CA Access Control Premium Edition

エンタープライズ管理ガイド

12.6

サードパーティに関する通知

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

サンプル スクリプトおよびサンプル SDK コード

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

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

CA Technologies 製品リファレンス

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

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

例：コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

ファイル ロケーションに関する規則

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

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

CA への連絡先

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

マニュアルの変更点

以下のドキュメントのアップデートは、本書の最新のリリース以降に行われたものです。

- PUPM の実装計画 (P. 133)
  - Connector Xpress の例: SUN ONE エンドポイントの設定 (P. 164) -- Connector Xpress で SUN ONE エンドポイントを設定する方法について説明するトピックの追加
  - Connector Xpress の例: Java コネクタ サーバでの SUN ONE エンドポイントの登録 (P. 166) -- Java コネクタ サーバで SUN ONE エンドポイントを登録する方法について説明するトピックの追加
- 特権アカウントの実装 (P. 181)
  - Sybase Server 接続情報 (P. 205) -- Sybase Server エンドポイント タイプ接続情報に関するトピックの追加
  - VMware ESX/ESXi 接続情報 (P. 208) -- VMWare ESX/ESXi エンドポイント タイプ接続情報に関するトピックの追加
  - エンドポイント CSV ファイルの作成 (P. 242) -- 行を追加するためのトピックの更新
  - 特権アカウント CSV ファイルの作成 (P. 248) -- 行を追加するためのトピックの更新

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

本書は CA Access Control Premium Edition のエンタープライズ管理およびエンタープライズ レポート、ならびに CA Access Control エンタープライズ管理 の Web ベースのインターフェースについて説明します。CA Access Control のエンタープライズ管理およびエンタープライズ レポートには、拡張ポリシー管理、レポート、およびワールドビュー エンタープライズ ビューアが含まれています。

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。

本書の対象読者

本書は、CA Access Control を使用するセキュリティ管理者およびシステム管理者の中でも、以下に示す CA Access Control のエンタープライズ管理機能およびエンタープライズ レポート機能の利用者を対象にしています。

- エンタープライズ ポリシー管理
- エンタープライズ レポート
- 企業のホスト アクセス管理を処理するための Web ベースのインターフェース
- 特権ユーザ パスワード管理(PUPM)

エンタープライズ管理

CA Access Control エンタープライズ管理 は Web ベースのユーザ インターフェースです。これを使用して、組織全体のアクセス関連管理タスクを実行できます。CA Access Control エンタープライズ管理 を使用すると、中央から組織全体へ適用するアクセス ポリシーの作成、個々のホストの管理、特権アカウントの管理、エンタープライズ レポートの作成など、多数の管理タスクを実行できます。

エンタープライズ管理インターフェース

CA Access Control エンタープライズ管理 インターフェースは、組織管理に必要な機能がすべて搭載されているエンタープライズ管理ツールです。CA Access Control エンタープライズ管理 インターフェースの一部であるツールを使用して、ホストの設定、ポリシーの作成および割り当て、ユーザ、グループ、管理タスクの管理、組織全体の特権アカウント アクセスの設定と管理を行うことができます。さらに、エンタープライズ レポートおよび監査機能も使用できます。

中央ポリシー管理

CA Access Control エンタープライズ管理 の中央ポリシー管理能力を使用して、統一されたポリシーを作成し、組織内のホストおよびホスト グループに割り当てます。CA Access Control エンタープライズ管理 インターフェースによって、ウィザードを使用した組織全体へのポリシー割り当てが可能になり、各ホストへのポリシーのデプロイメント プロセスのステータスを表示できます。

さらに、CA Access Control エンタープライズ管理 の中央ポリシー管理能力を使用して、ポリシー デプロイメント プロセスのトラブルシューティング、既存ポリシーの割り当て解除、アップグレード、ダウングレードを行うことができます。

エンタープライズ ビュー

CA Access Control エンタープライズ管理 を使用して、CA Access Control、PUPM、UNAB ホストに関する情報の表示、一元管理を行うことができます。CA Access Control エンタープライズ管理 ワールドビューには、各ホスト タイプ、前回の更新時間、各ホストで設定されているデバイスのタイプが表示され、ホストの設定変更、リモート管理が可能です。

特権ユーザ パスワード管理

特権ユーザ パスワード管理（PUPM）は、組織内の最も強力なアカウントに関連付けられたすべてのアクティビティを保護、管理、追跡するプロセスです。

CA Access Control エンタープライズ管理 は、管理対象デバイス上の特権アカウントに対して、一元的な、ロール ベースのアクセス管理を提供します。CA Access Control エンタープライズ管理 は、特権アカウントおよびアプリケーション ID パスワードの安全なストレージ、およびポリシーに基づいた特権アカウントおよびパスワードへのアクセス制御を提供します。

さらに、PUPM は特権アカウントおよびアプリケーション パスワード ライフサイクルを管理し、環境設定ファイルおよびスクリプトからの任意のパスワードの削除を許可します。

UNAB 管理

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、すべてのユーザが単一のリポジトリを使用して、すべてのプラットフォームに、同じユーザ名とパスワードでログインできることを意味します。

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。これによって、Windows でのユーザおよびグループの管理と同様に、UNIX ユーザおよびグループの一元管理が可能になります。

CA Access Control エンタープライズ管理 のセントラル ポリシー管理機能を使用して、ログイン ルール セットを含むログイン ポリシーを作成し割り当てて、UNIX ホストへのアクセスを制御します。

エンタープライズ レポート

CA Access Control エンタープライズ管理 のレポート オプションを使用すると、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 か所で確認できます。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 は、一度の設定だけで各エンドポイントからデータの収集および中央のサーバへのデータのレポートを独立して実行します。また、手動による操作を必要とせず、エンドポイントのステータスを継続的にレポートします。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。

CA Access Control エンタープライズ管理 には、すぐに使用できる事前定義済みレポート セットが用意されていて、各エンドポイントに関する情報が表示されます。さらに、既存レポートをカスタマイズすることも、独自のレポートを作成することもでき、目的の情報を表示します。

第 2 章: CA Access Control エンタープライズ管理 の管理

このセクションには、以下のトピックが含まれています。

管理スコープ

CA Access Control エンタープライズ管理 では、管理アクセス ロールまたは特権アクセス ロールを割り当てて、ユーザおよび管理者に権限を割り当てます。ロールには、CA Access Control エンタープライズ管理 のアプリケーション機能に対応するタスクが含まれています。

ロールによって、特権の管理が単純化されます。ユーザに実行する各タスクを関連付ける代わりに、ユーザに 1 つのロールを割り当てることができます。ユーザは、割り当てられたロールで、すべてのタスクを実行することができます。次に、タスクを追加して、ロールを編集できます。ロールを持つ各ユーザは、新規タスクを実行できるようになりました。ロールからタスクを削除すると、ユーザはそのタスクを実行できなくなります。

ユーザが CA Access Control エンタープライズ管理 にログインすると、ユーザのロールに応じたタブが表示されます。ユーザに対して表示されるのは、そのロールに割り当てられたタブおよびタスクのみです。

ロールを別々のユーザに割り当てることで、1 ユーザが全タスクを完了できるようになるのを阻止できます。これは、企業が職務分掌要件に準拠するのに役立つ場合があります。しかし、1 ユーザに複数のロールを割り当てることができます。

CA Access Control エンタープライズ管理 の管理ロール

CA Access Control エンタープライズ管理 の定義済み管理ロールは、要件に応じて企業の管理者およびユーザに割り当てることができる基本的なロール セットです。CA Access Control エンタープライズ管理 には、そのまま使用できる以下のような管理ロールが用意されています。

- **CA Access Control ホスト マネージャ** - ホストおよび論理ホスト グループを定義します。

  この管理ロールによって、ユーザはホストおよびホスト グループの作成、ホストのホスト グループへの割り当て、および変更を行うことができます。ポリシーの定義およびデプロイはできませんが、ポリシーの表示、およびワールドビューへのアクセスが可能です。

- **CA Access Control ポリシー デプロイヤ** - 環境全体へのポリシーのデプロイの責任者になります。

  この管理ロールによって、ユーザはポリシーのホストおよびホスト グループへの割り当て、ポリシーのアップグレードおよびダウングレード、ホスト設定のリセット、およびデプロイメント監査へのアクセスを行うことができます。ポリシーおよびホストの表示はできますが、ポリシーおよびホストの定義およびワールドビューへのアクセスはできません。

- **CA Access Control ポリシー マネージャ** - ポリシー作成の責任者になります。

  この管理ロールによって、ポリシーの作成、変更、表示、削除を行うことができます。管理ロールでは、ホストまたはホスト グループにポリシーをデプロイできませんが、ユーザはポリシーを表示し、ワールドビューにアクセスできます。

- **CA Access Control ユーザ マネージャ** - CA Access Control エンタープライズ管理 のユーザ管理責任者になります。ユーザおよびグループの作成および管理、CA Access Control エンタープライズ管理 ロールのユーザへの割り当てを行います。

  注: CA Access Control ユーザ マネージャは、管理ロールを新規作成できません。システム マネージャのみが新しい管理ロールを作成できます。

- **システム マネージャ** - CA Access Control エンタープライズ管理 の管理責任者になります。

  この管理ロールを持つユーザは、CA Access Control エンタープライズ管理 内のすべてのタスクを実行、作成、管理できます。

  このロールは、組織内の実際の管理ロールを定義するために実装フェーズで、または緊急時に使用します。このロールを割り当てるのは最小数のユーザ(理想的には 1 ユーザのみ)とし、そのユーザのアクションを注意深く監視することをお勧めします。

- **レポート** - 英語版レポートの管理責任者になります。このロールが割り当てられたユーザはレポートをスケジュールおよび表示できます。

- **UNAB 管理者** - UNAB の管理を担当します。このロールが割り当てられたユーザは、UNAB ホストおよびホスト グループを設定し、ログイン認可ポリシーを管理し、移行競合を解決できます。

  注: システム マネージャ ロールが割り当てられたユーザには、UNAB 管理者ロールも割り当てられます。

- **CA Enterprise Log Manager ユーザ** - CA Enterprise Log Manager レポートの表示を担当します。このロールが割り当てられたユーザは CA Enterprise Log Manager レポートを表示できます。

- **CA Enterprise Log Manager 管理者** - CA Enterprise Log Manager レポートの管理責任者になります。このロールが割り当てられたユーザは、CA Access Control エンタープライズ管理 の CA Enterprise Log Manager レポートを管理し、CA Enterprise Log Manager サーバへの接続を管理できます。

- **委任マネージャ** - 作業アイテムの委任を担当します。このロールが割り当てられたユーザは、作業アイテムをユーザに委任できます。

- **自己マネージャ** - 自身のユーザ アカウントの管理責任者になります。このロールが割り当てられたユーザは、自分のアカウントで管理アクションを実行できます。これには、アカウント パスワードの変更、ユーザ プロファイルの修正、割り当てられたロール、サブミットされたタスク、および承認待ちのアイテムの表示が含まれます。

  注: デフォルトでは、システムでのすべてのユーザに自己マネージャ ロールが割り当てられます。

管理ロールの作成

CA Access Control エンタープライズ管理 内の事前定義済み管理ロールが組織の要件に適していない場合は、新規管理ロールを作成できます。

管理ロールを作成する方法

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. ［ユーザおよびグループ］をクリックします。
   b. ［ロール］サブタブをクリックします。
   c. 左側のタスク メニューで［管理ロール］ツリーを展開します。
      ［管理ロールの作成］タスクが使用可能なタスク リストに表示されます。
2. ［管理ロールの作成］をクリックします。
   ［管理ロールの作成：管理ロールの選択］ページが表示されます。
3. （オプション）既存の管理ロールを選択して、新規管理ロールをそのコピーとして、以下のように作成します。
   a. ［ロールのコピーの作成］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管理ロールのリストが表示されます。
   c. 新規管理ロール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。
   ［管理ロールの作成］タスク ページが表示されます。管理ロール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［プロファイル］タブにある、以下のフィールドに入力します。

   名前

   ロールの名前を定義します。

   説明

   テキストによるロールの説明です。

   有効

   ロールをユーザおよびグループに割り当て可能かどうかを指定します。

6. 以下のようにして、タスクをロールに追加します。
   a. [タスク]タブをクリックします。
   b. (オプション) [タスクのフィルタ]ドロップダウン リストから、タスク カテゴリを選択します。

      このカテゴリのタスクがロードされます。

      注: タスク カテゴリは、このカテゴリのタスクが CA Access Control エンタープライズ管理 に表示されるタブに一致します。
   c. [タスクの追加]ドロップダウン リストからタスクを選択します。

      タスクがロールに追加されます。
   d. b から c までの手順を繰り返して、更にタスクをロールに追加します。
7. メンバおよびスコープ ルールを追加します (P. 29)。
8. [サブミット]をクリックします。

