定されたディレクトリにのみインストールされます。 定義されている場合、ライセンス プログラムは $CASHCOMP にインストールされます。 $CASHCOMP が定義されていない場合に、-lic_dir を指定しないと、ライセンス プログラムは /opt/CA/SharedComponents ディレクトリにインストールされます。 CAWIN は、ライセンス パッケージの場合と同じディレクトリにインストールされます。

-nolink

CA Access Control をデフォルト パス(/opt/CA/AccessControl)にインストールする際に /etc ディレクトリ内の seos.ini へのリンクが作成されないように指定します。

デフォルト以外のディレクトリに CA Access Control をインストールすると、CA Access Control により /etc ディレクトリ内の seos.ini へのリンクが作成されます。 これにより、CA Access Control はインストール場所を「検出」できます。 デフォルト パスにインストールしており、(セキュリティ上の要件により)/etc ディレクトリを更新しない場合は、このオプションを使用します。

-nolog

インストール プロセスに対してログが保持されないように指定します。 デフォルトでは、インストール プロセスに関連付けられたすべてのトランザクションが ACInstallDir/AccessControl_install.log に格納されます(ここで、 ACInstallDir は、CA Access Control のインストール ディレクトリです)。

-no_tng_int

インストール時に selogrd と Unicenter イベント管理との統合が設定されないよう指定します。

このオプションを指定しない場合、インストール スクリプトにより Unicenter イベント管理がインストールされているかどうかがチェックされます。 インストール スクリプトは、Unicenter イベント管理がインストールされているとみなすと、selogrd.cfg に以下の行を追加して selogrd と Unicenter イベント管理との統合を設定します。

```
uni hostname
```

-post program_name

インストールが完了した後で実行するプログラムを指定します。

-pre program_name

インストールの開始前に実行するプログラムを指定します。

-rcert certificate.pem

ルートの証明書ファイルへの完全パス名を指定します。

注: このオプションを使用すると、スクリプトでは tar ファイルを抽出し、このファイルをユーザにより提供されたファイルと再パッケージ化し、デフォルト ファイル(def_root.pem)と置き換えます。

-rkey certificate.key

ルートの鍵ファイルへの完全パス名を指定します。

注: このオプションを使用すると、スクリプトでは tar ファイルを抽出し、このファイルをユーザにより提供されたファイルと再パッケージ化し、デフォルト ファイル(def_root.key)と置き換えます。

-rootprop

sepass による root のパスワードの変更が Policy Model に送信されるように指定します。

注: インストールの完了後は、seos.ini ファイルの AllowRootProp トークンを使用してこのオプションを設定できます。 seos.ini 初期化ファイルの詳細については、「 リファレンス ガイド」を参照してください。

-savecfg <response_file>

対話式のインストールで入力した応答を後で -autocfg オプションで使用できるように保存します。

-stop

STOP(スタック オーバーフロー保護)機能を使用できるようにします。

-system_resolve

システム関数の使用を指定します。この関数は、システム上のネットワーク キャッシュの省略を定義します。

注: このオプションを IBM AIX プラットフォームで使用することはできません。

-v

CA Access Control パッケージのバージョンを表示します。

-verbose

インストール時にインストールに関するメッセージが画面に表示されるように指定します。 対話形式のインストールではデフォルトになっています。-autocfg オプションを使用するときは、これらのメッセージを確認したい場合にのみ、このオプションを設定します。

install_base スクリプトのしくみ

install_base スクリプトで実行される内容は以下のとおりです。

1. デフォルト インストール ディレクトリを変更するかどうかを確認するメッセージが表示されます。
2. 指定したインストール オプションが表示され、インストールを続行するかどうかを確認するメッセージが表示されます。
3. tar.Z ファイルからインストール場所にデータが抽出されます(デフォルトの場所または target_dir で指定された場所)。
4. プラットフォームが異なると、実行されるアクションも異なります。
   - Sun Solaris の場合、CA Access Control の syscall スクリプトが /etc/name_to_sysnum ファイルに追加されます。 元のファイルは /etc/name_to_sysnum.bak として保存されます。 ブート シーケンスの一部となる /etc/rc2.d/S68SEOS ファイルが作成されます。
   - IBM AIX の場合、SEOS_syscall スクリプトがロードされます。
5. CA Access Control データベースの割り当て、初期設定、およびフォーマットが実行され、seos.ini ファイルが作成されます。 データベース ファイルは、ACInstallDir/seosdb ディレクトリに配置されます(ACInstallDir は CA Access Control のインストール ディレクトリです)。
6. マシンが NIS+ であるかどうかが判断されます。
   - マシンが NIS+ であると判断された場合は、[passwd]セクションの nis_env トークンが nisplus に設定されます。
   - それ以外の場合、マシンが NIS であれば、nis_env トークンが nis に設定されます。

     さらに、rpc.nisd が実行中の場合は、[passwd]セクションの NisPlus_server トークンが yes に設定されます。
7. サポートされている 32 ビット プラットフォーム Sun Solaris、IBM AIX、HP-UX、および Linux では、(キャッシュを使用する)NIS または DNS でマシンが実行されているかどうかが、このスクリプトによって判断されます。 NIS または DNS でマシンが実行されていると判断された場合は、自動的に lookaside データベースが作成され、seos.ini ファイルの[seosd]セクションにある 2 つのトークン(under_NIS_server および use_lookaside)が yes に設定されます。

   注: 他のプラットフォームの場合は、lookaside データベースをインストールするかどうかを確認するメッセージ、およびインストール先ディレクトリを指定するように指示するメッセージが表示されます。

8. 以下の追加情報を入力するよう促されます(これらの設定は、インストールの終了後いつでも変更できます)。

   - 監査ファイルの読み取りができる監査者グループの名前。
   - すべての UNIX ユーザ、ユーザ グループ、およびホストを CA Access Control データベースに追加するかどうか。
   - データベースを PMDB にサブスクライブするかどうか。サブスクライブする場合は、そのデータベース名。

     この質問に応答しても、データベースを PMDB に実際にサブスクライブしたことにはなりません。サブスクリプションを後で作成した場合に、指定された PMDB がこのデータベースに更新情報を提供するだけです。

     この質問に対しては、以下のように指定すれば問題ありません。

目的のアクション	指定方法
特定の PMDB にデータベースをサブスクライブする	PMDB の名前。形式は pmd_name@hostname
(少なくとも後から指定するまで)どの PMDB にもデータベースをサブスクライブしない	Enter キー

     上記のいずれも指定しないで「_NO_MASTER_」と入力すると、データベースを任意の PMDB にサブスクライブできます。 ただし、このように指定すると PMDB の選択ができなくなるため、問題が発生する可能性があります。

   - パスワード Policy Model 名。
   - CA Access Control のセキュリティ管理者となるユーザ。
   - CA Access Control で企業ユーザをサポートするかどうか。サポートする場合、任意のユーザをセキュリティ管理者として定義するかどうか。
   - FIPS 専用インストールを選択した場合、暗号化に関係する FIPS 専用オプションを指定するかどうか。
   - FIPS 専用の暗号化を選択しなかった場合、デフォルトの暗号化方式を変更するかどうか。

     CA Access Control では、対称鍵、公開鍵、およびこの 2 つの組み合わせを、選択可能な暗号化オプションとして用意しています。
   - 公開鍵暗号化を選択した場合、CA Access Control では、サブジェクトの証明書とルートの証明書を提供する方法を指定できます。

     選択内容に応じて、CA Access Control では SSL を容易に設定できます。

- 対称暗号化を選択した場合、新しい暗号化鍵を設定するかどうか。

  注: 暗号化の詳細については、「リファレンス ガイド」の「sechkey」を参照してください。

- ベースライン セキュリティ ルールをインストールするかどうか。

  ベースライン セキュリティ ルールをインストールすることで、管理者はシステム、パスワードおよびログ ファイルの保護を強化するための 2 つのルール セットを含むパッケージをインストールできます。 このうちの 1 つのルール セットは、すべてのプラットフォームに適用され、CA Access Control ファイルを保護します。 もう 1 つのルール セットは UNIX ファイルを保護し、Sun Solaris、HP-UX および IBM AIX の各プラットフォームに固有のルール セットです。 この 2 つのルール セットは、いずれか一方のみをインストールすることはできません。 ベースライン セキュリティ ルールは警告モードでインストールされます。情報は提供されますが、実際に保護は適用されません。 したがって、ルールを理解した後に警告モードを解除することをお勧めします。

- リモート ホストから CA Access Control を起動できるようにするかどうか。

- レポート エージェントを有効にするかどうか。有効にする場合は、CA Enterprise Log Manager を有効にするかどうか。

  レポート エージェントは Message Queue にデータベースのスケジュールされたスナップショットを送信します。 レポート エージェントを有効にする場合は、配布サーバのホスト名、使用するポート、キューの名前を定義する必要があります。 CA Enterprise Log Manager を有効にする場合は、さらに監査ログ ファイルのタイムスタンプされたバックアップを保持するように指定することもできます。

- PUPM エージェントを有効にするかどうか。

  PUPM エージェントは、ローカル コンピュータを PUPM 用に設定し、このコンピュータから特権アカウントのパスワードを取得できるようにします。 PUPM エージェントを有効にする場合は、配布サーバのホスト名、使用するポート、キューの名前を定義する必要があります。

- このエンドポイントを、拡張ポリシー管理のために設定するかどうか。設定する場合は、偏差計算結果の送信先である配布ホスト(DH)名。

  dhName@hostName という形式で DH ホスト名を定義します。たとえば、host123.comp.com という名前のホストに配布サーバをインストールした場合は、DH__@host123.comp.com を使用する必要があります。

インストール後の設定処理

インストールが完了したら、CA Access Control を環境に合わせて設定する必要があります。

インストール後の設定を行う方法

1. パス設定に ACInstallDir/bin ディレクトリを追加します。

   デフォルトでは、インストール ディレクトリは /opt/CA/AccessControl です。

2. seos.ini（163 ページ） ファイル トークンをチェックして、設定が要件を満たしていることを確認します。

   必要に応じて設定を変更します。

3. CA Access Control のマニュアル ページにアクセスできるようにするには、自分の MANPATH に ACInstallDir/man ディレクトリを追加します。

   たとえば、csh を使用している場合、現在のセッションでマニュアル ページにアクセスできるようにするには、以下のコマンドを入力します。

   ```
   setenv MANPATH $MANPATH:/opt/CA/AccessControl/man
   ```

   今後のセッションでマニュアル ページにアクセスできるようにするには、.login、.profile、または .cshrc ファイルに同様の行を追加します。

CA Access Control の起動

X Window 環境で作業している場合は、CA Access Control を起動し、それがシステムに適切にインストールされていることを確認します。重要なシステム保護を開始するには、以下の手順に従ってください。

1. root（スーパーユーザ）権限でログインし、2 つのウィンドウを開きます。
2. いずれかのウィンドウで以下のコマンドを入力します。

   ```
   seload
   ```

   seload コマンドで 3 つのデーモン（エンジン、エージェント、および Watchdog）が起動されるまで待機します。

3. 3 つのデーモンを起動した後、もう一方のウィンドウに移動して以下のコマンドを入力します。

   ```
   secons -t+ -tv
   ```

   CA Access Control によって、オペレーティング システムのイベントを報告するメッセージがファイルに記録されます。 secons -tv コマンドを入力すると、メッセージが画面上にも表示されます。

4. seload コマンドを指定した最初のウィンドウで、以下のコマンドを入力します。

   ```
   who
   ```

   CA Access Control のトレース メッセージが書き込まれる 2 番目のウィンドウに注意して、CA Access Control が who コマンドの実行をインターセプトし、そのことについて報告するかどうかを確認します。 who コマンドのインターセプトが報告された場合、CA Access Control はシステムに適切にインストールされています。

5. 必要な場合は、さらにコマンドを入力して CA Access Control の反応を確認します。

   データベースには、アクセスの試行を禁止するためのルールがまだ準備されていません。 この場合でも、CA Access Control はシステムを監視しているため、CA Access Control がインストールされ実行されているシステムの動作を確認し、CA Access Control がインターセプトするイベントを確認することができます。

6. 以下のコマンドを入力して、seosd デーモンを停止します。

   ```
   secons -s
   ```

   以下のメッセージが画面に表示されます。

   ```
   CA Access Control は現在停止中です。
   ```

エンドポイントへの拡張ポリシー管理の設定

拡張ポリシー管理サーバ コンポーネントをインストールしたら、拡張ポリシー管理を行うために企業内の各コンピュータを設定する必要があります。 その際、サーバ コンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: この手順では、拡張ポリシー管理を行うために CA Access Control の既存のインストールを設定する方法を示します。 エンドポイント上に CA Access Control をインストールした時にこの情報を指定している場合は、再びエンドポイントを設定する必要はありません。

エンドポイントを設定して拡張ポリシー管理を実行できるようにするには、コマンド ウィンドウを開き、次のコマンドを入力します。

```
dmsmgr -config -dhname dhName
```

dhName

エンドポイントが対応する分散ホスト(DH)名のカンマ区切り形式のリストを定義します。

例: DH__@centralhost.org.com

このコマンドでは、拡張ポリシー管理を行うためにエンドポイントが設定されます。また、定義された DH と動作するようにエンドポイントが設定されます。

注: 詳細については、「リファレンス ガイド」の「dmsmgr -config」コマンドの説明を参照してください。

レポート作成のための UNIX エンドポイントの設定

CA Access Control エンドポイント管理 およびレポート ポータルのインストールおよび設定の完了後、配布サーバにデータを送信して処理するようにエンドポイントを設定できます。そのためには、レポート エージェントを有効にして設定します。

注: CA Access Control をインストールすると、レポート作成のためにエンドポイントを設定することが可能になります。 この手順では、インストール時にこのオプションを設定しなかった場合、レポートを送信するための既存のエンドポイントを設定する方法について説明します。

レポート作成のための UNIX エンドポイントの設定方法

1. Run ACSharedDir/lbin/report_agent.sh:

   ```
   report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number [-rqueue queue_name]
   ```

   設定オプションを省略すると、デフォルト設定が使用されます。

   注: report_agent.sh スクリプトの詳細については、「リファレンス ガイド」を参照してください。

2. データベース内に +reportagent ユーザを作成します。

   このユーザは、ADMIN 属性および AUDITOR 属性、ならびローカル端末への書き込みアクセス権を有する必要があります。 また、epassword をレポート エージェント共有秘密キー(配布サーバのインストール時に定義)に設定する必要があります。

3. レポート エージェント プロセス用に SPECIALPGM を作成します。

   SPECIALPGM は、root ユーザを +reportagent ユーザにマップします。

注: レポート エージェントを有効にしたら、CA Access Control 構成設定を変更してパフォーマンス関連の設定を変更できます。 レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

例: selang を使用してレポート作成に UNIX Endpoint を設定する

次の selang コマンドは、レポート エージェントを有効にして設定した場合に、どのように必要なレポート エージェント ユーザを作成し、レポート エージェント プロセスの特別なセキュリティ権限を指定するかを示します。

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) ¥
Nativeuid(root) pgmtype(none)
```

CA Access Control のカスタマイズ

CA Access Control を使用して本格的にセキュリティを実装するには、適用するセキュリティ ポリシーを定義する必要があります。 ポリシーの定義に要する時間は、サイトの規模および選択したセキュリティの管理方法によって異なります。

たとえば大学の場合、通常は CA Access Control に学生を定義せず、resource _default の設定のみに基づいてアクセスを規制することになるでしょう。 一方、銀行の場合は、すべてのユーザを CA Access Control に定義し、特定のリソースには特定のユーザのみがアクセスできるように、すべてのリソースのアクセス リストを設定することが考えられます。 したがって、ユーザ数が同じであっても、CA Access Control の実装にかかる時間は銀行よりも大学の方が短くなります。

セキュリティ管理者は、プロジェクトの目的を定義する必要があります。 サイトのポリシーに関する決定は慎重に行う必要があります。 CA Access Control には、各サイトでセキュリティ ポリシーを実装する際に便利な複数のカスタマイズ可能なファイルが含まれています。

trustedプログラム

trusted プログラムとは、プログラムが変更されていない場合のみ、実行できるプログラムです。 通常、これは setuid/setgid プログラムです。 CA Access Control では、通常のプログラムも trusted として指定できます。 プログラムが改ざんされていないことが確実な場合は、そのプログラムを PROGRAM クラスに登録します。このクラスは、CA Access Control によってその整合性が保護されます。

trusted プログラムは、 program pathing と併用できます。これにより、ユーザは trusted プログラムによって特定のタスクのみを実行できます。

注: プログラム パスの詳細については、「UNIX エンドポイント管理ガイド」を参照してください。

CA Access Control には、ユーザがすべての setuid プログラムと setgid プログラムを trusted として登録するためのスクリプトが用意されています。

1. setuid プログラムと setgid プログラムをすべて記憶する手間を省くために、以下に示すように seuidpgm プログラムを使用します。 このプログラムはファイル システムを検索して、setuid プログラムと setgid プログラムをすべて検出し、検出されたすべてのプログラムを PROGRAM クラスで登録するために selang のコマンドのスクリプトを作成します。

   以下のコマンドを発行します。

   ```
   seuidpgm -q -l -f ¥ > ¥opt¥CA¥AccessControl¥seuid.txt
   ```

   このようにして実行された seuidpgm プログラムは、以下の処理を行います。

   - (/ から始めて)ファイル システム全体を検索します。
   - メッセージを表示しません(-q オプションを指定すると、「cannot chdir」メッセージは表示されません)。
   - シンボリック リンクをすべて無視します(-l)。
   - FILE クラスと PROGRAM クラスの両方にプログラムを登録します(-f)。
   - ファイル ¥opt¥CA¥AccessControl¥seuid.txt にコマンドを出力します。

   注: seuidpgm 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。

2. テキスト エディタを使用して seuid.txt ファイルをチェックし、trusted として登録するすべての setgid/setuid プログラムがこのファイルに含まれていること、およびそれ以外のプログラムが含まれていないことを確認します。 必要に応じてファイルを編集します。

3. selang を使用して、編集したコマンド ファイルを実行します。 seosd デーモンが実行中でない場合は、-l スイッチを指定します。

   ```
   selang [-l] -f ¥opt¥CA¥AccessControl¥seuid.txt
   ```

   selang の実行が完了するまで数分かかる場合があります。

4. seosd デーモンがまだ実行されていない場合は、seosd デーモンを再起動します。次に、システムが所定の動作を実行しているかどうか、setuid プログラムが起動できるかどうかを確認します。

5. セキュリティ管理者が知らない間に、trusted ではない新しい setuid プログラムまたは setgid プログラムが追加されて実行されるのを防ぐために、PROGRAM クラスのデフォルトのアクセス権を NONE に設定しておくことをお勧めします。

   以下の selang コマンドを入力して、このデフォルトのアクセス値を設定します。

   ```
   chres PROGRAM _default defaccess(none)
   ```

注: CA Access Control を長く使用しているユーザは、この接続に UACC クラスを使用することを思い付くかもしれません。 UACC クラスはこのバージョンでも存在するので、リソースのデフォルト アクセス権の指定に使用できます。 ただし、使いやすさを考慮した場合、クラスのデフォルト アクセス権を指定するには、そのクラスの _default レコードを使用することをお勧めします。 _default を使用した指定は、同じクラスの UACC を使用した指定より優先されます。

登録した setuid プログラム、setgid プログラム、および通常プログラムを表す PROGRAM クラスのレコードには、実行可能ファイルの以下の属性が格納されます。

- デバイス番号
- Inode
- 所有者
- グループ
- Size
- 作成日
- 作成日時
- 最終変更日
- 最終変更時刻
- MD5 シグネチャ
- SHA1 シグネチャ
- チェックサム CRC(巡回冗長チェック)

登録する各プログラムの最も重要な属性は、そのプログラムが trusted であることです。これは、そのプログラムが実行しても安全であることを意味します。 すでに記載された属性に変化があると、プログラムの trusted ステータスは失われます。その場合、CA Access Control は、そのプログラムが実行されないようにすることができます。

未登録プログラムの使用の監視

データベースに適切なプログラムをすべて登録できたかどうかわからない場合は、以下のコマンドを使用して、未登録のプログラムの有無を調べることができます。

```
chres PROGRAM _default warning
```

この warning プロパティにより、PROGRAM クラスに警告モードが設定されます。つまり、未登録の setuid プログラムまたは setgid プログラムが使用されるたびに、特別な監査レコードが警告として表示されます。ただし、未登録プログラムの使用は妨げられません。

監査ログの確認

監査ログで untrusted レコードを手動で検索することができます。または、特定のプログラムが untrusted プログラムになったときに通知されるように、特別な通知方法を設定することができます。 特別な通知方法を設定すると、ユーザは untrusted になったプログラムを使用することを、管理者に連絡する必要がなくなるので便利です。管理者は、ファイルが untrusted プログラムになったという通知を受け取ったらすぐにファイルをチェックします。

注: 特別な監査通知を設定する方法については、「エンドポイント管理ガイド」を参照してください。

保護

trusted ではない setuid コマンドおよび setgid コマンドの実行を阻止するには、以下のコマンドを発行します。

注: データベースには、自動的にユーザ「nobody」が含められます。

```
newres PROGRAM _default defaccess(none) ¥
owner(nobody) audit(all)
```

CA Access Control では、新規プログラムまたは変更されたプログラムを実行する前に管理者の承認を要求することにより、バックドアまたはトロイの木馬から保護します。

たとえば、新しく有用な setuid プログラムを受け取ったとします。 このプログラムがトロイの木馬でないことが確実で、すべてのユーザがこのプログラムを実行できるようにしたいとします。 このプログラムを trusted プログラムとして登録するには、以下のコマンドを発行します。

```
newres PROGRAM program-pathname ¥ defaccess(EXEC)
```

untrusted プログラムから trusted プログラムへの再変換

プログラムのサイズや変更日時、またはその他の監視対象プロパティの変更により、このプログラムが untrusted 状態になった場合、管理者がそのプログラムを再度 trusted 状態にして、データベースにその承認を再度登録するまで、このプログラムを再び実行することはできません。 プログラムを再度 trusted 状態にするには、以下のコマンドを入力します。

```
editres PROGRAM progam_name trust
```

注: seretrust ユーティリティを使用して、プログラムを再度 trusted 状態にすることもできます。 このユーティリティおよびそのオプションの詳細については、「リファレンス ガイド」を参照してください。

初期設定ファイル

このセクションでは、CA Access Control によって初期設定時に読み込まれるさまざまなファイルについて説明します。 デフォルトでは、初期設定ファイルは、seos.ini ファイルがあるディレクトリ(CA Access Control のインストール ディレクトリ)に作成されます。

seos.ini

seos.ini ファイルでは、グローバル パラメータを設定します。

注: ファイルおよびサポート対象のトークンの構造の詳細については、「リファレンス ガイド」を参照してください。

seos.ini ファイルは、インストール時の初期状態では保護されており、CA Access Control の実行中は更新できません。ただし、すべてのユーザは READ 権限でいつでも seos.ini ファイルにアクセスできます。 CA Access Control が実行中であっても権限のあるユーザが seos.ini ファイルを更新できるようにするために、以下のコマンドを入力します。

```
newres FILE ACInstallDir/seos.ini owner(authUser) defacc(read)
```

ACInstallDir は CA Access Control のインストール ディレクトリであり、デフォルトでは /opt/CA/AccessControl です。

このコマンドにより、ファイルのデフォルトのアクセス権は「読み取り」に設定されます。ただし、ファイルの所有者である authUser のみに、ファイルの更新権限が与えられます。

注: 多数のユーティリティがその実行中に seos.ini ファイルにアクセスするので、このファイルのデフォルトのアクセス権を「読み取り」に設定しておくことが重要です。 ファイルを読み込めない場合、ユーティリティの実行は失敗します。

トレース フィルタ ファイル

このオプションのファイルには、あらゆる種類の CA Access Control トレース メッセージを除外するためのフィルタ マスクを指定するエントリが保存されています。

トレース フィルタ ファイルでは、フィルタ処理で除外するトレース メッセージ(つまり、トレース ファイルに表示しないトレース メッセージ)を指定します。 表示を抑止するメッセージのグループを識別するマスクを各行に指定します。 たとえば、以下のファイルでは、WATCHDOG または INFO で始まるすべてのメッセージ、および BYPASS で終わるすべてのメッセージを表示しません。

```
WATCHDOG*
*BYPASS
INFO*
```

デフォルトでは、trcfilter.init という名前のトレース フィルタ ファイルが使用されます。 seos.ini ファイルの[seosd]セクションで trace_filter トークンの値を編集して、トレース フィルタ ファイルの名前および場所を変更できます。

トレース レコードをフィルタするには、必要に応じてファイルを編集します。 ファイルに注釈(コメント行)を追加するには、行の先頭にセミコロン(;)を入力します。

trcfilter.init ファイルは、ユーザ トレースによって生成された監査レコードをフィルタしません。 これらの監査レコードをフィルタするには、audit.cfg ファイルを編集します。

注: 詳細については、「リファレンス ガイド」にある「seosd ユーティリティ」を参照してください。

拡張ポリシー管理クラス

作成した複数ルールのポリシー(selang コマンド)は、格納し、指定の方法で企業に展開することができます。 このポリシー ベースの方法を使用すれば、ポリシー バージョンを格納した上で、それらをホストまたはグループ ホストに割り当てることができます。 ポリシーは割り当てられると、デプロイのためにキューに登録されます。 あるいは、ホストまたはホスト グループに対するポリシー バージョンのデプロイおよびデプロイ解除を直接行うこともできます。

注: 拡張ポリシー管理の詳細については、「エンタープライズ管理ガイド」を参照してください。

拡張ポリシー管理の設定

拡張ポリシー ベースの管理を使用するように企業内の設定をするには、DMS および DH を中央の 1 つの場所にインストールし、拡張ポリシー管理を行うために各エンドポイントを設定します(165 ページ)。

インストール後に、拡張ポリシー管理を行うために階層を設定するには、dmsmgr ユーティリティを使用します。

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。

エンドポイントのポリシー偏差計算の設定

各エンドポイントは、ポリシー偏差計算が可能なように設定する必要があります。 通常、この設定はインストール中に行います。 この手順は、そうではなく、インストール後にその設定を実行することを目的にしています。

エンドポイントにポリシー偏差計算を設定するには、以下の selang コマンドを入力します。

```
so dms+(DMS@host)
```

DMS@host

上記の形式で指定された DMS の名前を定義します。

sesu および sepass ユーティリティ

オペレーティング システムの passwd コマンドの代わりに sepass を使用し、su の代わりに sesu を使用することをお勧めします。 そのためには、元のシステム バイナリを保存し、sepass および sesu へのシンボリック リンクとそれぞれ置き換える必要があります。この処理が終了したら、これらのユーティリティが常に使用できることを確認します。

ほとんどのオペレーティング システムでは、CA Access Control がロードされていなくても、sepass および sesu ユーティリティが動作します。 ただし、一部のオペレーティング システム(たとえば、AIX)では、CA Access Control がロードされていないと、これらのユーティリティは動作しません。 このようなオペレーティング システムのために、CA Access Control ではラッパー スクリプトを用意しています。

sesu および sepass ラッパー スクリプト

sesu および sepass ラッパー スクリプトは、以下のディレクトリにあります。