   ロールが作成されます。

特権アクセス ロール

CA Access Control エンタープライズ管理 の特権的アクセスロールは、要件に応じて、企業の管理者およびユーザに割り当てることができるロールの基本的なセットを提供します。CA Access Control エンタープライズ管理 には、そのまま使用できる以下のような特権アクセス ロールが用意されています。

- **Break Glass** - このロールが割り当てられたユーザは、Break Glass 特権アカウント パスワードのチェックアウトを実行できます。Break Glass チェックアウトを実行すると、特権アクセスが割り当てられていないエンドポイントに即座にアクセスできます。このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- **エンドポイント特権アクセス ロール** - このロールが割り当てられたユーザは、指定されたエンドポイント タイプ 上で特権アカウント タスクを実行できます。新しいエンドポイント タイプを初めて定義すると、CA Access Control は対応するエンドポイント特権アクセス ロールを作成します。たとえば、CA Access Control エンタープライズ管理 で Windows エンドポイントを初めて作成すると、CA Access Control は Windows エージェントレス接続エンドポイント特権アクセス ロールを作成します。

- **特権アカウント リクエスト** - このロールが割り当てられたユーザは、特権アカウント パスワードのリクエストをサブミットまたは削除できます。 このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- **PUPM 承認者** - このロールが割り当てられたユーザは、CA Access Control エンタープライズ管理 ユーザがサブミットした特権アカウント リクエストに応答できます。このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- **PUPM 監査マネージャ** - この特権アカウント ロールが割り当てられたユーザは、特権アカウント アクティビティの監査および CA Enterprise Log Manager 監査収集パラメータの管理を行うことができます。
- **PUPM ポリシー マネージャ** - このロールが割り当てられたユーザは、ロール メンバとメンバ ポリシーの管理、ロール所有者の割り当て、およびロールの作成と削除を行うことができます。
- **PUPM ターゲット システム マネージャ** - このロールが割り当てられたユーザは、パスワード ポリシーと特権アカウントを管理でき、さらに特権アカウント検出ウィザードを使用してエンドポイント上の特権アカウントを検出できます。
- **PUPM ユーザ** - このロールが割り当てられたユーザは、使用が許可されている特権アカウント パスワードをチェックインおよびチェックアウトできます。このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- **PUPM ユーザ マネージャ** - このロールが割り当てられたユーザは、CA Access Control エンタープライズ管理 ユーザ、グループ、およびパスワード ポリシーを管理し、ユーザの作業アイテムを管理できます。

特権アクセス ロールをユーザに割り当てる場合は、以下のことに注意してください。

- 特権アカウント リクエストに応答するには、PUPM 承認者ロールを持っており、かつ要求ユーザのマネージャである必要があります。
- ユーザが Break Glass、特権アカウント リクエスト、または PUPM ユーザ ロールを持っているが、エンドポイント特権アクセス ロールを持っていない場合、そのユーザはどのエンドポイントにもアクセスできません。 つまり、そのユーザは事実上タスクを実行できません。
- エンドポイント特権アクセス ロールを持っているが、他のロールを持っていない場合、ユーザはどのタスクも実行できません。

特権アクセス ロールの作成

特権アクセス ロールは、<pump> の使用時に、ロール メンバ、管理者、所有者が実行できるタスク、たとえば、特権アカウントのチェックインおよびチェックアウトを定義します。CA Access Control エンタープライズ管理 内の事前定義済み特権アクセス ロールが組織の要件に適していない場合は、新規ロールを作成できます。

特権アクセス ロールの作成方法

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. [ユーザおよびグループ]をクリックします。
   b. [ロール]サブタブをクリックします。
   c. 左側のタスク メニューで[特権アクセス ロール]ツリーを展開します。

      [特権アクセス ロールの作成]タスクが使用可能なタスク リストに表示されます。
2. [特権アクセス ロールの作成]をクリックします。

   [ロールの作成: 特権アクセス ロールの選択]ページが表示されます。
3. (オプション)既存の特権アクセス ロールを選択して、新規ロールをそのコピーとして、以下のように作成します。
   a. [ロールのコピーの作成]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特権アクセス ロールのリストが表示されます。
   c. 新規特権アクセス ロール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。

   [管理ロールの作成]タスク ページが表示されます。管理ロール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[プロファイル]タブにある、以下のフィールドに入力します。

   名前

   ロールの名前を定義します。

   説明

   テキストによるロールの説明です。

   有効

   ロールをユーザおよびグループに割り当て可能かどうかを指定します。

6. 以下のようにして、タスクをロールに追加します。
   a. [タスク]タブをクリックします。
   b. (オプション)[タスクのフィルタ]ドロップダウン リストから、タスク カテゴリを選択します。

      このカテゴリのタスクがロードされます。

      注: タスク カテゴリは、このカテゴリのタスクが CA Access Control エンタープライズ管理 に表示されるタブに一致します。

   c. [タスクの追加]ドロップダウン リストからタスクを選択します。

      タスクがロールに追加されます。

   d. b から c までの手順を繰り返して、更にタスクをロールに追加します。
7. メンバおよびスコープ ルールを追加します (P. 29)。
8. [サブミット]をクリックします。

   ロールが作成されます。

ロールのユーザへの割り当て方法

以下の方法を使用して、ロールをユーザに割り当てることができます。

- 複数のユーザをロールに追加、またはロールから削除するには、[ロール メンバ/管理者の変更]タスクを使用します。
- 単一ユーザへのロールの追加、または単一ユーザからのロールの削除を行うには、[ユーザの変更]タスクで[管理ロール]タブまたは[特権アクセス ロール]タブを使用します。
- ロールのメンバ ポリシーの変更は、[管理ロールの変更]タスクで[メンバ]タブ、または[特権アクセス ロールの変更]タブを使用します。

管理ロールへのユーザの追加方法

管理ロールを作成したら、そのロールにメンバおよび管理者を追加できます。ロールのメンバであるユーザは、そのロールから発生する権限を割り当てます。ロールにメンバを追加するには、あらかじめ以下の手順を行う必要があります。

1. 管理ロールのメンバ ポリシー定義を変更して、このルールのメンバを定義します。

   ロールのメンバ ポリシーを変更すると、変更対象のロールに他のロールのメンバであるユーザを追加できます。

   例: *where Logon Name = "Administrator" or Admin roles = "SystemManager"*

2. 管理者がこのロールに対してメンバを追加または削除できることを確認します。

3. ユーザがこのロールに追加される、またはこのロールから削除されるときに発生するアクションを定義します。

   例: *Add SystemManager to Admin Roles, Remove SystemManager from Admin Roles*.

4. 管理ポリシーを変更して、管理ルールでユーザを管理者としてこのロールに追加し、そのユーザに管理者特権を割り当てます。

   ロール管理者として割り当てたユーザには、このロールにメンバを追加する権限が付与されます。

   これで、メンバをこのロールに追加できます。

メンバおよびスコープのルールの追加

ロールのプロファイルおよびタスクを定義したら、メンバ、管理者、および所有者を追加します。

メンバおよびスコープのルールの追加方法

1. [メンバ] タブをクリックし、以下の操作を行います。
   a. ［追加］をクリックします。
   b. メンバ ポリシー (P. 31)のメンバ ルールとスコープ ルールを指定し、［OK］をクリックします。
   c. （オプション）［管理者の追加］で、このロールのメンバを追加または削除し、［アクションの追加］および［アクションの削除］ (P. 32)を指定できます。

   ロール用のメンバ ポリシーが作成されます。
2. [管理者] タブをクリックし、以下の操作を行います。
   a. ［追加］をクリックします。
   b. 管理ルールとスコープ ルールを指定し、管理ポリシー (P. 32)の管理者特権を指定して、［OK］をクリックします。
   c. （オプション）［管理者の選択］で、このルールの管理者を追加または削除し、［アクションの追加］および［アクションの削除］ (P. 32)を指定できます。

   ロール用の管理ポリシーが作成されます。
3. ［所有者］タブをクリックし、［追加］をクリックし、所有者ルール (P. 32)を指定し、［OK］をクリックします。

   ポリシー用の所有者ルールが作成されます。

メンバ ポリシー

*メンバ ポリシー*は、ロール内のタスクを実行できるユーザを定義します。メンバ ポリシーには、以下が含まれています。

- **メンバ ルール** - ロールを実行できるユーザを定義します。
- **スコープ ルール** - ユーザが管理できるオブジェクトを定義します。

たとえば、管理ロール、接続、特権アカウント、およびポリシーはすべてオブジェクトです。 スコープ ルールにはこれ以外にも多くのオブジェクトを指定できます。各メンバ ポリシーは複数のメンバ ルールを持つことができ、各メンバ ルールは複数のスコープ ルールを持つことができます。

例: ニューヨークの CA Access Control ホスト マネージャ用のメンバ ポリシー

Don Hailey は、Forward, Inc の IT マネージャで、「システム マネージャ」管理ロールを持っています。Don は、New York の CA Access Control「ホスト マネージャ」管理ロールを持つ従業員が Forward, Inc の New York 事務所のみのホストおよびホスト グループを管理できる管理ロールを作成したいと考えています。New York の従業員は全員 NY 従業員グループのメンバで、New York のホストおよびホスト グループの名前はすべて「NY」で始まります。

Don は以下のメンバ ポリシーを作成します。メンバ ポリシーには、2 つのメンバ ルールが含まれている。最初のメンバ ルールには、スコープ ルールが含まれていない。2 番目のメンバ ルールには、2 つのスコープ ルールが含まれている。

- メンバ ルール 1 - 管理ロールに "AC ホスト マネージャ" が含まれている。
- メンバ ルール 2 - グループ "NY 従業員" のメンバであるユーザ。スコープ ルール - 名前が "NY" で始まるホスト、および名前が "NY" で始まるホスト グループ。

アクションの追加および削除

管理ロールの管理者がそのロールへのユーザの割り当ておよびそのロールからのユーザの割り当て解除をできるように指定する場合、その管理ロールのアクションの追加および削除を指定する必要があります。

アクションの追加および削除には、以下が含まれます。

- **アクションの追加** - ロールのメンバ ルールのいずれかで、ユーザが必ず条件に一致するようにします。
- **アクションの削除** - ロールのメンバ ルールのいずれかで、ユーザが必ず条件に一致しないようにします。

管理ポリシー

*管理ポリシー*は、管理ロールの管理者であるユーザを指定します。管理ロールの管理者は管理ロールのメンバ ポリシーを管理し、管理ロールへのユーザとグループの追加および管理ロールからのユーザとグループの削除を行います。

管理ポリシーには、以下が含まれます。

- **管理ルール** - ロールの管理者であるユーザを定義します。
- **スコープ ルール** - 管理者が管理可能なユーザを定義します。
- **管理者権限** - 管理者がその管理ロールのメンバおよび管理者を管理できるかどうかを指定します。

ロール所有者

ロール管理者は、管理ロールへのタスクの追加および管理ロールからのタスクの削除を行います。定義できる所有者ルールは 1 つのみですが、そのルール内で、異なるグループのメンバを指定できます。

管理タスクの作成

CA Access Control エンタープライズ管理 内の事前定義済み管理タスクがユーザの組織要件に適していない場合、新しい管理タスクを作成できます。

管理タスクの作成方法

1. [ユーザおよびグループ]タブを選択し、[タスク]リンクを選択し、[管理タスクの作成]をクリックします。

   [管理タスクの作成: 管理タスクの選択]ページが表示されます。

2. [新規管理タスクの作成]を選択し、[OK]をクリックします。

   [管理タスクの作成]ページの[プロファイル]タブが表示されます。

   注: 既存の管理タスクのコピーを作成するには、[管理タスクのコピーの作成]を選択し。コピーする管理タスクを検索し、管理タスクを選択し、[OK]をクリックします。

3. [タスク名]および[説明]に入力します。 フィールドにカーソルを合わせると、名前が[タグ]フィールドに表示されます。
4. メニューのタスク リストで、タスクの位置を選択します。
5. このタスクが属するカテゴリを選択します。
6. (オプション) 最大 3 タスクまで、順序およびカテゴリ名を選択します。
7. このタスクが属するプリマリ オブジェクトを選択します。プライマリ オブジェクトは、このタスクが属する可能性のある最上位のカテゴリです。
8. タスクに関連付けるアクションを選択します。
9. ユーザおよびアカウントをタスクと同期する場合に選択します。
10. 以下のいずれかのオプションを選択します。

    メニューで非表示

    タスクを表示しない場合に選択します。

    パブリック タスク

    タスクをすべてのユーザが利用できるようにする場合に選択します。

    監査の有効化

    このタスクの監査イベントのログ記録を有効にする場合に選択します。

    ワークフローの有効化

    ワークフローを有効にする場合に選択します。

Web サービスの有効化

Web サービスを使用したタスクへのアクセスを有効にする場合に選択します。

ワークフロー プロセス

タスクに関連付けるワークフロー プロセスを選択します。

11. タスクの優先度を選択します。
12. [サブミット]を選択します。

CA Access Control エンタープライズ管理 は管理タスクを作成します。

詳細情報:

検索画面の追加 (P. 34)
タブの追加 (P. 35)
フィールド、イベントおよびロール使用の設定 (P. 35)

検索画面の追加

このタスクに関連付ける検索画面を選択します。このタブで、このタスクの既存の検索画面を選択するか、このタスク専用の検索オプションの情報を表示し、実際に提供する新規検索画面を作成するか、選択できます。

検索画面の追加方法

1. [参照]ボタンを選択して既存の検索画面を検索するか、新規検索画面を作成します。

   注: 既存の検索画面のコピーを作成するには、[別のタスクからのスコープのコピー]を選択し。コピーする管理タスクを検索し、管理タスクを選択し、[OK]をクリックします。
2. 新しい検索画面を作成するには、[新規]をクリックします。
3. 作成する検索画面のタイプを選択します。
4. 必要な情報を入力して、[OK]をクリックします。

   新規検索画面がタスクに追加されます。

タブの追加

［タブ］画面を使用して、このタスクで使用するタブ コントローラ、およびこのタスクで表示するタブを選択します。

タブの追加方法

1. このタスクで使用するタブ コントローラを選択します。

   注: 既存のタブ定義のコピーを作成するには、［別のタスクからのタブのコピー］を選択し。コピーする管理タスクを検索し、管理タスクを選択し、［OK］をクリックします。

2. メニューからのこのタスクで表示されるタブを選択します。
3. ［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 は新しいタスクにタブを追加します。

フィールド、イベントおよびロール使用の設定

フィールド、イベントおよびロール使用はタブを使用し、タスクがアクセスするフィールド、タスクが関連付けられているイベント、およびタスクが表示されるユーザ ロールに関する情報を表示します。これらのフィールドに表示される情報は変更できません。

設定を変更すれば、これらのタブに表示される情報を変更できます。たとえば、このタスクが表示される管理ロールを変更するには、管理ロールの設定を変更して、このタスクを含めるか除外します。

ユーザ、グループおよび管理ロール

ユーザを作成する場合、ユーザに 1 つ以上の *管理ロール*または*特権的アクセス ロールを割り当てます*。管理ロールには、CA Access Control エンタープライズ管理 内のアプリケーション機能に対応するタスクが含まれています。管理ロールをユーザに割り当てると、そのユーザは管理ロールに含まれているタスクを実行できます。タスクによってユーザは、ポリシーの作成およびデプロイ、ホスト グループの作成、他のユーザの管理などの CA Access Control 機能を実行できます。

特権アクセス ロールは、管理対象エンドポイント上の特権アカウント管理に対応するタスクを定義します。特権アクセス ロールをユーザに割り当てる場合、そのユーザは特権アカウント パスワードのチェックインおよびチェックアウトなどの特権アカウント管理タスクを実行できます。

管理をより容易にするために、ユーザ グループを作成し、グループに管理ロールを割り当てることができます。これにより、グループ内のユーザはそれぞれ、その管理ロール内の全タスク完了できます。

詳細情報:

ユーザの作成 (P. 38)
グループのタイプ (P. 42)

Active Directory の制限事項

Active Directory をユーザ ストアとして使用する場合は、CA Access Control エンタープライズ管理 でユーザとグループを作成および削除できません。以下のタスクはインターフェースに表示されず、管理ロールまたは特権アクセス ロールに割り当てることができません。

- ユーザの作成
- ユーザの削除
- ロール メンバ/管理者の変更
- グループの作成
- グループの削除

Active Directory ユーザに管理ロールを割り当てると、CA Access Control エンタープライズ管理 はユーザ プロファイルを変更し、このユーザに割り当てられた管理ロールを登録されたアドレス フィールドに記録します。

注: [ユーザ DN:]パラメータに、読み取り専用権限を持ったユーザを定義できます。ただし、読み取り専用権限を持ったユーザを定義する場合、CA Access Control エンタープライズ管理でユーザに管理ロールまたは特権アクセス ロールを割り当てることはできません。代わりに、Active Directory グループを指すように各ロールのメンバ ポリシーを変更します。

ユーザの作成

ユーザは、CA Access Control エンタープライズ管理 内のタスクを実行します。CA Access Control エンタープライズ管理 のインストール時にシステム マネージャ ロールでユーザを作成します。CA Access Control エンタープライズ管理 を開始して職務分掌を実行する際に、追加ユーザを作成します。

注: Active Directory をユーザ ストアとして使用する場合は、CA Access Control エンタープライズ管理 でユーザを作成できません。

ユーザの作成方法

1. CA Access Control エンタープライズ管理 内で、[ユーザおよびグループ]をクリックします。

   [ユーザの作成]タスクが使用可能なタスクリストに表示されます。

2. [ユーザの作成]をクリックします。

   [ユーザの作成: ユーザの選択]ウィンドウが表示されます。

3. (オプション)既存のユーザを選択して、新規ユーザをそのコピーとして、以下のように作成します。

   a. [ユーザのコピーの作成]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ユーザのリストが表示されます。

   c. 新規ユーザ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。

   [ユーザの作成]タスク ページが表示されます。既存のオブジェクトからユーザを作成した場合、ダイアログ ボックスのフィールドにはすでに既存オブジェクトの値が入力されています。

5. [プロファイル]タブでフィールドにデータを入力します。以下のフィールドには、説明が必要です。

   ユーザ ID

   CA Access Control エンタープライズ管理 に対してユーザを識別する文字列を定義します。これは、ログインに使用されるユーザ名です。

   パスワードの変更が必要

   最初のログイン時にユーザに強制的にパスワードを変更させるように指定します。

   有効

   ユーザが CA Access Control エンタープライズ管理 にログインできるかどうかを指定します。

6. (オプション)[管理ロール]タブをクリックして、以下のように、管理ロールをユーザに割り当てます。

   a. [管理ロールの追加]をクリックします。

      [管理ロールの選択]セクションが表示されます。

   b. 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ロールのリストが表示されます。

   c. ユーザに割り当てる管理ロールを選択し、[選択]をクリックします。

   管理ロールがユーザに割り当てられます。

7. (オプション)[特権アクセス ロール]タブをクリックして、以下のように、特権アクセス ロールをユーザに割り当てます。

   a. [特権アクセス ロールの追加]をクリックします。

      [特権アクセス ロールの選択]セクションが表示されます。

   b. 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ロールのリストが表示されます。

   c. ユーザに割り当てる特権アクセス ロールを選択し、[選択]をクリックします。

   特権アクセス ロールがユーザに割り当てられます。

8. (オプション) [グループ]タブをクリックして、以下のように、グループにユーザを追加します。
   a. [グループの追加]をクリックします。
      [グループの選択]セクションが表示されます。
   b. 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グループのリストが表示されます。
   c. ユーザに割り当てるグループを選択し、[選択]をクリックします。
   ユーザがグループに追加されます。
9. [サブミット]をクリックします。
   ユーザが作成されます。

ユーザ パスワードのリセット

何回かログインに失敗した後にユーザ アカウントがロックされた場合、またはユーザがパスワードを紛失または忘れた場合に、ユーザのパスワードをリセットします。

ユーザ パスワードのリセット方法

1. CA Access Control エンタープライズ管理 内で、[ユーザおよびグループ]をクリックします。
   [ユーザ パスワードのリセット]が使用可能なタスクリストに表示されます。
2. [ユーザ パスワードのリセット]をクリックします。
   [ユーザ パスワードのリセット]検索ページが表示されます。
3. 検索クエリを入力し、[検索]をクリックします。
   検索条件に従って、検索結果が表示されます。
4. ユーザ アカウントを選択し、[選択]をクリックします。
   [パスワードのリセット]ウィンドウが開きます。
5. [パスワードの確認]フィールドにアカウント パスワードを入力します。
6. (オプション) [パスワードの変更が必要]オプションを選択します。
7. [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 によってユーザのパスワードがリセットされます。

ユーザの有効化または無効化

ユーザ アカウントを有効にし、ユーザがアカウントのクレデンシャルを使用して CA Access Control エンタープライズ管理 にログインできるようにします。ユーザ アカウントを無効にし、ユーザの CA Access Control エンタープライズ管理 へのアクセスを阻止し、ユーザ プロファイルをシステム内に保持します。

ユーザーアカウントを有効または無効にする方法

1. CA Access Control エンタープライズ管理 内で、[ユーザおよびグループ]をクリックします。

   [ユーザの有効化/無効化]タスクが使用可能なタスク リストに表示されます。

2. [ユーザの有効化/無効化]をクリックします。

   [ユーザの有効化/無効化]ページが表示されます。

3. 検索クエリを定義し、[検索]をクリックします。

   検索クエリに一致するユーザのリストが表示されます。

4. 無効化または有効化するユーザ アカウントを、以下のように指定します。

   - そのアカウントを無効にするユーザをクリアします。
   - そのアカウントを有効にするユーザを選択します。

5. [選択]をクリックします。

   指定した変更のサマリ画面が表示されます。

6. [はい]をクリックして、加えた変更を確認します。

   CA Access Control エンタープライズ管理 によって、要求された変更を実行するタスクがサブミットされます。

グループのタイプ

複数のタイプのグループを作成することも、これらのタイプを組み合わせて作成することもできます。

- **静的グループ**

  対話形式で追加されるユーザのリスト

- **動的グループ**

  LDAP クエリに一致する場合、ユーザはグループに属します (ユーザ ストアとして LDAP ディレクトリが必要です)。

  注: 動的グループ　クエリ フィールドを表示するために、関連するプロファイル画面を編集して、タスクにそれを含める必要があります。

- **ネストされたグループ**

  他のグループを含むグループです (ユーザ ストアとして LDAP ディレクトリが必要です)。

  注: ユーザが属する静的グループ、動的グループ、ネスト グループを表示するには、ユーザ オブジェクトの[グループ]タブを使用します。タブは[ユーザの表示]または[ユーザの変更]タスクで表示されます。

静的グループまたは動的グループの作成

複数のユーザを 1 つの静的グループに関連付けることができます。グループ メンバシップ リストにユーザを追加したり、リストから削除して、グループを管理できます。グループのメンバを表示するには、[グループの表示]または[グループの変更]タスクで[メンバシップ]タブを使用します。

CA Access Control エンタープライズ管理 を使用して LDAP フィルタ クエリを定義して、動的グループを作成し、実行時のグループ メンバシップを決定できます。

注: [メンバシップ]タブには、グループに明示的に追加されたメンバのみ表示されます。Active Directory をユーザ ストアとして使用する場合は、CA Access Control エンタープライズ管理 でグループを作成できません。

静的グループまたは動的グループの作成方法

1. ユーザ管理権限を持つユーザとして CA Access Control エンタープライズ管理 にログインします。
2. [グループ]-[グループの作成]を選択します。

   グループの作成の検索画面が表示されます。
3. [グループの作成]を選択し、[OK]をクリックします。

   [グループ プロフィール]タブが表示されます。
4. [グループ名]および[説明]に入力します。
5. [メンバシップ]タブに移動します。

   注: グループの動的メンバシップを変更できるのは、[グループの変更]タスクを持つ管理者のみです。
6. [ユーザの追加]をクリックします。

   選択したユーザ検索ウィンドウが開きます。
7. 検索クエリを入力し、[検索]をクリックします。

   検索条件に従って、検索結果が表示されます。
8. ユーザを選択し、[選択]をクリックします。

   [管理者]タブに移動します。
9. [サブミット]をクリックします。

   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。

注: ユーザをグループ管理者として割り当てる場合は、その管理者がグループの管理に必要な適切なスコープを持つロールが割り当てられていることを確認してください。

LDAP フィルタ クエリ - 動的グループ クエリ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 を使用して LDAP フィルタ クエリを定義して、動的グループを作成し、実行時のグループ メンバシップを決定できます。

フィルタ クエリは、以下の形式で指定します。

LDAP:///*search_base_DN*??*search_scope*?*searchfilter*

search_base_DN

LDAP ディレクトリ内の検索開始ポイントを指定します。クエリにベース DN を指定しない場合は、グループの組織がデフォルトのベース DN となります。

search_scope

検索範囲を指定します。以下の値を使用できます。

- **sub** - ベース DN レベルとそれより下位にあるエントリを返します。
- **one** - URL で指定するベース DN より 1 レベル下のエントリを返します。
- **base** - 検索オプションとしてベースを無視し、代わりに 1 つのエントリを使用します。

one または *base* を使用すると、ベース DN 組織内のユーザのみが取得されます。

sub を使用すると、ベース DN 組織と、ツリー内のすべての下位組織にある全ユーザが取得されます。

searchfilter

検索範囲内のエントリに適用するフィルタを指定します。検索フィルタの入力時には、以下のような標準の LDAP クエリ構文を使用します。

`([logical_operator]Comparison)`

logical operator

論理演算子を定義します。以下のいずれかです。

- **|** - 論理 OR
- **&** - 論理 AND
- **!** - 論理 NOT

Comparison

AttributeOperatorValue を定義します。

- *Attribute* - LDAP 属性の名前を定義します。
- *Operator* - 比較演算子を指定します。以下のいずれかになります。**=**（等しい）、**<=**（小さいまたは等しい）、**>=**（大きいまたは等しい）、または **~=**（ほぼ等しい）。
- *Value* - 属性データの値を定義します。