```
ACInstallDir¥samples¥wrappers
```

このファイルには、以下のファイルが含まれています。

ファイル	説明
sesu_wrap.sh	sesu のラッパー スクリプト
sepass_wrap.sh	sepass のラッパー スクリプト
README	これらのラッパーの用途および概念に関する情報が含まれるテキスト ファイル

ラッパー スクリプトを使用した sesu の実行

CA Access Control がロードされていないときに sesu ユーティリティがオペレーティング システムで動作しない場合は、ラッパー スクリプトを使用して sesu ユーティリティを実行します。

注: CA Access Control がロードされていないとき sesu ユーティリティが動作しない場合は、この手順のみを実行する必要があります。

ラッパー スクリプトを使用して sesu を実行する方法

1. テキスト エディタを使用して、sesu_wrap.sh スクリプトを開きます。

   テキスト エディタにラッパー スクリプトが表示されます。

2. 必要ならば、以下の 2 つの変数を変更します。

   SEOSDIR

   CA Access Control インストール ディレクトリを定義します。 デフォルトでは、デフォルトのインストール ディレクトリに設定されています。

   ```
   ¥opt¥CA¥AccessControl
   ```

   SYSSU

   交換対象の元の su システム バイナリの名前を定義します。 デフォルトでは、以下のディレクトリに設定されます。

   ```
   ¥usr¥bin¥su.orig
   ```

3. sesu ユーティリティを指す su シンボリック リンクではなく、sesu_wrap.sh ラッパー スクリプトを指す su シンボリック リンクを代わりに使用します。

   su を実行するたびに、sesu ラッパー スクリプトが sesu ユーティリティを実行します。

ラッパー スクリプトを使用した sepass の実行

CA Access Control がロードされていないとき、sepass ユーティリティがオペレーティング システムで動作しない場合は、ラッパー スクリプトを使用して sepass ユーティリティを実行します。

注: CA Access Control がロードされていないとき sepass ユーティリティが動作しない場合は、この手順のみを実行する必要があります。

ラッパー スクリプトを使用して sepass を実行する方法

1. テキスト エディタを使用して、sepass_wrap.sh スクリプトを開きます。

   テキスト エディタにラッパー スクリプトが表示されます。

2. 必要ならば、以下の 2 つの変数を変更します。

   SEOSDIR

   CA Access Control インストール ディレクトリを定義します。 デフォルトでは、デフォルトのインストール ディレクトリに設定されています。

   ```
   ¥opt¥CA¥AccessControl
   ```

   SYSPASSWD

   交換対象の元の sepass システム バイナリの名前を定義します。 デフォルトでは、以下のディレクトリに設定されます。

   ```
   ¥usr¥bin¥passwd.orig
   ```

3. sesu ユーティリティを指す su シンボリック リンクではなく、sesu_wrap.sh ラッパー スクリプトを指す su シンボリック リンクを代わりに使用します。

   passwd を実行するたびに、sepass ラッパー スクリプトが sepass ユーティリティを実行します。

メンテナンス モードの保護(サイレント モード)

CA Access Control には、メンテナンス モード(サイレント モードとも呼ばれる)が実装されています。CA Access Control デーモンがメンテナンスのために停止した場合は、このモードにより保護されます。 メンテナンス モードでは、これらのデーモンが停止している間、CA Access Control ではイベントが拒否されます。

CA Access Control は、稼動している場合には、セキュリティを脅かすイベントをインターセプトして、イベントを許可するかどうかをチェックします。 メンテナンス モードをアクティブにしないと、CA Access Control サービスが停止している間、すべてのイベントが許可されます。 メンテナンス モードをアクティブにした場合は、CA Access Control デーモンが停止すると、イベントは拒否されます。このため、システムのメンテナンスが行われている間、ユーザの活動は停止されます。

メンテナンス モードは調整することができます。デフォルトでは、無効です。

CA Access Control セキュリティ サービスが停止している間は、以下のような状態になります。

- メンテナンス モードがアクティブである場合、セキュリティを脅かすイベントはすべて拒否されます(ただし、特別な場合、およびメンテナンス ユーザによって実行されるイベントは除きます)。
- メンテナンス モードが無効である場合、CA Access Control は介入せず、実行はオペレーティング システムに渡されます。

メンテナンス モードがアクティブでセキュリティが停止しているときに拒否されたイベントは、監査ログ ファイルに記録されません。

メンテナンス モードを有効にするには、以下の手順に従います。

重要: root がメンテナンス ユーザでない場合、メンテナンス ユーザ用に開いているセッションがあることを確認します。そのようなセッションがない場合、ログインすることはできません。

1. CA Access Control デーモンが停止していることを確認します。
2. seini ユーティリティを使用して、トークン silent_deny の値を yes に変更します。

   トークンは、SEOS_syscall セクションにあります。

   ```
   seini -s SEOS_syscall.silent_deny yes
   ```

3. トークン silent_admin の値を数値の UNIX UID に変更し、CA Access Control デーモンが停止している間、この UNIX UID がコンピュータにアクセスできるようにします。

   ```
   seini -s SEOS_syscall.silent_admin <maintenance_UID>
   ```

   注: root は、デフォルトのメンテナンス モード ユーザ(UID 0)です。

   重要: メンテナンス ユーザが root でない場合は、メンテナンス モードで CA Access Control を起動できるように CA Access Control 認証デーモン setuid を root ユーザに設定します。 この変更を行うには、以下のコマンドを入力します。
   chmod 6111 seosd

4. seload コマンドを使用して、CA Access Control デーモンを起動します。

   注: メンテナンス モード ユーザが root でない場合は、seosd コマンドを使用して CA Access Control デーモンを起動します。

Unicenter セキュリティ統合ツールのインストール

UNIX 環境では、2 種類の Unicenter セキュリティの統合インストールのいずれかを使用します。

完全統合

完全統合のインストールは、CA Access Control で Unicenter セキュリティが使用されている場合に便利です。この統合では、Unicenter セキュリティのデータが CA Access Control にインポートされます。したがって、CA Access Control は、自分のホストまたはホストのグループから使用できるセキュリティ システムになります。

最小統合

最小統合のインストールは、CA Access Control に Unicenter セキュリティが含まれていない場合や、CA Access Control に Unicenter セキュリティが含まれているが使用されていない場合に便利です。

Unicenter セキュリティを完全統合でインストールする方法

重要: 移行を実行するには、root でログインする必要があります。CA Access Control をインストールした後に、su(ユーザ ID 切り替え)コマンドで root に切り替わることはできません。

Unicenter セキュリティと CA Access Control を完全統合でインストールするには、以下の手順に従います。

1. CA Access Control をインストールします。ただし、インストール時には、CA Access Control データベースにデータを追加しません。

   データベースへデータを追加しないようにするには、画面に以下のプロンプトが表示されたときに、デフォルトの[いいえ]を選択します。

   ユーザ、グループおよびホストをインポートしますか? [y/N]:

2. マスタ ノードから uni_migrate_master.sh スクリプトを実行します。

   注: マスタ ノードは、Unicenter セキュリティ データベースのホスト マシンです。

3. 各サテライト ノード(Unicenter セキュリティが制御する各マシン)から uni_migrate_node.sh スクリプトを実行します。

4. マスタ ノードから uni_migrate_node.sh スクリプトを実行します。

   マスタ ノードは、他のすべてのノードが統合された後に Unicenter セキュリティを無効にするための最後のマシンです。

5. $CAIGLBL0000/secopts ファイルを手動で編集して、SSF_SCOPE_DATA キーワードと SSF_SCOPE_KEYWORD キーワードを No に設定します。

インストール スクリプトにより、以下のタスクが実行されます。

- シェル スクリプト defclass.sh を実行して、ユーザ定義のセキュリティのアセット タイプを CA Access Control データベースの CA Access Control クラスとして定義します。
- プログラム migopts を実行して、現在の Unicenter セキュリティ環境を読み込み、同等の CA Access Control 環境に変換します。
- プログラム exporttngdb を実行して、現在の Unicenter セキュリティのデータベース オブジェクトを読み込み、CA Access Control のデータベース オブジェクトに変換します。
- Unicenter セキュリティ デーモンを停止して無効にします。

Unicenter セキュリティと CA Access Control を最小統合でインストールするには、以下の手順に従います。

1. すべてのノードから uni_migrate_node.sh スクリプトを実行します。
2. $CAIGLBL0000/secopts ファイルを手動で編集して、SSF_SCOPE_DATA キーワードと SSF_SCOPE_KEYWORD キーワードを No に設定します。

インストール上の注意事項

- Unicenter の統合および移行インストールの実行後に、Unicenter TNG のログイン インターセプトを実行しないことをお勧めします。 Unicenter の統合および移行インストールが正常に完了すると、Unicenter TNG のログイン インターセプトは無効になります。
- Unicenter TNG のデータ スコーピング ルールとキーワード スコーピング ルール (-DT サフィックスまたは -KW サフィックスが付いた Unicenter TNG のアセット タイプを対象とするルール) は、CA Access Control の移行プロセスではサポートされていません。 移行プロセスでは、このタイプのルールは無視されます。
- Unicenter セキュリティは現在使用されていないため、Unicenter セキュリティのアセット タイプ (CA-USER、CA-ACCESS、CA-USERGROUP、CA-ASSETGROUP、CA-ASSETTYPE、および CA-UPSNODE) に対して実装された Unicenter セキュリティ ルールはどれも使用されていません。 このようなアセット タイプまたはそれらから派生したタイプを対象とするルールは、移行プロセスではすべて無視されます。

  uni_migrate_node.sh と uni_migrate_master.sh で使用できる -e (-edit) オプションにより、CA Access Control データベースを入力するルールを参照および編集できます。
- Unicenter TNG の完全統合または最小統合を実行する場合は、install_base スクリプトに -uni オプションを指定して、Unicenter Integration and Migration パッケージをインストールする必要があります。 Unicenter の統合および移行インストールでは、Unicenter の統合および移行のスクリプトとバイナリ ファイルが ACInstallDir/tng ディレクトリにインストールされます。

- 複数のコマンドを記述している場合は、移行中に selang -c を使用しないでください。 代わりに、selang -f input_file_name を使用してください。

Solaris 10 ゾーンの実装

Solaris 10 には、「ゾーン」と呼ばれる、Solaris のさまざまなインスタンスに類似した仮想的な OS サービスが用意されています。 すべての Solaris 10 システムに、「グローバル ゾーン」と呼ばれるマスター ゾーンが含まれています。 非グローバル ゾーンはマスター ゾーンに沿って動作するので、グローバル ゾーンから非グローバル ゾーンを設定、監視、および制御することができます。

環境内の各ゾーン(または選択したゾーン)は、CA Access Control を使用して保護することができます。 これにより、ゾーンごとにさまざまなルールおよびポリシーを定義して、ゾーンごとにさまざまなアクセス制約を定義することができます。

Solaris 10 ゾーンへの CA Access Control のインストールは、通常のインストールとまったく同じです。以下に示す方法のいずれかを使用して、インストールできます。

- Solaris ネイティブ パッケージを使用した CA Access Control のインストール

  CA Access Control のインストールおよびアンインストールは、Solaris ネイティブ パッケージ ツール(pkgadd および pkgrm)を使用して行うようになっています。

  インストールした Solaris ネイティブ パッケージを使用してインストールを行う場合は、以下のいずれかが可能です。

  - すべてのゾーンへの CA Access Control のインストール(123 ページ)

    Solaris 10 に CA Access Control をインストールする方法としてお勧めできる最も簡単な方法は、グローバル ゾーンまたはすべてのすべてのゾーン(非アクティブ ゾーンおよび将来的に作成されるゾーンを含む)にインストールするというものです。

  - 選択したゾーンへの CA Access Control のインストール(128 ページ)

    お勧めする方法ではありませんが、Solaris ネイティブ パッケージ ツールを使用して、選択したゾーンに CA Access Control をインストールすることができます。 ただし、CA Access Control が非グローバル ゾーン内で動作するためには、CA Access Control をグローバル ゾーンにもインストールする必要があります。

  Solaris ネイティブ パッケージを使用してインストールしてある場合、すべてのゾーンから CA Access Control をアンインストールするにはネイティブ パッケージを使用します。

- install_base スクリプトを使用した、各ゾーンへの CA Access Control のインストール（145 ページ）

  install_base スクリプトを使用すると、このスクリプトを実行したゾーンに CA Access Control がインストールされます。

  CA Access Control が任意の非グローバル ゾーンで動作するためには、グローバル ゾーンにも CA Access Control をインストールする必要があります。

  install_base スクリプトを使用して CA Access Control をインストールしてある場合は、個々の非グローバル ゾーンからその CA Access Control をアンインストールできます。 ただし、CA Access Control カーネルは、CA Access Control がすべてのゾーンで停止された後で、グローバル ゾーンからのみアンインストール可能です。

  重要: install_base を使用してグローバル ゾーンから CA Access Control をアンインストールし、その後すべてのゾーンからアンインストールする場合、ユーザはゾーンからロックアウトされる場合があります。 Solaris ゾーンへの CA Access Control のインストールおよび Solaris ゾーンからの CA Access Control のアンインストールは、Solaris ネイティブ パッケージを使用して行うことをお勧めします。

ゾーンの保護

CA Access Control では、任意のコンピュータを保護する場合と同じ方法で Solaris 10 ゾーンを保護します。 各ゾーンはそれぞれ、他のゾーンと分離して保護され、CA Access Control で定義する各ルールは該当するゾーンで作業しているユーザにのみ適用されます。 グローバル ゾーンに適用するルールは、非グローバル ゾーンで認識可能なリソースをカバーするルールであっても、グローバル ゾーンからそれらのリソースにアクセスするユーザにのみ適用されます。

注: 必要に応じて非グローバル ゾーンのリソースを、非グローバル ゾーンおよびグローバル ゾーンの両方で確実に保護してください。

例: グローバル ゾーンのルールおよび非グローバル ゾーンのルール

以下の例では、非グローバル ゾーン(myZone1)ファイルを保護するルールを定義します。 システム ファイルはすべて、グローバル ゾーンから常に認識可能です。

保護するファイルは、/myZone1/root/bin/kill(グローバル ゾーンからのパス)。 このファイルを保護するには、以下の CA Access Control ルールを定義します。

- グローバル ゾーンでは:

```
nu admin_pers owner(nobody)
nr FILE ¥myZone1¥root¥bin¥kill defaccess(none) owner(nobody)
authorize FILE /myZone1/root/bin/kill uid(admin_pers) access(all)
```

- myZone1(非グローバル ゾーン)では:

```
nu admin_pers owner(nobody)
nr FILE ¥bin¥kill defaccess(none) owner(nobody)
authorize FILE ¥bin¥kill uid(admin_pers) access(all)
```

グローバル ゾーンと非グローバル ゾーンの両方でこれらのルールを使用することで、ユーザ(admin_pers)を定義し、保護すべきリソースとしてファイルを定義し、そのファイルにアクセスする権限をユーザに付与しました。 このような処理を両方のゾーンで行わなければ、リソースはリスクを伴います。

新しいグローバル ゾーンの設定

Solaris ネイティブ パッケージを使用してすべてのゾーンに CA Access Control をインストールする場合、初めてのインストールの後に作成したゾーンにも CA Access Control が自動的にインストールされます。 ただし、インストール後の CA Access Control 手順スクリプトは、非グローバル ゾーンから、新しいゾーンに対して実行する必要がありますが、これらのスクリプトは新しいゾーンの設定が完了した後でないと実行できません。 特に、「zlogin -C zonename」コマンドを実行する必要があります(名前サービス、root パスワードなどの設定を完了させる必要があります)。

重要: 「zlogin -C zonename」コマンドを実行しなかった場合、または新しいゾーンのブートおよびログインを早急に行った場合、CA Access Control のインストールは不完全なものとなります。これは、インストール後スクリプトが実行されていないからです。

注: 新しいゾーンの正しい設定方法の詳細については、Sun の「System Administration Guide: Solaris Containers--Resource Management and Solaris Zones 」を参照してください。このドキュメントは Sun Microsystems Documentation の Web サイトにあります。

Solaris ブランド ゾーンへのインストール

Solaris の制限とは、pkgadd が、Solaris 10 のグローバル ゾーンにインストールされているアプリケーションのブランド ゾーンへのプロパゲートをサポートしていないことを意味します。 または、CA Access Control は、syscall ではなく ioctl を使用してカーネルモジュールとの通信を行う必要があります。

Solaris ブランド ゾーンへのインストール方法

1. pkgadd を使用して、CA Access Control を Solaris グローバル ゾーンにインストールします。
2. pkgadd を使用して、CA Access Control を Solaris ブランド ゾーンにインストールします。

   注: グローバル ゾーンにインストールする場合、インストール パラメータ ファイルによって、インストールが自動的に実行されます。
3. ブランド ゾーンで、seos.ini エントリ SEOS_use_ioctl が 1 に設定されていることを確認します。必要に応じて、修正します。

   これで、CA Access Control が ioctl を使用する設定になっていることが確認されます。
4. グローバル ゾーンで、seos.ini エントリ SEOS_use_ioctl が 1 に設定されていることを確認します。

   これで、CA Access Control が ioctl を使用する設定になっていることが確認されます。

   これでインストールが完了し、CA Access Control をブランド ゾーンで起動できるようになります。

   重要: SEOS_use_ioctl が 0 に設定されている場合は、すべてのゾーンにおける通信に ioctl を使用するように CA Access Control を変更する必要があります。 この変更を行い、すべてのゾーンを再起動すると、インストールは完了します。

通信での ioctl の使用

CA Access Control を Solaris ブランド ゾーンにインストールする場合は、syscall ではなく ioctl を使用してカーネル モジュールと通信する必要があります。

通信に ioctl を使用するように CA Access Control を変更するには、以下の手順に従います。

1. グローバル ゾーンおよびそれ以外のすべてのゾーンで、CA Access Control を停止します。

   最後のゾーンは secons -sk を使用して停止します。これにより、イベント インターセプトが無効になり、カーネル モジュールをアンロードするための準備が開始されます。

2. グローバル ゾーンで CA Access Control カーネル モジュールをアンロードします（SEOS_load -u）。

   注: SEOS_load -u コマンドを実行すると、CA Access Control のアンロードの前に、CA Access Control が非グローバル ゾーンで実行されることは決してありません。

3. CA Access Control がインストールされている各ゾーン（グローバル、非グローバル、およびブランド ゾーン）で、seos.ini エントリ SEOS_use_ioctl を 1 に設定します（デフォルトでは、0 に設定されています）。

4. カーネル モジュールをグローバル ゾーンにロードします（SEOS_load）。

   これによって、擬似デバイスがインストールされ、CA Access Control が ioctl によってカーネル モジュールと通信し、ioctl を使用できるようになるために再起動が必要なゾーンを識別できるようになります。

5. 再起動が必要と認識された、CA Access Control がインストールされている、各非グローバル ゾーンおよびブランド ゾーンを再起動します。

ゾーン内での CA Access Control の起動および停止

Solaris 10 ゾーン内での CA Access Control の起動および停止は、通常、Solaris コンピュータでの CA Access Control の起動および停止の場合と同じ方法で実行されます。

ゾーンでの CA Access Control の起動には、以下の例外が適用されます。

- CA Access Control カーネル モジュール（SEOS_load）は、グローバル ゾーンからしかロードできません。
- 非グローバル ゾーンで CA Access Control を起動するには、事前にグローバル ゾーンに CA Access Control カーネル モジュールをロードする必要があります。

  CA Access Control カーネル モジュールがグローバル ゾーンにロードされたら、任意のグローバル ゾーンで、任意の順序で CA Access Control を起動および停止することができます。

ゾーンでの CA Access Control の停止には、以下の例外が適用されます。

- 1 つ以上のゾーンで メンテナンス モード(167 ページ)が有効になっている場合、CA Access Control カーネル モジュールをアンロードすることはできません。
- すべてのゾーンで CA Access Control を任意の順序で停止するには、各ゾーンで secons -s コマンドを実行します。
- すべてのゾーンで CA Access Control を同時に停止するには、GHOST レコードにすべてのゾーンを追加し、グローバル ゾーンから secons -s ghost_name コマンドを発行します。

  この方法は、すべてのゾーンで CA Access Control をアップグレードするときに有用です。
- 最後のゾーンは secons -sk を使用して停止します。これにより、イベント インターセプトが無効にされ、CA Access Control カーネル モジュールをアンロードするための準備が行われます。
- CA Access Control カーネル モジュール(SEOS_load -u)は、グローバル ゾーンからしかアンロードできません。

  注: SEOS_load -u コマンドを実行すると、CA Access Control のアンロードの前に、CA Access Control が非グローバル ゾーンで実行されることは決してありません。

非グローバル ゾーン内での CA Access Control の起動

通常の場合と同様に非グローバル ゾーンから CA Access Control を起動することができますが、それにはまずグローバル ゾーンで CA Access Control カーネル モジュールをロードする必要があります。

非グローバル ゾーン内で CA Access Control を起動する方法

1. グローバル ゾーン内で SEOS_load コマンドを入力して、CA Access Control カーネル モジュールをロードします。

   CA Access Control カーネルがロードされると、任意のゾーンで CA Access Control を起動できるようになります。

   注: CA Access Control カーネルはロードされますが、CA Access Control はグローバル ゾーン内のイベントをインターセプトしません。
2. 非グローバル ゾーンでは、seload コマンドを入力して CA Access Control を起動します。

   非グローバル ゾーンは、CA Access Control によって保護されます。

   注: 非グローバル ゾーンでは、CA Access Control をリモートで起動することもできます。 詳細については、「リファレンス ガイド」の「seload」コマンドの説明を参照してください。

zlogin ユーティリティによる保護

zlogin ユーティリティを使用することで、管理者はゾーンに入ることができます。 非グローバル ゾーンにログインできるユーザを制御するには、このユーティリティに対して LOGINAPPL リソースを追加する必要があります。

zlogin ユーティリティを保護するために、CA Access Control には事前に定義された LOGINAPPL リソースがあります。

CA Access Control の自動起動

CA Access Control をテストして、その機能に問題がない場合は、CA Access Control の保護機能を実装することができます。

システムの起動時に seosd デーモンが自動的に起動して、リソースがすぐに保護されるように設定するには、ACInstallDir/samples/system.init/sub-dir ディレクトリを使用します。ここで、sub-dir はオペレーティング システム用のディレクトリです。 各サブディレクトリには、README ファイルと、それぞれのオペレーティング システムでこのタスクを実行するための手順が含まれています。

第 6 章: CA Enterprise Log Manager との統合

このセクションには、以下のトピックが含まれています。

CA Enterprise Log Manager について

CA Enterprise Log Manager は、IT のコンプライアンスおよび保証に重点的に取り組んでいます。 これを使用することによって、IT アクティビティを収集し、標準化し、集約して報告し、コンプライアンス違反が発生した場合にアクションを必要とするアラートを生成することができます。 異なるセキュリティ デバイスおよびセキュリティ以外のデバイスからデータを収集できます。

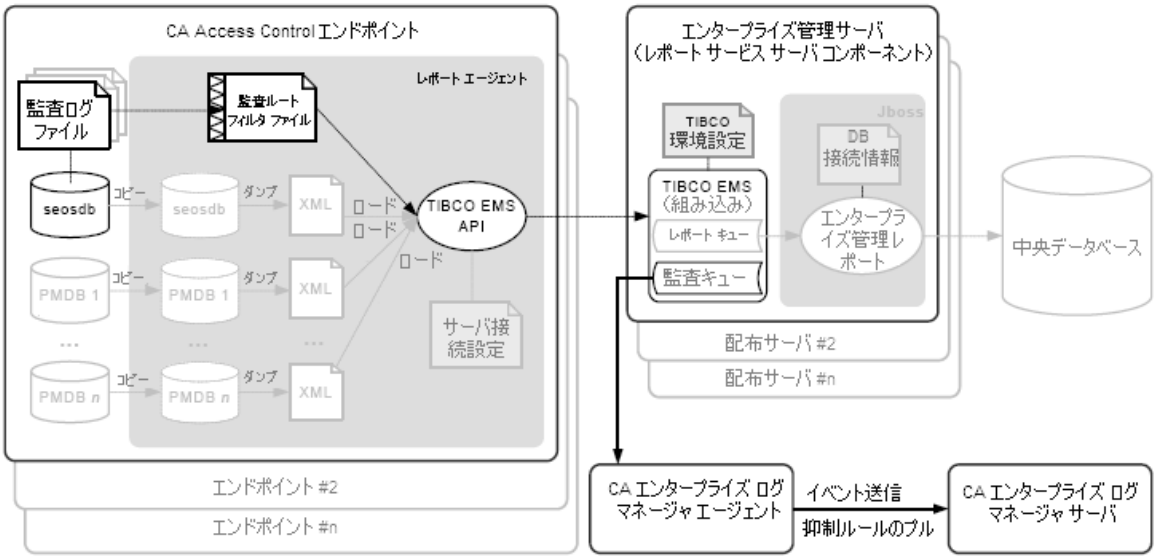
CALM 統合アーキテクチャ

CA Enterprise Log Manager との統合により、それぞれのエンドポイントから CA Access Control 監査イベントを送信して、CA Enterprise Log Manager で収集とレポートを実行できます。

ローカル エンドポイント上の監査ファイルから配布サーバ上のリモート監査キューに、監査イベントを送信するように CA Access Control を設定できます。 次に、CA Enterprise Log Manager コネクタが監査キューに接続して、そこからイベント(メッセージ)をプルできるように設定します。 CA Enterprise Log Manager はこれらのイベントを処理して、CA Enterprise Log Manager サーバに送信します。

CA Access Control インストールは CA Enterprise Log Manager 統合をサポートします。

以下の図に、CA Enterprise Log Manager 統合コンポーネントのアーキテクチャを示します。



上図は、以下のことを示します。

- CA Access Control データベース(seosdb)が含まれる各エンドポイントには、レポート エージェント コンポーネントがインストールされています。
- レポート エージェントはエンドポイントから監査データを収集し、配布サーバに送信します。
- 配布サーバは監査データを監査キューに蓄積します。
- CA Enterprise Log Manager エージェントは監査キューからイベントを収集し、処理のために CA Enterprise Log Manager サーバに送信します。

注: CA Enterprise Log Manager 統合はレポートするサービス コンポーネントに依存します。 そのため、CA Enterprise Log Manager 統合では使用されないその他のレポート サービスのコンポーネントや機能もアーキテクチャに含まれます。 そのようなコンポーネントや機能は、図中で淡色表示されています。

注: デフォルトでは、CA Access Control エンタープライズ管理 はエンタープライズ管理サーバに配布サーバをインストールします。 可用性を高める場合は、別のコンピュータに配布サーバをインストールします。

詳細情報:

レポート サービスのアーキテクチャ(201 ページ)

CA Enterprise Log Manager 統合コンポーネント

CA Enterprise Log Manager 統合では次の CA Access Control コンポーネントを使用します。

- Report Agent は、各 CA Access Control または UNAB エンドポイント上で実行される Windows サービスまたは UNIX デーモンで、配布サーバ上の指定された Message Queue のキューに情報を送信します。 CA Enterprise Log Manager 統合の場合、レポート エージェントが監査ログ ファイルからエンドポイント監査メッセージを定期的に収集し、収集したイベントを設定済みの配布サーバ上にある監査キューに送信します。
- メッセージ キューは、配布サーバのコンポーネントの 1 つで、レポート エージェントが送信するエンドポイント情報を受信するように設定されています。 レポートに関しては、メッセージ キューは、CA Access Control Web サービスを使用して、中央データベースからエンドポイント データベースのスナップショットを転送します。 冗長性およびフェールオーバを実現するために、複数の配布サーバを使用して情報の収集および転送を行うことができます。

注: これらのコンポーネントは、CA Access Control エンタープライズ レポーティング サービスの一部です。 デフォルトでは、CA Access Control エンタープライズ管理 はエンタープライズ管理サーバに配布サーバをインストールします。

CA Enterprise Log Manager 統合では次の CA Enterprise Log Manager コンポーネントも使用します。

- CA Enterprise Log Manager エージェントは、コネクタによって設定される汎用サービスであり、そのそれぞれが単一のイベント ソースから生のイベントを収集して、そのイベントを処理のために CA Enterprise Log Manager サーバに送信します。 CA Access Control 監査データの場合、エージェントが CA Access Control コネクタをデプロイします。
- CA Access Control コネクタは、CA Access Control 監査イベント ソース用の使いやすい CA Enterprise Log Manager 統合です。 コネクタによって、CA Access Control 配布サーバからの生のイベント収集およびイベント ログ ストアへの変換済みイベントのルール ベース伝送が可能になり、イベント ログ ストアでイベントはホット データベースに挿入されます。
- コレクション サーバは、受信イベント ログの調整、ホット データベースへの受信イベント ログの挿入、ウォーム データベースに対する設定サイズに達したときのホット データベースの圧縮、および関連管理サーバへのウォーム データベースの定期的な自動アーカイブを専門に行う CA Enterprise Log Manager サーバです。

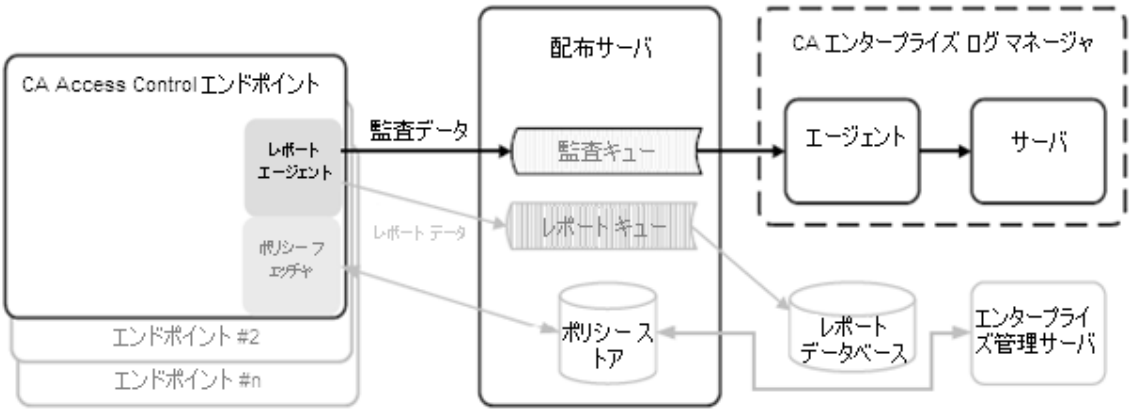
注: CA Enterprise Log Manager コンポーネントの詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

詳細情報:

レポート サービスのアーキテクチャ(201 ページ)

CA Access Control と CA Enterprise Log Manager 間の監査データ フローの概要

CA Access Control が CA Enterprise Log Manager とどのように統合されるか、また、この統合の設定に関して何を検討すべきか理解するには、最初に CA Access Control と CA Enterprise Log Manager の間の監査データのフローを検討する必要があります。以下の図は、CA Access Control が監査イベントを配布サーバ上のメッセージ キューにルーティングする方法を示しています。配布サーバ上で、CA Enterprise Log Manager エージェントの CA Access Control コネクタによってイベントのプル、マップ、および変換が行われ、CA Enterprise Log Manager サーバに送信されます。



1. レポート エージェントはローカル エンドポイントの監査ファイルから監査イベントを収集し、フィルタリング ポリシーを適用し、配布サーバ上にあるリモート監査キューにイベントを格納します。
2. CA Enterprise Log Manager エージェントによってデプロイされた CA Enterprise Log Manager コネクタが監査キューと接続し、そこからイベント(メッセージ)をプルします。
3. CA Enterprise Log Manager コネクタ/エージェントはデータ マッピングおよび解析ファイルを使用して Common Event Grammar(CEG)にイベントをマップし、CA Enterprise Log Manager サーバにイベントをルーティングする前に、抑制および要約ルールを適用します。
4. CA Enterprise Log Manager サーバはイベントを受け取り、場合により、イベントを格納する前に追加の抑制および要約ルールを適用します。

注: CA Enterprise Log Manager の動作の詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

CA Access Control に対する CA Enterprise Log Manager のセット アップ方法

CA Enterprise Log Manager を使用して、すべての CA Access Control エンドポイントからの監査データを含むレポートを作成するには、最初にエンタープライズ レポートを実装します。 CA Enterprise Log Manager との統合の前に、エンタープライズ レポートを実装する必要があります。これは、エンタープライズ レポートによってエンドポイントでレポート エージェントが有効になったためです。 エンタープライズ レポートを実装したら、CA Enterprise Log Manager を CA Access Control 用に設定します。

CA Access Control に対して CA Enterprise Log Manager をセット アップするには、以下の手順に従います。

1. CA Enterprise Log Manager サーバをインストールします。

   注: 詳細については、「CA Enterprise Log Manager Implementation Guide」を参照してください。

2. CA Enterprise Log Manager エージェントを配布サーバ上またはその近辺にインストールします。

   エージェントは配布サーバからアクセス可能であり、指定されたポートを使用して、配布サーバと通信する必要があります。 CA Enterprise Log Manager サーバにもアクセス可能である必要があります。

   注: CA Enterprise Log Manager エージェントをインストールする前に、オペレーティング システムが CA Enterprise Log Manager エージェントをサポートしていることを確認してください。 エージェントのインストールの詳細については、「CA Enterprise Log Manager Agent Installation Guide」を参照してください。

3. CA Access Control エンタープライズ管理 をインストールします。

   注: 詳細については、「実装ガイド」を参照してください。

4. エージェントの新しいコネクタを作成します。

   CA Enterprise Log Manager エージェントをインストールして CA Enterprise Log Manager サーバとの通信を開始したら、新しいコネクタを作成し、そのコネクタが CA Access Control のイベント ソース(配布サーバ上の監査キュー)にアクセスできるように設定する必要があります。

   注: 以下のトピックでは、統合が成功するために設定する必要がある、コネクタの詳細およびコネクタ設定要件など、CA Access Control のイベント収集に必要な設定について説明します。 F コネクタの作成方法の詳細については、「CA Enterprise Log Manager Administration Guide」および「オンライン ヘルプ」をご覧ください。

5. CA Access Control エンタープライズ管理 から CA Enterprise Log Manager への接続を作成します。

6. (オプション)監査コレクタを設定します。

7. 監査データ収集用の CA Access Control エンドポイントを設定します。

詳細情報:

エンタープライズ レポート機能 (201 ページ)
レポート サービス サーバ コンポーネントの設定方法 (203 ページ)

コネクタの詳細

CA Enterprise Log Manager エージェントをコンピュータにインストールすると、そのコンピュータが CA Enterprise Log Manager サーバ管理インターフェースに表示されます ([管理]-[Log Collection]-[Agent Explorer]-[Default Agent Group]-[computer_name] をクリック)。 このとき、コネクタを作成する必要があります。 このトピックでは、コネクタ作成ウィザードの[コネクタの詳細]ページで行う必要がある設定について説明します。

注: イベント収集をカスタマイズできるその他のオプション設定については、「CA Enterprise Log Manager Administration Guide」および「オンライン ヘルプ」を参照してください。

移行

テンプレートとして使用する統合を指定します。

AccessControl_R12SP1_TIBCO_Connector を選択します。

任意でコネクタ名を変更して、説明を追加することもできます。 さらに、コネクタによって処理されるイベントに抑制ルールを適用できます。

抑制および要約ルール

コネクタを作成してコネクタの詳細を指定したら、任意で Connector Creation ウィザードの[Apply Suppression Rules]ページで抑制ルールを適用できます。

CA Access Control の抑制および要約ルールに関する理想モデルの名前は、ホスト IDS/IPS です。 ルールを作成する場合、イベントを特定するために必要に応じてイベント カテゴリ、イベント クラス、およびイベント アクションの値を選択してください。

注: イベント収集をカスタマイズできるその他のオプション設定については、「CA Enterprise Log Manager Administration Guide」および「オンライン ヘルプ」を参照してください。 フィールドの意味や個々の値の詳細については、CA Enterprise Log Manager オンライン ヘルプの「Common Event Grammar Reference」を参照してください。

コネクタ設定の要件

コネクタを作成してコネクタの詳細を指定したら、コネクタを設定できます。 このトピックでは、イベント収集を開始するために、コネクタ作成ウィザードの[コネクタ設定]ページで行う必要がある設定について説明します。

注: イベント収集をカスタマイズできるその他のオプション設定については、「CA Enterprise Log Manager Administration Guide」および「オンライン ヘルプ」を参照してください。

TIBCO サーバ

TIBCO サーバのホスト名または IP アドレスを次の形式で指定します。