例: (&(city=Boston)(state=Massachusetts))

デフォルト: (objectclass=*)

動的クエリを作成する場合、以下の点に注意が必要です。

- 「LDAP」プレフィックスは小文字である必要があります。以下に例を示します。

  `ldap:///o=MyCorporation??sub?(title=Manger)`

- LDAP サーバ ホスト名またはポート番号は指定できません。検索はすべて、ユーザの環境で設定した LDAP ディレクトリ内で行われます。

例: LDAP クエリのサンプル

以下に、LDAP クエリの例を示します。

説明	クエリ
マネージャになっているユーザ全員	ldap:///o=MyCorporation??sub?(title=Manger)

説明	クエリ
ニューヨーク西支店のマネージャ全員	ldap:///o=MyCorporation??one?(&(title=Manager)(office=NYWest))
携帯電話を持っている技術者全員	ldap:///o=MyCorporation??one? (&(employeetype=technician)(mobile=*))
従業員番号が 1000 から 2000 までのすべての従業員	ldap:///o=MyCorporation, (& (ou=employee) (employeenumber >=1000) (employeenumber <=2000))
雇用期間が 6 か月を超えるヘルプデスク管理者全員	ldap:///o=MyCorporation,(& (cn=helpdeskadmin) (DOH => 2004/04/22) **注**: このクエリの場合、ユーザの雇用日を示す DOH 属性を作成する必要があります。

注: 「>」(より大きい)と「<」(より小さい)による比較は、算術式ではなく辞書式です。これらの使用法の詳細については、LDAP ディレクトリ サーバのマニュアルを参照してください。

グループ メンバの変更

メンバとグループを追加または削除するには、このオプションを使用します。 この手順を使用して、メンバのグループ リストを変更します。

グループ メンバの変更方法

1. ユーザ管理権限を持つユーザとして CA Access Control エンタープライズ管理 にログインします。
2. [グループ]-[グループ メンバの変更]を選択します。

   [グループ メンバの変更]画面が表示されます。
3. グループを選択し、[選択]をクリックします。

   グループ メンバ リストが開きます。
4. メンバを削除するには、メンバ名の隣のチェック ボックスをクリアします。
5. メンバを追加するには、[ユーザの追加]をクリックします。
   a. 検索クエリを入力し、[検索]をクリックします。

      検索条件に従って、検索結果が表示されます。
   b. ユーザを選択し、[選択]をクリックします。

      ユーザはグループ メンバとして追加されます。

6. グループを追加するには、[グループの追加]ボタンをクリックします。
   a. 検索クエリを入力し、[検索]をクリックします。
      検索条件に従って、検索結果が表示されます。
   b. グループを選択し、[選択]をクリックします。
      グループが追加されます。
7. [サブミット]をクリックします。
   タスク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。

監査データ

監査データによって、CA Access Control エンタープライズ管理 環境で実行される操作の履歴レコードが提供されます。管理データには、以下のようなものがあります。

- 特定期間のシステム アクティビティ。
- 特定期間に変更されたオブジェクトのリスト。
- ユーザに割り当てられたロール
- 特定のユーザアカウントで実行された操作

*イベント*の監査データが生成されます。イベントは CA Access Control エンタープライズ管理 タスクによって生成される操作です。たとえば、「ユーザの作成」タスクは「Access Role イベントの割り当て」イベントを含んでいる可能性があります。

CA Access Control エンタープライズ管理 は監査データを中央データベース内に格納します。監査データを CA Enterprise Log Manager へルーティングするために、監査コレクタを設定できます。

注: CA Enterprise Log Manager との統合については、「*実装ガイド*」を参照してください。

詳細情報:

サブミット済みタスクの検索 (P. 48)
タスクの詳細の表示 (P. 52)
イベントの詳細の表示 (P. 53)
サブミット済みタスクのクリーンアップ (P. 53)
メッセージ キュー監査メッセージの Windows イベント ログへのルーティング (P. 56)
メッセージ キュー監査メッセージの UNIX syslog へのルーティング (P. 58)

サブミット済みタスクの検索

サブミット済みタスクによって、CA Access Control エンタープライズ管理 環境内のタスクに関する情報が提供されます。CA Access Control エンタープライズ管理 が実行するアクションに関する高度な詳細情報を検索し、表示することができます。詳細画面によって、各タスクおよびイベントに関する追加情報が提供されます。

タスクのステータスに応じて、タスクのキャンセルまたは再サブミットを実行できます。

サブミット済みタスクによって、タスクの処理を最初から最後まで追跡できます。

サブミット済みタスクの検索方法

1. CA Access Control エンタープライズ管理 で、[システム]-[監査]サブタブをクリックします。

   [サブミット済みタスクの表示]タスクが、使用可能なタスク リストに表示されます。

2. [サブミット済みタスクの表示]をクリックします。

   [サブミット済みタスクの表示]ページが表示されます。

3. 検索条件 (P. 49)を指定し、表示する行数を入力して、[検索]をクリックします。

   検索条件に適合するタスクが表示されます。

サブミット済みタスクの表示に関する検索属性

処理用にサブミットされたタスクを確認するには、[サブミット済みタスクの表示]で検索機能を使用します。以下の条件に基づいて、タスクを検索できます。

開始者

検索条件となるタスクを開始したユーザの名前を識別します。ユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

承認者

検索条件としてタスク承認者の名前を識別します。ユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

注: タスクのフィルタとして[承認タスク実行者]条件を選択した場合は、デフォルトにより[承認タスクの表示]条件も有効になります。

タスク名

検索条件としてタスク名を識別します。[タスク名の条件]フィールドの値として「=」、「以下を含む」、「以下で開始:」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を指定し、テキストフィールドに「ユーザの作成」と入力すると、「タスク名 = ユーザの作成」という検索基準を指定できます。

タスクのステータス

検索条件となるタスク ステータス (P. 51)を識別します。タスクのステータスを選択するには、[Where task status equals]を有効にし、条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- 一部完了
- キャンセル済み
- スケジュール済み

タスク優先度

検索条件としてタスクの優先度を識別します。タスク優先度を選択するには、[タスク優先度の条件]を有効にして条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

実行対象

選択したオブジェクト インスタンスに対して実行されるタスクを識別します。オブジェクト インスタンスを選択しない場合は、そのオブジェクトの全インスタンスに対して実行されたタスクがすべて表示されます。

注: このフィールドは、[サブミット済みタスクの設定]画面で[次に対し設定を実行]フィールドを指定した場合にのみ表示されます。[サブミット済みタスク]タブを設定するには、この画面を使用します。

日付範囲

サブミット済みタスクの検索範囲を識別します。開始日と終了日を指定する必要があります。

[サブミット解除されたタスクの表示]

監査済み状態のタスクを識別します。他のタスクを開始したタスクや、サブミットされていないタスクが識別されます。このタブを選択した場合は、そのようなタブがすべて監査され、表示されます。

承認タスクの表示

ワークフローの一部として承認すべきタスクを識別します。

詳細情報:

タスク ステータスの説明 (P. 51)

タスク ステータスの説明

サブミット済みタスクのステータスは、以下のいずれかになります。タスクのステータスに基づいて、タスクのキャンセルや再サブミットなどのアクションを実行できます。

注: タスクをキャンセルまたは再サブミットするには、タスク ステータスに基づいてキャンセル ボタンと再サブミット ボタンが表示されるように[サブミット済みタスクの表示]を設定する必要があります。

実行中

以下のいずれかが発生した場合に表示されます。

- ワークフローが開始されたが、まだ完了していない場合
- 現在のタスクの前に開始されたタスクが実行中の場合
- ネスト タスクが開始されたが、まだ完了していない場合
- プライマリ イベントが開始されたが、まだ完了していない場合
- セカンダリ イベントが開始されたが、まだ完了していない場合

この状態のタスクはキャンセルすることができます。

注: タスクをキャンセルすると、現在のタスクに関する未完了のネスト イベントとタスクがすべてキャンセルされます。

キャンセル済み

実行中のタスクまたはイベントのいずれかをキャンセルした場合に表示されます。

拒否

CA Access Control エンタープライズ管理 がワークフロー プロセスの一部であるイベントまたはタスクを拒否した場合に表示されます。. 拒否されたタスクは再サブミットすることができます。

注: タスクを再サブミットすると、CA Access Control エンタープライズ管理 によって失敗または拒否されたネスト タスクとイベントがすべて再サブミットされます。

一部完了

一部のイベントまたはネスト タスクをキャンセルした場合に表示されます。一部完了したイベントまたはネスト タスクは再サブミットすることができます。

完了

タスクが完了した場合に表示されます。現在のタスクのネスト タスクとネスト イベントがすべて完了すると、タスクが完了します。

失敗

現在のタスクに含まれるタスク、ネスト タスク、またはネスト イベントが無効の場合に表示されます。このステータスは、タスクが失敗した場合に表示されます。失敗したタスクは再サブミットすることができます。

スケジュール済み

タスクを後で実行するようスケジュール設定されている場合に表示されます。この状態のタスクはキャンセルすることができます。

タスクの詳細の表示

CA Access Control エンタープライズ管理 では、サブミット済みタスクのステータス、ネスト タスク、タスクに関連付けられたイベントなどのタスクの詳細が提供されます。

サブミット済みタスクの詳細を表示する方法

1. [サブミット済みタスクの表示]ページで、選択されたタスクの横にある右矢印アイコンをクリックします。

   タスクの詳細が表示されます。

   注: イベントとネスト タスク(ある場合)は、[Task Details]ページに表示されます。タスクおよびイベントごとのタスク詳細を表示できます。

2. [Close]をクリックします。

   [タスクの詳細]タブが閉じ、CA Access Control エンタープライズ管理 の[サブミット済みタスクの表示]タブにタスク リストが表示されます。

イベントの詳細の表示

CA Access Control エンタープライズ管理 では、サブミット済みイベントのステータス、イベント属性、イベントに関する追加情報などのイベントの詳細が提供されます。

サブミット済みイベントの詳細を表示する方法

1. [タスクの詳細の表示]ページで、イベントの横にある右矢印アイコンをクリックします。

   イベントの詳細が表示されます。

2. [Close]をクリックします。

   [イベントの詳細]ページが閉じます。

サブミット済みタスクのクリーンアップ

CA Access Control エンタープライズ管理 は、PUPM 監査データなどの監査データを中央データベースに格納します。ただし、中央データベースに大量の監査データを格納すると、データベースのパフォーマンスに影響が及ぶ場合があります。データベースのパフォーマンスを改善するために、サブミット済みタスクのクリーンアップ ウィザードを使用して、サブミット済みタスクを中央データベースから削除します。

重要: サブミット済みタスクをクリーンアップすることにより、監査データがデータベースから削除されます。データの損失を回避するために、監査イベントを CA Enterprise Log Manager にルーティングしてからクリーンアップ タスクを実行することをお勧めします。

クリーンアップ タスクはすぐにまたは一定の間隔で繰り返し実行するようにスケジューリングできます。サブミット済みタスクのクリーンアップは、大量のシステムリソースを消費する場合があります。そのため、このタスクを営業時間外にスケジューリングすることをお勧めします。

サブミット済みタスクのクリーンアップ方法

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. [タスク]サブタブをクリックします。
   c. [サブミット済みタスクのクリーンアップ]をクリックします。

      [サブミット済みタスクのクリーンアップ : 繰り返し]ページが表示されます。
2. 以下の*いずれか*の操作を実行します。
   - タスクをすぐに実行するには、[即実行]を選択し[次へ]をクリックします。

     [サブミット済みタスクのクリーンアップ : サブミット済みタスクのクリーンアップ]ページが表示されます。
   - 繰り返しスケジュールを作成するには、[新規ジョブのスケジュール]を選択して、表示されるすべて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。

     タイムゾーン

     エンタープライズ管理サーバのタイム ゾーンを指定します。

     ユーザの所在地がサーバとは異なるタイムゾーンにある場合は、新規ジョブのスケジューリング時に、ユーザのタイムゾーンかサーバのタイムゾーンのいずれかを選択できます。既存のジョブを修正する場合は、タイムゾーンは変更できません。