```
Protocol://server IP or name:Port number
```

たとえば、CA Access Control エンタープライズ管理 のインストール時に、SSL を使用して通信するかどうかを指定します。 そのいずれかによって、以下の一方を指定します。

- SSL を選択しなかった場合、以下の値を指定します。

  ```
  tcp://ACDistributionServer:7222
  ```

- SSL を選択した場合、以下の値を指定します。

  ```
  ssl://ACDistributionServer:7243
  ```

上記のポート値は、配布サーバが使用するデフォルトのポートです。 配布サーバのインストール時に別の値を定義した場合は、そのポート値を使用します。

TIBCO ユーザ

TIBCO サーバ認証のためのユーザ名を指定します。

たとえば、CA Access Control エンタープライズ管理 のインストール時に、SSL を使用して通信するかどうかを指定します。 そのいずれかによって、以下の一方を指定します。

- SSL を選択しなかった場合、ユーザ名を入力しませんでした。 このフィールドは空のままにします。

  配布サーバは匿名認証を使用します。

- SSL を選択した場合、CA Access Control エンタープライズ管理 のインストール時に定義したユーザ名を指定します。

TIBCO パスワード

TIBCO サーバ認証のためのパスワードを指定します。

たとえば、CA Access Control エンタープライズ管理 のインストール時に、SSL を使用して通信するかどうかを指定します。 そのいずれかによって、以下の一方を指定します。

- SSL を選択しなかった場合、パスワードを入力しませんでした。 このフィールドは空のままにします。

  配布サーバは匿名認証を使用します。

- SSL を選択した場合、CA Access Control エンタープライズ管理 のインストール時に定義したパスワードを指定します。

イベント ログ名

イベント ソースのログ名を指定します。

デフォルトの「eTrust Access Control」を使用します。

PollInterval

TIBCO サーバが使用不可になった場合、または切断された場合に、イベントをポーリングするまでエージェントが待機する秒数を指定します。

SourceName

TIBCO キューの識別子を指定します。

デフォルトの「queue_audit」を使用します。

TIBCO キュー

ログ センサによるメッセージ(イベント)の読み取り元である TIBCO キューの名前を指定します。

デフォルトの「queue/audit」を使用します。

コレクション スレッドの数

TIBCO キュー メッセージを読み取るためにログ センサが生成するスレッドの数を指定します。

イベントに対応するように、また CA Enterprise Log Manager エージェント システムに十分な CPU がある場合に、この値を調整してください。

制限: 最小値は 1 です。 ログ センサが生成できるスレッドの最大数は 20 です。

レポート エージェントによる監査イベントの収集とルーティングに関する概要

CA Enterprise Log Manager 統合の場合、レポート エージェントが監査ログ ファイルからエンドポイント監査メッセージを定期的に収集し、そのイベントを設定済み配布サーバ上の監査キューにルーティングします。 レポート エージェントの設定をチューニングすると、パフォーマンスを向上させることができます。

注: レポート エージェントは CA Access Control エンタープライズ レポート サービスの一部であり、エンドポイント レポートの目的でデータベース スナップショットの送信も担当します。 このプロセスは、CA Enterprise Log Manager への監査イベント ルーティングのためにレポート エージェントが行うアクションのみを示します。

監査収集を有効にしたかどうか(audit_enabled 設定)に関係なく、レポート エージェントは以下のことを行います。

- エンドポイント監査ファイルを読み取ってメモリにコミットすることによって、新しい監査レコードを収集します。

  レポート エージェントは、audit_read_chunk 構成設定に定義した監査レコードの数を読み取り、再び監査ファイルを読み取るまで、audit_sleep 構成設定に定義した間だけ待機します。 レポート エージェントは、アクティブな監査ログおよびすべてのバックアップ監査ファイル内の読み取られていないレコードを読み取ります。 そして、監査フィルタ ファイルに定義した監査フィルタ(audit_filter 構成設定)を通過するレコードをメモリにコミットします。

- メモリにある監査レコードのグループを audit_queue 設定で定義した配布サーバ メッセージ キューに送信します。

  次のいずれかの場合に該当すると、レポート エージェントは監査レコードを送信します。

  - メモリのレコードの数が audit_send_chunk 構成設定で定義された数に達する。
  - 最後の監査レコードが送信されてからの経過時間が audit_timeout 設定で定義された間隔に等しい。

例: 監査収集とルーティングに関するレポート エージェントのデフォルト設定

この例は、レポート エージェントのデフォルト構成設定がどのように設定されているか、その設定がどのような環境に適するか、およびその設定がパフォーマンスにどのように影響するかを示します。

平均的な環境で、秒あたりのイベント数(EPS) 30 を想定しています。 したがって、レポート エージェントは毎秒通過する 30 のイベントを読み取ります。 その他の実行中のアプリケーションに対する影響(CPU 使用およびコンテキスト スイッチ)を減らすために、以下のようにレポート エージェントのイベント読み取りを 10 秒ごとに 300 としています。

```
audit_sleep=10
audit_read_chunk=300
```

レポート エージェントと配布サーバ間のメッセージ伝送のために CA Access Control が使用するメッセージ バスは、短い間隔で小さなパケットを処理するよりも長い間隔で送信される大きなパケットを処理するのに適しています。 次の構成設定は、レポート エージェントが収集する監査レコードの数が定義された数に達すると、それらのレコードをレポート エージェントが配布サーバに送信するように指定しています。 1 秒間 30 イベントとすると、レポート エージェントがおよそ 1 分(60 秒)間隔で監査レコードを送信するようにするには、レポート エージェントを次のように設定する必要があります。

```
audit_send_chunk=1800
```

ただし、夜間などの時間帯で 1 秒間 30 未満のイベントになると、1 分間 1800 未満のイベントになります。 レポート エージェントがなおも定期的に監査レコードを配布サーバに送信するようにするために、次のように監査レコード送信間隔を最大 5 分に設定します。

```
audit_timeout=300
```

CA Enterprise Log Manager からのイベントのフィルタリング

CA Access Control がログ ファイルに書き込む監査レコードの一部を CA Enterprise Log Manager に送信しないようにするには、フィルタ ファイルを使用して CA Access Control が配布サーバに送信しないレコードを定義します。

注: フィルタリングされた監査イベントはローカルの監査ファイルに書き込まれますが、CA Access Control はそれを配布サーバのメッセージ キューに送信しません。 ローカルの監査ファイルから監査メッセージを除外するには、logmgr セクションの AuditFiltersFile 構成設定で定義されているファイル(デフォルトでは audit.cfg)にあるフィルタ ルールを変更します。

CA Enterprise Log Manager からのイベントをフィルタリングするには、監査フィルタ ポリシーを作成し、そのポリシーを有効にするエンドポイントに割り当てます。

注: または、エンドポイントの監査ルーティング フィルタ ファイルを直接編集することもできます。 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。

例: 監査フィルタ ポリシー

監査フィルタ ポリシーの例を以下に示します。

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

この例は、次の行を auditrouteflt.cfg ファイルに書き込みます。

```
FILE;*;*;R;P
```

この行は、ファイル リソースへの読み取りアクセスのためにアクセサが行った許可された試行を記録した監査レコードをフィルタします。 CA Access Control はこの監査レコードを配布 サーバに送信しません。

SSL を使用した安全な通信

CA Access Control エンタープライズ管理 をインストールする場合、SSL を使用して配布サーバとレポート エージェントの間の通信を保護するか、通信を保護しないか選択できます。 いずれのオプションを選択した場合でも、エンドポイントにレポート エージェントをインストールするときと同じオプションを指定する必要があります。

たとえば、SSL を使用してレポート エージェントと配布サーバ間の通信を暗号化することを選択した場合（デフォルト設定）、CA Access Control エンタープライズ管理 のインストール時に、以下のような認証情報を指定する必要があります。

- レポート エージェントが配布サーバと通信するために必要なパスワードです。

これは、CA Enterprise Log Manager エージェントの［Connector Configuration］ページで、エンドポイントの CA Access Control レポート エージェントを設定するときに指定するパスワードです。

レポート エージェントをインストールするときに、同じ情報を指定する必要があります。正しい証明書とパスワード情報を提供できるレポート エージェントのみが、配布サーバ上の監査キューにイベントを書き込むことができ、書き込まれたイベントは CA Enterprise Log Manager によって取得されます。

CA Enterprise Log Manager 統合のための監査ログ ファイルのバックアップ

監査データを収集するために、レポート エージェントは構成設定に従って CA Access Control 監査ログ ファイルを読み取ります。 レポート エージェントは、設定された時間間隔で設定された数の監査レコードを監査ログ ファイルから読み取ります。 デフォルトのレガシー インストールの場合、またはインストール時に監査ログ ルーティングを有効にしていない場合、CA Access Control はサイズによる監査ログ バックアップ ファイルのみを保存します。 監査ログが設定された最大サイズに達するたびに、既存の監査ログ バックアップ ファイルが上書きされてバックアップ ファイルが作成されます。 そのため、レポート エージェントがすべてのレコードを読み取る前に、バックアップ ファイルが上書きされる可能性があります。

CA Access Control が監査ログ ファイルのタイムスタンプ付きバックアップを保存するように設定することを強くお勧めします。 こうすると、保存されるべき監査ログ ファイルの設定された最大数に達するまで、CA Access Control はバックアップの監査ログ ファイルを上書きしません。 これは、エンドポイント上へのインストール時に、監査ログ ルーティング サブ機能を有効にした場合のデフォルト設定です。

例: 監査ログ バックアップの設定

この例は、推奨の構成設定がどのように CA Enterprise Log Manager 統合に影響するかを示します。 エンドポイント上へのインストール時に、監査ログ ルーティング サブ機能を有効にすると、CA Access Control は logmgr セクションの以下の環境設定を行います。

```
BackUp_Date=yes
audit_max_files=50
```

この場合、CA Access Control は監査ログ ファイルの各バックアップ コピーにタイムスタンプを付け、最大 50 のバックアップ ファイルを保存します。 これによって、レポートエージェントがすべての監査レコードをファイルから読み取ったり、必要に応じてバックアップ ファイルを安全に保管するために手動でコピーしたりすることが行いやすくなります。

重要: audit_max_files を 0 に設定すると、CA Access Control はバックアップ ファイルを削除せずに蓄積し続けます。 バックアップ ファイルを外部プロシージャによって管理する場合、CA Access Control がデフォルトでバックアップ ファイルを保護することに注意してください。

CA Enterprise Log Manager 統合用の既存エンドポイントの設定

CA Access Control エンタープライズ管理 がインストールされ設定されていれば、レポート サーバを有効にし設定して、監査データをレポート サーバに送信するように、エンドポイントを設定できます。

注: CA Access Control をインストールすると、監査データの収集および送信のためにエンドポイントを設定することが可能になります。 この手順は、インストール時にこのオプションを設定しなかった場合に、監査データ送信のために既存のエンドポイントを設定する方法です。

Windows で CA Enterprise Log Manager 統合のために既存のエンドポイントを設定する方法

1. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   [プログラムの追加と削除]ダイアログ ボックスが表示されます。

2. プログラム リストをスクロールして CA Access Control を選択します。

3. [変更]をクリックします。

   CA Access Control のインストール ウィザードが表示されます。

   レポート エージェント機能および監査ルーティング サブ機能が有効になるように、CA Access Control インストールを変更するウィザードのプロンプトに従います。

   また、監査ログ ファイルのタイムスタンプ付きバックアップを保存するように指定していることを確認してください。

UNIX で CA Enterprise Log Manager 統合のために既存のエンドポイントを設定する方法

1. AccessControlSharedDir/lbin/report_agent.sh を実行します。

   ```
   report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number [-rqueue queue_name] -audit -bak
   ```

   設定オプションを省略すると、デフォルト設定が使用されます。

   注: report_agent.sh スクリプトの詳細については、「リファレンス ガイド」を参照してください。

2. データベース内に +reportagent ユーザを作成します。

   このユーザは、ADMIN 属性および AUDITOR 属性、ならびローカル端末への書き込みアクセス権を有する必要があります。 また、epassword をレポート エージェント共有秘密鍵(レポート サーバのインストール時に定義したもの)に設定する必要があります。

3. レポート エージェント プロセス用に SPECIALPGM を作成します。

   SPECIALPGM は、root ユーザを +reportagent ユーザにマップします。

注: レポート エージェントおよび監査ルーティングを有効にした後、パフォーマンス関連の CA Access Control 構成設定を変更できます。 作業を行う前に、レポート エージェントが監査イベントを収集してレポート サーバにルーティングする方法(187 ページ)について理解しておいてください。 レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

例: selang を使用した CA Enterprise Log Manager 統合のための UNIX エンドポイントの設定

次の selang コマンドは、レポート エージェントを有効にして設定した場合に、どのように必要なレポート エージェント ユーザを作成し、レポート エージェント プロセスの特別なセキュリティ権限を指定するかを示します。

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \
Nativeuid(root) pgmtype(none)
```

CA Enterprise Log Manager 統合用の既存の UNIX エンドポイントの設定

CA Access Control エンタープライズ管理 のインストールおよび設定の完了後、監査データを配布サーバに送信するようにエンドポイントを設定することができます。これを行うには、レポート エージェントを有効にして設定します。

注: CA Access Control をインストールすると、監査データの収集および送信のためにエンドポイントを設定することが可能になります。 この手順は、インストール時にこのオプションを設定しなかった場合に、監査データ送信のために既存のエンドポイントを設定する方法です。

CA Enterprise Log Manager 統合用の既存の UNIX エンドポイントの設定

1. ACSharedDir/lbin/report_agent.sh を実行します。

   ```
   report_agent config -server hostname [-proto {ssl|tcp}] [-port port_number [-rqueue queue_name] -audit -bak
   ```

   設定オプションを省略すると、デフォルト設定が使用されます。

   注: report_agent.sh スクリプトの詳細については、「リファレンス ガイド」を参照してください。

2. データベース内に +reportagent ユーザを作成します。

   このユーザは、ADMIN 属性および AUDITOR 属性、ならびローカル端末への書き込みアクセス権を有する必要があります。 また、epassword をレポート エージェント共有秘密キー(配布サーバのインストール時に定義)に設定する必要があります。

3. レポート エージェント プロセス用に SPECIALPGM を作成します。

   SPECIALPGM は、root ユーザを +reportagent ユーザにマップします。

注: レポート エージェントおよび監査ルーティングを有効にした後、パフォーマンス関連の CA Access Control 構成設定を変更できます。 この操作を行う前に、レポート エージェントが監査イベントを収集して配布サーバにルーティングする方法について (187 ページ)理解しておく必要があります。 レポート エージェントの構成設定の詳細については、「リファレンス ガイド」を参照してください。

例: selang を使用した CA Enterprise Log Manager 統合のための UNIX エンドポイントの設定

次の selang コマンドは、レポート エージェントを有効にして設定した場合に、どのように必要なレポート エージェント ユーザを作成し、レポート エージェント プロセスの特別なセキュリティ権限を指定するかを示します。

```
eu +reportagent admin auditor logical epassword(Report_Agent) nonative
auth terminal (terminal101) uid( +reportagent) access(w)
er specialpgm (/opt/CA/AcessControl/bin/ReportAgent) Seosuid(+reportagent) \

Nativeuid(root) pgmtype(none)
```

CA Access Control イベントのクエリおよびレポート

CA Access Control のクエリ、レポート、およびアクション警告は、CA Enterprise Log Manager インターフェースの[Server Resource Protection]タグにまとめられています。

注: 詳細情報については、http://ca.com/support の CA Enterprise Log Manager 製品ページで、CA Enterprise Log Manager - Reports - Complete List リンクをクリックしてください。

CA Access Control 内の CA Enterprise Log Manager レポートを有効にする方法

CA Access Control エンタープライズ管理 で CA Enterprise Log Manager レポートを表示できるようにするには、CA Access Control エンタープライズ管理 で CA Enterprise Log Manager レポートを有効にし、CA Enterprise Log Manager 証明書をエクスポートして追加し、CA Access Control エンタープライズ管理 から CA Enterprise Log Manager への接続を設定する必要があります。

1. 高度な設定により、CA Enterprise Log Manager レポートを有効にします。(61 ページ)
2. CA Enterprise Log Manager の trusted 証明書をエクスポートして、キーストアに追加します。(195 ページ)
3. CA Enterprise Log Manager への接続を設定します。
4. (オプション) 監査コレクタを設定します。

   PUPM 監査イベントを CA Enterprise Log Manager に送信する場合は、監査コレクタを設定します。

CA Enterprise Log Manager の trusted 証明書のキーストアへの追加

CA Enterprise Log Manager レポートは、トラステッド証明書を使用して認証されます。証明書は、レポートに表示されている情報がトラステッド CA Enterprise Log Manager ソースのものであることを証明します。トラステッド CA Enterprise Log Manager ソースはデータの信頼性を証明します。

CA Access Control エンタープライズ管理 で CA Enterprise Log Manager を表示するには、まず証明書をエクスポートし、次にそれをキーストアに追加します。

CA Enterprise Log Manager の trusted 証明書のキーストアへの追加方法

1. Web ブラウザで CA Enterprise Log Manager サーバの URL を「https://host:port」形式で入力します。

   セキュリティの警告ダイアログ ボックスが開きます。

2. [証明書の表示]をクリックします。

   [証明書]ダイアログ ボックスが表示されます。

3. [詳細]-[ファイルへのコピー]をクリックします。

   [証明書のエクスポート]ウィザードが表示されます。

4. 以下の指示に従って、ウィザードを完了します。

   - ファイル形式のエクスポート - Base-64 エンコード X.509 (.CER) を選択します。
   - エクスポートするファイル - エクスポートされた証明書ファイルの完全パス名を定義します。

     たとえば、「C:¥certificates¥computer.base64.cer」のように指定します。

   エクスポートが正常に完了したことを通知するメッセージが表示されます。

5. 証明書をキーストアにインポートします。 以下に例を示します。

   ```
   C:¥jdk1.5.0¥jre¥lib¥security>c:¥jdk1.5.0¥bin¥keytool.exe -import -file
   computer.base64.cer -keystore
   C:¥jboss-4.2.3.GA¥server¥default¥deploy¥IdentityMinder.ear¥custom¥ppm¥truststo
   re¥ssl.keystore
   ```

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。

7. [はい]をクリックして、証明書を信頼します。

   証明書がキーストアに追加されます。

CA Enterprise Log Manager との接続の設定

CA Access Control エンタープライズ管理 は CA Access Control の関連情報を記載したレポートを表示するために CA Enterprise Log Manager と通信します。 これらのレポートを表示するには、CA Enterprise Log Manager への接続を設定する必要があります。

CA Enterprise Log Manager との接続の設定方法

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、ELM ツリーを展開します。

   [CA Enterprise Log Manager 接続の管理]タスクが使用可能なタスク リストに表示されます。
2. [CA Enterprise Log Manager 接続の管理]をクリックします。

   [CA Enterprise Log Manager 接続の管理: PrimaryCALMServer]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

   CA Enterprise Log Manager 接続の名前を識別します。

   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 CA Enterprise Log Manager の名前を定義します。

   例: host1.comp.com

   ポート番号

   CA Enterprise Log Manager ホストが通信に使用するポートを定義します。

   デフォルト: 5250

認証局署名済み SSL 証明書

CA Enterprise Log Manager への接続に認証局が署名した SSL 証明書を使用するかどうかを指定します。

証明書名

証明書の名前を定義します。

パスワード

証明書のパスワードを定義します。

4. [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 が CA Enterprise Log Manager の接続設定を保存します。

例: CA Enterprise Log Manager 証明書情報の取得

以下の例では、CA Access Control エンタープライズ管理 内で CA Enterprise Log Manager 接続設定を作成および管理する際に必要な CA Enterprise Log Manager 証明書情報の取得方法を示しています。

1. 以下の形式で、Web ブラウザに CA Enterprise Log Manager の URL を入力します。

   ```
   https://host:port/spin/calmapi/products.csp
   ```

   例: https://localhost:5250/spin/calmapi/products.csp

2. 有効なユーザ名とパスワードを入力して、CA Enterprise Log Manager にログインします。

3. CA Enterprise Log Manager に証明書を登録するための登録オプションを選択します。

   新しい製品の登録画面が表示されます。

4. 証明書名とパスワードを入力し、登録を選択します。

   証明書の登録が正常に完了したことを通知するメッセージが表示されます。

監査コレクタの設定

CA Access Control エンタープライズ管理 は PUPM 監査イベントを収集し、ローカルに格納します。 監査イベントを CA Enterprise Log Manager に送信するように、CA Access Control エンタープライズ管理 を設定できます。

監査コレクタの設定方法

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、ELM ツリーを展開します。

      [監査コレクタの作成]タスクが使用可能なタスク リストに表示されます。
2. [監査コレクタの作成]をクリックします。

   [監査コレクタの作成: 監査コレクタ検索画面]が表示されます。
3. (オプション)既存の監査コレクタを選択し、新規監査コレクタをそのコピーとして、以下のように作成します。
   a. [ELM 送信者タイプのオブジェクトのコピーの作成]を選択します。
   b. 検索属性を選択し、フィルタ値を入力し、[検索]をクリックします。

      フィルタ条件に一致する ELM 送信者のリストが表示されます。
   c. 新規監査コレクタのベースとして使用するオブジェクトを選択します。
4. [OK]をクリックします。

   [監査コレクタの作成]タスク ページが表示されます。 監査コレクタを既存のオブジェクトから作成した場合、ダイアログ ボックスのフィールドには、既存オブジェクトの値がすでに入力されています。
5. 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。

   ジョブの有効化

   監査コレクタを有効にするかどうかを指定します。

   名前

   監査コレクタの名前を定義します。

   キュー JNDI

   CA Access Control エンタープライズ管理 が PUPM 監査イベント メッセージを送信する宛先のメッセージ キュー キューの名前を定義します。

   例: queue/audit

スリープ

データベース クエリの間隔を分単位で定義します。

デフォルト: 1

タイムアウト

監査イベント メッセージのメッセージ キューへの送信に関して、コレクタのタイムアウト期間を分単位で定義します。

デフォルト: 10

注: このタイムアウト期間が経過すると、キュー内のメッセージ数が[メッセージ ブロック サイズ]フィールドで定義されたレベルに達していなくとも、コレクタはメッセージを送信します。

メッセージ ブロック サイズ

データベースに蓄積するメッセージの最大数を定義します。この数に達すると、メッセージはキューに送信されます。

デフォルト: 100

6. [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 は監査コレクタを作成します。

第 7 章: エンタープライズ レポート機能の実装

このセクションには、以下のトピックが含まれています。

エンタープライズ レポート機能

CA Access Control エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ (CA Access Control レポート ポータル) を使用して、レポート機能を提供します。 エンタープライズ レポート機能を使用すると、各エンドポイント (ユーザ、グループ、およびリソース) のセキュリティ ステータスを 1 つの場所で確認できます。 CA Access Control レポートは、誰が何をできるか、つまり、各エンドポイントにデプロイされるルールおよびポリシー、およびポリシー偏差を記述します。

各エンドポイントからのデータの収集は、スケジュールで設定することも、オンデマンドで行うこともできます。 各エンドポイントに接続しなくても、誰がどのリソースへのアクセスを許可されているかを確認することができます。 CA Access Control のエンタープライズ レポート機能は、1 度セットアップすれば、独立して機能して、手動操作を必要とせずに、各エンドポイントからデータの収集および中央サーバへのデータの継続的なレポートを実行します。 つまり、たとえ収集サーバがダウンした状態であっても、各エンドポイントは自身のステータスについてレポートします。

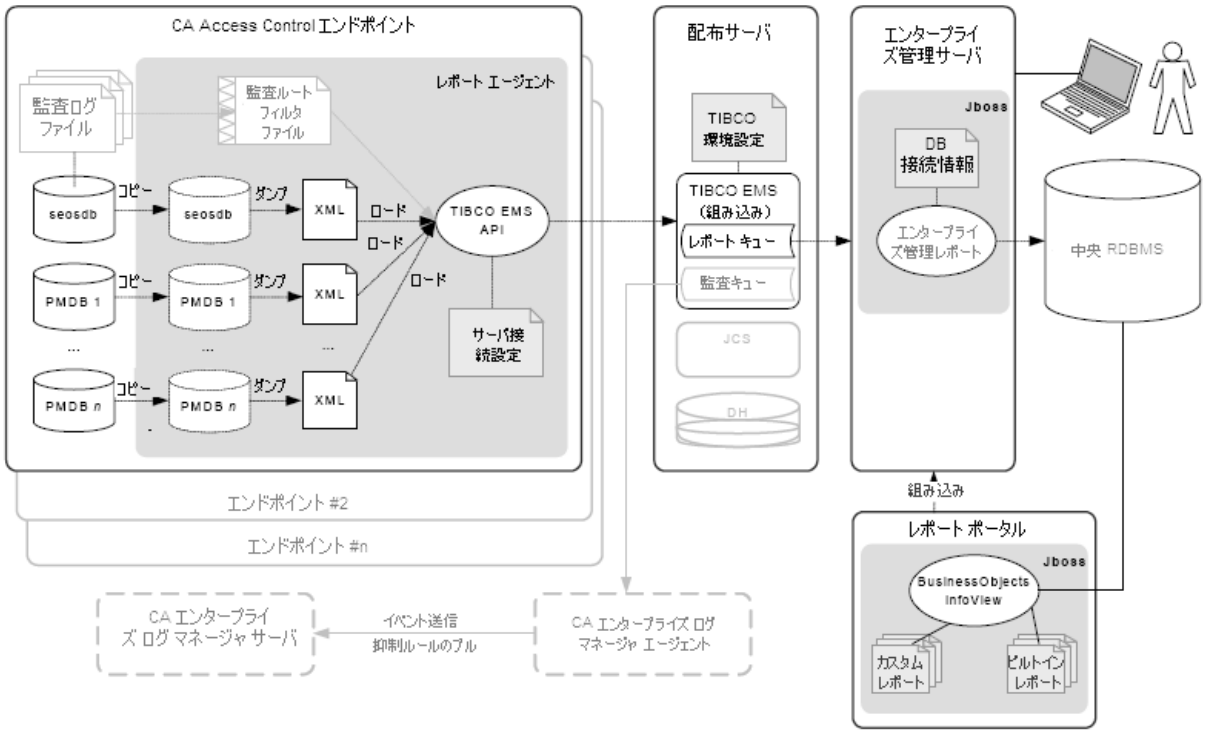
レポート サービスのアーキテクチャ

CA Access Control レポート サービスは、CA Access Control エンタープライズ レポートの作成に対応するサーバ ベースのプラットフォームを提供します。 このサービスを使用して、すべての CA Access Control エンドポイントから取得したデータを含むレポートを作成できます。 作成したレポートは、Web 対応のアプリケーション上で表示および管理できます。

レポート サービスでは、既存の CA Access Control インフラストラクチャ上にレポート環境を構築できます。

注: エンタープライズ レポー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。

以下の図に、レポート サービス コンポーネントのアーキテクチャを示します。 この図では、コンポーネント間でのデータの流れについても示します。



上図は、以下のことを示します。

- CA Access Control データベース(seosdb)および任意の数の Policy Model (PMDB)が含まれる各エンドポイントには、レポート エージェント コンポーネントがインストールされています。
- レポート エージェントはエンドポイントからデータを収集し、配布サーバに送信して処理します。
- 簡単なエンタープライズ モデルでは、1 つの配布サーバを使用して、すべてのエンドポイント データを処理し、処理したデータを中央データベースに送信して、格納します。 配布サーバ コンポーネントを複製することで、大規模な企業環境においてフォルト トレランスおよび高速処理を実現する設計が可能です。
- 中央データベース(RDBMS)を使用して、エンドポイント データを格納します。
- レポート ポータルを利用すると、中央データベース内のデータにアクセスして組み込み型のレポートを作成すること、またはデータについて問い合わせを行いカスタム レポートを作成することができます。

レポート サービス サーバ コンポーネントの設定方法

エンタープライズ レポート機能を使用して、すべての CA Access Control エンドポイントのデータを含むレポートを作成するには、CA Access Control レポート サービス サーバ コンポーネントをインストールし、設定します。 サーバ コンポーネントがインストールされたら、各エンドポイントでレポート エージェントを設定します。

注: レポート エージェントのインストールおよび設定は、CA Access Control エンドポイントのインストールの一環として行われるものであり、この手順では取り扱いません。

レポート サービス サーバ コンポーネントをセットアップするには、以下の手順に従います。

1. まだ CA Access Control エンタープライズ管理 をインストールし設定していない場合は、そうします。
2. レポート ポータル(CA Business Intelligence)をセットアップします。