     週単位のスケジュール

     タスクが特定の曜日（複数指定可）の特定の時間に実行されるように指定します。

     時間は 24 時間形式で、「17:15」のように指定します。

     詳細なスケジュール

     cron 式を使用して、タスクを実行する時間を指定できます。

     [Next]をクリックします。

     [サブミット済みタスクのクリーンアップ : サブミット済みタスクのクリーンアップ]ページが表示されます。

3. 以下のフィールドに値を入力します。

最短期間

最終状態（完了、失敗、拒否、キャンセル、または中止）のタスクの最短期間を指定します。CA Access Control エンタープライズ管理 は、このタスクを中央データベースから削除します。

監査タイムアウト

（オプション）監査状態のタスクの最短期間を指定します。CA Access Control エンタープライズ管理 は、このタスクを中央データベースから削除します。

注: 監査状態のタスクは、サブミットされていません。

時間制限

（オプション）クリーンアップ操作を実行するために CA Access Control エンタープライズ管理 が要する最長期間を指定します。

タスク制限

（オプション）CA Access Control エンタープライズ管理 が中央データベースから削除するタスクの最大数を指定します。

［完了］をクリックします。

CA Access Control エンタープライズ管理 は、指定した時間にサブミット済みタスクを中央データベースから削除します。

メッセージ キュー監査メッセージの Windows イベント ログへのルーティング

Windows で有効

エンタープライズ管理サーバを設定して、メッセージ キュー監査メッセージを Windows イベント ログにルーティングできます。エンタープライズ管理サーバが監査ログに監査メッセージを書き込むたびに、対応するイベントがイベント ログに送信されます。

メッセージ キュー監査メッセージを Windows イベント ログにルーティングする方法

1. JBoss アプリケーション サーバが実行中の場合は、停止します。
2. 以下のディレクトリに移動します。ここで *JBOSS_HOME* は JBoss をインストールしたディレクトリです。

   JBOSS_HOME¥server¥default¥conf¥
3. jboss-log4j.xml ファイルを開きます。
4. "ENTM_NTEventLog" というアペンダをクラスに追加します。

   このアペンダは、監査に使用するクラスおよびデータの表示方法を指定します。
5. "EventLog" というロガーを作成します。

   アペンダが監査メッセージ用の入力チャネルとしてバインドするロガーを指定します。
6. ファイルを保存して閉じます。
7. NTEventLogAppender.dll ファイルを Windows System32 ディレクトリにコピーします。

   注: NTEventLogAppender.dll ファイルは、Apache log4j 1.2.16 バンドルに存在します。Apache log4j 1.2.16 は、Apache Logging Services の Web サイトからダウンロードできます。
8. JBoss アプリケーション サーバを起動します。

   エンタープライズ管理サーバが、メッセージ キュー監査メッセージを Windows イベント ログにルーティングするようになりました。

例: メッセージ キュー監査メッセージを Windows イベント ログへ送信するように jboss-log4j.xml ファイルを変更

以下の例は、メッセージ キュー監査メッセージを Windows イベント ログにルーティングするように設定された jboss-log4j.xml ファイルの一部です。

```
 <appender name="ENTM_NTEventLog"
                        class="org.apache.log4j.nt.NTEventLogAppender">
    <param name="Source" value="CA Access Control Enterprise Management"/>
    <layout class="org.apache.log4j.SimpleLayout"/>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_NTEventLog"/>
</logger>
```

この例では、以下の変更を加えました。

- "ENTM_NTEventLog" という新しいアペンダを追加しました。
- "org.apache.log4j.nt.NTEventLogAppender" というクラスを追加しました。
- パラメータ名 "Source" を定義しました。
- 値 "CA Access Control Enterprise Management" を定義しました。
- レイアウト クラス "org.apache.log4j.SimpleLayout" を定義しました。
- ロガー名 "EventLog" を定義しました。
- appender-ref ref として "ENTM_NTEventLog" を定義しました。

メッセージ キュー監査メッセージの UNIX syslog へのルーティング

UNIX で有効

エンタープライズ管理サーバを設定して、メッセージ キュー監査メッセージを UNIX syslog にルーティングできます。エンタープライズ管理サーバが監査メッセージを監査ログに書き込むたびに、対応するイベントが syslog に送信されます。

メッセージ キュー監査メッセージを UNIX syslog にルーティングする方法

1. JBoss アプリケーション サーバが実行中の場合は、停止します。
2. 以下のディレクトリに移動します。ここで *JBOSS_HOME* は JBoss をインストールしたディレクトリです。

   ```
   JBOSS_HOME¥server¥default¥conf¥
   ```

3. jboss-log4j.xml ファイルを開きます。
4. "ENTM_UNIXEventLog" というアペンダをクラスに追加します。

   このアペンダは、監査に使用するクラスおよびデータの表示方法を指定します。

5. "EventLog" というロガーを作成します。

   アペンダが監査メッセージ用の入力チャネルとしてバインドするロガーを指定します。

6. ファイルを保存して閉じます。
7. /etc/syslog.conf ファイルを開き、syslog がメッセージを /var/log/messages ファイルにルーティングすることを確認します。
8. /etc/sysconfig/syslog パラメータ ファイルを開き、リモート モード オプションが以下のエントリに表示されることを確認します。

   ```
   SYSLOGD_OPTIONS="-m 0-r"
   ```

9. syslog デーモンを再起動します。以下のコマンドを実行します。

   ```
   /etc/rc.d/init.d/syslog restart
   ```

   syslog デーモンが起動します。

10. JBoss アプリケーション サーバを起動します。

    エンタープライズ管理サーバは、メッセージ キュー監査メッセージを UNIX syslog にルーティングするようになります。

例: メッセージ キュー監査メッセージを UNIX syslog へ送信するように jboss-log4j.xml ファイルを変更

以下の例は、LogAppender オブジェクトの作成後の jboss-log4j.xml ファイルの一部です。

```
<appender name="ENTM_UNIXSysLog"
                        class="org.apache.log4j.net.SyslogAppender">
    <param name="Facility" value="USER"/>
    <param name="FacilityPrinting" value="false"/>
    <param name="SyslogHost" value="localhost"/>
    <layout class="org.apache.log4j.PatternLayout">
        <param name="ConversionPattern" value="%p - [CA AC ENTM]: %m%n"/>
    </layout>
</appender>

<logger name="EventLog">
    <appender-ref ref="ENTM_UNIXSysLog"/>
</logger>
```

この例では、以下の変更を加えました。

- アペンダ "ENTM_UNIXSysLog" を追加しました。
- クラス "org.apache.log4j.net.SyslogAppender" を作成しました。
- パラメータ名 "Facility" および値 "USER" を定義しました。
- パラメータ名 "FacilityPrinting" および値 "localhost" を定義しました。
- パラメータ名 "SyslogHost" および値 "localhost" を定義しました。
- レイアウト クラス "org.apache.log4j.PatternLayout" を定義しました。
- パラメータ名 "ConversionPattern" および値 "%p - [CA AC ENTM]: %m%n" を定義しました。
- ロガー名 "EventLog" を定義しました。
- appender-ref ref="ENTM_UNIXSysLog" を定義しました。

電子メール通知

電子メール通知は CA Access Control エンタープライズ管理 ユーザにシステム内のイベントを通知します。また、電子メールテンプレートから生成されます。電子メール通知を有効にすると、CA Access Control エンタープライズ管理 は以下のいずれかが発生した場合に電子メール通知を生成できます。

- 承認または拒否を必要とするイベントが保留中の場合。
- 承認者がイベントを承認した場合。
- 承認者がイベントを拒否した場合。
- イベントが開始、失敗、または完了した場合。
- CA Access Control エンタープライズ管理 ユーザが作成または変更された場合。

注: 電子メール通知を有効にする方法の詳細については、「実装ガイド」を参照してください。

電子メール テンプレート

CA Access Control エンタープライズ管理 は、電子メール テンプレートから電子メール通知を生成します。各電子メール テンプレートには、以下の情報が含まれています。

- **配信情報** - 電子メールの受信者リスト。
- **件名** - 電子メールの件名で使用するテキスト。
- **コンテンツ** - 電子メール本文。本文には通常、静的テキストと変数の両方が含まれています。CA Access Control エンタープライズ管理 は、電子メールをトリガするタスクまたはイベントに基づいてこれらを解決します。

電子メール テンプレートは以下のディレクトリにあります。*JBoss_home* は、JBoss をインストールしたディレクトリです。

```
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/emailTemplates/default
```

emailTemplates ディレクトリには、5 つのサブディレクトリが含まれます。各フォルダはイベント状態と関連付けられます。以下の表では、各サブディレクトリにある電子メールテンプレートの目的をリストします。

サブディレクトリ	目次
承認	■ CertifyRoleEvent.tmpl - 使用されなくなりました。 ■ CheckOutAccountPasswordEvent.tmpl - 特権アカウント パスワード要求が承認されたことを受信者に通知します。 ■ CreatePrivilegedAccountExceptionEvent.tmpl - 特権アカウント パスワード要求が指定した期間承認されたことを受信者に知らせます。(このテンプレートは特権アカウント要求タスクに該当します)。 ■ defaultEvent.tmpl - イベントが承認されたことを受信者に知らせます。 ■ defaultTask.tmpl - タスクが承認されたことを受信者に知らせます。 ■ ForgottenPasswordEvent.tmpl - 使用されなくなりました。 ■ SelfRegisterUserEvent.tmpl - 使用されなくなりました。

サブディレクトリ	目次
完了	■ AccumulatedProvisioningRolesEvent.tmpl - 使用されなくなりました。 ■ CertificationNonCertifiedActionCompletedNotificationEvent.tmpl - 使用されなくなりました。 ■ CertificationNonCertifiedActionPendingNotificationEvent.tmpl - 使用されなくなりました。 ■ CertificationRequiredFinalReminderNotificationEvent.tmpl - 使用されなくなりました。 ■ CertificationRequiredNotificationEvent.tmpl - 使用されなくなりました。 ■ CertificationRequiredReminderNotificationEvent.tmpl - 使用されなくなりました。 ■ CheckOutAccountPasswordEvent.tmpl -- チェックアウトした特権アカウントのパスワードを受信者に通知します。 ■ CreateProvisioningUserNotificationEvent.tmpl - 使用されなくなりました。 ■ defaultEvent.tmpl - CA Access Control エンタープライズ管理 がイベントを完了したことを受信者に知らせます。 ■ defaultTask.tmpl - CA Access Control エンタープライズ管理 がタスクを完了したことを受信者に知らせます。 ■ ForgottenPassword.tmpl - 使用されなくなりました。 ■ ForgottenUserID.tmpl - 使用されなくなりました。 ■ Self Registration.tmpl - 使用されなくなりました。
Invalid	■ AssignProvisioningRoleEvent.tmpl - 使用されなくなりました。 ■ DefaultEvent.tmpl - イベントが失敗したことを受信者に知らせます。 ■ DefaultTask.tmpl - タスクが失敗したことを受信者に知らせます。

サブディレクトリ	目次
Pending	■ BreakGlassCheckOutAccountEvent.tmpl - Break Glass チェックアウトが実行されたこと承認者に知らせます。 ■ CertifyRoleEvent.tmpl - 使用されなくなりました。 ■ CheckOutAccountPasssswordEvent.tmpl -- 特権アカウントのチェックアウトに対応する必要があることを承認者に知らせます。 ■ defaultEvent.tmp - ワークリスト項目に対応する必要があることを承認者に知らせます。 ■ defaultTask.tmpl -- タスクに対応する必要があることを承認者に通知します。 ■ ModifyUserEvent.tmpl - 使用されなくなりました。
拒否	■ CertifyRoleEvent.tmpl - 使用されなくなりました。 ■ CheckOutPasswordEvent.tmpl - 特権アカウント パスワード要求が拒否されたことを受信者に通知します。 ■ CreatePrivilegedAccountExceptionEvent.tmpl - 指定した期間の特権アカウントへのアクセス要求が拒否されたことを受信者に通知します（このテンプレートは、特権アカウント要求タスクに対応します）。 ■ defaultEvent.tmpl - イベントが拒否されたことを受信者に通知します。 ■ defaultTask.tmpl - タスクが拒否されたことを受信者に通知します。 ■ ForgottenPasswordEvent.tmpl - 使用されなくなりました。 ■ SelfRegisterUserEvent - 使用されなくなりました。

電子メール通知のしくみ

電子メール通知は、システムのイベントを CA Access Control エンタープライズ管理 ユーザに通知します。以下のプロセスでは、電子メール通知が動作するしくみについて説明します。

1. イベントが発生すると、CA Access Control エンタープライズ管理 はイベントに対して電子メール通知が有効になっているかどうかを確認します。
2. 電子メール通知が有効な場合、CA Access Control エンタープライズ管理 は適切なサブディレクトリ内のイベント タイプを検索します。

   たとえば、電子メールが特権アカウント要求を承認するために送信される場合、CA Access Control エンタープライズ管理 は Approved サブディレクトリの中を検索します。
3. CA Access Control エンタープライズ管理 のサブディレクトリにイベントと同じ名前の電子メール テンプレートが存在するかを確認します。次に、以下を実行します。
   - イベントと同じ名前の電子メール テンプレートが存在する場合、CA Access Control エンタープライズ管理 は電子メール テンプレートを受信者に送信します。
   - イベントと同じ名前の電子メール テンプレートが存在しない場合、defaultEvent.tmpl 電子メール テンプレートを受信者に送信します。

注: 電子メール通知の設定方法の詳細については、「実装ガイド」を参照してください。

電子メール テンプレートのカスタマイズ

CA Access Control エンタープライズ管理 は、電子メール テンプレートから電子メール通知を生成します。ユーザのエンタープライズ要件に適した電子メール テンプレートをカスタマイズできます。

電子メール テンプレートをカスタマイズする方法

1. 編集 可能な形式でテンプレートを開きます。
2. 以下のいずれかまたは両方の操作を行い、電子メール テンプレートを変更します。
   - テンプレートの本文に静的テキストを入力します。
   - テンプレートに動的コンテンツを指定するには、電子メール テンプレート API で変数を使用します。
3. テンプレートを保存して閉じます。

注: 電子メール テンプレート API の詳細については、「*CA Identity Manager 管理ガイド*」を参照してください。

第 3 章: エンタープライズ実装の表示

このセクションには、以下のトピックが含まれています。

ワールド ビュー

CA Access Control エンタープライズ管理 のワールド ビューでは、接続された DMS で管理する CA Access Control のエンタープライズ実装を表示することができます。

ワールド ビューを使用して以下のことが可能です。

- 接続した DMS に所属するエンドポイントを識別できます。
- エンドポイント タイプを識別できます。これは、CA Access Control、PMDB、PUPM、UNAB の 1 つ以上になります。
- 各エンドポイントが前回 DMS にハートビートを送信した日時を確認できます。
- デプロイされたポリシー、オペレーティング システムの種類、エンドポイント上の管理対象デバイスなど、エンドポイントの詳細を表示します。
- CA Access Control エンドポイント管理 を開いて、CA Access Control エンドポイントを管理します。
- UNAB ホストまたは PUPM 管理対象デバイスを変更します。

CA Access Control のエンタープライズ実装の表示

CA Access Control エンタープライズ管理 を使用して、CA Access Control のエンタープライズ実装を表示することができます。このエンタープライズ「ワールド ビュー」は、すべてのエンドポイントと、エンドポイントが分類される論理ホスト グループと、エンドポイント上にデプロイされているポリシー、エンドポイントにある管理対象デバイスを含むスナップショットです。

CA Access Control のエンタープライズ実装の表示方法

1. CA Access Control エンタープライズ管理 で、[ワールド ビュー]タブをクリックし、左側のタスク メニューにある[ワールド ビュー]リンクをクリックします。

   [ワールド ビュー]ページが開き、[検索]セクションが表示されます。

2. (オプション) 検索条件を定義します。

   2 種類の検索を使用できます。

   - **シンプル** - 単純な検索を使用して、ホスト名マスクを定義し、結果のフィルタリングに使用するエンドポイントのタイプを指定します。
   - **詳細** - [詳細]リンクをクリックして、指定されたホスト グループ、割り当て済みポリシー、管理対象デバイス名マスク、管理対象デバイス タイプで、結果をフィルタリングすることもできます。

   注: デフォルトでは、ワールド ビューは、CA Access Control エンタープライズ管理 が接続される DMS に定義されたすべてのエンドポイントについての結果を表示します。

3. [Go]をクリックします。

   定義した条件に一致する結果が、以下のいずれかのカテゴリ別に表示されます。

   - **ホスト名による検索結果** - これは、DMS で定義するホスト(エンドポイント)です。これが、結果を表示するデフォルトの表示カテゴリになります。
   - **ホスト グループによる検索結果** - これは、ユーザが定義する論理ホスト グループです。
   - **ポリシーによる検索結果** - これは、エンドポイントにデプロイされるポリシーです。
   - **管理対象デバイスによる検索結果** - これは、エンドポイント上の管理対象デバイスです。

CA Access Control エンドポイント管理 を開いてエンドポイントを管理

CA Access Control エンタープライズ管理 では Single-Sign On (SSO) がサポートされているため、ユーザはエンドポイントを管理する CA Access Control エンドポイント管理 に容易にログインすることができます。

Windows エンドポイントを管理するために自動ログインを設定する場合、CA Access Control エンタープライズ管理 と CA Access Control エンドポイントに同一のユーザ名およびパスワードを使用していること、また CA Access Control エンドポイント管理 を使用してエンドポイントを管理するための端末アクセス権限があることを確認してください。

注: UNIX エンドポイントを管理するために自動ログインを設定するには、エンドポイントに CA Access Control エンドポイント管理 SSO を設定する必要があります。

CA Access Control エンドポイント管理 を開いてエンドポイントを管理する方法

1. ワールド ビューを使用して、管理する 1 つまたは複数のエンドポイントを表示します。
2. [アクション]列で[管理]をクリックします。

   CA Access Control エンドポイント管理 が開き、エンドポイントのホスト名およびユーザのクレデンシャルが自動的に入力されます。ログインに使用している CA Access Control エンタープライズ管理 ユーザが CA Access Control エンドポイント管理 に存在しない場合は、クレデンシャルを手動で入力する必要があります。

詳細情報:

CA Access Control のエンタープライズ実装の表示 (P. 68)
CA Access Control エンドポイント管理 SSO のための UNIX エンドポイントの設定 (P. 70)

CA Access Control エンドポイント管理 SSO のための UNIX エンドポイントの設定

CA Access Control エンタープライズ管理 を使用すると、CA Access Control エンドポイント管理 に簡単にログインして、CA Access Control エンタープライズ管理 が管理する任意のエンドポイントを管理できます。自動ログインでは、Active Directory クレデンシャルを使用して CA Access Control エンタープライズ管理 にログインします。CA Access Control エンタープライズ管理 はクレデンシャルを保持し、ユーザが CA Access Control エンドポイント管理 を開いてエンドポイントを管理する場合に、エンドポイントにクレデンシャルを提供します。 CA Access Control エンドポイント管理 を使用した CA Access Control への自動ログインは、CA Access Control エンタープライズ管理 への認証時に使用するユーザ アカウントに依存します。

注: UNAB エンドポイントへの自動ログインを設定するには、CA Access Control エンタープライズ管理 と UNAB の両方が同じ Active Directory を使用することを確認します。

重要: UNIX ユーザとして使用するユーザは、Active Directory 内で設定します。

CA Access Control エンドポイント管理 SSO のための UNIX エンドポイントの設定

1. CA Access Control エンドポイントで、seos.ini ファイルを開き、[OS_User]セクションを見つけて、トークン osuser_enabled の値を「**1**」に設定します。

   エンタープライズ ユーザおよびエンタープライズ グループを有効にします。

2. [seos]セクションを見つけて、トークン auth_login の値を pam に設定します。

   使用されるログイン権限メソッドは PAM です。

3. CA Access Control エンドポイント管理 コンピュータ用の TERMINAL レコードを作成します。

   CA Access Control エンドポイント管理 コンピュータは TERMINAL アクセスに割り当てられます。

4. XUSER として CA Access Control エンタープライズ管理 にログインするために使用するユーザ アカウントを設定して、そのアカウントに管理者属性を割り当てます。書式 *<DOMAIN-NAME>user_account* を使用します。
5. 読み取りと書き込みのアクセス権限で TERMINAL クラス内の superadmin ユーザ用の ACL を定義します。以下に例を示します。

```
Defaccess         : R, W

ACLs              :

    Accessor                Access

    DOMAIN¥user(XUSER   ) R, W
```

ユーザは CA Access Control エンタープライズ管理 Server を使用してエンドポイントを管理できます。

PUPM エンドポイントの変更

CA Access Control エンタープライズ管理 ワールド ビューを使用すると、PUPM エンドポイント管理対象デバイスの設定を変更できます。管理対象デバイスは、特権アカウントを使用して管理するアプリケーションです。PUPM エンドポイントは、ロール ベースの管理システムを使用してアカウントへのアクセス権を付与し、パスワード データベースに特権アカウントを格納します。管理対象デバイスは、PUPM エンドポイント自体または企業にインストールされる場合があります。

PUPM エンドポイントの変更

1. [ワールドビュー]-[ワールドビュー]タスクを選択します。

   [ワールド ビュー]検索画面が表示されます。
2. クエリを入力し、[実行]をクリックします。

   クエリの検索結果が表示されます。
3. 変更対象の PUPM エンドポイントの行で、下矢印(表示)アイコンをクリックします。

   エンドポイント上にある管理対象デバイスの詳細情報が表示されます。
4. [変更]をクリックし、エンドポイント設定を変更します。

   [エンドポイントの変更]ウィンドウが表示され、エンドポイント設定が表示されます。
5. エンドポイント設定を変更し、[サブミット]をクリックします。

   タスクが完了したことを通知するメッセージが表示されます。

詳細情報:

エンドポイントの作成 (P. 194)

第 4 章: ポリシーの一元管理

このセクションには、以下のトピックが含まれています。

ポリシータイプ

CA Access Control エンタープライズ管理 では、CA Access Control エンドポイントおよび UNAB ホストを管理する、CA Access Control ポリシー、UNAB 設定ポリシーおよび UNAB ログイン ポリシーの 3 種類のポリシーを使用します。

CA Access Control ポリシーを使用して、リソースへのアクセス管理および CA Access Control エンドポイントへのアクセサ権限の設定などに関する、企業全体で統一されたポリシーを作成します。

UNAB ログイン ポリシーを使用して、企業の UNIX ホストへのアクセスを管理します。ログイン ポリシーは、UNAB が実行されている UNIX ホストへのユーザのログインを制御します。CA Access Control エンタープライズ管理 は、ロードされた権限リストをベースにして、ログイン ポリシーを自動的に作成、割り当て、表示します。

UNAB 環境設定ポリシーを使用して、リモート UNAB ホスト上の環境設定ファイルのトークンの値を設定し、組織内への UNAB ホストのデプロイおよび設定が容易にできるようにします。

詳細情報:

UNAB ログイン認証の管理 (P. 321)
UNAB ホストまたはホスト グループの設定 (P. 323)

ポリシーの一元管理の方法

CA Access Control を使用すると、以下の 方法で 1 台のコンピュータから複数のデータベースを管理できます。

- **自動的なルール ベースのポリシー更新** -- 中央のデータベース(PMDB)で定義した通常のルールは、設定された階層内のデータベースに自動的に伝達されます。

  注: デュアル コントロールは、この方法でのみ使用できます。また、UNIX でのみ使用可能です。自動的なルール ベース ポリシー更新のデュアル コントロールの詳細は、「*UNIX エンドポイント管理ガイド*」で説明しています。また、自動的なルール ベース ポリシー更新の詳細は、「*Windows エンドポイント管理ガイド*」でも説明しています。

- **拡張ポリシー管理** -- デプロイしたポリシー(ルールの集合)は、ホストまたはホスト グループの割り当てに基づいて、すべてのデータベースに伝達されます。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。この機能を使用するには、追加のコンポーネントをインストールおよび設定する必要があります。

  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

作成するポリシー(selang コマンド)は格納してから、定義した方法でエンタープライズにデプロイできます。このポリシー ベースの方法を使用すると、ポリシーを格納してから、それらのポリシーをホストまたはホスト グループに割り当てられます。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。

デプロイ マップ サーバ(DMS)である中央データベースは、企業のポリシー、バージョン、割り当て、およびデプロイに関するすべての情報を収集します。したがって、デプロイのステータス、デプロイの偏差、およびデプロイの階層に関するレポートを容易に作成できます。

注: デュアル コントロールはこの方法では使用 *できません*。UNIX でのみ使用可能です。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。

拡張ポリシー ベース管理のしくみ

拡張ポリシー ベース管理では、ポリシー バージョンを格納、デプロイ、およびデプロイ解除することができると同時に、後でデプロイのステータス、デプロイの偏差、およびデプロイ配布をチェックすることができます。

以下の方法で、高度なポリシー ベースの管理作業を行います。

1. ポリシーを作成します。

   各ポリシーには、1 組の selang コマンド スクリプトが含まれています。最初のスクリプトは、「*デプロイメント スクリプト*」で、ポリシーを構成する selang コマンドのセットが含まれています。2 つ目のスクリプトは、「*デプロイ解除スクリプト*」と呼び、*エンドポイント データベースからポリシーをデプロイ解除(削除)するために必要なコマンドが含まれます。*