   重要: Oracle Database 11g を使用する場合は、CA Access Control Premium Edition Report Portal (ディスク 2) DVD で利用可能な BusinessObjects XI Release 2.1 SP5 修正プログラムをインストールします。
3. CA Business Intelligence への接続を設定します。
4. CA Access Control レポートを展開します。
5. スナップショット定義を作成します。

詳細情報:

レポート作成のための Windows エンドポイントの設定(102 ページ)
レポート作成のための UNIX エンドポイントの設定(158 ページ)

レポート ポータル コンピュータのセットアップ方法

レポート ポータルを使用すると、CA Access Control エンタープライズ管理 が中央データベースに格納するエンドポイント データにアクセスして、組み込みレポートの作成、またはデータを問い合わせて、カスタム レポートの作成を行うことができます。 レポート ポータルは、CA Business Intelligence を使用します。

注: レポート ポータルの旧バージョン、または CA Business Intelligence または BusinessObjects EnterpriseXI がスタンドアロンでインストールされている場合、アップグレードの必要はなく、既存のインストールを代わりに使用できます。

重要: Oracle Database 11g を使用する場合は、CA Access Control Premium Edition Report Portal（ディスク 2）DVD で利用可能な BusinessObjects XI Release 2.1 SP5 修正プログラムをインストールします。

レポート ポータルをセットアップするには、以下の手順に従います。

1. まだ実行していない場合は、中央データベースおよび配布サーバをセットアップします。

   注: エンタープライズ管理サーバのインストール時に、中央データベースおよび配布サーバをセットアップします。

2. ご使用のオペレーティング システムに対応する CA Business Intelligence をインストールします。

   CA Business Intelligence インストール ファイルは、CA Access Control Premium Edition レポート ポータル光ディスクに格納されています。

   注: インストール情報の詳細については、「CA Business Intelligence Installation Guide」をご覧ください。これは、CA Access Control Premium Edition ブックシェルフからご利用いただけます。

   レポート ポータルがセット アップされ、これで CA Access Control レポート パッケージをデプロイできるようになりました。

例: Windows への CA Business Intelligence のインストール

以下の手順は、Windows への CA Business Intelligence のインストール方法を示しています。

1. 光ディスク ドライブに CA Access Control Premium Edition Report Portal for Windows DVD を挿入します。
2. ¥Disk1¥InstData¥VM フォルダに移動し、install.exe をダブルクリックします。

   CA Business Intelligence のインストール ウィザードが起動します。

3. 以下の表を使用して、インストール ウィザードを完了します。

情報	アクション
インストール言語	使用するサポート対象インストール言語を選択し、[OK]をクリックします。 **注**: 英語以外のサポート対象言語いずれかにインストールするローカライズされたオペレーティング システムが必要です。
使用許諾契約書	[使用許諾契約書の条項に同意します]を選択し、[次へ]をクリックします。
インストール タイプ	[標準]を選択して、[次へ]をクリックします。
インストール先	[次へ]をクリックして、デフォルト値をそのまま使用します。
BusinessObjects XI 管理者パスワード	「P@ssw0rd」と 2 回入力して、パスワードを設定、確認し、[次へ]をクリックします。 **注**: パスワード ルールについては、「CA Business Intelligence Installation Guide」をご覧ください。これは、CA Access Control Premium Edition ブックシェルフからご利用いただけます。
Web サーバ設定	[次へ]をクリックして、デフォルト設定をそのまま使用します。
CMS データベース設定	以下の情報を入力して、[次へ]をクリックします。 ■ MySQL root パスワード: P@ssw0rd ■ ユーザ名: cadbusr ■ パスワード: C0nf1dent1al ■ データベース名: MySQL1
監査の有効化	[次へ]をクリックして、デフォルト設定をそのまま使用します。
監査データベース設定	以下の情報を入力して、[次へ]をクリックします。 ■ ユーザ名: cadbusr ■ パスワード: C0nf1dent1al ■ データベース名: MySQL1
設定の確認	設定を確認し、[インストール]をクリックして、インストールを完了します。

インストールが開始されます。完了まで、約 1 時間かかる場合もあります。

詳細情報:

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 (49 ページ)

CA Business Intelligenceへの接続の設定

CA Access Control エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ(CA Access Control レポート ポータル)を使用して、レポート機能を提供します。 レポート ポータルをインストールし、レポートを展開した後に、CA Identity Manager 管理コンソールから CA Business Intelligence への接続を設定する必要があります。

CA Business Intelligence への接続の設定方法

1. CA Identity Manager 管理コンソールを有効にします(62 ページ)。
2. CA Identity Manager 管理コンソールを開きます(62 ページ)。
3. [環境]-[ac-env]-[詳細設定]-[レポート]をクリックします。

   [レポート プロパティ]ウィンドウが表示されます。
4. データベースおよび Business Objects のプロパティを入力します。

   注: 詳細については、CA Identity Manager 管理コンソールのオンライン ヘルプをご覧ください。オンライン ヘルプは、アプリケーションからアクセスできます。

   重要: Business Objects ポート フィールドで、レポート ポータルで使用されるポート番号を入力する必要があります。 デフォルトのポートは 8080 です。 Business Objects レポート フォルダで、「CA Access Controlr12」と入力します。
5. [保存]を選択します。

   CA Identity Manager 管理は Business Intelligence 設定を保存します。 これで、CA Access Control エンタープライズ管理 からのレポートの表示に、CA Business Objects を使用できるようになりました。

レポート パッケージのデプロイ

レポート パッケージは.BIAR ファイルで、これによって CA Access Control の 標準レポートがデプロイされます。 レポート パッケージには、レポート ポータル上でのデプロイに使用するアーティファクトおよびディスクリプタの集合体が含まれています。 これらの標準レポートを使用するには、レポート パッケージ ファイルを BusinessObjects InfoView にインポートする必要があります。

注: このパッケージは、レポート ポータルの旧バージョンと下位互換性があります。 最新のレポート パッケージを利用するためにレポート ポータルをアップグレードする必要はありません。 また、ローカライズされたレポート パッケージをデプロイできます。これは、横に並んだ、別々の .biar ファイルとして提供されます。

Windows レポート ポータルでのレポート パッケージのデプロイ

標準の CA Access Control レポートを使用するには、BusinessObjects InfoView にレポート パッケージ ファイルをインポートする必要があります。

注: この手順では、同じパッケージの以前のバージョンがまだデプロイされていない Windows にレポート パッケージをデプロイする方法について説明します。

Windows レポート ポータルにレポート パッケージをデプロイする方法

1. まだ実行していない場合は、中央データベース、配布サーバ、レポート ポータルをセットアップします。
2. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Windows DVD を挿入し、¥ReportPackages フォルダに移動します。
3. biconfig.zip の内容を System_Drive:¥temp フォルダに抽出します。
4. 以下のファイルを光ディスク ドライブから System_Drive:¥temp フォルダにコピーします。
   - ¥ReportPackages¥RDBMS¥AC_BIAR_Config.xml
   - ¥ReportPackages¥RDBMS¥AC_BIAR_File.biar

   RDBMS

   使用している RDBMS のタイプを定義します。

   例: Oracle

   AC_BIAR_Config.xml

   使用する RDBMS のインポート構成ファイル(.xml)の名前を定義します。

   例: Oracle Database 11g の場合、これは import_biar_config_oracle11g.xml になり、SQL Server 2005 の場合、これは import_biar_config_mssql_2005.xml になります。

   AC_BIAR_File.biar

   使用する言語と RDBMS の CA Access Control レポート ファイル(.biar)の名前を定義します。

   注: 使用する RDBMS のインポート構成ファイルの <biar-file name> プロパティはこのファイルをポイントし、デフォルトで使用する RDBMS の英語バージョンの名前に設定されます。

5. 必要に応じて、System_Drive:¥temp¥AC_BIAR_Config.xml ファイルを編集します。

   以下は、設定が必要な XML プロパティです。

   <biar-file name>

   CA Access Control レポート ファイル（.biar）への完全なパス名を定義します。これは以前にコピーしたファイルです。

   <networklayer>

   使用する RDBMS でサポートされているネットワーク層を定義します。

   制限：OLEDB、Oracle OCI

   <rdms>

   使用している RDBMS のタイプを定義します。

   制限：MS SQL Server 2005、Oracle 10、Oracle 11

   <username>

   作成済みの RDBMS 管理ユーザのユーザ名を定義します。

   <password>

   作成済みの RDBMS 管理ユーザのパスワードを定義します。

   <datasource>

   以下のいずれかを定義します。

   - （Oracle） Transparent Network Substrate （TNS）の名前。
   - （SQL Server 2005）作成したデータベース。

   <server>

   SQL Server 2005 コンピュータの名前を定義します。 Oracle Database 11g の場合は、空のままにします。

6. コマンド プロンプトを開き、以下のコマンドを実行します。

   ```
   System_Drive:\BO\biconfig.bat -h host_name -u user_name -p password -f
   ac_biar_config.xml
   ```

   以下に例を示します。

   ```
   biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
   C:\BO\import_biar_config_oracle11g.xml
   ```

   バッチ ファイルにより、CA Access Control レポートが InfoView にインポートされます。この処理が完了するまで数分かかる場合があります。 バッチ ファイルと同じフォルダに作成されるログ ファイル（biconfig.log）は、インポートが成功したかどうかを示します。

例: サンプル Oracle Database XE インポート構成ファイル

以下のコードの一部は、Oracle Database XE のインポート構成ファイル（import_biar_config_oracle11g.xml）の編集方法の例です。データベースは、エンタープライズ管理用の中央データベースを準備した際にセットアップしました。

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:/temp/AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
        <networklayer>Oracle OCI</networklayer>
        <rdms>Oracle 11</rdms>
        <username>ciadb01</username>
        <password>P@ssw0rd</password>
        <datasource>XE</datasource>
        <server></server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

例: サンプル Microsoft SQL Server 2005 インポート構成ファイル

以下のコードの一部は、rdbms.org にインストールされ、r125db データベースを持つ、SQL Server 2005 のインポート構成ファイル（import_biar_config_mssql2005.xml）の編集方法の例です。データベースは、エンタープライズ管理用の中央データベースを準備した際に、作成しました。

```
<?xml version="1.0"?>
<biconfig version="1.0">
  <step priority="1">
    <add>
      <biar-file name="c:/temp/AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
        <networklayer>OLE DB</networklayer>
        <rdms>MS SQL Server 2005</rdms>
        <username>dbAdmin</username>
        <password>P@ssw0rd</password>
        <datasource>r125db</datasource>
        <server>rdbms.org</server>
      </biar-file>
    </add>
  </step>
</biconfig>
```

CA Access Control r12.0 でインストールしたレポート ポータルへのレポート パッケージのデプロイ

標準の CA Access Control レポートを使用するには、BusinessObjects InfoView にレポート パッケージ ファイルをインポートする必要があります。

注: この手順では、CA Access Control r12.0 でインストールした既存の CA Business Intelligence for Windows にレポート パッケージをデプロイする方法について説明します。

CA Access Control r12.0 でインストールしたレポート ポータルにレポート パッケージをデプロイする方法

1. 光ディスク ドライブに CA Access Control Premium Edition r12.5 Server Components for Windows DVD を挿入し、¥ReportPackages ディレクトリに移動します。
2. インストール ファイル用に一時フォルダを作成します。
   - Windows の場合は、C ドライブのルートの下に BO フォルダを作成します。
   - Solaris の場合は、directory /work/bo を作成します。
3. 光ディスクドライブから同じ一時ディレクトリに、以下のファイルをコピーします:
   - /ReportPackages/RDBMS/AC_BIAR_Config.xml
   - /ReportPackages/RDBMS/AC_BIAR_File.biar

   RDBMS

   使用している RDBMS のタイプを定義します。

   例: Oracle

   AC_BIAR_Config.xml

   使用する RDBMS のインポート構成ファイル(.xml)の名前を定義します。

   例: Oracle Database 11g の場合、これは import_biar_config_oracle11g.xml になり、SQL Server 2005 の場合、これは import_biar_config_mssql_2005.xml になります。

   AC_BIAR_File.biar

   使用する言語と RDBMS の CA Access Control レポート ファイル(.biar)の名前を定義します。

   注: 使用する RDBMS のインポート構成ファイルの <biar-file name> プロパティはこのファイルをポイントし、デフォルトで使用する RDBMS の英語バージョンの名前に設定されます。
4. 使用するプラットフォーム用の CA Access Control Premium Edition r12.0 Server Components DVD を光ディスク ドライブに挿入し、/ReportPortal ディレクトリに移動します。

   注: この DVD は r12.0 に付属しているメディアの一部です。

5. 以下のいずれかの操作を行います。
   - Windows の場合、DVD の ¥ReportPortal¥BO ディレクトリ(最大 2 GB)の内容を作成した C:¥BO フォルダにコピーします。
   - Solaris の場合、CA Access Control Premium Edition Server Components DVD にある /ReportPortal/bo_install.tar.gz ファイルのデータを作成した /work/bo フォルダに抽出します。
6. BO_Files/biek-sdk/biekInstall.properties ファイルのコピーを以下のように編集します。

```
BIEK_CONNECT_LAYER=networklayer
BIEK_CONNECT_DB=rdms
BIEK_CONNECT_USER=rdbms_adminUserName
BIEK_CONNECT_PASSWORD=rdbms_adminUserPass
BIEK_CONNECT_SOURCE=rdbms_Datasource
BIEK_CONNECT_SERVER=rdbms_hostName
BIEK_BO_USER=InfoView_adminUserName
BIEK_BO_PASSWORD=InfoView_adminUserPass
BIEK_BIAR_FILE=AC_BIAR_File.biar
```

networklayer

使用する RDBMS でサポートされているネットワーク層を定義します。

制限: 大文字と小文字を区別します。

rdms

使用している RDBMS のタイプを定義します。

制限: 大文字と小文字を区別します。

rdbms_adminUserName

作成済みの RDBMS 管理ユーザのユーザ名を定義します。

rdbms_adminUserPass

作成済みの RDBMS 管理ユーザのパスワードを定義します。

rdbms_Datasource

Oracle データベースの Transparent Network Substrate(TNS)の名前を定義します。

rdbms_hostName

RDBMS サーバのホスト名を定義します。

InfoView_adminUserName

InfoView 管理ユーザのユーザ名を定義します。 デフォルトでは、このユーザは Administrator となります。

InfoView_adminUserPass

InfoView 管理ユーザのパスワードを定義します。 デフォルトでは、このユーザにパスワードは付与されていません（空のままにします）。

AC_BIAR_File.biar

CA Access Control レポート ファイル（.biar）への完全なパス名を定義します。これは以前にコピーしたファイルです。

7. 以下のいずれかの操作を実行します。

   - Windows の場合は、バッチ ファイル BO_Files/biek-sdk/importBiarFile.bat を起動します。
   - UNIX の場合は、BO_Files/biek-sdk/importBiarFile.sh スクリプト ファイルを実行します。

   このファイルにより、CA Access Control レポートが InfoView にインポートされます。終了まで数分かかります。

第 8 章: UNAB ホストのインストールとカスタマイズ

このセクションには、以下のトピックが含まれています。

UNAB ホストのインストールとカスタマイズ

UNIX 認証ブローカ (UNAB) では、Active Directory データ ストアを使用して、UNIX コンピュータにログインできます。 これは、すべてのユーザに対して単一のリポジトリを使用できることを意味します。ユーザは同じユーザ名とパスワードですべてのプラットフォームにログインできます。

UNIX アカウントと Active Directory の統合により、UNIX のユーザおよびグループの基本的なプロパティが Active Directory に転送され、厳密な認証およびパスワードのポリシーが実現されます。 これにより、UNIX のユーザとグループを Windows のユーザとグループを管理しているのと同じ場所で管理できます。

注: インストール時に、UNAB はどの既存の PAM モジュールも置換しません。 UNABPAM は既存の PAM スタックに挿入されます。

はじめに

UNAB をインストールするには、事前に準備要件を満たし、必要な情報をそろえておく必要があります。 UNAB の実装および事前検証の実行を完了するために必要な手順を見直すことをお勧めします。

インストール モード

UNAB では 2 つのインストール モードがサポートされています。

- 完全統合 - 完全統合モードでは、UNIX ホストは、ユーザの認証および権限付与の両方を Active Directory サーバに依存します。
- 部分統合 - 部分統合モードでは、UNIX ホストは、ユーザの認証のみを Active Directory に依存し、権限付与に関しては、UNIX ベースのユーザ ストアを使用します。 部分統合モードは、UNIX ユーザ ストアを保守する場合に使用します。

UNAB の実装方法

UNAB を実装する前に、組織内の UNAB のカスタマイズ、インストール、設定を実行する上で必要な手順を見直すことをお勧めします。

1. UNIX コンピュータ名が正しく解決されたことを確認します (215 ページ)。
2. UNAB インストール パッケージをカスタマイズします。

   注: UNAB のインストール先に予定しているすべての UNIX ホストについて UNAB インストール パッケージをカスタマイズする必要はありません。 インストール パッケージを一度カスタマイズし、それを使用して、UNAB を組織にインストールします。
3. CA Access Control エンタープライズ管理 と連動するように UNAB を設定します (219 ページ)。

   CA Access Control エンタープライズ管理 サーバ ユーザ インターフェースを使用して、UNAB エンドポイントを管理します。
4. UNAB パッケージを UNIX ホストへインストールします。

   注: システム要件およびオペレーティング システム サポートの詳細については、「リリース ノート」をご覧ください。
5. (オプション)システム適合性を確認します (243 ページ)。

   uxpreinstall ユーティリティは、システムが UNAB 要件と互換性があることを確認します (UNAB をインストールしないと、uxpreinstall ユーティリティを実行できません)。
6. Active Directory に UNIX ホストを登録します (244 ページ)。

7. UNAB を開始します(244 ページ)。

   これによって、UNAB デーモン(uxauthd)が開始されます。

8. CA Access Control エンタープライズ管理 でログイン許可ポリシーを作成し、ポリシーを UNAB エンドポイントへ割り当てます。

   ログイン ポリシーによって、UNIX ホストへのアクセスを許可または拒否されるエンタープライズ ユーザを定義します。

   注: ログイン ポリシーの詳細については、「エンタープライズ管理ガイド」を参照してください。

9. UNIX ホスト上の UNAB をアクティブにします(245 ページ)。

   UNAB をアクティブにすると、エンタープライズ ユーザが UNIX ホストにログインします。

10. (オプション) ユーザおよびグループを Active Directory へ移行します(249 ページ)。

    この移行プロセスでは、UNIX ユーザおよびグループの属性を Active Directory へコピーし、ユーザが 1 つの場所からホストへのアクセスを管理できるようにします。

UNIX コンピュータの名前解決の確認

UNAB が機能するには、UNIX コンピュータおよび Active Directory コンピュータの両方が、UNIX コンピュータの IP アドレスを、ドメイン名を含む同じコンピュータ名に名前解決できる必要があります。

UNIX コンピュータ名が正しく解決されることを確認するには、UNIX コンピュータおよび Active Directory コンピュータの両方から UNIX コンピュータの IP アドレスを指定して nslookup コマンドを実行します。

例: UNIX コンピュータ名が正しく解決されることを確認する

この例では、Windows の Active Directory コンピュータおよび UNIX コンピュータの両方で、computer.com という名前のコンピュータに対して nslookup コマンドを実行した結果を示します。

```
Server:       computer.com
Address:      123.456.789.1
123.456.789.1.in-addr.arpa    name = computername.com
```

RPM Package Manager のインストール

RPM Package Manager（RPM）は、個々のソフトウェア パッケージを作成、インストール、クエリ、確認、更新、および消去することができるコマンドライン ユーティリティです。RPM は、UNIX プラットフォームで使用するためのものです。

注: 詳細については、RPM Package Manager の Web サイト（http://www.rpm.org）および RPM に関する UNIX のマニュアル ページを参照してください。

CA Access Control に用意されている RPM パッケージを使用して、インストールした UNAB を、RPM を使用してインストールされたその他すべてのソフトウェアと同様に管理できます。

UNAB パッケージのカスタマイズ

UNAB をインストールするには、RPM パッケージををカスタマイズして、使用許諾契約への同意を示す必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の説明に従って、customize_uxauth_rpm スクリプトを使用してください。 カスタム UNAB RPM インストール パッケージを作成するには、ご使用のコンピュータで rpmbuild ユーティリティが使用可能である必要があります。

UNAB パッケージのカスタマイズ

1. カスタマイズするパッケージを、CA Access Control Endpoint Components for UNIX DVD の /UNAB ディレクトリからファイル システムの一時的な保存場所にコピーします。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

2. （オプション）以下のコマンドを入力して、インストール パラメータ ファイルの言語を設定します。

   ```
   customize_uxauth_rpm -r -l lang [-d pkg_location] pkg_filename
   ```

3. 以下のコマンドを入力して、使用許諾契約を表示します。

   ```
   customize_uxauth_rpm -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 以下のコマンドを入力して、使用許諾契約への同意を示します。

   ```
   customize_uxauth_rpm -w keyword [-d pkg_location] [pkg_name]
   ```

6. (オプション) 以下のコマンドを入力して、インストール ディレクトリを変更します。

   ```
   customize_uxauth_rpm -i install_loc [-d pkg_location] [pkg_name]
   ```

7. (オプション) 以下のコマンドを入力して、デフォルトの暗号化ファイルを変更します。

   ```
   customize_uxauth_rpm -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

8. 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

   ```
   customize_uxauth_rpm -g -f tmp_params [-d pkg_location] pkg_filename
   ```

9. インストール要件に合わせて、インストール パラメータ ファイルを編集します (219 ページ)。

   このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

10. 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

    ```
    customize_uxauth_rpm -s -f tmp_params [-d pkg_location] pkg_filename
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

customize_uxauth_rpm コマンド - CustomizeUNABRPM パッケージ

customize_eac_rpm コマンドは、 UNAB RPM パッケージのカスタマイズ スクリプトを実行します。

注: パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_rpm -h [-l]
customize_uxauth_rpm -a [-d pkg_location] pkg_filename
customize_uxauth_rpm -w command [-d pkg_location] pkg_filename
customize_uxauth_rpm -r [-d pkg_location] [-l lang] pkg_filename
customize_uxauth_rpm -i install_loc [-d pkg_location] [pkg_name]
customize_uxauth_rpm -s [-f tmp_params] [-d pkg_location] pkg_filename
customize_uxauth_rpm -g [-f tmp_params] [-d pkg_location] pkg_filename
customize_uxauth_rpm -t tmp_dir [-d pkg_location] pkg_filename
```

pkg_filename

カスタマイズする UNAB パッケージのファイル名を定義します。

注: -d オプションを指定しない場合は、パッケージ ファイルの完全パス名を定義する必要があります。

-a

使用許諾契約を表示します。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはパッケージ ファイルへの完全パス名が pkg_filename であるとみなします。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションを使用した場合のみ可能です。

注: 指定可能なサポート対象言語の一覧については、customize_eac_rpm -l -h を実行してください。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作用の一時ディレクトリを設定します。

UNAB インストール パラメータ ファイル - UNAB インストールのカスタマイズ

UNAB パラメータ ファイルには、必要に応じてカスタマイズできるインストール パラメータが含まれています。

このファイルの形式は以下のとおりです。

AUDIT_BK

監査ファイルのタイムスタンプ付きバックアップを保存するかどうかを指定します。

注: 監査データを配布サーバに送る場合は、この値を「yes」に設定します。 この値を「yes」に設定した場合、CA Access Control は、監査ファイルが audit_size 設定で指定したサイズ制限に達すると、そのファイルをバックアップし、タイムスタンプを付けます。 これによって、すべての監査データがレポート エージェントで使用可能になります。

制限: yes、no

デフォルト: no

UXACT_CONTAINER

UNIX コンピュータが登録される、Active Directory 内のコンテナ名を定義します。

デフォルト: COMPUTERS

DISTRIBUTION_SRV_HOST

配布サーバのホスト名を指定します。

制限：任意の有効なホスト名

デフォルト：none

DISTRIBUTION_SRV_PROTOCOL

配布サーバの通信プロトコルを指定します。

制限：tcp、ssl

デフォルト：ssl

DISTRIBUTION_SRV_PORT

配布サーバのポート番号を指定します。

オプション：ssl: 7243、tcp: 7222

デフォルト：7243

DISTRIBUTION_SHARED_SECRET

レポート エージェントが配布サーバへの認証に使用する、共有秘密鍵を指定します。

制限：任意の有効な文字列

デフォルト：none

注：配布サーバをインストールした際と同じ共有秘密鍵を指定する必要があります。

DISTRIBUTION_SRV_QNAME

スナップショットの送信先のキューの名前を指定します。

制限：キュー名を表す文字列。

デフォルト：queue/snapshots

DISTRIBUTION_SRV_SCHEDULE

レポート エージェントがレポートを生成し、配布サーバに送信する時間を定義します。

このトークンは次の形式を使用します：時間@曜日[,曜日 2][...]

デフォルト：00:00@Sun,Mon,Tue,Wed,Thu,Fri,Sat

ENABLE_ELM

レポート エージェントが配布サーバにエンドポイント監査データを送信するかどうかを指定します。 これによって、ユーザは CA Enterprise Log Manager と統合されます。

注: この値を「yes」に設定する場合、監査のバックアップを保存する (AUDIT_BK=yes)ように、CA Access Control を設定してください。

制限: yes、no

デフォルト: no

GROUP_CONTAINER

UNIX グループの定義を含む Active Directory コンテナのコンテナ名を定義します。

INTEGRATION MODE

UNAB の統合モードを指定します。

制限: 1 - 部分統合、2 - 完全統合

NTP_SRV

(NTP)サーバの名前または IP アドレスを定義します。

デフォルト: none

TIME_SYNCH

UNAB がシステム時間を NTP (Network Time Protoco)サーバと同期するかどうかを指定します。

注: この値を「yes」に設定すると、NTP_SRV トークンの値を指定する必要があります。 この値を「no」に設定すると、UNAB は、/etc/ntp.conf で定義されたシステム時間に対して、UNIX メカニズムを使用します。

制限: yes、no

デフォルト: no

USER CONTAINER

UNIX ユーザの定義を含む Active Directory コンテナのコンテナ名を定義します。

UXACT_RUN

インストール中に uxconsole -register コマンドを実行するかどうかを指定します。

制限: yes、no

デフォルト: no

注: uxconsole -register コマンドは、Active Directory サーバの Computers コンテナに UNIX コンピュータを登録します。

UXACT_ADMINISTRATOR

Active Directory の管理者のユーザ名を定義します。

UXACT_ADMIN_PASSWORD

Active Directory の管理者のアカウント パスワードを定義します。

UXACT_DOMAIN

UNIX コンピュータが所属するドメインを定義します。

UXACT_RUN_AGENT

インストール プロセスの終了時に UNAB デーモンを起動するかどうかを指定します。

制限: yes、no

デフォルト: yes

UXACT_SERVER

Active Directory サーバの名前を定義します。

UXACT_PORT

Active Directory のリスニング ポートを定義します。

デフォルト: 389

UXACT_VERB_LEVEL

詳細レベルを定義します。

制限: 0 ～ 7

デフォルト: 3

UNAB のインストール

Active Directory ユーザ アカウントを使用して、UNIX コンピュータにログインするには、アクセスする各 UNIX コンピュータに UNAB をインストールする必要があります。

UNAB をインストールする方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. インストール CD 上で UNAB のインストール プログラムがある場所を見つけます。

   以下に例を示します。

   ```
   mnt/UNIX/auth_DVD/CDPATH/uxauth-1-0.10.i386.rpm
   ```
3. rpm コマンドを使用して、UNAB パッケージをインストールします。

   インストール プロセスが開始されます。

   インストール プロセスが正常に完了したことを通知するメッセージが表示されます。
4. インストール ログ ファイル(uxauth-rpm.log)を参照して、インストール プロセスに関する情報を確認します。

   ログ ファイルは、UNAB のインストール ディレクトリに格納されています。

   デフォルトでは、UNAB は以下の場所にインストールされます。

   ```
   /opt/CA/uxauth/
   ```

例: Red Hat Linux 上に UNAB をインストールする

以下の例では、UNAB パッケージを Red Hat Linux x86 ES 4.0 コンピュータにインストールする方法を示します。

この例では、インストール パッケージは、インストール メディア上にあります(/mnt/UNIX/auth_DVD にマウントされています)。

```
cd /mnt/UNIX/auth_DVD/CDPATH
rpm -i uxauth-1-0.10.i386.rpm
```

インストールが正常に完了したことの確認

UNAB のインストールの完了後、インストールが正常に完了したことを確認する必要があります。

インストールが正常に完了したことを確認するには、uxauth コマンドを入力します。

uxauth

UNAB ネイティブ パッケージの名前を定義します。

UNAB が正常にインストールされた場合、このパッケージがインストールされていることを通知するメッセージが表示されます。

UNAB のアンインストール

UNAB をアンインストールする場合、インストールした UNIX コンピュータからパッケージを削除する必要があります。

UNAB をアンインストールするには、スーパーユーザとして以下のコマンドを入力します。

```
rpm -e uxauth
```

uxauth

UNAB ネイティブ パッケージの名前を定義します。

アンインストール プロセスが開始されます。

プロセスが正常に完了したことを通知するメッセージが表示されます。

Solaris ネイティブ パッケージングのインストール（UNAB）

Solaris のネイティブ パッケージングは、コマンドライン ユーティリティとして提供されます。このため、各パッケージを個別に作成、インストール、削除、およびレポートすることができます。

注: Solaris ネイティブ パッケージングの詳細については、Sun Microsystems の Web サイトならびに pkgadd、pkgrm、pkginfo、および pkgchk に関するマニュアル ページを参照してください。

通常のインストールの代わりに、UNAB に用意されている Solaris ネイティブ パッケージを使用することができます。 このため、インストールした UNAB を、Solaris ネイティブ パッケージングを使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、UNAB をアンインストールするには、pkgrm コマンドを使用する必要があります。

Solaris ネイティブ パッケージのカスタマイズ

Solaris ネイティブ パッケージングを使用して、UNAB をインストールできる前に、インストール パッケージをカスタマイズして、使用許諾契約への同意を指定します。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

注: 以下の手順に従って、UNAB パッケージをカスタマイズします。 パッケージを手動で変更することはお勧めしません。 代わりに、以下の説明に従って、customize_uxauth_pkg スクリプトを使用してください。

Solaris ネイティブ パッケージのカスタマイズ方法

1. カスタマイズするパッケージを、CA Access Control Endpoint Components for UNIX DVD の /UNAB ディレクトリからファイル システムの一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

   重要: パッケージを抽出する際には、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうしないと、Solaris ネイティブ パッケージング ツールはそのパッケージを破損したものとみなします。

2. （オプション）customize_uxauth_pkg スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   英語以外のスクリプト メッセージを使用する場合は、pre.tar ファイルをそのスクリプト ファイルと同じディレクトリに配置します。 pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび UNAB のエンド ユーザ使用許諾契約が含まれています。

   注: customize_uxauth_pkg スクリプト ファイルと pre.tar ファイルは、ネイティブ パッケージの抽出先と同じ場所に格納されています。

3. （オプション）以下のコマンドを入力して、インストール パラメータ ファイルの言語を設定します。

   ```
   customize_uxauth_pkg -r -l lang [-d pkg_location] [pkg_name]
   ```

4. Enter the following command to display the license agreement:

   ```
   customize_uxauth_pkg -a [-d pkg_location] pkg_name
   ```

5. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

6. 以下のコマンドを入力して、使用許諾契約への同意を示します。

   ```
   customize_uxauth_pkg -w keyword [-d pkg_location] [pkg_name]
   ```

7. （オプション）以下のコマンドを入力して、インストール ディレクトリを変更します。

   ```
   customize_uxauth_pkg -i install_loc [-d pkg_location] [pkg_name]
   ```

8. （オプション）以下のコマンドを入力して、デフォルトの暗号化ファイルを変更します。

   ```
   customize_uxauth_pkg -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

   ```
   customize_uxauth_pkg -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. インストール要件に合わせて、インストール パラメータ ファイルを編集します。(219 ページ)

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

    ```
    customize_uxauth_pkg -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

customize_uxauth_pkg コマンド - Solaris ネイティブ パッケージのカスタマイズ

customize_uxauth_pkg コマンドは、UNAB Solaris ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な UNAB Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_pkg -h [-l]
customize_uxauth_pkg -a [-d pkg_location] [pkg_name]
customize_uxauth_pkg -w command [-d pkg_location] [pkg_name]
customize_uxauth_pkg -r [-d pkg_location] [-l lang] [pkg_name]
customize_uxauth_pkg -l install_loc [-d pkg_location] [pkg_name]
customize_uxauth_pkg -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_uxauth_pkg -g [-f tmp_params] [-d pkg_location] [pkg_name]
customize_uxauth_pkg -t tmp_dir [-d pkg_location] [pkg_name]
```

pkg_name

（オプション）カスタマイズする UNAB パッケージの名前です。 パッケージを指定しない場合、スクリプトはデフォルトでメインの UNAB パッケージ（uxauth）を選択します。

-a

使用許諾契約を表示します。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります（角かっこ [ ]内）。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

d pkg_location

（オプション）ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注： -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力（stdout）に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-t tmp_dir

インストール操作用の一時ディレクトリを設定します。

UNAB Solaris ネイティブ パッケージのインストール

UNAB Solaris のネイティブ パッケージを使用すると、Solaris 上で UNAB を簡単にインストールできます。

注: 以下の手順では、UNAB がデフォルトの設定でインストールされます。 インストールする前に、CA Access Control パッケージをカスタマイズすることもできます。

UNAB Solaris ネイティブ パッケージのインストール方法

1. （オプション）Solaris ネイティブ インストール時のデフォルトを設定します。

   a. インストール管理ファイルを現在の場所にコピーします。

      ```
      convert_eac_pkg -p
      ```

      インストール管理ファイルを現在の場所に myadmin という名前でコピーします。

      インストール管理ファイルを編集して、pkgadd のインストール時のデフォルトを変更できます。 pkgadd -a オプションを使用すれば、UNAB など、特定のインストール用に変更されたファイルを使用できます。 ただし、このファイルは UNAB に固有のものではありません。

   b. インストール管理ファイル（myadmin）を必要に応じて編集し、そのファイルを保存します。

      これで、他のインストールに影響を及ぼすことなく、変更したインストール設定を CA Access Control ネイティブ インストールのために使用できます。

   注: Solaris ネイティブ パッケージングでは、デフォルトで、ユーザによる操作を必要とする場合があります。 インストール管理ファイルおよびこのファイルの使い方の詳細については、pkgadd（1M） および admin（4） に関する Solaris のマニュアルページを参照してください。

2. 以下のようにパッケージをインストールします。

   ```
   pkgadd [-a dir/myadmin] -d pkg_location uxauth
   ```

   -a dir/myadmin

      手順 1 で作成した myadmin インストール管理ファイルの場所を定義します。

      このオプションを指定しない場合、pkgadd ではデフォルトのインストール管理ファイルが使用されます。

   pkg_location

      UNAB パッケージ（uxauth）が格納されているディレクトリを定義します。

      重要: パッケージは、公開場所（つまり、グループおよび全員に対する読み取りアクセス権が設定された場所）に配置する必要があります。 たとえば、/var/spool/pkg です。

注: Solaris ネイティブ パッケージは、CA Access Control Endpoint Components for UNIX DVD の NativePackages ディレクトリにあります。

これで、UNAB のインストールは完了しましたが、まだ起動されていません。

選択したゾーンへの UNAB Solaris ネイティブ パッケージのインストール

Solaris のネイティブ パッケージングを使用し、選択したゾーンに UNAB をインストールすることができます。 ただし、UNAB をグローバル ゾーンにもインストールする必要があります。

注: Solaris ネイティブ パッケージを使用して、UNAB をすべてのゾーンにインストールすることをお勧めします。

選択したゾーンに UNAB をインストールする方法

重要: すべてのゾーンで必ず同じ UNAB バージョンを使用するようにしてください。

1. グローバル ゾーンから以下のコマンドを実行して、CA Access Control をインストールします。

   ```
   pkgadd -G -d pkg_location uxauth
   ```

   pkg_location

   UNAB パッケージ（uxauth）が格納されているディレクトリを定義します。

   重要: パッケージは、公開場所（つまり、グループおよび全員に対する読み取りアクセス権が設定された場所）に配置する必要があります。 たとえば、/var/spool/pkg です。

   このコマンドによって、UNAB がグローバル ゾーンにのみインストールされます。

2. グローバル ゾーン内で SEOS_load コマンドを入力して、UNAB カーネル モジュールをロードします。

   注: UNAB カーネルはロードされますが、UNAB はグローバル ゾーン内のイベントをインターセプトしません。

3. UNAB をインストールするそれぞれの非グローバル ゾーンで以下の操作を行います。

   a. 非グローバル ゾーンの一時的な保存場所に uxauth パッケージをコピーします。

b. 非グローバル ゾーンから以下のコマンドを発行します。

```
pkgadd -G -d pkg_location uxauth
```

このコマンドは、作業元である非グローバル ゾーンに UNAB をインストールします（前の手順でコピーしたパッケージを使用）。

これで、内部ゾーンで UNAB を開始できるようになります。

注: UNAB をグローバル ゾーンから削除する前に、すべての非グローバル ゾーンからアンインストールする必要があります。

HP-UX ネイティブ パッケージのインストール

HP-UX のネイティブ パッケージは、GUI とコマンドライン ユーティリティのセットとして提供されます。これにより、個々のソフトウェア パッケージの作成、インストール、削除、およびレポート作成を行うことができます。 HP-UX ネイティブ パッケージでは、リモート コンピュータにソフトウェア パッケージをインストールすることもできます。

注: HP-UX のネイティブ パッケージである、Software Distributor-UX（SD-UX）の詳細については、HP の Web サイト（http://www.hp.com）を参照してください。 swreg、swinstall、swpackage、および swverify については、man ページも参照できます。

通常のインストールの代わりに、UNAB に用意されている SD-UX ネイティブ パッケージを使用することができます。 これにより、インストールした UNAB を、SD-UX を使用してインストールされた他のソフトウェアと同様に管理できます。

重要: パッケージのインストール後、UNAB をアンインストールするには、swremove コマンドを使用する必要があります。

UNAB SD-UX 形式パッケージのカスタマイズ

ネイティブ パッケージを使用して UNAB をインストールする前に、UNAB パッケージをカスタマイズして、使用許諾契約への同意を示す必要があります。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、UNAB パッケージをカスタマイズしてください。

サポート対象の各 HP-UX オペレーティング システムに対する Software Distributor-UX（SD-UX）形式パッケージは、CA Access Control Endpoint Components for UNIX DVD の UNAB ディレクトリに格納されています。

SD-UX 形式パッケージのカスタマイズ

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージを必要に応じてカスタマイズできます。

   重要: パッケージを展開するときは、パッケージのディレクトリ構造全体のファイル属性が保持されていることを確認する必要があります。そうでないと、HP-UX ネイティブ パッケージング ツールによってパッケージが破損していると見なされます。

2. customize_uxauth_depot スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび UNAB のエンド ユーザ使用許諾契約が含まれています。

   注: customize_unab_depot スクリプト ファイルおよび pre.tar ファイルは以下のディレクトリにあります。

   ```
   /uxauth/FILESET/opt/CA/uxauth/lbin
   ```

3. 以下のコマンドを入力して、使用許諾契約を表示します。

   ```
   customize_uxauth_depot -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 以下のコマンドを入力して、使用許諾契約への同意を示します。

   ```
   customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
   ```

6. (オプション) 以下のコマンドを入力して、インストール パラメータ ファイルの言語を設定します。

   ```
   customize_uxauth_depot -r -l lang [-d pkg_location] [pkg_name]
   ```

7. (オプション) 以下のコマンドを入力して、インストール ディレクトリを変更します。

   ```
   customize_uxauth_depot -i install_loc [-d pkg_location] [pkg_name]
   ```

8. (オプション) 以下のコマンドを入力して、デフォルトの暗号化ファイルを変更します。

   ```
   customize_uxauth_depot -s -c certfile -k keyfile [-d pkg_location] [pkg_name]
   ```

9. (オプション) 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

   ```
   customize_uxauth_depot -g -f tmp_params [-d pkg_location] [pkg_name]
   ```

10. (オプション) インストール要件に合わせて、インストール パラメータ ファイルを編集します (219 ページ)。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. (オプション) 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

    ```
    customize_uxauth_depot -s -f tmp_params [-d pkg_location] [pkg_name]
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

例: 使用許諾契約への同意を指定する

ネイティブ パッケージのインストール時に使用許諾契約に同意するには、パッケージをカスタマイズします。 以下の例は、パッケージ ファイルの抽出先のディレクトリ上にある x86 UNAB SD-UX パッケージをカスタマイズして、使用許諾契約への同意を示す方法を説明しています。

```
cp /mnt/AC_DVD/UNAB/_HPUX11_Ux_PKG_1*.tar.Z /tmp
cd /tmp
zcat _HPUX11_Ux_PKG_1*.tar.Z | tar -xvf -
/uxauth/FILESET/opt/CA/uxauth/lbin/customize_eac_depot -w keyword -d /tmp uxauth
```

これで、/tmp ディレクトリにあるカスタマイズされたパッケージを使用して、UNAB をインストールできるようになりました。

詳細情報:

customize_eac_depot コマンド - SD-UX 形式パッケージのカスタマイズ (136 ページ)

customize_uxauth_depot コマンド - SD-UX 形式パッケージのカスタマイズ

customize_uxauth_depot コマンドは、SD-UX 形式パッケージ用の UNAB ネイティブ パッケージのカスタマイズ スクリプトを実行します。

このコマンドを使用する場合は、以下の点を考慮する必要があります。

- このスクリプトは、利用可能な UNAB Solaris ネイティブ パッケージのいずれでも機能します。
- パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。
- ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_depot -h [-l]
customize_uxauth_depot -a [-d pkg_location] [pkg_name]
customize_uxauth_depot -w keyword [-d pkg_location] [pkg_name]
customize_uxauth_depot -r [-l lang] [-d pkg_location] [pkg_name]
customize_uxauth_depot -l install_loc [-d pkg_location] [pkg_name]
customize_uxauth_depot -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
[pkg_name]
customize_uxauth_depot -g [-f tmp_params] [-d pkg_location] [pkg_name]
```

pkg_name

(オプション)カスタマイズする UNAB パッケージの名前です。 パッケージを指定しない場合、スクリプトはデフォルトでメインの UNAB パッケージ (uxauth)を選択します。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、uxauth パッケージにのみ利用できます

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、uxauth パッケージにのみ利用できます

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

UNAB HP-UX ネイティブ パッケージのインストール

インストールした UNAB を、インストールされたほかのソフトウェアと同様に管理するには、カスタマイズされた UNAB SD-UX 形式パッケージをインストールします。 UNAB SD-UX 形式パッケージを使用すると、HP-UX に UNAB を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。

UNAB HP-UX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

   HP-UX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. UNAB パッケージをカスタマイズします(231 ページ)。

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. 以下のコマンドを使用して、カスタマイズされたパッケージを SD-UX に登録します。

   ```
   swreg -l depot pkg_location
   ```

   pkg_location

   UNAB パッケージが格納されるディレクトリを定義します。

4. 以下のコマンドを使用して、UNAB パッケージをインストールします。

   ```
   swinstall -s pkg_location uxauth
   ```

   SD-UX は、pkg_location ディレクトリから、パッケージのインストールを開始します。

   これで、UNAB のインストールは完了しましたが、まだ起動されていません。

詳細情報:

SD-UX 形式パッケージのカスタマイズ(133 ページ)
ネイティブ インストールの際に考慮するその他の事項(113 ページ)

HP-UX パッケージのアンインストール

インストールされている UNAB HP-UX パッケージをアンインストールするには、インストール時とは逆の手順で、UNAB パッケージをアンインストールする必要があります。

CA Access Control パッケージをアンインストールするには、メインの UNAB パッケージをアンインストールします。

```
swremove uxauth
```

AIX ネイティブ パッケージのインストール

AIX ネイティブ パッケージは、GUI およびコマンドライン ユーティリティのセットとして提供されます。これを使用して、個別のソフトウェア パッケージを管理できます。

通常のインストールの代わりに、UNAB に用意されている AIX ネイティブ パッケージを使用することができます。 これにより、インストールした UNAB を、AIX installp を使用してインストールされた他のソフトウェアと同様に管理できます。

注: 一部の AIX バージョンはいくつかのパッケージ形式(installp、SysV、RPM)をサポートしていますが、UNAB では AIX のネイティブ パッケージ形式(installp)のみが提供されます。

重要: パッケージのインストール後、UNAB をアンインストールするには、installp コマンドを使用する必要があります。

bff ネイティブ パッケージ ファイルのカスタマイズ

ネイティブ パッケージを使用して UNAB をインストールする前に、UNAB パッケージをカスタマイズして、使用許諾契約への同意を示します。 また、パッケージをカスタマイズする際に、カスタム インストール設定を指定することもできます。

注: パッケージを手動で変更することはお勧めしません。 代わりに、以下の手順に記載されているスクリプトを使用して、UNAB パッケージをカスタマイズしてください。

サポート対象の各 AIX オペレーティング システムに対する installp 形式ネイティブ パッケージ(bff ファイル)は、CA Access Control Endpoint Components for UNIX DVD の UNAB ディレクトリにあります。

bff ネイティブ パッケージ ファイルのカスタマイズ方法

1. カスタマイズするパッケージを、ファイル システム上の一時的な保存場所に展開します。

   ファイル システムの読み取り/書き込み可能な領域で、パッケージ(bff ファイル)を必要に応じてカスタマイズできます。

   重要: この領域のディスク容量は、再パッケージングの一時的なファイルを格納できるように、少なくともパッケージの 2 倍のサイズである必要があります。

2. customize_uxauth_bff スクリプト ファイルおよび pre.tar ファイルをファイル システム上の一時的な保存場所にコピーします。

   pre.tar ファイルは、圧縮された tar ファイルであり、インストール メッセージおよび UNAB のエンド ユーザ使用許諾契約が含まれています。

   注: customize_uxauth_bff スクリプト ファイルおよび pre.tar ファイルは、ネイティブ パッケージと同じ場所に格納されています。

3. 以下のコマンドを入力して、使用許諾契約を表示します。

   ```
   customize_uxauth_bff -a [-d pkg_location] pkg_name
   ```

4. 使用許諾契約の最後に表示される角かっこ内部のキーワードをメモします。

   次の手順でこのキーワードを指定します。

5. 以下のコマンドを入力して、使用許諾契約への同意を示します。

   ```
   customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
   ```

6. (オプション)以下のコマンドを入力して、インストール パラメータ ファイルの言語を設定します。

   ```
   customize_uxauth_bff -r -l lang [-d pkg_location] pkg_name
   ```

7. (オプション)以下のコマンドを入力して、インストール ディレクトリを変更します。

   ```
   customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
   ```

8. (オプション) 以下のコマンドを入力して、デフォルトの暗号化ファイルを変更します。

   ```
   customize_uxauth_bff -s -c certfile -k keyfile [-d pkg_location] pkg_name
   ```

9. 以下のコマンドを入力して、インストール パラメータ ファイルを取得します。

   ```
   customize_uxauth_bff -g -f tmp_params [-d pkg_location] pkg_name
   ```

10. (オプション) インストール要件に合わせて、インストール パラメータ ファイルを編集します (219 ページ)。

    このファイルによって、パッケージのインストール時のデフォルト設定を行うことができます。

11. (オプション) 以下のコマンドを入力して、カスタマイズされたパッケージのインストール パラメータを設定します。

    ```
    customize_uxauth_bff -s -f tmp_params [-d pkg_location] pkg_name
    ```

    これで、パッケージを使用して、カスタマイズされたデフォルト設定で UNAB をインストールできるようになりました。

customize_eac_bff コマンド - bff ネイティブ パッケージ ファイルのカスタマイズ

customize_uxauth_bff コマンドによって、bff ネイティブ パッケージ ファイル用の、<uxauth> ネイティブ パッケージ カスタマイズ スクリプトが実行されます。

このスクリプトは、AIX で使用可能な <uxauth> ネイティブ パッケージのいずれでも機能します。 パッケージをカスタマイズするには、パッケージがファイル システム上の読み取り/書き込み可能なディレクトリにある必要があります。

重要: パッケージの抽出場所には、再パッケージの中間ファイルを保存するために、少なくともパッケージの 2 倍のサイズが必要です。

注: ローカライズされたスクリプト メッセージを使用するには、pre.tar ファイルをスクリプト ファイルと同じディレクトリに置く必要があります。

このコマンドの形式は以下のようになります。

```
customize_uxauth_bff -h [-l]
customize_uxauth_bff -a [-d pkg_location] pkg_name
customize_uxauth_bff -w keyword [-d pkg_location] pkg_name
customize_uxauth_bff -r [-d pkg_location] [-l lang] pkg_name
customize_uxauth_bff -i install_loc [-d pkg_location] pkg_name
customize_uxauth_bff -s {-f tmp_params | -c certfile | -k keyfile} [-d pkg_location]
pkg_name
customize_uxauth_bff -g [-f tmp_params] [-d pkg_location] pkg_name
```

pkg_name

カスタマイズする UNAB パッケージ(bff ファイル)の名前です。

-a

使用許諾契約を表示します。

-c certfile

ルートの証明書ファイルの完全パス名を定義します。

注: このオプションは、CAeAC パッケージにのみ利用できます。

-d pkg_location

(オプション)ファイル システム上でパッケージを配置するディレクトリを指定します。パッケージのあるディレクトリを指定しない場合、スクリプトはデフォルトで /var/spool/pkg を指定します。

-f tmp_params

情報の作成および取得元となるインストール パラメータ ファイルの完全パスおよび名前を指定します。

注: -g オプションを使用する場合、ファイルを指定しないと、インストール パラメータは標準出力(stdout)に出力されます。

-g

インストール パラメータ ファイルを取得し、それを -f オプションで指定されたファイルに配置します。

-h

コマンドの使用法を示します。 -l オプションと共に使用されると、サポート対象言語の言語コードを表示します。

-i install_loc

パッケージのインストール ディレクトリを install_loc に設定します。

-k keyfile

ルートの秘密鍵ファイルの完全パス名を定義します。

注: このオプションは、uxauth パッケージにのみ利用できます

-l lang

インストール パラメータ ファイルの言語を lang に設定します。 言語の設定は、-r オプションと組み合わせたときのみ可能です。

注: サポートされている、指定可能な言語コードを一覧表示するには、-h オプションと組み合わせて実行します。 デフォルトでは、インストール パラメータ ファイルは英語で記述されています。

-r

パッケージをリセットして、元のパッケージと同様にデフォルト値を使用するようにします。

-s

指定されたパッケージを設定して、-f オプションで指定された、カスタマイズされたインストール パラメータ ファイルからの入力を使用するようにします。

-w キーワード

エンド ユーザ使用許諾契約にユーザが同意していることを指定するキーワードを定義します。 このキーワードは、ユーザ使用許諾契約の最後にあります(角かっこ[ ]内)。 使用許諾契約ファイルを検索するには、-a オプションを使用します。

UNAB AIX ネイティブ パッケージのインストール

インストールした UNAB を、インストールされたほかのソフトウェアと同様に管理するには、UNAB AIX ネイティブ パッケージをカスタマイズしてインストールします。 UNAB AIX のネイティブ パッケージ(bff ファイル)を使用すると、AIX に UNAB を簡単にインストールできます。

重要: 使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 CA Access Control エンタープライズ管理 を使用して UNAB エンドポイントを管理する場合は、UNAB をインストールする前に、UNAB エンドポイントを CA Access Control エンタープライズ管理に登録する必要があります。

UNAB AIX ネイティブ パッケージのインストール方法

1. root ユーザとしてログインします。

   AIX ネイティブ パッケージを登録し、インストールするには、root アカウントに関連した権限が必要です。

2. UNAB パッケージをカスタマイズします(237 ページ)。

   使用許諾契約に記載されているキーワードを使用して、使用許諾契約への同意を示すには、パッケージをカスタマイズする必要があります。 また、パッケージをカスタマイズしてカスタム インストールを指定することも可能です。

3. (オプション)インストールするパッケージのレベル(バージョン)を記録します。

   ```
   installp -l -d pkg_location
   ```

   pkg_location

   UNAB パッケージ(uxauth)が格納されているディレクトリを定義します。

   pkg_location 内の各パッケージについて、AIX ではパッケージ レベルの一覧が作成されます。

   注: AIX ネイティブ パッケージのインストール オプションの詳細については、installp の man ページを参照してください。

4. 以下のコマンドを使用して、UNAB パッケージをインストールします。

   ```
   installp -ac -d pkg_location uxauth[pkg_level]
   ```

   pkg_level

   前に記録したパッケージのレベル番号を定義します。

   AIX は、pkg_location ディレクトリから、 UNAB パッケージのインストールを開始します。

   これで、UNAB のインストールは完了しましたが、まだ起動されていません。

詳細情報:

ネイティブ インストールの際に考慮するその他の事項(113 ページ)

AIX パッケージのアンインストール

インストールされている UNAB AIX パッケージをアンインストールするには、インストール時とは逆の手順で、UNAB パッケージをアンインストールする必要があります。

UNAB パッケージをアンインストールするには、メインの UNAB パッケージをアンインストールします。

```
installp -u uxauth
```

CA Access Control エンタープライズ管理 を使用した UNAB の管理

CA Access Control エンタープライズ管理 を使用して、UNAB エンドポイントを管理できます。 ここでは、ワールドビューからの UNAB エンドポイントの表示、ログイン ポリシーおよび設定ポリシーの作成および割り当て、また移行処理中に検出された競合の解決が可能です。 CA Access Control エンタープライズ管理 で UNAB エンドポイントを管理できるように、CA Access Control エンタープライズ管理 に UNAB を登録します。 UNAB インストール パッケージをカスタマイズして、パッケージ パラメータを変更します。

注: この手順を完了してから、UNAB をインストールします。

CA Access Control エンタープライズ管理 を使用した UNAB の管理

1. UNAB パッケージからインストール パラメータを抽出して、一時ファイルに保存します。
2. テキストエディタで一時ファイルを開きます。
3. ユーザの組織に合わせて、以下のパラメータを変更します。

   DISTRIBUTION_SRV_HOST

   配布サーバのホスト名を指定します。

   制限: 任意の有効なホスト名

   デフォルト: none

   DISTRIBUTION_SRV_PROTOCOL

   配布サーバの通信プロトコルを指定します。

   制限: tcp、ssl

   デフォルト: ssl

   DISTRIBUTION_SRV_PORT

   配布サーバのポート番号を指定します。

   制限: ssl: 7243、tcp: 7222

   デフォルト: 7243

   DISTRIBUTION_SHARED_SECRET

   ReportAgent が認証のために配布サーバで使用する、共有秘密キーを指定します。

   制限: 任意の有効な文字列

   デフォルト: none

4. カスタマイズしたパッケージにインストール パラメータを設定します。
5. カスタマイズしたパッケージを使用して、UNAB をインストールします。

   インストールの完了後、CA Access Control エンタープライズ管理 を使用して UNAB エンドポイントを管理します。

システム適合性の確認

UNAB をインストールした後に、uxpreinstall ユーティリティを実行して、インストール先のオペレーティング システムおよび追加のシステム要件が所定の要件に準拠していることを検証します。

重要: uxpreinstall ユーティリティは実在する問題または潜在的な問題を報告しますが、その修正は行いません。 このユーティリティを使用して、オペレーティング システムまたは UNAB を設定することはできません。

注: uxpreinstall 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。

システムの適合性を確認するには、スーパーユーザとして UNIX コンピュータにログインし、uxpreinstall ユーティリティを実行します。

uxpreinstall ユーティリティが実行され、完了すると、プロセスの結果が表示されます。

例: uxpreinstall ユーティリティを実行する

この例では、Active Directory ドメイン domain.com に対して、管理者ユーザのクレデンシャルで、詳細レベル 3 で uxpreinstall ユーティリティを実行します。

```
./uxpreinstall -u administrator -w admin -d domain.com -v 3
```

UNAB の開始

ユーザが Active Directory から UNIX コンピュータへログインするには、UNAB が実行中である必要があります。

UNAB を開始するには、uxauthd デーモンを実行します。

UNAB の開始方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB ディレクトリを見つけます。
3. 以下のコマンドを入力します。

   ```
   ./uxauthd -start
   ```

   UNAB デーモンが開始されます。

   デーモンが実行中であることを通知するメッセージが表示されます。

Active Directory での UNIX ホストの登録

Active Directory に定義されたユーザが UNIX コンピュータにログインできるようにするには、Active Directory サーバに UNAB をインストールした各 UNIX コンピュータを登録する必要があります。

Active Directory では、コンピュータ オブジェクト名に対して NetBIOS に基づいた文字数制限があるため、ドメイン名サフィックスのない UNIX コンピュータのホスト名は 15 文字以下である必要があります。 UNIX コンピュータのホスト名が 15 文字を超える場合は、登録できません。 たとえば、engineering-dept-sol2 という名前の UNIX コンピュータを Active Directory に登録できません。これは、ホスト名が 15 文字を超えるためです。 eng-dept-sol2.example.com という名前の UNIX コンピュータを登録できます。これは、ドメイン名 (eng-dept-sol2) のないホスト名が 15 文字より少ないためです。 UNIX コンピュータのホスト名を表示するには、ホスト名コマンドを実行します。

注: UNAB のインストール中またはインストール後に、各 UNIX コンピュータを Active Directory に 1 回のみ登録する必要があります。

重要: UNIX (SFU) 用の Microsoft Services を使用している場合、uxauth.ini ファイルの[マップ]セクションで属性名を指定しないと、UNAB を登録できません。 uxauth.ini ファイル内で属性名を指定しないと、単に SFU の中で定義されるユーザは UNAB が実行されている UNIX ホストにログインできません。 uxauth.ini ファイルの詳細については、「リファレンス ガイド」を参照してください。

Active Directory での UNIX ホストの登録方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB bin ディレクトリに移動します。 デフォルトのディレクトリは、以下の通りです。

   ```
   /opt/CA/uxauth/bin
   ```

3. 以下のコマンドを実行します。

   ```
   ./uxconsole -register [-a admin] [-w pass] [-d domain] [-v level] [-n] [-o container] [-s server] [port #]
   ```

   注: デフォルトの設定を使用するには、引数を指定せずに uxconsole - register コマンドを実行します。 ユーザは必要な追加情報を入力するよう求められます。 uxconsole -register 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。

   UNAB は Active Directory に UNIX コンピュータを登録します。

例: Active Directory での UNIX ホストの登録方法

この例では、UNIX コンピュータを Active Directory に登録する方法を示します。 この例では、管理者は、 -register コマンドを実行して、UNIX コンピュータを Active Directory に登録します。 管理者は、ユーザ名 (-a administrator) およびパスワード (-w admin) を使用して入力し、詳細レベルを設定し (-v 3)、UNAB エージェントがインストールの最後に実行されないように指定し、(-n)Active Directory での、コンテナ名を指定します(-o OU=COMPUTERS)。

```
./uxconsole -register -a administrator -w admin –v 3 -n -o OU=COMPUTERS
```

UNAB のアクティブ化

Active Directory で UNIX ホストを登録した後、UNAB をアクティブにする必要があります。 アクティブ化は、UNAB の実装プロセスの最終ステップです。 一旦 UNAB がアクティブ化されれば、UNAB は Active Directory のパスワードをベースに、ユーザのログインを認証します。

UNAB をアクティブにする方法

1. UNIX コンピュータにスーパーユーザとしてログインします。
2. UNAB bin ディレクトリに移動します。 デフォルトのディレクトリは、以下の通りです。

   ```
   /opt/CA/uxauth/bin
   ```

3. 以下のコマンドを実行します。

   ```
   uxconsole -activate
   ```

   -activate

   Active Directory ユーザのログインがアクティブ化されることを指定します。

   UNAB がアクティブにされます。

注: UNAB をアクティブにすると、Active Directory アカウントを持っているローカル ユーザが、UNIX ホストに継続してログインできるようになります。

例: UNAB のアクティブ化

以下の例は、UNAB のインストールおよび登録後、Active Directory アカウントを使用して、UNIX コンピュータにログインする方法を示しています。

1. ターミナル ウィンドウを開きます。
2. UNIX ホストへの接続

   ```
   telnet computer.com
   ```

   ユーザは UNIX コンピュータに接続され、UNIX シェルが開きます。
3. Active Directory アカウントのユーザ名およびパスワードを入力します。

   ログインが成功した場合、前回の路銀の詳細を通知するメッセージが表示されます。

ユーザ情報の表示

UNAB は、ユーザ アカウントに関する情報を表示できます。たとえば、アカウント タイプ(ローカルまたはエンタープライズ ユーザ アカウント)、ログイン ステータス(許可または拒否)、ログイン理由などです。 ローカルおよびエンタープライズ アカウントの一覧表示、アカウント情報の詳細の表示を選択できます。

ユーザ情報の表示方法

1. bin ディレクトリに移動します。 デフォルトでは、このディレクトリは以下のパスにあります。

   ```
   /opt/CA/uxauth/bin
   ```
2. 以下のいずれかのコマンドを実行します。

   ```
   uxconsole -manage -find -user <filter>
   ```

   ```
   uxconsole -manage -show -user <filter>
   ```

注: uxconsole 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。

UNIX コンポーネント用の ID 管理のインストール

Active Directory ユーザの UNIX ホストへのログインを管理するには、Active Directory に UNIX コンポーネント用の Windows ID 管理をインストールします。