2. CA Access Control エンタープライズ管理 または policydeploy ユーティリティのいずれかを使用して、DMS にポリシーの詳細を格納します。また、CA Access Control は次に自動バージョン管理を使用して、ポリシーを格納します。

   ポリシーの詳細には、ポリシーの説明、デプロイメント スクリプトおよびデプロイメント解除スクリプト、およびポリシーの依存関係含まれています。が

3. ポリシーが DMS にすでに存在するかどうかによって、CA Access Control は以下の*いずれか*を実行します。

   - ポリシー名が DMS に存在しない場合、CA Access Control はポリシー (*policy_name*#01) および論理ポリシー オブジェクト (GPOLICY class) の最初のバージョンを作成し、ポリシー バージョンを論理ポリシーのメンバとして追加します。
   - ポリシー名が DMS にすでに存在する場合、検出された最新のポリシー バージョンに 1 を加えた新しいポリシー バージョンが作成され、このポリシー バージョンが論理ポリシー (GPOLICY オブジェクト) のメンバとして追加されます。

4. その段階であると判断した場合は、CA Access Control エンタープライズ管理または policydeploy ユーティリティを使用して、格納されたポリシーをターゲット データベースにデプロイします。CA Access Control は、DMS でデプロイメント タスク (DEPLOYMENT オブジェクト) を自動的に作成します。

   .注: CA Access Control は、格納されたポリシーの最新のファイナライズされたポリシー バージョンをデプロイします。作成する新しいポリシー バージョンは、割り当てられたホストに自動的に送信されません。割り当てられたホストを手動で最新のポリシー バージョンにアップグレードする必要があります。

   注: CA Access Control エンタープライズ管理 は、UNAB ログインおよびプロシージャ ポリシーの作成後、ポリシーを自動的にデプロイします。UNAB ログインおよび設定ポリシーのみを UNAB ホストに割り当てできます。

5. CA Access Control は DMS にデプロイメント パッケージ (GDEPLOYMENT オブジェクト) を自動的に作成します。

   デプロイメント パッケージは、前の手順で作成されたすべてのデプロイ タスクをグループ分けします。

6. DMS はデプロイ タスクを配布ホスト (DH) に送信します。

7. エンドポイントは, (policyfetcher を使用して) 新しいポリシー デプロイ タスクがないかどうかを定期的にチェックし、保留中のデプロイメント タスクを DH から取得し、ターゲット データベース上で各ルール (デプロイメント スクリプトで指定された selang コマンド) を実行します。

8. エンドポイントは、デプロイメント タスク ステータス(失敗、成功)、失敗したコマンドに関する selang の結果メッセージ、および HNODE 上のポリシー ステータスで DH を更新します。

   注: ポリシーのデプロイがエラーになった場合、CA Access Control エンタープライズ管理 の[デプロイメント監査]を使用して、失敗したコマンドに関する selang の出力を詳述します。そうしない場合、ポリシーのデプロイがエラーになったコンピュータ上で、ログ ファイルを表示する必要があります。

9. DH は、デプロイ タスクのステータスやポリシー ステータスが格納されている DMS でそれらの情報を更新します。

注: UNAB ログイン ポリシーおよび UNAB 設定ポリシーは、拡張ポリシー ベース管理とは同様に機能しません。

詳細情報:

ポリシーの依存関係 (P. 97)
ポリシー検証 (P. 98)
割り当てパス (P. 94)
ホスト アクセス制御および UNAB 設定の仕組み (P. 320)

デプロイメント メソッドがデプロイメント タスクに影響を及ぼす仕組み

格納されたポリシーをターゲット データベースにデプロイすると、CA Access Control は DMS 上にデプロイメント タスクを自動的に作成します。デプロイメント タスク(DEPLOYMENT オブジェクト)は作業指令であり、エンドポイントで実行するために DMS 別に生成されます。各デプロイメント タスクは、それぞれ 1 つのエンドポイント用であり、エンドポイントにデプロイする必要があるポリシー バージョンに関する情報が含まれています。

注: CA Access Control は、UNAB のログイン ポリシーおよび設定ポリシーをデプロイするために、異なるデプロイメント メソッドを使用しています。

格納されたポリシーをデプロイするために使用するメソッドは、CA Access Control が作成するデプロイメント タスクに影響します。以下は、異なるメソッドを使用した結果を示しています。

- 1 つ以上のホストへのポリシー(GPOLICY オブジェクト)の割り当て

  CA Access Control は、各ホストについて、ポリシーの最新のファイナライズされたバージョンのデプロイメント タスクを作成します。

- 1 つ以上のホスト グループへのポリシー（GPOLICY オブジェクト）の割り当て

  CA Access Control は、ホスト グループの 1 つのメンバである各ホストについて、ポリシーの最新のファイナライズされたバージョンのデプロイメント タスクを作成します。

- 格納されたポリシー（GPOLICY オブジェクト）が割り当てられているホスト グループへのホストの追加

  CA Access Control は、新規ホストについて、ポリシーの最新のファイナライズされたバージョンのデプロイメント タスクを作成します。

- ホストへのポリシーの再デプロイ

  CA Access Control は、各ホストについて、ポリシーの最新のファイナライズされたバージョンのデプロイメント タスクを作成します。

- HNODE でのポリシーのリストア（ホストでデプロイが必要なポリシーを再デプロイ）

  CA Access Control は、ホスト上にデプロイする必要がある各ポリシーについて、ホストで有効になっているポリシー バージョンのデプロイメント タスクを作成します。

- 1 つ以上のホストでのデプロイ済みポリシーのアップグレード

  ホストに格納されているポリシー バージョンがホストにデプロイされているポリシー バージョンより新しい場合、CA Access Control は、各ホストについて、最新のファイナライズされたポリシー バージョンのデプロイメント タスクを作成します。

例：ポリシーのホストへの割り当て

ポリシー IIS をホスト「host1.comp.com」および「host2.comp.com」に割り当てると、CA Access Control は 2 つのデプロイメント タスクを作成します。1 つは最新の IIS ポリシー バージョンを host1.comp.com にデプロイするタスクで、もう 1 つは最新の IIS ポリシー バージョンを host2.comp.com にデプロイするタスクです。

例：ポリシーのホスト グループへの割り当て

ホスト グループ「Servers」には、「hostA.comp.com」と「hostB.comp.com」の 2 つのメンバがあります。ポリシー IIS をホスト グループ「Servers」に割り当てると、CA Access Control では 2 つのデプロイメント タスクが作成されます。1 つは最新の IIS ポリシー バージョンを「hostA.comp.com」にデプロイするタスクで、もう 1 つは最新の IIS ポリシー バージョンを「hostB.comp.com」にデプロイするタスクです。

例: ホストの割り当て済みポリシーを持つホスト グループへの追加

ホスト グループ Servers は 2 つの割り当て済みポリシー(「IIS」と「ORACLE」)を持っています。ホスト test.comp.com をホスト グループに追加すると、CA Access Control は 2 つのデプロイメント タスクを作成します。1 つは最新の IIS ポリシー バージョンを test.comp.com にデプロイするタスクで、もう 1 つは最新の ORACLE ポリシー バージョンを test.comp.com にデプロイするタスクです。

例: ホストのリストア

ホストには、policy1 と policy2 の 2 つのポリシーが割り当てられています。ホストをリストアすると、CA Access Control は 2 つのデプロイメント タスクを作成します。1 つは最新のファイナライズされた policy1 バージョンをホストにデプロイするタスクで、もう 1 つは最新のファイナライズされた policy2 バージョンをホストにデプロイするタスクです。

例: デプロイ済みポリシーのアップグレード

ポリシー IIS は 2 つのホスト、host1.comp.com および host2.comp.com 上にデプロイされていますが、ポリシー IIS の最新バージョンは host1.comp.com にデプロイされていません。両方のホスト上でポリシー IIS をアップグレードすると、CA Access Control は 1 つのデプロイメント タスクのみを作成して、最新の IIS ポリシー バージョンを host1.comp.com にデプロイします。

詳細情報:

ホスト アクセス制御および UNAB 設定の仕組み (P. 320)

DMS が保持するエンドポイント データ

環境に拡張ポリシー管理を設定すると、企業内のエンドポイントは設定された DH 経由で、以下の 3 種類のステータス変更を DMS に通知します。

- ポリシーのデプロイおよびデプロイ解除

  ポリシーのデプロイまたはデプロイ解除を実行している場合、エンドポイントは通知を送信します。操作の結果に従って、以下の詳細が更新されます。

  - ポリシーの詳細
  - デプロイのステータス([成功]、[失敗]など)
  - 実行に失敗したポリシー コマンドの selang コマンド出力
  - HNODE ポリシー ステータス([デプロイされました]、[デプロイされましたがエラーがあります]など)

- ホスト ハートビート

  各エンドポイントは設定可能な一定の間隔でハートビートを送信し、ホストがオンラインであることを確認します。

- 偏差ステータス

  各ハートビート送信後、エンドポイントはポリシー偏差を計算し、結果(偏差の検出または未検出)を送信します。

  注: policyfetcher により、エンドポイントと DH 間でのデプロイメントと偏差のステータスの競合が検出された場合は、エンドポイントから受け取った情報に基づいて競合を解決します。

エンドポイントが DMS を更新する仕組み

各エンドポイントは、設定した DH を使用して、ハートビート(ホスト ステータス)、ポリシー ステータスおよび偏差ステータスに関する通知を DMS に送信します。このような DMS 通知は以下のようにして処理されます。

1. DH が通知メッセージを更新ファイルに格納します。

   これは、エンドポイントからのハートビートならびにポリシー デプロイおよびデプロイ解除通知です。

2. DH がそのサブスクライバである DMS にアクセスします。

   - DMS が使用可能でない場合、すべてのメッセージが正常に送信されるまで DH は定期的に DMS との通信を試行します。
   - DMS が使用可能な場合、DH は格納した通知を送信します。

3. DMS が各 DH から受け取った情報を、後で使用するために格納します。

   レポートを作成するたびに、CA Access Control では DMS から情報が取得されます。

.注: UNAB エンドポイントは、DMS を更新するために異なるプロセスを使用します。

詳細情報:

ホスト アクセス制御および UNAB 設定の仕組み (P. 320)

拡張ポリシー管理クラス

CA Access Control が使用する特定のクラスによって、DMS は以下の操作を行います。

- 各コンピュータにデプロイされたポリシーのステータスの最新マップを保持します。
- デプロイメント情報を DH に送信し、エンドポイントが含めるべき関連ポリシー デプロイメント情報を取得できるようにします。

注: これらのクラスに含まれているプロパティの詳細については、「*selang リファレンス ガイド*」を参照してください。

DEPLOYMENT クラス

DEPLOYMENT クラスの各オブジェクトはそれぞれ、ポリシー *デプロイメント タスク* を表わします。ホストに対してポリシーの割り当てまたは割り当て解除を行った場合やポリシーを直接デプロイまたはデプロイ解除した場合、CA Access Control は DMS でデプロイ タスクを自動的に作成します。デプロイメント タスクはまた、次の 3 つの場合に作成されます。割り当てられたポリシーを持つホスト グループにホストを追加（割り当て）またはそのホスト グループからホストを削除（割り当て解除）したときと、ホスト上のポリシーをダウングレードまたはアップグレードしたときと、ホストをリセットまたは復元したときです。

エンドポイントは、このオブジェクトを作業指令として使用します。エンドポイントは保留中の DEPLOYMENT オブジェクト内の情報に基づいてポリシー バージョンをデプロイまたはデプロイ解除します。各作業指令は、それぞれ 1 つのエンドポイントのためのものであり、エンドポイントでデプロイすることが必要なポリシー バージョンに関する情報が含まれています。さらに、DEPLOYMENT オブジェクトは、デプロイが成功したかどうかを示すステータス プロパティ、およびポリシー デプロイ タスクからの selang コマンド出力を含む結果プロパティ（result_message）を保持します。

注: 別の割り当てパスの結果として HNODE にポリシーがすでに存在している場合、デプロイメント タスクは空になる（アクション ステータスを持たなくなる）可能性があります。

詳細情報:

格納されたポリシー バージョンの割り当て (P. 108)
割り当てられたポリシーの割り当て解除 (P. 109)
割り当てられたホストを最新のポリシー バージョンにアップグレード (P. 110)
割り当てられたホストを特定のポリシー バージョンにダウングレード (P. 111)

GDEPLOYMENT クラス

GDEPLOYMENT クラスの各レコードは、*デプロイメント パッケージ*を表します。デプロイメント パッケージは DMS 上で自動的に作成され、特定のホスト向けに同じトランザクション（ポリシー割り当て、アップグレードなど）の結果として作成されるすべてのデプロイメント タスクをひとまとめにします。つまり、作成する各トランザクションが、必要な数のデプロイ タスク（DEPLOYMENT オブジェクト）を作成し、それをホスト（GDEPLOYMENT オブジェクト）ごとにグループ化します。