UNIX コンポーネント用の ID 管理は「UNIX 属性」という名前の新規タブを、Active Directory で定義されている各ユーザ アカウントに追加します。 このタブを使用して、ユーザおよびグループの UNIX パラメータを設定します。

UNIX コンポーネント用の ID 管理のインストール方法

1. 管理者として Active Directory コンピュータにログインします。
2. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   [アプリケーションの追加と削除]ウィンドウが開きます。
3. [Windows コンポーネントの追加と削除]をクリックします。

   Windows コンポーネント ウィザードが表示されます。
4. [Active Directory サービス]オプションを強調し、[詳細]を選択します。

   [Active Directory サービス]ダイアログ ボックスが表示されます。
5. [UNIX 用 ID 管理]チェックボックスを選択し、[詳細]を選択します。

   [UNIX 用 ID 管理]画面が表示されます。
6. 利用可能なオプションをすべて選択し、[OK]を選択します。
7. [次へ]を選択します。

   操作が正常に完了したことを通知するメッセージが表示されます。

Active Directory ユーザの UNIX 属性の設定

UNAB を使用して、Active Directory ユーザ属性を管理するには、Active Directory ユーザ アカウントの[UNIX 属性]タブ内のユーザ設定を設定します。

注: ユーザ アカウント プロパティを定義する場合、このユーザがログオン可能なコンピュータを指定する必要はありません。 これらの設定は、UNIX ホストには適用されません。

Active Directory ユーザの UNIX 属性の設定

1. 管理者として Active Directory コンピュータにログインします。
2. [スタート] - [設定] - [コントロール パネル] - [管理ツール]の順にクリックします。

   [管理ツール]ウィンドウが開きます。

3. [Active Directory ユーザーとコンピュータ]アイコンをダブルクリックします。

   [Active Directory ユーザーとコンピュータ]ウィンドウが開きます。

4. ユーザ アカウントをダブルクリックします。

   ユーザ アカウント プロパティが表示されます。

5. [UNIX 属性]タブをクリックします。

   [UNIX 属性]タブが表示されます。

6. [UNIX 属性]タブの以下のフィールドに値を入力します。

   NIS ドメイン

   ユーザが所属する NIS ドメインの名前を定義します。

   例: unixauth

   UID

   UNIX コンピュータ上のユーザ ID 番号を定義します。

   ホーム ディレクトリ

   UNIX コンピュータ上のユーザのホーム ディレクトリを定義します。

   例: /home/user

   ログイン シェル

   ユーザ アカウントのログイン シェルを定義します。

   例: /bin/sh

   プライマリ グループ名/GID

   ユーザが所属するプライマリ グループ名または GID を定義します。

   例: UNIXUsers

   重要: ユーザ アカウントを定義する場合、有効なグループ名/GID が割り当てられていることを確認してください。

7. [OK]をクリックします。

   ユーザの UNIX 属性が設定されます。

UNAB の設定

uxauth.ini ファイルでは、起動時と実行時の UNAB のアクションを設定します。uxauth.ini ファイルには、必要に応じて変更できるデフォルトの値の セットが含まれています。

UNAB の設定方法

1. UNAB を実行している UNIX ホストにログインします。
2. デフォルトでは、以下のディレクトリに格納されている uxauth.ini ファイルを開きます。

   ```
   /opt/CA/uxauth
   ```

3. 設定を確認し、必要に応じて変更します。

ユーザとグループの移行

ユーザを UNIX ホストから Active Directory に移行すると、管理タスクを単一の管理アプリケーションに統合できるため、UNIX ホスト上でのユーザおよびグループの管理が容易になります。 UNIX ユーザを Active Directory に移行すれば、UNIX ホストへのアクセスを制御するだけで済み、各 UNIX ホスト上でパスワードや shadow ファイルを管理する必要はなくなります。

ユーザとグループを UNIX ホストから Active Directory へ(完全統合モードで)移行すると、Active Directory がユーザの認証と権限付与を実行します。

移行のしくみ

UNIX ホスト上で移行プロセスを開始すると、UNAB は以下のタスクを実行します。

1. ローカル ユーザおよび NIS/NIS+ ユーザのリストを取得します。

   Active Directory で、リスト上の各ユーザ名、および各ユーザが以下のいずれかを行っているかどうかを検証します。

   - ユーザが Active Directory に存在し、ユーザの UNIX 属性が UNIX ホストに表示される属性と同じ場合、ユーザ アカウントは移行されます。
   - ユーザが Active Directory に存在し、ユーザの UNIX 属性のいくつかが不足している場合、UNAB はユーザを移行せず、不足しているプロパティをログに記録します。
   - ユーザが Active Directory に存在し、ユーザが UNIX 属性を持っていない場合、UNAB はユーザを移行し、不足している属性を追加します。
   - ユーザが Active Directory 内に存在しない場合:

     UNAB は、Active Directory 内にユーザ アカウントを作成しません。

2. ローカル グループおよび NIS/NIS+ グループのリストを取得します。

   Active Directory で、グループ名、および各グループが以下のいずれかを行っているかどうかを検証します。

   - グループが Active Directory に存在し、グループの UNIX 属性が UNIX ホストの属性と同じ場合、グループが移行されます。
   - グループが Active Directory に存在し、グループの ID が UNIX ホスト上の ID と異なる場合、UNAB は、そのメンバを含むグループを Active Directory に移行しません。
   - グループが Active Directory に存在し、グループ ID が同一であるが、一部の UNIX 属性が不足している場合、UNAB はグループを Active Directory へ移行し、不足している属性を補完します。
   - グループが Active Directory 内に存在しない場合:

     UNAB は、グループを Active Directory に移行しません。

Active Directory への UNIX ユーザおよびグループの移行

1 つの場所からのホストへのアクセスを管理するために、ローカル UNIX ホストから Active Directory へユーザを移行します。

UNIX ユーザおよびグループの Active Directory への 移行

1. root ユーザとして UNIX コンピュータにログインします。
2. UNAB インストール bin ディレクトリに移動します。このディレクトリのデフォルトのパスは、以下になります。

   ```
   /opt/CA/uxauth/bin
   ```

3. -uxconsole -migrate コマンドを実行します。

   ```
   ./uxconsole -migrate -scope {l|n|a} [-users] [-groups] {-mode {p|f} | -input file}
   [-emulate] [-admin name -pw passwd] [-v {1-5}]
   ```

   uxconsole プログラムは、UNIX ユーザおよびグループを Active Directory へ移行します。

   操作が正常に完了したことを通知するメッセージが表示されます。

注: uxconsole 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。

レポート作成のための UNAB の設定

UNAB のインストールおよび設定すると、データを配布サーバに送信して処理するように設定することができます。これを行うには、レポート エージェントを有効にして設定します。 UNAB のインストール時にレポート エージェントを設定しなかった場合は、レポート エージェントを有効化する際に設定してください。

注: 下の手順は、レポートを送信できるように既存の UNAB エンドポイントを設定する方法を示しています。 CA Access Control と UNAB を同じコンピュータ上にインストールしている場合、レポート エージェントの設定は 1 回で済みます。

レポート作成用に UNAB を設定するには、ACSharedDir/lbin/report_agent.sh を実行します。

```
report_agent config {-server hostname [-proto {ssl|tcp}] [-port port_number] [-rqueue queue_name] -schedule <time@day> [,day2][...] > [-audit] | [-silent] ]
```

環境設定オプションのいずれかを省略すると、スクリプトによってそのオプションのデフォルト値が設定されます。

注: report_agent.sh スクリプトおよび レポート エージェント設定の詳細については、「リファレンス ガイド」を参照してください。

第 9 章: エンドポイント管理 のインストール

このセクションには、以下のトピックが含まれています。

エンドポイント管理サーバの準備方法

CA Access Control エンドポイント管理 をインストールする前に、サーバを準備する必要があります。

重要: 同じコンピュータに 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、以下の手順を実行する必要はありません。 インストール プログラムは、CA Access Control エンタープライズ管理 インストールの一環として CA Access Control エンドポイント管理 のインストールを行います。

エンドポイント管理サーバを準備するには、以下の手順を実行します。

1. サポートされている Java Development Kit (JDK) をインストールします。

   注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA Access Control Premium EditionThird Party Components DVD に格納されています。 サポートされている JBoss バージョンの詳細については、「リリース ノート」を参照してください。

2. サポートされている JBoss バージョンをインストールします。

   JBoss をサービス (UNIX ではデーモン) として実行することをお勧めします。

   注: 事前にインストールが必要なサードパーティ ソフトウェアは、CA Access Control Premium EditionThird Party Components DVD に格納されています。 サポートされている JBoss バージョンの詳細については、「リリース ノート」を参照してください。

3. CA Access Control をインストールします。

   注: CA Access Control のエンドポイントのインストールに関する手順に従ってください。

4. (Windows のみ)コンピュータを再起動します。

5. CA Access Control サービスを停止します(secons -s)。

   これで、サーバの準備が整いましたので、CA Access Control エンドポイント管理をインストールできます。

グラフィカル インターフェースを使用した CA Access Control エンドポイント管理 のインストール

グラフィカル インストールでは、ウィザードを使用して CA Access Control エンドポイント管理 のインストールをサポートおよびガイドします。

グラフィカル インターフェースを使用して CA Access Control エンドポイント管理 をインストールする方法

1. サーバの適切な準備が整っていること(253 ページ)を確認します。

2. 以下のいずれかの操作を行います。

   - Windows の場合

     a. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Windows DVD を挿入します。

     b. CA Access Control Product Explorer(ProductExplorerx86.EXE)を開きます。

        CA Access Control の Product Explorer が表示されます。

     c. Components フォルダを展開し、CA Access Control エンドポイント管理 を選択し、[インストール]をクリックします。

   - UNIX の場合

     a. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Solaris DVD を挿入します。

     b. X Window 端末セッションを使用してホストに接続します。

     c. 光ディスク ドライブをマウントします。

     d. EndPointMgmt ディレクトリを探して、install.bin を実行します。

   InstallAnywhere ウィザードがロードを開始します。

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。

   JBoss フォルダ

   JBoss アプリケーション サーバがインストールされる場所を定義します。

   用意されている JBoss バージョンを使用する場合、これは、JBoss zip ファイルの内容を展開した場所になります。

   Web サービス情報

   CA Access Control Web サービスをインストールする場所と、このサービスに使用するポート(デフォルトは 5248)を指定します。

   完全なコンピュータ名

   アプリケーション サーバ(ローカル コンピュータ)の名前を定義します。 この名前は、このアプリケーションにアクセスする際、URL 内で使用する必要があります。

   これでインストールは終了です。

コンソールを使用した CA Access Control エンドポイント管理 のインストール

テキスト専用ターミナルからインストールするため、または、InstallAnywhere ウィザードに必要な X Server グラフィックス ソフトウェアがないためにグラフィカル インストールを使用しない場合は、コンソール インストールを使用して CA Access Control エンドポイント管理 をインストールできます。

コンソールを使用して CA Access Control エンドポイント管理 をインストールする方法

1. サーバの適切な準備が整っていること(253 ページ)を確認します。
2. 以下のいずれかの操作を行います。
   - Windows の場合
     a. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Windows DVD を挿入します。
     b. コマンド ラインを開き、光ディスク ドライブの以下のディレクトリに移動します。
     c. 以下のコマンドを入力します。

```
install_EM_r12_SP1.exe -i console
```

- UNIX の場合

  a. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Solaris DVD を挿入します。

  b. X Window 端末セッションを使用してホストに接続します。

  c. 光ディスク ドライブをマウントします。

  d. ターミナル ウィンドウを開き、光ディスク ドライブの EndPointMgmt ディレクトリに移動します。

  e. 以下のコマンドを入力します。

```
install_EM_r12_SP1.bin -i console
```

InstallAnywhere コンソールが数分後に表示されます。

3. 必要に応じてプロンプトを完了します。 以下のインストール入力には、説明が必要です。

数字によるロケールの選択

インストールしたいロケールを表わす数を定義します。

注: 英語以外のサポート対象言語いずれかにインストールするローカライズされたオペレーティング システムが必要です。

JBoss フォルダ

JBoss アプリケーション サーバがインストールされる場所を定義します。

用意されている JBoss バージョンを使用する場合、これは、JBoss zip ファイルの内容を展開した場所になります。

Web サービス情報

CA Access Control Web サービスをインストールする場所と、このサービスに使用するポート(デフォルトは 5248)を指定します。

完全なコンピュータ名

アプリケーション サーバ(ローカル コンピュータ)の名前を定義します。 この名前は、このアプリケーションにアクセスする際、URL 内で使用する必要があります。

これでインストールは終了です。

Windows での CA Access Control エンドポイント管理 のアンインストール

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 システムにログオンしていることを確認してください。

Windows での CA Access Control エンドポイント管理 のアンインストール方法

1. JBoss が実行中の場合は、停止します。
2. [スタート]-[コントロール パネル]-[プログラムの追加と削除]を選択します。

   [プログラムの追加と削除]ダイアログ ボックスが表示されます。
3. プログラム リストをスクロールして CA Access Control エンドポイント管理 を選択します。
4. [変更と削除]をクリックします。

   CA Access Control エンドポイント管理 のアンインストール ウィザードが表示されます。
5. ウィザードの手順に従って、CA Access Control エンドポイント管理 をアンインストールします。

   アンインストールが完了し、コンピュータから CA Access Control エンドポイント管理 が削除されます。
6. ウィザードを終了するには、[完了]をクリックしてください。

Solaris での CA Access Control エンドポイント管理 のアンインストール

コンピュータから CA Access Control エンドポイント管理 を削除するには、CA Access Control エンドポイント管理 に付属のアンインストール プログラムを使用する必要があります。

Solaris での CA Access Control エンドポイント管理 のアンインストール方法

1. 以下のいずれかの操作を実行して JBoss を停止します。
   - JBoss ジョブ ウィンドウから、プロセスを中断します(Ctrl+C)。
   - 別のウィンドウで、以下のように入力します。

     ```
     ./JBoss_path/bin/shutdown -S
     ```

2. 以下のコマンドを入力します。

   "/ACEMInstallDir/Uninstall_CA Access Control エンドポイント管理 /Uninstall_CA_Access_Control_Endpoint_Management"

   ACEMInstallDir

   CA Access Control エンドポイント管理 のインストール ディレクトリを定義します。 デフォルトでは、このパスは次のとおりです。

   /opt/CA/AccessControlServer/EndpointManagement/

   InstallAnywhere がアンインストール ウィザードまたはコンソールをロードします。

   注: アンインストールでは、インストール時に使用したのと同じメソッドがロードされます。 つまり、コンソールを使用してインストールした場合は、アンインストールでもコンソールを使用します。 ウィザードを使用してインストールした場合は、アンインストールでもウィザードがロードされます。

3. プロンプトに従って、CA Access Control エンドポイント管理 をアンインストールします。

   アンインストールが完了し、コンピュータから CA Access Control エンドポイント管理 が削除されます。

CA Access Control エンドポイント管理 の起動

CA Access Control エンドポイント管理 をインストールしたら、CA Access Control および Web アプリケーション サーバを起動する必要があります。

CA Access Control エンドポイント管理 を起動する方法

1. CA Access Control サービスを起動します。

   CA Access Control エンドポイント管理 を起動するには、CA Access Control が動作している必要があります。

2. (Windows のみ)以下を行います。

   a. 以下に示す追加サービスを開始します。これらのサービスは、seosd -start を実行してもロードされません。

      - CA Access Control Web サービス
      - CA Access Control メッセージ キュー(存在する場合)

   b. 以下のいずれかの方法で、JBoss アプリケーション サーバを起動します。

      - [スタート]-[プログラム]-[CA]-[Access Control]-[タスク エンジンの開始]をクリックします。

        注: タスク エンジンは、初回のロード時に多少時間がかかる場合があります。

- [サービス]パネルから JBoss アプリケーション サーバ サービスを開始します。

JBoss アプリケーション サーバのロードが完了すると、CA Access Control エンドポイント管理 の Web ベース インターフェースにログインできます。

3. (UNIX のみ)/JBOSS_DIR/bin/run.sh と入力します。

注: JBoss アプリケーション サーバは、初回のロード時に多少時間がかかる場合があります。

JBoss アプリケーション サーバのロードが完了すると、CA Access Control エンドポイント管理 の Web ベース インターフェースにログインできます。

CA Access Control エンドポイント管理 を開く

CA Access Control エンドポイント管理 をインストールして起動すると、CA Access Control エンドポイント管理 用の URL を使用してリモート コンピュータから Web ベースのインターフェースを開くことができます。

CA Access Control エンドポイント管理 を開く方法

1. Web ブラウザを開き、使用しているホストに合わせて URL を入力します。

   http://enterprise_host:port/acem

2. 以下の情報を入力します。

   User Name

   CA Access Control の管理タスクを実行する権限を有するユーザの名前を定義します。

   注: ログインに使用するユーザ名にはコンピュータ名が含まれている必要があります(たとえば、Windows の場合は myComputer¥Administrator、UNIX の場合は root)。

パスワード

CA Access Control ユーザのパスワードを定義します。

ホスト名

管理タスクを実行するエンドポイントの名前を定義します。 これに相当するのはホストまたは PMDB であり、次の形式で指定します。
PMDB_name@host_name

注: CA Access Control エンドポイント管理 がインストールされているコンピュータからエンドポイントを管理する(TERMINAL リソースを使用して)権限が必要になります。

[ログイン]をクリックします。

[ダッシュボード]タブ上で CA Access Control エンドポイント管理 が開きます。

注: CA Access Control エンドポイント管理 をインストールした Windows コンピュータから CA Access Control エンドポイント管理 を開くこともできます。それには、[スタート]-[プログラム]-[CA]-[Access Control]-[エンドポイント管理]をクリックします。

例: CA Access Control エンドポイント管理 を開く

Web ブラウザに次の URL を入力して、ネットワーク上の任意のコンピュータから CA Access Control エンドポイント管理 を開きます。

```
http://appserver123:18080/acem
```

この URL から、CA Access Control エンドポイント管理 が appserver123 という名前のホストにインストールされ、デフォルトの JBoss ポート 18080 を使用していることがわかります。

第 10 章: Disaster Recovery Deployment のインストール

このセクションには、以下のトピックが含まれています。

ディザスタ リカバリの概要

サブシステムのクラッシュまたはその他の障害発生時に、ディザスタ リカバリによってユーザのシステムをリストアします。

ディザスタ リカバリの目的は、可能な限り多くのデータをリストアし、バックアップおよびリストアで必要なリソースを制限することです。

注: ディザスタ リカバリ設定を使用すると、重大なシステム障害の発生時に拡張ポリシー管理コンポーネントをより容易に復元できます。 他の CA Access Control コンポーネントの個別バックアップが必要な場合もあります。

CA Access Control でのディザスタ リカバリ

ディザスタ リカバリの展開によって、重大なシステム障害発生時に、拡張ポリシー管理コンポーネントのリストアが容易になります。 エンドポイントが運用環境に接続できない場合、運用環境がリストアされるまで、エンドポイントはディザスタ リカバリ環境に接続します。

ディザスタ リカバリの展開には、以下の利点があります。

- ディザスタ リカバリ DMS のデータベースは運用環境 DMS のデータベースの複製です。 これは、運用環境 DMS データベースが破損した場合に、ポリシーのコピーがあることを意味します。
- エンドポイントは運用環境またはディザスタ リカバリ環境に接続できます。 運用環境が停止した場合でも、エンドポイントはデータをディザスタ リカバリ環境に送信するので、重大なシステム障害が発生した場合でも、ポリシーのステータスおよび偏差に関する情報は失われません。
- 障害復旧後、再度各エンドポイントをサブスクライブする必要はありません。

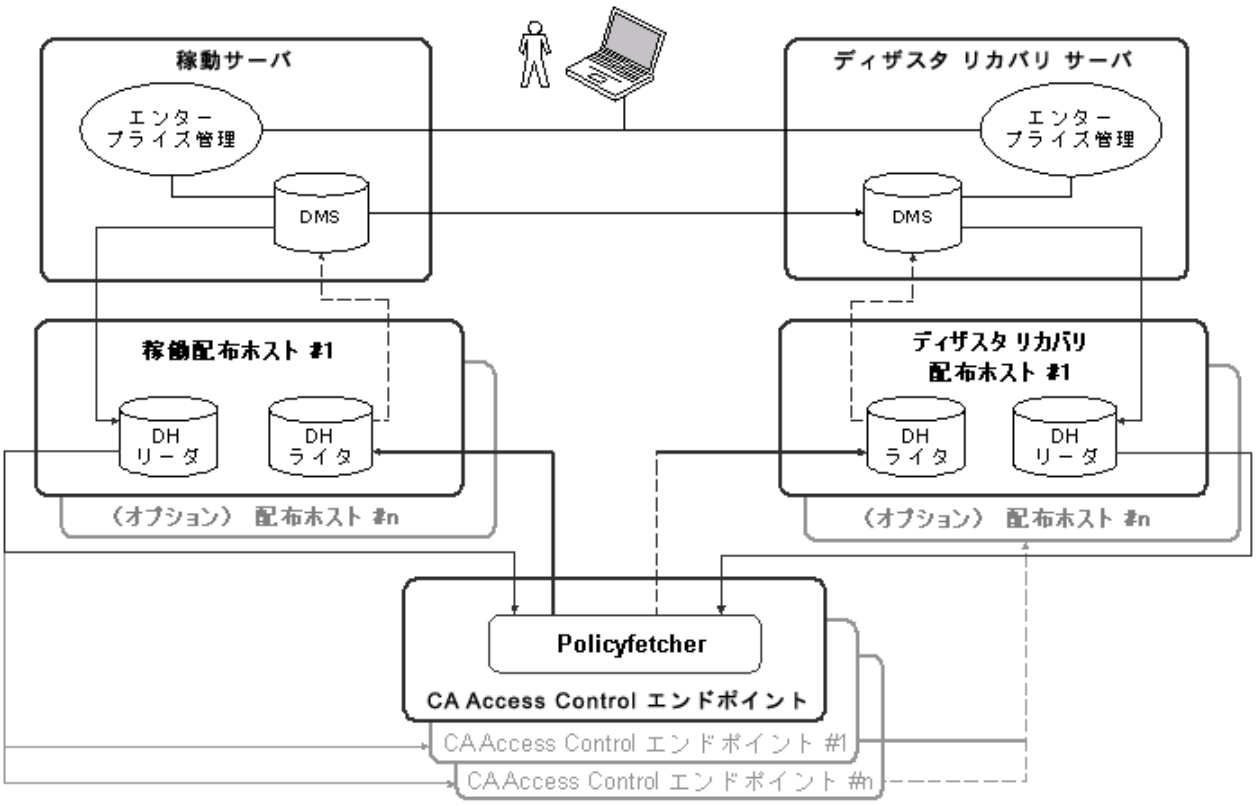
以下の CA Access Control コンポーネントは、ディザスタ リカバリ プロセス中にバックアップまたはリストアされません。 これらのコンポーネントを別々にバックアップします。

- パスワード ポリシー モデル
- PMDB
- RDBMS
- CA Access Control エンドポイント管理
- CA Access Control エンタープライズ管理
- エンドポイント上のデータ
- CA Access Control 監査ファイル
- レポート
- UNAB ポリシー
- メッセージ キュー

注: DMS がバックアップされると、DMS 監査ファイルが保存されます。

ディザスタ リカバリ アーキテクチャ

以下の図は、ディザスタ リカバリ構成で、CA Access Control をどのように展開するかを示しています。



ディザスタ リカバリのコンポーネント

ディザスタ リカバリ構成に CA Access Control をデプロイするには、以下のコンポーネントが必要です。

- 運用環境の場合:
  - CA Access Control エンタープライズ管理 の 1 インストール
  - 中央データベース(RDBMS)
  - 配布サーバの 1 つ以上のインストール
- ディザスタ リカバリ環境の場合:
  - CA Access Control エンタープライズ管理 の 1 インストール
  - 中央データベース(RDBMS)

- 配布サーバの 1 つ以上のインストール

ディザスタ リカバリのデプロイを計画する場合は、以下の点も考慮する必要があります。

- DMS はプラットフォーム、オペレーティング システム、CA Access Control のバージョンが同じ状態で保存されたバックアップ ファイルからでないとリストアできません。たとえば、CA Access Control r12.0 SP1 を使用した DMS のバックアップ ファイルから CA Access Control r12.5 を使用して DMS をリストアすることはできません。
- DMS のバックアップ ファイルは、安全な場所、できれば CA Access Control アクセス ルールで保護された場所に保存してください。
- お使いの RDBMS に対して、クラスタリングまたは、その他のフェールオーバ ソリューションをセットアップできます。

エンドポイント上のディザスタ リカバリの展開の仕組み

ディザスタ リカバリを展開すると、運用環境配布サーバ データベースの複製が作成され、エンドポイントから送信されたデータがシステム障害で失われないようになり、障害発生後の運用環境のリストアが容易になります。

注: ディザスタ リカバリ設定を使用すると、重大なシステム障害の発生時に拡張ポリシー管理コンポーネントをより容易に復元できます。 他の CA Access Control コンポーネントの個別バックアップが必要な場合もあります。

以下のプロセスでは、エンドポイント上へのディザスタ リカバリの展開の仕組みについて説明します。

1. 運用環境とディザスタ リカバリの配布サーバのリストと照合して、作業するエンドポイントを設定します。
2. 指定された時間に、エンドポイントは、運用環境内で CA Access Control エンタープライズ管理 への接続を試行します。
   a. エンドポイントは、リストの最初の運用環境配布サーバへの接続を試行します。接続できなかった場合、エンドポイントは、その配布サーバへの接続を指定された回数試行します。 以下のいずれかのイベントが発生します。
      - エンドポイントは運用環境配布サーバに接続します。 このステップで、プロセスが終了します。
      - エンドポイントは運用環境配布サーバに接続できません。 プロセスは、ステップ b に移動します。

      注: エンドポイントが配布サーバへの接続を試行する回数は、policyfetcher セクションの max_dh_command_retry 設定で定義されています。

b. エンドポイントは、リストの 2 番目の運用環境配布サーバへの接続を試行します。このように、リストに掲載されているサーバに順に（必要に応じて、定義されているのと同じ回数）接続を試行します。 以下のいずれかのイベントが発生します。

- エンドポイントは運用環境配布サーバに接続します。 このステップで、プロセスが終了します。
- エンドポイントはどの運用環境配布サーバにも接続できず、サイクルが終了します。 プロセスは、ステップ 3 に移動します。

3. エンドポイントは、指定されたサイクル数、ステップ 2 を繰り返します。 以下のいずれかのイベントが発生します。

- エンドポイントは運用環境配布サーバに接続します。 このステップで、プロセスが終了します。
- エンドポイントは運用環境配布サーバに接続しません。 プロセスは次のステップに移動します。

注: エンドポイントが配布サーバへの接続を試行する回数は、policyfetcher セクションの max_dh_retry_cycles 設定で定義されています。

4. エンドポイントは、リストの最初のディザスタ リカバリ配布サーバへの接続を試行します。 エンドポイントがこの配布サーバに接続できなかった場合、エンドポイントはリストの 2 番目のディザスタ リカバリ配布サーバへの接続を試行します。エンドポイントがディザスタ リカバリ配布サーバに接続するまで、それ以降、リストに掲載されているサーバに順に接続を試行します。

注: エンドポイントが運用環境またはディザスタ リカバリの配布サーバに接続できない場合、エンドポイントは DMS にハートビートを送信しません。 エンドポイントがオンラインかオフラインかどうかを決定するには、最後のハートビート通知が DMS にいつ送信されたかを確認します。

5. ディザスタ リカバリ配布サーバに接続した後、エンドポイントは継続して、運用環境配布サーバへの接続を試行します。 以下のいずれかのイベントが発生します。

- エンドポイントは運用環境配布サーバに接続し、運用環境に戻ります。
- エンドポイントは運用環境配布サーバに接続しません。 エンドポイントはディザスタ リカバリ環境に残り、ステップ 4 を繰り返します。

注: policyfetcher セクションの詳細については、「リファレンス ガイド」を参照してください。

ディザスタ リカバリの展開をインストールする方法

ディザスタ リカバリ コンポーネントを相互に適切にサブスクライブしていることを確認するには、運用環境とディザスタ リカバリのコンポーネントを、以下のプロセスで指定する順番で設定する必要があります。

ディザスタ リカバリを設定しておけば、重大なシステム障害の発生時に、拡張ポリシー管理コンポーネントのリストアが容易になります。 たとえば、中央データベース（RDBMS）など、他の CA Access Control コンポーネントを別々にバックアップする必要があるかもしれません。

重要: CA Access Control の別の運用環境またはバージョンを使用するバックアップファイルから、DMS をリストアできません。. CA Access Control の同一のプラットフォーム、オペレーティング システムおよびバージョン上に、運用環境とディザスタ リカバリの環境が展開されていることを確認します。

注: このプロセスでは、個別のホストに DMS および DH をインストールします。

以下のプロセスでは、ディザスタ リカバリ展開をインストールする方法について説明します。

1. 中央データベース（RDBMS）をセットアップします。
2. 運用環境 CA Access Control エンタープライズ管理 をセットアップします（266 ページ）。
3. ディザスタ リカバリ CA Access Control エンタープライズ管理 をセットアップします（267 ページ）。
4. 運用環境配布サーバをセットアップします（268 ページ）。
5. ディザスタ リカバリ配布サーバをセットアップします（270 ページ）。
6. エンドポイントをセットアップします。（272 ページ）.

注: RDBMS は、クラスタ、またはサイト間のデータ同期を許可する何らかの仕組み上にインストールすることをお勧めします。

運用環境 CA Access Control エンタープライズ管理 のセットアップ

運用環境 CA Access Control エンタープライズ管理 は DMS を含んでいます。 DMS は、各エンドポイントのポリシー バージョン、ポリシー スクリプトおよびポリシー デプロイメント ステータスに関する最新情報を格納します。 運用環境 DMS を使用して、組織のポリシーをデプロイおよび管理します。 運用環境 DH とディザスタ リカバリ DMS は運用環境 DMS にサブスクライブしているので、他のディザスタ リカバリ コンポーネントをセットアップする前に、運用環境 DMS をセットアップする必要があります。これによって、後にインストール プロセスで、サブスクリプションが正常に設定されるようになります。

運用環境 CA Access Control エンタープライズ管理 のセットアップ方法

1. 運用環境 CA Access Control エンタープライズ管理 をインストールします(43 ページ)。
2. ローカル DH を無効にし、配布サーバ上の DH を使用する場合は、運用環境 CA Access Control エンタープライズ管理 上で以下のコマンドを実行して、DMS を設定します。

   ```
   dmsmgr -remove -dh name
   ```

   -dh name

   ローカル ホストで名前を指定した DH を削除します。

   例: dmsmgr -remove -dh DH

   上記の例では、DH という名の DH をホストから削除します。

   運用環境 DMS はサブスクライバなしで作成されます。

ディザスタ リカバリ CA Access Control エンタープライズ管理 のセットアップ

重大なシステム障害発生時に、ディザスタ リカバリ CA Access Control エンタープライズ管理 はユーザのエンタープライズ ポリシーをデプロイおよび管理します。 ディザスタ リカバリ CA Access Control エンタープライズ管理 は運用環境 CA Access Control エンタープライズ管理 のサブスクライバであるため、そのデータベースには、運用環境 CA Access Control エンタープライズ管理 と同じ、ポリシー バージョン、ポリシー スクリプト、およびエンドポイント デプロイメント ステータスに関する情報が含まれています。

注: ディザスタ リカバリ CA Access Control エンタープライズ管理 をセットアップする前に、運用環境 CA Access Control エンタープライズ管理 をセットアップする必要があります。

ディザスタ リカバリ CA Access Control エンタープライズ管理 のセットアップ方法

1. ディザスタ リカバリ サーバ上に CA Access Control エンタープライズ管理 をインストールします(43 ページ)。

2. ローカル DH を無効にし、配布サーバ上の DH を使用する場合は、ディザスタ リカバリ CA Access Control エンタープライズ管理 上で以下のコマンドを実行する必要があります。

   ```
   dmsmgr -remove -dh name
   ```

   -dh name

   ローカル ホストで名前を指定した DH を削除します。

   例: dmsmgr -remove -dh DH

   ディザスタ リカバリ DMS はサブスクライバなしで作成されます。

3. 運用環境 CA Access Control エンタープライズ管理 へ移動します。
4. 運用環境 CA Access Control エンタープライズ管理 上で以下のコマンドを実行します。

   ```
   sepmd -n prDMS_name drDMS_name
   ```

   prDMS_name

   運用環境 DMS の名前を定義します。

   drDMS_name

   ディザスタ リカバリ DMS の名前を定義します。 ディザスタ リカバリ DMS は、「drDMS_name@hostname」形式で指定します。

ディザスタ リカバリ CA Access Control エンタープライズ管理 は、運用環境 CA Access Control エンタープライズ管理 にサブスクライブされ、同期されます。

運用環境配布サーバのセットアップ

運用環境配布サーバには、DH が含まれています。 DH は、運用環境 DMS で作成されたポリシー デプロイメントをエンドポイントに配布し、デプロイメント ステータスの更新をエンドポイントから受け取って、運用環境 DMS に送ります。

運用環境 DHS とディザスタ リカバリ DMS は運用環境 DMS にサブスクライブしているので、他のディザスタ リカバリ コンポーネントをセットアップする前に、運用環境 DMS をセットアップしてください。 これによって、後にインストール プロセスで、サブスクリプションが正常に設定されるようになります。

運用環境配布サーバのセットアップ方法

1. 運用環境配布サーバ をインストールします。
2. 運用環境配布サーバ上で以下のコマンドを実行して、DH を設定します。

   ```
   dmsmgr -remove -auto

   dmsmgr -create -dh name -parent name\
   [-admin user[,user...]] [-desktop host[,host...]]
   ```

-dh name

ローカル ホストで指定した名前で DH を作成します。

-parent name

DH がエンドポイント通知を送る先の運用環境 DMS を定義します。 運用環境 DMS を「DMS_name@hostname」の形式で指定します。

-admin user[,user...]

(オプション) 作成される DH の管理者として、内部ユーザを定義します。

-desktop host[,host...]

(オプション) 作成した DH があるコンピュータに対して TERMINAL アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、常に作成された DH に対する管理権限が与えられます。

運用環境 DH が作成されます。

3. 以下のコマンドを実行します。

```
sepmd -n prDMS_name prDH_name
```

prDMS_name

運用環境 DMS の名前を定義します。

prDH_name

運用環境 DH の名前を定義します。 名前は、「DMS_name@hostname」という形式で指定します。

例: DH__@prdh.com

DH は運用環境 DMS にサブスクライブし、同期されます。

4. 配布サーバと運用環境 DMS の間をルーティングするメッセージ キューをセットアップします (283 ページ)。
5. 各運用環境配布サーバについて、ステップ 1-4 を繰り返します。

ディザスタ リカバリ配布サーバのセットアップ

ディザスタ リカバリ配布サーバは運用環境配布サーバのサブスクライバであるため、そのデータベースには、運用環境配布サーバと同じ、ポリシー バージョン、ポリシー スクリプト、およびエンドポイント デプロイメント ステータスに関する情報が含まれています。

注: ディザスタ リカバリ配布サーバをセットアップする前に、運用環境配布サーバをセットアップする必要があります。

ディザスタ リカバリ配布サーバのセットアップ方法

1. ディザスタ リカバリ配布サーバ上に配布サーバをインストールします、
2. ディザスタ リカバリ配布サーバ上で以下のコマンドを実行して、DH を設定します。

```
dmsmgr -remove -auto

dmsmgr -create -dh name -parent name\
[-admin user[,user...]] [-admin user[,user...]]
```

-dh name

ローカル ホストに指定した名前で DH を作成します。

-parent name

DH がエンドポイント通知を送る先のディザスタ リカバリ DMS を定義します。ディザスタ リカバリ DMS は、「DMS_name@hostname」形式で指定します。

-admin user [,user...]]

(オプション) 作成される DH の管理者として、内部ユーザを定義します。

-desktop host[,host...]

(オプション) 作成された DH があるコンピュータに対して TERMINAL アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、常に作成された DH に対する管理権限が与えられます。

ディザスタ リカバリ DH が作成されます。

3. ディザスタ リカバリ配布サーバ上で、以下のコマンドを実行します。

   ```
   sepmd -n drDMS_name drDH_name
   ```

   drDMS_name

   ディザスタ リカバリ DMS の名前を定義します。

   drDH_name

   ディザスタ リカバリ DH の名前を定義します。 名前は、「drDH_name@hostname」という形式で指定します。

   例: DH__@drdh.com

   DH はディザスタ リカバリ DMS にサブスクライブし、同期されます。

4. 配布サーバと運用環境 DMS の間をルーティングするメッセージ キューをセットアップします。(283 ページ)

5. 各ディザスタ リカバリ DH について、ステップ 1-4 を繰り返します。

CA Access Control 配布サーバのインストール

この手順を完了して、CA Access Control 配布サーバをインストールします。 ディザスタ リカバリ環境で稼働するように CA Access Control を設定するには、少なくとも 2 つの配布サーバを別々のコンピュータにインストールし、それらのサーバ間でファイルが伝達されるように設定する必要があります。 CA Access Control 配布サーバ インストール ウィザードで示される手順に従って、このプロセスを実行します。

CA Access Control 配布サーバのインストール方法

1. JBoss アプリケーション サーバが動作している場合は、これを終了させます。
2. CA Access Control サービスを停止します。

   重要: 手動で、CA Access Control Web サービスおよび CA Access Control メッセージ キュー サービスを停止します。 ユーザが secons -s コマンドを発行する場合、これらのサービスは停止しません。 これらのサービスが存在するのは、すでに CA Access Control エンドポイント管理 をインストールしている場合のみです。

3. 以下の手順を実行します。

   a. 光ディスク ドライブに CA Access Control Premium Edition Server Components for Windows DVD を挿入します。

   b. CA Access Control Product Explorer(ProductExplorerx86.EXE)を開きます。

      CA Access Control の Product Explorer が表示されます。

   c. [コンポーネント]フォルダを展開し、CA Access Control 配布サーバを選択し、[インストール]をクリックします。

      InstallAnywhere ウィザードがロードを開始します。

4. 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 コネクタ サーバ

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。

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を定義します。

制限: 最低 6 文字

CA Access Control 配布サーバのインストールが完了します。

エンドポイントのセットアップ

運用環境およびディザスタ リカバリの環境に拡張ポリシー管理をインストールしたら、拡張ポリシー管理用に、組織内の各エンドポイントを設定する必要があります。 その際、サーバ コンポーネントとの間で情報の送信先および受信元として機能するエンドポイントを設定します。

注: インストール プロセスの一部として、拡張ポリシー管理サーバ コンポーネントのホスト名を指定します。 以下の形式で、運用環境 DH の名前を入力します。
prDH_name@hostname[, prDH_name@hostname..]

エンドポイントのセットアップ方法

1. 拡張ポリシー管理クライアント コンポーネントを有効にした状態で、CA Access Control エンドポイント機能をエンドポイント ホストにインストールします。

   CA Access Control エンドポイント機能性はホストにインストールされます。また、エンドポイントは運用環境 DH にサブスクライブします。

2. エンドポイントで selang コマンド ウィンドウを開きます。
3. 以下のコマンドを入力します。

```
so dh_dr+(drDH_name[, drDH_name...])
```

drDH_name

ディザスタ リカバリ DH の名前を定義します。形式: drDH_name@hostname。

エンドポイントはディザスタ リカバリ DH にサブスクライブします。

4. 運用環境とディザスタ リカバリの配布サーバの URL のリストを指定します。
   - UNIX: accommon.ini ファイルの[通信]セクション内の Distribution_Server パラメータを変更します。
   - Windows: Windows レジストリで Distribution_Sever 値を変更します。 このパラメータは以下にあります。

     ```
     HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥common¥communication
     ```

   注: Distribution_Server 値の詳細については、「リファレンス ガイド」を参照してください。

   注: または、指定された selang コマンドでポリシーを作成し、それをエンドポイントにデプロイして、エンドポイントをディザスタ リカバリ DH にサブスクライブできます。ポリシーの作成とデプロイの詳細については、「エンタープライズ管理ガイド」を参照してください。

ディザスタ リカバリ プロセス

ディザスタ リカバリ プロセスには、「バックアップ」と「リストア」の 2 つの段階があります。バックアップ段階では、DMS データベース内のデータは別のディレクトリにコピーされます。 リストア段階では、dmsgmr ユーティリティは、バックアップ DMS ファイルを使用して既存の DMS をリストアするか、または DMS を作成します。

注: ディザスタ リカバリ設定を使用すると、重大なシステム障害の発生時に拡張ポリシー管理コンポーネントをより容易に復元できます。 他の CA Access Control コンポーネントの個別バックアップが必要な場合もあります。

リストアできるデータ

DMS をリストアする場合、dmsmgr は、別の DMS のバックアップ ファイルを使用して新しい DMS を作成します。 DH をリストアする場合、dmsmgr は DMS バックアップ ファイルのデータを DH リーダ ディレクトリにコピーします。 いずれの場合も、同じデータをリストアします。

リストアするデータは DMS データベース内のデータの複製で、その内容は以下のとおりです。

- ユーザの組織のポリシー、バージョンおよび割り当てに関する情報
- デプロイメントおよびポリシー ステータス、デプロイメント偏差およびデプロイメント階層に関する情報
- ホストとホスト グループの定義
- 設定
- updates.dat ファイル
- レジストリ エントリ
- DMS 監査ファイル

注: DH__Writer は一時的なデータベースであるため、リストアする必要はありません。

DMS をリストアする場合

DMS をリストアする場合、dmsmgr は、別の DMS のバックアップ ファイルを使用して新しい DMS を作成します。 以下のシナリオは、運用環境 DMS をリストアする場合です。

- 運用環境システムに致命的な障害が発生している。
- 運用環境 DMS データベースが破損している。
- 新しい運用環境 DMS を別のホストにセットアップする必要がある。

以下のシナリオは、ディザスタ リカバリ DMS をリストアする場合です。

- ディザスタ リカバリ DMS が運用環境 DMS と同期していない。
- ディザスタ リカバリ DMS データベースが破損している。
- 新しいディザスタ リカバリ DMS を別のホストにセットアップする必要がある。

注: DMS は、既存の DMS 上に、または DMS が存在しない新規ディレクトリにリストアできます。

DH をリストアする場合

DH のリストア時、dmsmgr は DMS バックアップ ファイルのデータを DH リーダ ディレクトリにコピーします。 以下のシナリオは、DH をリストアする場合です。

- 運用システムに致命的な障害が発生している。
- DH データベースが壊れている。
- DH が DMS と同期していない。
- 新しい DH を異なるホストにセットアップする必要がある。

注: DH ライタは一時的なデータベースであるため、リストアする必要はありません。 DH をリストアする前に、DH ライタが既存の DH ファイル構造に存在していることを確認してください。

DMS のリストア方法

dmsmgr ユーティリティがどのように DMS をリストアするか理解することは、リストア プロセスで発生する可能性がある問題の診断に役立ちます。

以下のプロセスでは、dmsmgr で DMS をリストアする方法について説明します。

1. dmsmgr は既存の DMS を削除します。
2. dmsmgr は、DMS のバックアップ ファイルを、指定した場所から DMS ディレクトリにコピーします。
3. dmsmgr は、DMS のすべてのサブスクライバを削除します。
4. 以下のいずれかのイベントが発生します。
   - 運用環境 DMS をリストアすると、dmsmgr は、バックアップ ファイルに格納されている最後のグローバル オフセットと同じオフセット値で、ディザスタ リカバリ DMS を、その最初のサブスクライバとして、運用環境 DMS に追加します。
   - 惨事復旧 DMS をリストアすると、dmsmgr は、バックアップ ファイルに格納されている最後のグローバル オフセットと同じオフセット値で、ディザスタ リカバリ DMS を運用環境 DMS に再サブスクライブします。
5. dmsmgr は各 DH を DMS にサブスクライブします。 各 DH は、オフセット値 0 および非同期ステータスを持っています。

   注: 同期してない場合、DH は DMS から更新を受け取れません。 非同期ステータスから DH を解放するには、DH をリストアします。

DH のリストア方法

dmsmgr ユーティリティがどのように DH をリストアするか理解することは、リストア プロセスで発生する可能性がある問題の診断に役立ちます。

以下のプロセスでは、dmsmgr で DH をリストアする方法について説明します。

1. dmsmgr は既存の DH を削除します。
2. dmsmgr は、DH のバックアップ ファイルを、指定した場所から DH ディレクトリにコピーします。
3. dmsmgr は、バックアップ ファイルに格納された最後のグローバル オフセットと等しいオフセット値を持つ DMS に DH をサブスクライブします。
4. dmsmgr は、DH 上の非同期フラグをクリアします。

オフセット値

updates.dat ファイルには、DMS がデプロイする各コマンドが格納されます。 新しいサブスクライバを作成するときに、Policy Model は updates.dat ファイル内のコマンドをサブスクライバに送信します。 各コマンドには、オフセット値という増分番号がインデックス付けされます。

DMS にサブスクライバを追加するときには、以下のオフセットを指定できます。

- 0 - Policy Model はすべてのコマンドをサブスクライバに送信します。
- 最後のオフセット - Policy Model はコマンドをサブスクライバに送信しません。
- 0 と最後のオフセットの間の整数 X - Policy Model は X から最後のオフセットまでのすべてのコマンドをサブスクライバに送信します。

非同期サブスクライバ

非同期サブスクライバとは、updates.dat ファイルが前回切り捨てられてから、更新を一切受け取っていないサブスクライバです。 サブスクライバに非同期フラグを立てると、CA Access Control はそのサブスクライバを無視し、そのサブスクライバにコマンドが一切送られなくなります。

非同期サブスクライバは、その親 DMS または Policy Model から、更新を一切受け取りません。 非同期フラグをクリアし、サブスクライバが更新を受け取るようにするには、サブスクライバをその親に再サブスクライブする必要があります。

親 DMS または Policy Model のサブスクライバがすべて非同期の場合、親には実質的にサブスクライバがないことになります。

障害からの復旧方法

運用システムに障害が発生した場合、エンドポイントはディザスタ リカバリ環境に対して機能します。 障害から復旧する際、ディザスタ リカバリ環境からリストアした運用環境に操作を戻します。

以下のプロセスは、障害から復旧する方法について説明します。

1. 運用環境の CA Access Control エンタープライズ管理 と配布サーバ上の CA Access Control を停止します。
2. ディザスタ リカバリ DMS に対するすべての管理作業を停止します。つまり、CA Access Control エンタープライズ管理 と policydeploy ユーティリティを停止します。
3. （オプション） updates.dat ファイルの自動切り捨てを実行します。
4. ディザスタ リカバリ DMS をバックアップします。 DMS は、以下のいずれかの方法でバックアップできます。
   - ローカル バックアップ (278 ページ)
   - リモート バックアップ (279 ページ)
5. 運用環境のデータベース（RDBMS）のリストア
6. ディザスタ リカバリ DMS のバックアップ ファイルから 運用環境の DMS をリストアします (280 ページ)。
7. 運用環境の DMS で CA Access Control を開始します。
8. 運用環境の DMS をバックアップできます。DMS のバックアップは、以下のいずれかの方法で行うことができます。
   - ローカル バックアップ (278 ページ)
   - リモート バックアップ (279 ページ)
9. 運用環境の DMS のバックアップ ファイルから 各運用環境の DH をリストアします (282 ページ)。
10. 各運用環境の配布サーバ上で CA Access Control を開始します。
11. すべての管理作業を運用環境の DMS に移動します。つまり、運用環境の CA Access Control エンタープライズ管理 で、CA Access Control エンタープライズ管理 と policydeploy ユーティリティを開始します。

12. (オプション)ディザスタ リカバリ DMS が運用環境の DMS と同期していない場合は、以下の手順を完了します。
    a. 運用環境の DMS のバックアップ ファイルからディザスタ リカバリ DMS をリストアします(281 ページ)。
    b. ディザスタ リカバリ DMS をバックアップできます。DMS のバックアップは、以下のいずれかの方法で行うことができます。
        - sepmd ユーティリティ(278 ページ)
        - selang のコマンド(279 ページ)
    c. ディザスタ リカバリ DMS のバックアップ ファイルから各ディザスタ リカバリ DH をリストア(282 ページ)します。

sempd を使用した DMS のバックアップ

DMS をバックアップして、エンドポイントにデプロイしたポリシー、および CA Access Control エンタープライズ管理 がエンドポイントから受け取ったレポート スナップショットを保存します。

DMS のバックアップでは、DMS データベースのデータを指定したディレクトリにコピーします。

sepmd ユーティリティは、ローカル ホストにのみ DMS をバックアップします。 DMS のバックアップ ファイルは、安全な場所、できれば CA Access Control アクセス ルールで保護された場所に保存してください。 DMS をバックアップする前に、updates.dat ファイルの自動切り捨てを実行することをお勧めします。

注: DMS は selang コマンドを使ってローカル ホストまたはリモート ホストにバックアップすることもできます。

sepmd を使用して DMS をバックアップする方法

1. 以下のコマンドを使用して、DMS をロックします。

    ```
    sepmd -bl dms_name
    ```

    DMS はロックされるため、サブスクライバにコマンドを送信できなくなります。

2. 以下のコマンドを使用して、DMS データベースをバックアップします。

   ```
   sepmd -bd dms_name [destination_directory]
   ```

   dms_name

   ローカル ホストにバックアップする DMS の名前を定義します。

   destination_directory

   DMS のバックアップ先ディレクトリを定義します。

   デフォルト: (UNIX) ACInstallDir/data/policies_backup/dmsName

   デフォルト: (Windows) ACInstallDir¥data¥policies_backup¥dmsName

   DMS データベースを宛先ディレクトリにバックアップします。

3. 以下のコマンドを使用して、DMS のロックを解除します。

   ```
   sepmd -ul dms_name
   ```

   DMS はロックが解除されるため、サブスクライバにコマンドを送信できるようになります。

selang を使用した DMS のバックアップ

DMS のバックアップでは、データを DMS データベースから指定したディレクトリにコピーします。

DMS は selang コマンドを使ってローカル ホスト、またはリモート ホストにバックアップできます。 DMS のバックアップ ファイルは、安全な場所、できれば CA Access Control アクセス ルールで保護された場所に保存してください。 DMS をバックアップする前に、updates.dat ファイルの自動切り捨てを実行することが推奨されます。

注: ローカル ホストに DMS をバックアップする場合は、sepmd ユーティリティも使用できます。

selang を使用して DMS をバックアップする方法

1. (オプション) selang を使ってリモート ホストから DMS に接続している場合は、以下のコマンドを使って DMS ホストに接続します。

   ```
   host dms_host_name
   ```

2. 以下のコマンドを使用して、PMD 環境に移動します。

   ```
   env pmd
   ```

3. 以下のコマンドを使用して、DMS をロックします。

   ```
   pmd dms_name lock
   ```

   DMS はロックされるため、サブスクライバにコマンドを送信できなくなります。

4. 以下のコマンドを使用して、DMS データベースをバックアップします。

   ```
   backuppmd dms_name [destination(destination_directory)]
   ```

   dms_name

   ローカル ホストにバックアップする DMS の名前を定義します。

   destination(destination_directory)

   DMS のバックアップ先ディレクトリを定義します。

   デフォルト: (UNIX) ACInstallDir/data/policies_backup/dmsName

   デフォルト: (Windows) ACInstallDir¥data¥policies_backup¥dmsName

   DMS データベースを宛先ディレクトリにバックアップします。

5. 以下のコマンドを使用して、DMS のロックを解除します。

   ```
   pmd dms_name unlock
   ```

   DMS はロックが解除されるため、サブスクライバにコマンドを送信できるようになります。

運用環境の DMS のリストア

運用環境の DMS のリストア時、dmsmgr はディザスタ リカバリ DMS バックアップ ファイルから運用環境の DMS にデータをコピーします。

注: dmsmgr ユーティリティを使用するには、オペレーティング システムへの完全な管理アクセス権が必要です。

運用環境の DMS をリストアするには、運用環境の DMS ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dms name -source path -replica name\
[-subscriber dhname[,dhname...]] [-admin user[,user...]]\
[-xadmin user[,user...]]
```

-admin user[,user...]

(UNIX)リストアされる DMS または DH の管理者として内部ユーザを指定します。

-dms name

ローカル ホストにリストアする DMS の名前を定義します。

-replica name

運用環境の DMS にサブスクライブするディザスタ リカバリ DMS の名前を定義します。 ディザスタ リカバリ DMS は「DMS 名@ホスト名」形式で指定します。

-subscriber dh_name[, dh_name...]

(オプション)リストアされる DMS がポリシーの更新を送信する DH のリストをカンマ区切りで定義します。 各 DH は DH_name@hostname という形式で指定します。

-source path

リストアするバックアップ ファイルが存在するディレクトリを定義します。

-xadmin user[,user...]

(UNIX)リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

運用環境の DMS がリストアされます。

注: 運用環境の DMS をリストアした後は、運用環境の DMS をバックアップし、そのバックアップ ファイルから運用環境の DH をリストアする必要があります。 これにより、運用環境の DMS と DH が同期されます。

ディザスタ リカバリ DMS のリストア

ディザスタ リカバリ DMS のリストア時、dmsmgr はバックアップ ファイルのデータをディザスタ リカバリ DMS ディレクトリにコピーします。

注: dmsmgr ユーティリティを使用するには、オペレーティング システムへの完全な管理アクセス権が必要です。

ディザスタ リカバリ DMS をリストアするには、ディザスタ リカバリ DMS ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dms name -source path -parent name¥
[-subscriber dhname[,dhname...]] [-admin user[,user...]]¥
[-xadmin user[,user...]]
```

-admin user[,user...]

(UNIX)リストアされる DMS または DH の管理者として内部ユーザを指定します。

-dms name

ローカル ホストにリストアする DMS の名前を定義します。

-parent name

リストアされたディザスタ リカバリ DMS がサブスクライブする運用環境の DMS の名前を定義します。 運用環境の DMS は DMS_name@hostname のフォーマットで指定します。

-source path

リストアするバックアップ ファイルが存在するディレクトリを定義します。

-subscriber dh_name[, dh_name...]

(オプション)リストアされる DMS がポリシーの更新を送信する DH のリストをカンマ区切りで定義します。 各 DH は DH_name@hostname という形式で指定します。

-xadmin user[,user...]

(UNIX)リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

ディザスタ リカバリ DMS がリストアされて、運用環境の DMS にサブスクライブされます。

注: ディザスタ リカバリ DMS をリストアした後は、ディザスタ リカバリ DMS をバックアップし、そのバックアップ ファイルからディザスタ リカバリ DH をリストアする必要があります。 これにより、ディザスタ リカバリ DMS と DH が確実に同期されます。

DH のリストア

dmsmgr ユーティリティを使用して、データを DMS バックアップ ファイルから DH_Reader ディレクトリにコピーして、DH をリストアします。DH ライタをリストアする必要はありません。これは、そのデータベースが一時的なものであるためです。 DH をリストアする前に、DH ライタが既存の DH ファイル構造に存在していることを確認してください。

注: DH ライタが既存の DH ファイル構造にない場合、または新しい DH をセットアップする場合は、DH をリストアする前に、dmsmgr -create 機能を使用して新しい DH を作成します。

注: dmsmgr ユーティリティを使用するには、オペレーティング システムへの完全な管理アクセス権が必要です。

DH をリストアするには、DH ホストで以下のコマンドを実行します。

```
dmsmgr -restore -dh name -source path -parent name¥
[-admin user[,user...]] [-xadmin user[,user...]] [-desktop host[, host...]]
```

-admin user[,user...]

(UNIX)リストアされる DMS または DH の管理者として内部ユーザを指定します。

-desktop host[, host...]

(オプション)リストアする DH があるコンピュータに対して TERMINAL アクセス権限を持つコンピュータのリストを定義します。

注: 指定の有無に関わらず、このユーティリティを実行している端末には、リストアする DH に対する管理権限が常に与えられます。

-dh name

ローカル ホストにリストアする DH の名前を定義します。

-parent name

リストアされた DH がサブスクライブする親 DMS の名前を定義します。 親 DMS は「DMS_name@hostname」という形式で指定します。

-source path

リストアするバックアップ ファイルが存在するディレクトリを定義します。

-xadmin user[,user...]

(UNIX)リストアされる DMS または DH の管理者としてエンタープライズ ユーザを定義します。

DH がリストアされて、DMS にサブスクライブされます。

メッセージ ルーティングの設定方法

CA Access Control エンタープライズ管理 の単一のインスタンスおよび複数の配布サーバで構成される環境で作業する場合、CA Access Control エンタープライズ管理 上の MQ をポイントするように、すべての配布サーバ上の MQ ルーティング設定を構成する必要があります。 これによって、CA Access Control エンドポイントが送信するすべてのメッセージが最終的に、CA Access Control 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 CA Access Control 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。
  - CA Access Control エンタープライズ管理 メッセージ キューへのルーティングを変更します。
  - CA Access Control エンタープライズ管理 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。

- CA Access Control エンタープライズ管理 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。

■ CA Access Control エンタープライズ管理 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。
- 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。
- CA Access Control エンタープライズ管理 メッセージ キューの名前を設定します。
- CA Access Control エンタープライズ管理 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 Server User's Guide」を参照してください。

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。
2. 配布サーバ上で、ファイル tibemsd.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。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin
   ```

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変更します。
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 Server User's Guide」を参照してください。

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。これは
# 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
######################
```

CA Access Control エンタープライズ管理 上のメッセージ キュー設定の変更

この手順では、CA Access Control エンタープライズ管理 上のメッセージ 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を示します。

CA Access Control エンタープライズ管理 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。
2. CA Access Control エンタープライズ管理 で、編集可能な形式で tibemsd.conf ファイルを開きます。 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。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin
   ```

3. [サーバ]パラメータに、ドットで区切られない、CA Access Control 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。

   CA Access Control エンタープライズ管理 上でメッセージ 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 Server User's Guide」を参照してください。

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 キュー接続設定 - 例

配布サーバ上の MQ から CA Access Control エンタープライズ管理へ、および CA Access Control エンタープライズ管理 上の MQ から配布サーバにメッセージをルーティングするために、組織内の各配布サーバ上の既存の MQ 設定、および CA Access Control エンタープライズ管理 上の MQ の設定を変更します。

例: 配布サーバ上のメッセージ キュー接続設定の設定

この例では、配布サーバ上のメッセージ キュー サーバ設定の設定方法を示します。CA Access Control エンタープライズ管理 上で実行中のメッセージ キュー サーバのパラメータを定義して、メッセージを CA Access Control エンタープライズ管理 に送る、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 CA Access Control エンタープライズ管理 コンピュータの名前に、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場合、名前を tibemsd.conf ファイルのサーバ トークンで定義されている、サーバの実際の名前に置き換える必要があります。

配布サーバ上のメッセージ キュー接続設定の設定方法

1. 配布サーバ上で、[スタート]-[プログラム]-[TIBCO]-[TIBCO EMS 4.4.1]-[EMS 管理ツールの開始]を選択します。

   [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. メッセージ キューに接続します。 以下のいずれかの操作を行います。

   - 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。
4. プロンプトが表示されたら、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=<dist_server-passwd>

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=
   ```

   例: create user ENTM_Name password=<acserver_user-passwd>

   ENTM-NAME

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   重要: CA Access Control エンタープライズ管理 コンピュータ上の tibemsdf.conf ファイルの[サーバ]パラメータで定義した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. 変更を有効にするために、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: CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定の設定

この例では、CA Access Control エンタープライズ管理 上のメッセージ キュー サーバ設定の設定方法を示します。 配布サーバにメッセージを送信するために、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 CA Access Control エンタープライズ管理 コンピュータの名前に、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場合、名前を tibemsd.conf ファイルの[サーバ]トークンで定義されている、サーバの実際の名前に置き換える必要があります。

CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定の設定方法

1. CA Access Control エンタープライズ管理 コンピュータ上で、[スタート]-[プログラム]-[TIBCO]-[TIBCO EMS 4.4.1]-[EMS 管理ツールの開始]を選択します。

   [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. メッセージ キューに接続します。 以下のいずれかの操作を行います。

   - 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. 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=
   ```

   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=
   ```

   例: create user DS_SERVER_NAME password=<distserver_user-passwd>

   DS_NAME

   配布サーバの短縮名を定義します。

   重要: CA Access Control エンタープライズ管理 コンピュータ上の tibemsdf.conf ファイルの[サーバ]パラメータで定義したのと同じ名前を指定します。

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。

   CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定を設定しました。

   注: メッセージ ルーティングの詳細については、「TIBCO Enterprise Message Server User's Guide」を参照してください。

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 CA Access Control エンタープライズ管理 へメッセージを転送するには、配布サーバ上のメッセージ キューから CA Access Control エンタープライズ管理 上のメッセージ キューへメッセージを転送するように、各メッセージ ルートを設定します。

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。 CA Access Control エンタープライズ管理 上のメッセージ キューの設定を提供するために、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. 配布サーバ上で、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。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin¥
   ```

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

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   重要: CA Access Control エンタープライズ管理 の tibemsdf.conf ファイルの [サーバ]パラメータで定義した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 Server User's Guide」を参照してください。

CA Access Control エンタープライズ管理 コンピュータ上のメッセージ キューの名前の設定

この手順では、CA Access Control エンタープライズ管理 上のメッセージ 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ために、CA Access Control エンタープライズ管理 上でメッセージ キューの設定を行います。

CA Access Control エンタープライズ管理 コンピュータ上でのメッセージ キューの名前の設定方法

1. CA Access Control エンタープライズ管理 で、編集可能な形式で queues.conf ファイルを開きます。 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。

   ```
   ¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥bin
   ```

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 Server User's Guide」を参照してください。

メッセージ ルート設定 - 例

配布サーバおよび CA Access Control エンタープライズ管理 上でメッセージ キュー設定を設定し、メッセージ キュー ルーティング設定を設定した後に、配布サーバおよび CA Access Control エンタープライズ管理 上でメッセージ ルートをセットアップする必要があります。

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のメッセージを CA Access Control エンタープライズ管理 上のメッセージ キューにルーティングするために、配布サーバと CA Access Control エンタープライズ管理 の間にルートをセットアップします。 組織内のすべての配布サーバ上で、この手順を完了する必要があります。

1. 配布サーバ上で、編集可能な形式でファイル routes.conf を開きます。 このファイルは、デフォルトで、以下のディレクトリにあります。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥MessageQueue¥tibco¥ems¥bin
   ```

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

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   ENTM_URL

   CA Access Control エンタープライズ管理 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。

例: CA Access Control エンタープライズ管理 でのメッセージ ルートのセットアップ

この例では、CA Access Control エンタープライズ管理 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 エンタープライズ管理 から配布サーバへ、配布サーバからエンドポイントへメッセージを送信するために、CA Access Control エンタープライズ管理 と配布サーバの間にルートをセットアップします。

1. CA Access Control エンタープライズ管理 上で、ファイル routes.conf を開きます。このファイルは、デフォルトで、以下のディレクトリにあります。

   ```
   ¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥bin
   ```

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 Server User's Guide」を参照してください。

第 11 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

ポリシー モデル (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. 拡張ポリシー管理環境を設定します。
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(299 ページ)

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。 ポリシー ファイルには pmdName_hostName_policy という名前が付けられます。

   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。 POLICY オブジェクトには pmdName_POLICY#01 という名前が付けられます。

   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 からのリソース ルールの移行(301 ページ)

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. 以下のいずれかが行われます。
   - 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. 詳細ポリシー管理環境を設定する。
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する(300 ページ)。
4. PMDB からユーザ ルールを移行します。.
5. PMDB からリソース ルールを移行します。(301 ページ).

詳細情報:

移行プロセスのしくみ(296 ページ)

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。

- 拡張ポリシー管理環境の設定
- PMD ホストを CA Access Control r12.5 以降にアップグレード

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。

   エンドポイントはアップグレードされました。

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 からのリソース ルールの移行

PMDB からのリソース ルールの移行は、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最後の手順です。 前の手順では以下を行いました。

- 拡張ポリシー管理環境の設定
- PMD ホストを CA Access Control r12.5 以降にアップグレード
- エンドポイントの移行
- PMDB からのユーザ ルールの移行

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 のリソース ルールからポリシーを作成し、移行した PMDB に対応するホスト グループに割り当てます。 また、PMDB のサブスクライバの解除、PMDB の削除、PMDB へのフィルタ ファイルの適用を選択することも可能です。

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 からのリソース ルールの移行方法

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. ユーザ名、パスワードおよび移行させる 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 ページが表示されます。

3. ポリシーの名前とわかりやすい説明を入力し、依存するユーザおよびグループのポリシーを使用してリソース ポリシーを作成することを選択します。

4. ルールをエクスポートする CA Access Control クラスを選択し、矢印を使用して選択したリスト フィールドに移動します。

   注: 特定クラスのリソースを変更するルールをエクスポートするときに、そのクラスのルールが別のクラスのルールに依存している場合、CA Access Control は両方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ます。

5. PMDB のユーザ ルールから作成したユーザ ポリシーの名前を従属ポリシー フィールドに入力するか、または、[...]をクリックして、作成したユーザ ポリシーの名前を選択します。［次へ］をクリックします。

   CA Access Control エンタープライズ管理 によって指定したリソース ルールが PMDB からエクスポートされます。［ポリシー スクリプト］ページが表示されます。

6. エクスポートされたリソース ルールを確認し、[次へ]をクリックします。

   CA Access Control エンタープライズ管理 は、ポリシー スクリプトを使用して、指定したユーザー ポリシーに依存する POLICY オブジェクトを作成します。［ホスト グループ］ページが表示されます。

7. 既存のホスト グループを選択し、[...]をクリックして移行した PMDB に対応するホスト グループの名前を選択します。

8. ［割り当てられたホスト］セクション中のホストのリストが、移行された PMDB のサブスクライバに一致することを確認し、[次へ]をクリックします。

   重要: CA Access Control は、このページで指定するホストおよびホスト グループにポリシーをデプロイします。 正しいホストおよびホスト グループを選択していることを確認してから、[次へ]をクリックします。

   CA Access Control エンタープライズ管理 は、ホストグループにポリシーを割り当てます。［オプション］ページが表示されます。

9. 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。

   選択したホストのサブスクライブを解除

   前画面で選択したエンドポイントによる移行 PMDB へのサブスクライブが解除されます。

   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 ファイルをリモートで追加

   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。

10. ［次へ］をクリックします。

    ［サマリ］ページが表示されます。 これで移行処理は完了です。

詳細情報:

ポリシーの作成と割り当て方法 (297 ページ)

クラスの依存関係

PMDB のルールをエクスポートする際、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。 特定クラスのリソースを変更するルールをエクスポートするように指定した場合、CA Access Control は以下に示すように、依存クラス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。

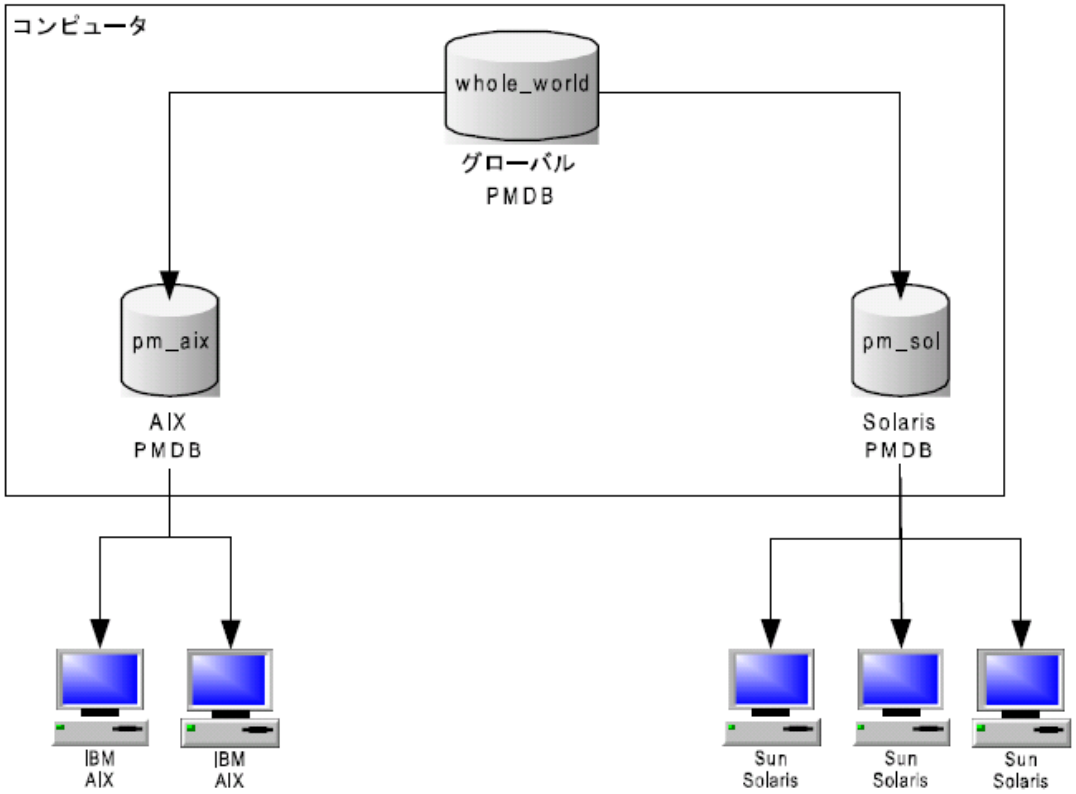
PMD 階層をフラット化した場合、各 PMDB を個別に移行します。 移行中、CA Access Control は階層環境にある各 PMDB に対応するホスト グループを作成します。各エンドポイントは、サブスクライブしていた PMDB に対応するすべてのホスト グループに追加されます。

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。

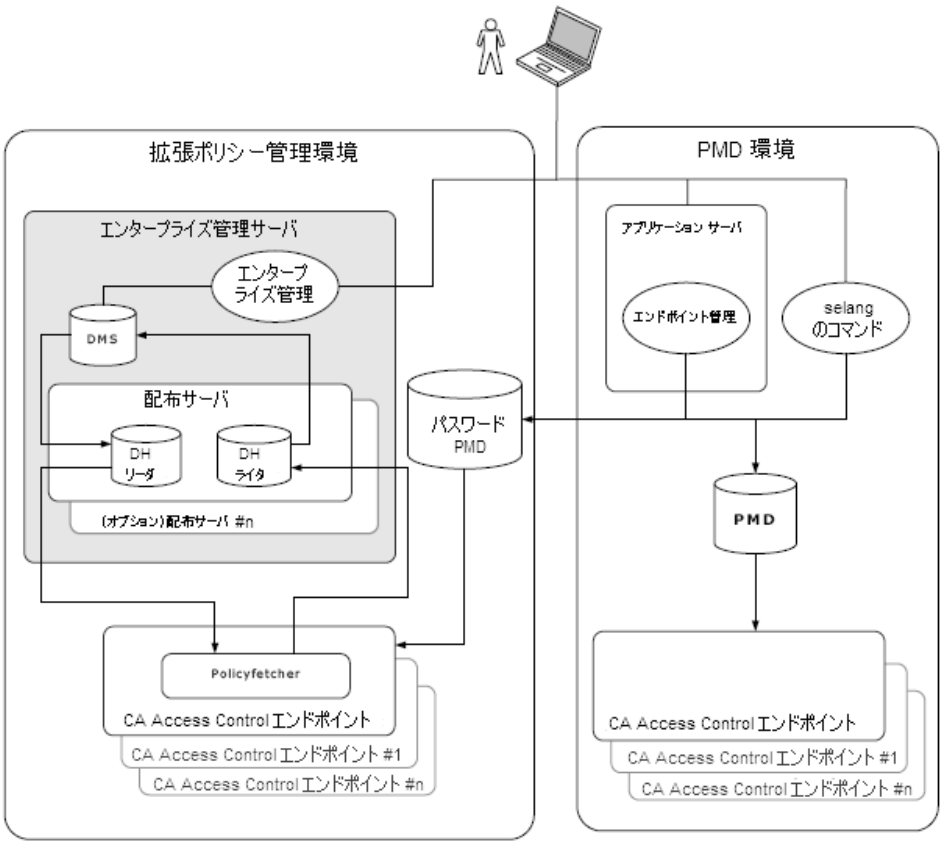
注: pm_aix PMDB にフィルタ ファイルを適用すると、whole_world PMDB からデプロイされたルールを IBM AIX エンドポイントで受信できなくなる場合があります。 拡張ポリシー管理環境では、IBM AIX エンドポイントは whole_world ホスト グループのメンバです。 whole_world ホスト グループにデプロイするすべてのルールは、フィルタされずにすべてのエンドポイントにデプロイされます。 拡張ポリシー管理環境でルールをデプロイする場合、この動作の変更に注意する必要があります。

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詳細ポリシー管理環境に定義されてる CA Access Control デプロイです。

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、詳細ポリシー管理環境で定義することもできます。 たとえば、詳細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 selang ルールを同じエンドポイントに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。

第 12 章: CA Access Control r12.0 SP1 の CA Access Control r12.5 へのアップグレード

このセクションには、以下のトピックが含まれています。

CA Access Controlr12.5 へのアップグレード

この章では、既存の CA Access Control r12.0 SP1 を CA Access Control r12.5 にアップグレードする手順について説明します。 この章のアップグレード処理では、ユーザが 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、CA Access Control エンタープライズ管理 が 1 台のコンピュータにインストールされ、DMS、DH、レポート サーバもそれぞれ別々のコンピュータにインストールされているものとします。

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: CA Access Control エンタープライズ管理 r12.5 へのアップグレードは、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 CA Access Controlr12.5 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 r12.5 へのアップグレードは、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。
- 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、CA Access Control エンタープライズ管理、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。
- CA Access Control エンタープライズ管理 r12.5 にアップグレードした後に、前の DMS は利用不可能になります。 サーバを開始する前に CA Access Control エンタープライズ管理、DMS および DH をアップグレードする必要があります。
- 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 ストアを使用することをお勧めします。

  重要: 組み込みユーザ ストアへの CA Access Control エンタープライズ管理 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。 Active Directory のインストールを選択した場合、既存ユーザおよびロールのレコードがすべて失われます。

CA Access Control r12.5 へのアップグレード方法

CA Access Controlr12.0 SP1 から CA Access Control r12.5 へのアップグレードを開始する前に、既存の CA Access Control r12.0 SP1 をアップグレードするために完了する必要のある手順を確認することをお勧めします。

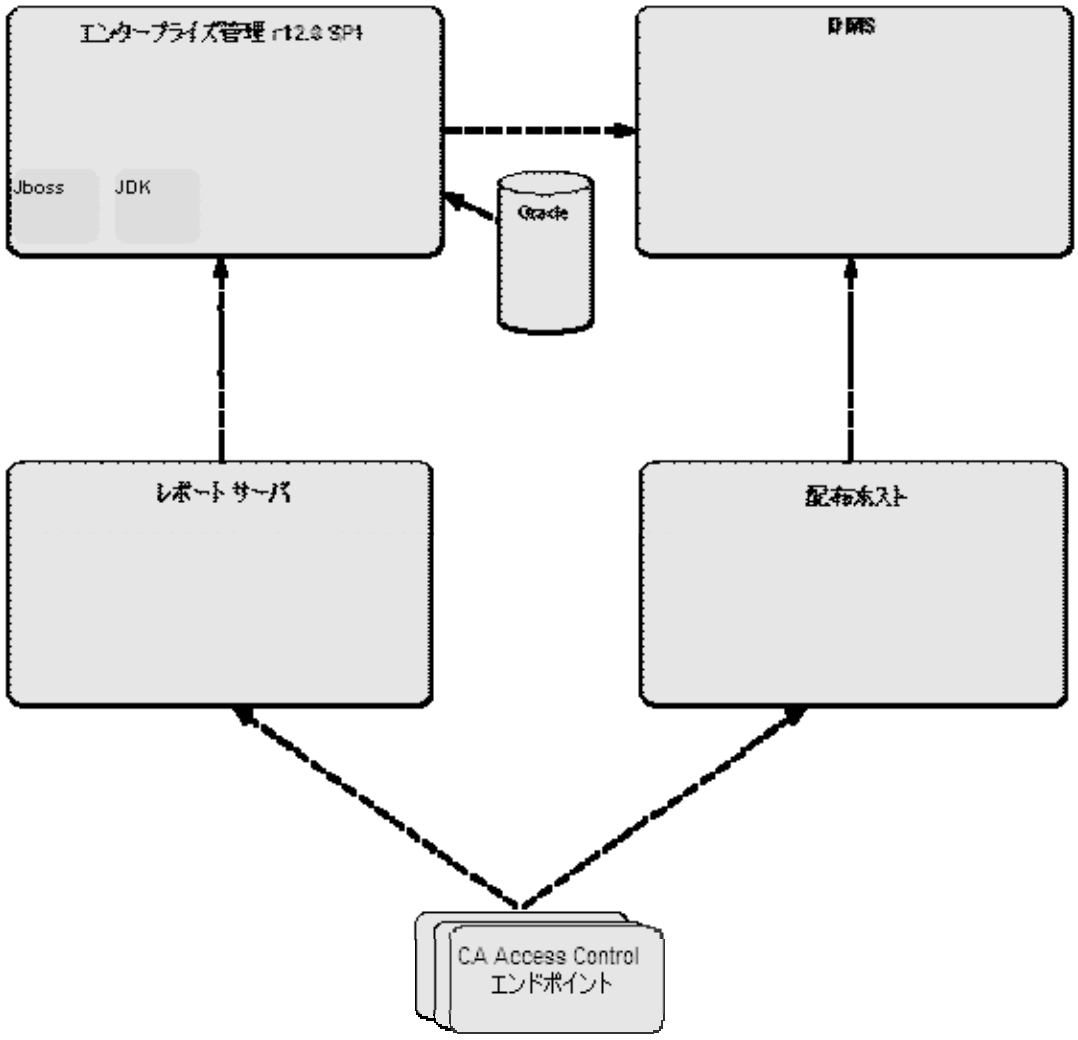
1. CA Access Control エンタープライズ管理 をアップグレードします。
    a. CA Access Control エンタープライズ管理 r12.0 SP1、JBoss および JDK をアンインストールします。
    b. 必須インストーラを使用して、JDK 1.5.0 および JBoss 4.2.3 をインストールします。
    c. CA Access Control エンタープライズ管理 をインストールします。
2. DMS コンピュータをアップグレードします。

    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。
3. DH コンピュータをアップグレードします。

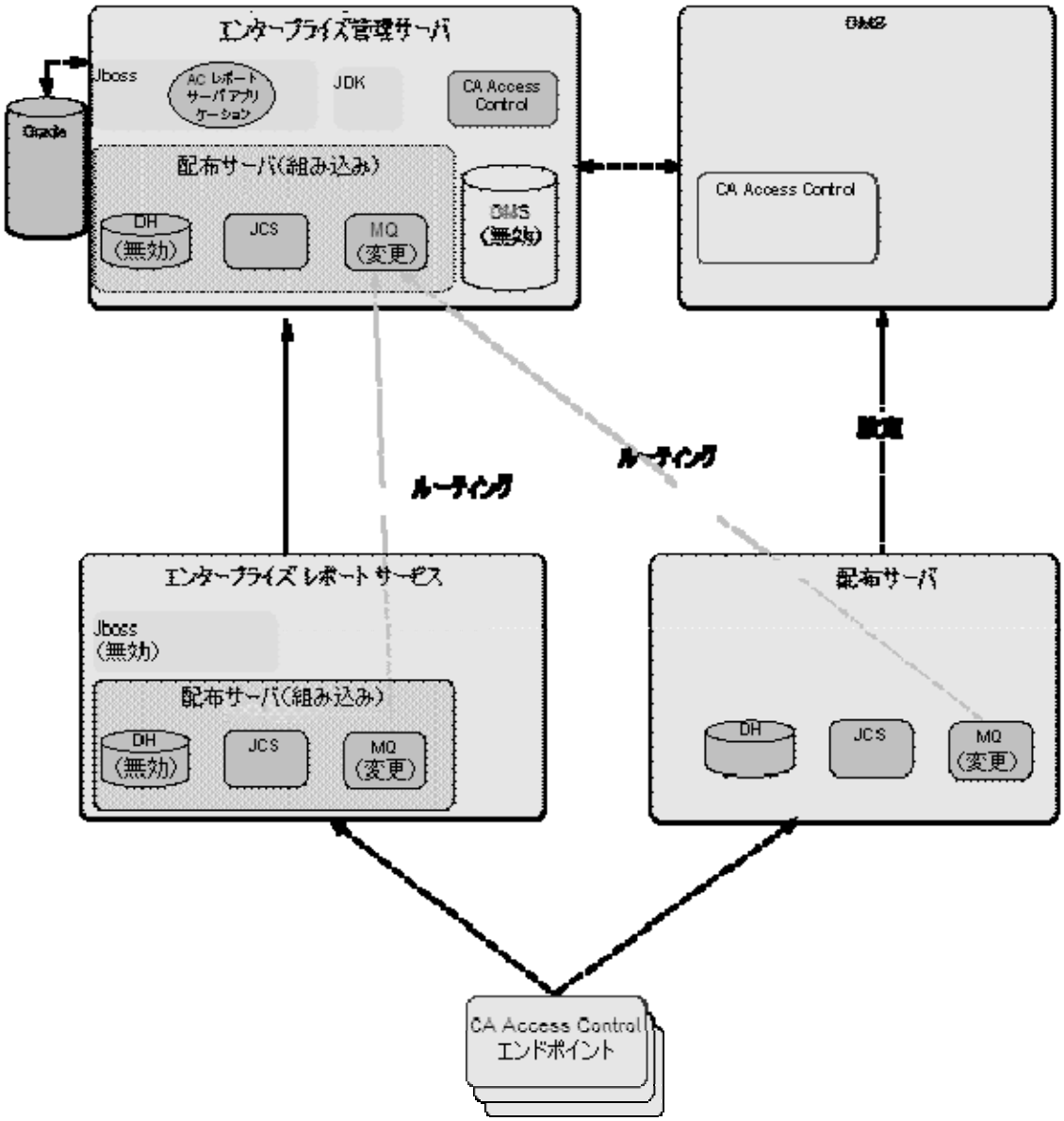
    注: 組織内のすべての DH をアップグレードする必要があります。 DH が CA Access Control エンタープライズ管理 と同じコンピュータにインストールされている場合、この手順を完了する必要はありません。
4. メッセージ キュー(MQ)ルート設定を定義します。
5. レポート サーバをエンタープライズ レポーティング サービスへ移行します。
6. DH を新しい DMS へサブスクライブします。
7. (オプション)CA Access Control をエンドポイントへインストールします。

CA Access Control のアップグレード プロセス

以下の図は、アップグレード前の、CA Access Control r12.0 SP1 展開アーキテクチャの例を示しています。



以下の図は、r12.5 へアップグレード後の、CA Access Control の展開の例を示しています。



CA Access Control エンタープライズ管理 のアップグレード

この手順では、CA Access Control エンタープライズ管理 のアップグレード手順、および CA Access Control エンタープライズ管理 のアップグレードを完了するのに必要な、インストール後の手順の詳細について説明します。

CA Access Control エンタープライズ管理 のアップグレード方法

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 (50 ページ)。
4. CA Access Control エンタープライズ管理 をインストールします (51 ページ)。

   CA Access Control エンタープライズ管理 で、以下もインストールします。

   - CA Access Control r12.5。
   - 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 (55 ページ)。
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: CA Access Control エンタープライズ管理 r12.5 へアップグレード後、既存の DMS は使用できなくなります。 CA Access Control エンタープライズ管理 r12.5 のインストール後に DMS をアップグレードします。 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。

   CA Access Control エンタープライズ管理 r12.5 がインストールされます。 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。

DMS のアップグレード

CA Access Control エンタープライズ管理 r12.5 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 r12.5 をインストールします (79 ページ)。

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。

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)をアップグレードする必要があります。 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する必要があります。

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 (271 ページ)。

   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 (283 ページ)を定義します。

   これで、配布サーバが設定されます。

DH の新しい DMS へのサブスクライブ

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。

DH を新しい DMS にサブスクライブする方法

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。

   例: 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。

   例: sepmd -s DMS__ DH__@<host_name>
4. CA Access Control エンタープライズ管理 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。

   例: 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。

レポート サーバのエンタープライズ レポーティング サービスへの移行

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。

レポート サーバのエンタープライズ レポーティング サービスへの移行方法

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(271 ページ)。
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(283 ページ)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(203 ページ) コンポーネントを設定できます。
4. DH を新しい DMS へサブスクライブします(316 ページ)。

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 r12.5 へ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 CA Access Control r12.5 に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 r12.5 をエンドポイントにインストールします(79 ページ)。

メッセージ ルーティングの設定方法

CA Access Control エンタープライズ管理 の単一のインスタンスおよび複数の配布サーバで構成される環境で作業する場合、CA Access Control エンタープライズ管理上の MQ をポイントするように、すべての配布サーバ上の MQ ルーティング設定を構成する必要があります。 これによって、CA Access Control エンドポイントが送信するすべてのメッセージが最終的に、CA Access Control 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 CA Access Control 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。
  - CA Access Control エンタープライズ管理 メッセージ キューへのルーティングを変更します。
  - CA Access Control エンタープライズ管理 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。
  - CA Access Control エンタープライズ管理 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。
- CA Access Control エンタープライズ管理 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。
  - 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。
  - CA Access Control エンタープライズ管理 メッセージ キューの名前を設定します。
  - CA Access Control エンタープライズ管理 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 Server User's Guide」を参照してください。

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。
2. 配布サーバ上で、ファイル tibemsd.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。

   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin
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変更します。
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 Server User's Guide」を参照してください。

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。これは
# 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
#######################
```

CA Access Control エンタープライズ管理 上のメッセージ キュー設定の変更

この手順では、CA Access Control エンタープライズ管理 上のメッセージ 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を示します。

CA Access Control エンタープライズ管理 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。
2. CA Access Control エンタープライズ管理 で、編集可能な形式で tibemsd.conf ファイルを開きます。 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。

   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin
3. [サーバ]パラメータに、ドットで区切られない、CA Access Control 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。

   CA Access Control エンタープライズ管理 上でメッセージ 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 Server User's Guide」を参照してください。

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 キュー接続設定 - 例

配布サーバ上の MQ から CA Access Control エンタープライズ管理へ、および CA Access Control エンタープライズ管理 上の MQ から配布サーバにメッセージをルーティングするために、組織内の各配布サーバ上の既存の MQ 設定、および CA Access Control エンタープライズ管理 上の MQ の設定を変更します。

例: 配布サーバ上のメッセージ キュー接続設定の設定

この例では、配布サーバ上のメッセージ キュー サーバ設定の設定方法を示します。CA Access Control エンタープライズ管理 上で実行中のメッセージ キュー サーバのパラメータを定義して、メッセージを CA Access Control エンタープライズ管理 に送る、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 CA Access Control エンタープライズ管理 コンピュータの名前に、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場合、名前を tibemsd.conf ファイルのサーバ トークンで定義されている、サーバの実際の名前に置き換える必要があります。

配布サーバ上のメッセージ キュー接続設定の設定方法

1. 配布サーバ上で、[スタート]-[プログラム]-[TIBCO]-[TIBCO EMS 4.4.1]-[EMS 管理ツールの開始]を選択します。

   [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. メッセージ キューに接続します。 以下のいずれかの操作を行います。

   - 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。

4. プロンプトが表示されたら、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=<dist_server-passwd>

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=
   ```

   例：create user ENTM_Name password=<acserver_user-passwd>

   ENTM-NAME

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   重要：CA Access Control エンタープライズ管理 コンピュータ上の tibemsdf.conf ファイルの[サーバ]パラメータで定義した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. 変更を有効にするために、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: CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定の設定

この例では、CA Access Control エンタープライズ管理 上のメッセージ キュー サーバ設定の設定方法を示します。 配布サーバにメッセージを送信するために、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 CA Access Control エンタープライズ管理 コンピュータの名前に、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場合、名前を tibemsd.conf ファイルの[サーバ]トークンで定義されている、サーバの実際の名前に置き換える必要があります。

CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定の設定方法

1. CA Access Control エンタープライズ管理 コンピュータ上で、[スタート]-[プログラム]-[TIBCO]-[TIBCO EMS 4.4.1]-[EMS 管理ツールの開始]を選択します。

   [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. メッセージ キューに接続します。 以下のいずれかの操作を行います。

   - 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. 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=
   ```

   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=
   ```

   例: create user DS_SERVER_NAME password=<distserver_user-passwd>

   DS_NAME

   配布サーバの短縮名を定義します。

   重要: CA Access Control エンタープライズ管理 コンピュータ上の tibemsdf.conf ファイルの[サーバ]パラメータで定義したのと同じ名前を指定します。

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。

   CA Access Control エンタープライズ管理 上のメッセージ キュー接続設定を設定しました。

   注: メッセージ ルーティングの詳細については、「TIBCO Enterprise Message Server User's Guide」を参照してください。

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 CA Access Control エンタープライズ管理 へメッセージを転送するには、配布サーバ上のメッセージ キューから CA Access Control エンタープライズ管理 上のメッセージ キューへメッセージを転送するように、各メッセージ ルートを設定します。

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。 CA Access Control エンタープライズ管理 上のメッセージ キューの設定を提供するために、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. 配布サーバ上で、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。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥ACMQ¥tibco¥ems¥bin¥
   ```

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

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   重要: CA Access Control エンタープライズ管理 の tibemsdf.conf ファイルの [サーバ]パラメータで定義した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 Server User's Guide」を参照してください。

CA Access Control エンタープライズ管理 コンピュータ上のメッセージ キューの名前の設定

この手順では、CA Access Control エンタープライズ管理 上のメッセージ 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ために、CA Access Control エンタープライズ管理 上でメッセージ キューの設定を行います。

CA Access Control エンタープライズ管理 コンピュータ上でのメッセージ キューの名前の設定方法

1. CA Access Control エンタープライズ管理 で、編集可能な形式で queues.conf ファイルを開きます。 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。

   ```
   ¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥bin
   ```

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 Server User's Guide」を参照してください。

メッセージ ルート設定 - 例

配布サーバおよび CA Access Control エンタープライズ管理 上でメッセージ キュー設定を設定し、メッセージ キュー ルーティング設定を設定した後に、配布サーバおよび CA Access Control エンタープライズ管理 上でメッセージ ルートをセットアップする必要があります。

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のメッセージを CA Access Control エンタープライズ管理 上のメッセージ キューにルーティングするために、配布サーバと CA Access Control エンタープライズ管理 の間にルートをセットアップします。 組織内のすべての配布サーバ上で、この手順を完了する必要があります。

1. 配布サーバ上で、編集可能な形式でファイル routes.conf を開きます。 このファイルは、デフォルトで、以下のディレクトリにあります。

   ```
   ¥Program Files¥CA¥AccessControlDistServer¥MessageQueue¥tibco¥ems¥bin
   ```

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

   CA Access Control エンタープライズ管理 コンピュータの短縮名を定義します。

   ENTM_URL

   CA Access Control エンタープライズ管理 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。

例: CA Access Control エンタープライズ管理 でのメッセージ ルートのセットアップ

この例では、CA Access Control エンタープライズ管理 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 エンタープライズ管理 から配布サーバへ、配布サーバからエンドポイントへメッセージを送信するために、CA Access Control エンタープライズ管理 と配布サーバの間にルートをセットアップします。

1. CA Access Control エンタープライズ管理 上で、ファイル routes.conf を開きます。このファイルは、デフォルトで、以下のディレクトリにあります。

   ```
   ¥Program Files¥CA¥AccessControlServer¥MessageQueue¥tibco¥ems¥bin
   ```

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 Server User's Guide」を参照してください。