デプロイメント パッケージによって、ポリシーのデプロイメントを追跡し、トラブルシューティングを行い、トリガ（デプロイメントが開始された理由）を記録できます。

HNODE クラス

HNODE クラスの各オブジェクトは、企業内のエンドポイントを表わします。表している特定のノード、そのノードが属するホスト グループ、そのノードがオンラインで最後に検出された時期に関する情報を保持します。さらに、各 HNODE オブジェクトは、（直接的または間接的な割り当てにより）それが表すノードで有効なポリシー バージョンに関する情報および各ポリシーのステータス（[デプロイされました]、[デプロイされましたがエラーがあります]など）に関する情報を保持します。

HNODE オブジェクトの名前は、実際のホスト名になります。例：
myhost.mydomain.com

GHNODE クラス

GHNODE クラスの各オブジェクトは、CA Access Control ノード（HNODE オブジェクト）のグループを表わします。これにより、ポリシーをデプロイするためにエンドポイントを論理グループにグループ分けすることができます。各 GHNODE オブジェクトは、それが表すノードに割り当てられたポリシーに関する情報を保持します。

POLICY クラス

POLICY クラスの各オブジェクトは、任意のホスト（HNODE オブジェクト）またはホストの論理グループ（GHNODE オブジェクト）にデプロイされるポリシー（GPOLICY オブジェクト）のバージョンを表します。このオブジェクトには、関連付けられたポリシー スクリプトが格納されている場所（どの RULESET オブジェクトか）およびそれがデプロイされる必要があるノードまたはノード グループに関する情報が含まれます。

オブジェクトの名前は、ポリシーの名前にバージョン番号のサフィックスが付いたものです（*policy_name#xx*）。

GPOLICY クラス

GPOLICY クラスの各レコードは、論理ポリシーを表わします。各レコードには、このポリシーに属するポリシー バージョン（POLICY オブジェクト）と割り当て先となるホストとホスト グループに関する情報が含まれます。

オブジェクトの名前は、論理ポリシーの名前です。

RULESET クラス

RULESET クラスの各オブジェクトは、ポリシー バージョンに関連付けられた、デプロイメント スクリプトおよびデプロイメント解除（削除）スクリプトを保持します。

オブジェクトの名前は、対応する POLICY オブジェクト名をベースにしています。

ホストおよびホスト グループ

拡張ポリシー管理を使用するには、CA Access Control が配置される組織のネットワークを定義する必要があります。これを行うには、HNODE オブジェクトを作成してエンドポイント（またはホスト）を表します。同時に、GHNODE オブジェクトを作成して論理ホスト グループを表します。ホストはそのプロパティとポリシー要求に応じて、複数の論理ホスト グループのメンバになることができます。たとえば、Red Hat オペレーティング システムと Oracle を実行しているホストがあるとします。そのホストは、Red Hat 論理ホスト グループのメンバとしてベースライン Red Hat アクセス制御ポリシーを取得することができ、また Oracle 論理ホスト グループのメンバとして Oracle アクセス制御ポリシーを取得することができます。

エンドポイントを企業内のホストとして定義

エンドポイントにポリシーをデプロイし、そのデプロイメント ステータスを表示するには、企業を管理に使用する DMS（デプロイメント マップ サーバ）でエンドポイントを定義する必要があります。CA Access Control を拡張ポリシー管理が有効になっているエンドポイントにインストールする場合、エンドポイントを表わす HNODE レコードが自動的に DMS 上に作成されます。DMS 上のエンドポイントを手動で定義する必要があるのは、CA Access Control をエンドポイントにインストールする前に環境をモデル化する場合のみです。

重要：ユーザは HNODE 名として完全修飾ホスト名を使用する必要があります。そうしないと、エンドポイントはそのデプロイメントを収集しません。

エンドポイントを企業内のホストとして定義する方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ホスト]サブタブを順にクリックし、左側のタスク メニューにある[ホスト]ツリーを展開します。

   [ホストの作成]タスクが使用可能なタスク リストに表示されます。

2. [ホストの作成]をクリックします。

   [ホストの作成：ホストの検索]画面が表示されます。

3. [ホスト タイプの新規オブジェクトの作成]が選択されていることを確認し、[OK]をクリックします。

   [ホストの作成]タスク ページが表示されます。

4. ダイアログ ボックスで以下のフィールドを完了します。

   名前

   エンドポイント(HNODE オブジェクト)の名前を定義します。これは DMS 上で一意の名前とする必要があります(強制)。

   説明

   (オプション)ホストの役割説明(フリー テキスト)を定義します。このフィールドを使用して、エンドポイントの識別に役立つ情報を記録できます。

   IP アドレス

   (オプション)ホストの IP アドレスを定義します。

5. [サブミット]をクリックします。

   タスクがサブミットされ、成功すると、新規ホスト(HNODE)が作成されたことを示すメッセージがすぐに表示されます。

自動ホスト グループ割り当ての動作のしくみ

拡張ポリシー管理が有効にして、エンドポイント上に CA Access Control をインストールすると、CA Access Control エンタープライズ管理 により、ホストが自動的にホスト グループへ割り当てられます。CA Access Control エンタープライズ管理では、ホスト タイプ、オペレーティング システム、インストールされている CA Access Control のバージョン、または定義した他の一般的な属性などの条件に基づいて、ホストがホスト グループへ割り当てられます。その後、ホスト グループへポリシーを割り当てることができます。

注: CA Access Control を Linux エンドポイントにインストールする際に、そのエンドポイントは自動的に「All Linux Hosts」ホスト グループに割り当てられます。そのエンドポイントに UNAB をインストールすると、そのエンドポイントは「All UNAB Hosts」ホスト グループにも自動的に割り当てられます。

CA Access Control エンタープライズ管理 では、以下の方法でホストが自動的にホスト グループへ割り当てられます。

1. エンドポイントでは、拡張ポリシー管理が設定されていると、ハートビートがエンタープライズ管理サーバに送信されます。

   ハートビートには、エンドポイント属性に関する情報が含まれています。

2. エンタープライズ管理サーバでは、ホスト グループの割り当て条件に対してエンドポイント属性が評価され、ホストが適切なホスト グループへ割り当てられます。

ワールド ビューを使用して、各ホスト グループに割り当てられたホストを表示できます。

デフォルトのそのまま使用できるホスト グループ

以下の表には、CA Access Control エンタープライズ管理 に標準装備されているデフォルトのホスト グループが一覧表示されています。

ホスト グループ名	説明
AIX 5.2	すべての AIX 5.2 ホスト用のデフォルト ホスト グループ
AIX 5.3	すべての AIX 5.3 ホスト用のデフォルト ホスト グループ

ホスト グループ名	説明
AIX 6.1	すべての AIX 6.1 ホスト用のデフォルト ホスト グループ
All Linux Hosts	すべての Linux ホスト用のデフォルト ホスト グループ
All UNAB Hosts	すべての UNIX ホスト用のデフォルト ホスト グループ
All Windows Hosts	すべての Windows ホスト用のデフォルト ホスト グループ
ESX Server 3.x	すべての ESX Server 3.x ホスト用のデフォルト ホスト グループ
ESX Server 4.x	すべての ESX Server 4.x ホスト用のデフォルト ホスト グループ
HP-UX 11.23	すべての HP-UX 11.23 ホスト用のデフォルト ホスト グループ
HP-UX 11.31	すべての HP-UX 11.31 ホスト用のデフォルト ホスト グループ
RedHat 3	すべての RedHat 3 ホスト用のデフォルト ホスト グループ
RedHat 4	すべての RedHat 4 ホスト用のデフォルト ホスト グループ
RedHat 5	すべての RedHat 5 ホスト用のデフォルト ホスト グループ
SLES 9	すべての SLES 9 ホスト用のデフォルト ホスト グループ
SLES 10	すべての SLES 10 ホスト用のデフォルト ホスト グループ
SLES 11	すべての SLES 11 ホスト用のデフォルト ホスト グループ
Solaris 8	すべての Solaris 8 ホスト用のデフォルト ホスト グループ
Solaris 9	すべての Solaris 9 ホスト用のデフォルト ホスト グループ
Solaris 10	すべての Solaris 10 ホスト用のデフォルト ホスト グループ

ホスト グループ名	説明
Windows Server 2003	すべての Windows Server 2003 ホスト用のデフォルト ホスト グループ
Windows Server 2003 R2	すべての Windows Server 2003 R2 ホスト用のデフォルト ホスト グループ
Windows Server 2008	すべての Windows Server 2008 ホスト用のデフォルト ホスト グループ
Windows Server 2008 R2	すべての Windows Server 2008 R2 ホスト用のデフォルト ホスト グループ

自動ホスト グループ割り当て条件の変更

CA Access Control エンタープライズ管理 では、オペレーティング システムのタイプなどの事前に定義されている条件を使用して、ホストが自動的にホスト グループへ割り当てられます。デフォルトでは、CA Access Control エンタープライズ管理 により、ホストのオペレーティング システムに応じて、各ホストが自動的にホスト グループへ追加されます。たとえば CA Access Control エンタープライズ管理 では、Windows Server 2003 R2 ホストは、「All Windows Hosts」および「Windows Server 2003 R2」のホスト グループへ自動的に割り当てられます。ホストをホスト グループへ自動的に割り当てるために CA Access Control エンタープライズ管理 で使用される追加条件を指定できます。

自動ホスト グループ割り当て条件の変更方法

1. エンタープライズ管理サーバで selang ウィンドウを開いて、DMS に接続します。
2. 以下の selang コマンドを使用して、ホスト グループを編集し、割り当て条件を指定します。

```
editres GHNODE host_group_name criteria+(attribute=value)
editres GHNODE host_group_name criteria+(attribute!=value)
editres GHNODE host_group_name criteria+(attribute=value)&&(attribute=value)
editres GHNODE host_group_name criteria+(attribute1=value1)
editres GHNODE host_group_name criteria+(attribute2=value2)
editres GHNODE host_group_name criteria-(attribute=value)
```

host_group_name

この条件を割り当てるホスト グループの名前を指定します。

attribute=value

ホスト グループの割り当て属性および値を指定します。このパラメータとして以下の値を使用できます。

HNODE_IP=*IP_address*

定義された IP アドレスが、CA Access Control エンタープライズ管理 によりホスト グループの割り当て条件へ追加されるように指定します。

例: HNODE_IP=172.24.123.456

NODE_TYPE={AC Windows | AC UNIX | AC UNAB}

指定されたエンドポイント タイプが、CA Access Control エンタープライズ管理 によりホスト グループの割り当て条件へ追加されるように指定します。

HNODE_VERSION={ACW | ACU | ACUNAB}:*version*

定義されたエンドポイント バージョンが、CA Access Control エンタープライズ管理 によりホスト グループの割り当て条件へ追加されるように指定します。

例: HNODE_VERSION=ACW:12.53

この例では、バージョン 12.53.1178 の CA Access Control Windows エンドポイントが、CA Access Control エンタープライズ管理 によりホスト グループの割り当て条件へ追加されるように指定されています。

ATTRIBUTES=("*attribute*")

定義された属性情報が、CA Access Control エンタープライズ管理 によりホスト グループの割り当て条件へ追加されるように指定します。

例: ATTRIBUTES=(Microsoft_Windows_Server_2003_R2)

注: 値フィールドにアスタリスクを指定できます。

これで、指定したホスト グループの割り当て条件が変更されました。

例: バージョン別のグループへのホストの割り当て

この例では、CA Access Control バージョン 12.53 をインストールしている Windows ホストのみを自動的に割り当てるように、「All Windows 12.53 Hosts」という名前のホスト グループの割り当て条件を変更します。

```
editres GHNODE ("All Windows 12.53 hosts") criteria+(HNODE_VERSION=ACW:12.53)
```

例: タイプおよびバージョン別でのグループへのホストの割り当て

この例では、タイプ(ACUNIX)および CA Access Control のバージョン別にホストを自動的に割り当てるように、「All UNIX hosts」という名前のホスト グループの割り当て条件を変更します。

```
editres GHNODE ("All UNIX hosts") criteria+(NODE_TYPE=AC
UNIX&&HNODE_VERSION=ACU:12.53)
```

例: タイプまたはバージョン別でのグループへのホストの割り当て

この例では、タイプ(UNAB)または UNAB のバージョン別にホストを自動的に割り当てるように、「All UNAB Hosts」という名前のホスト グループの割り当て条件を変更します。

```
editres GHNODE ("All UNAB Hosts") criteria+(NODE_TYPE=ACUNAB)
editres GHNODE ("All UNAB Hosts") criteria+(HNODE_VERSION=ACUNAB:12.53)
```

例: タイプ別でのホストの除外

この例では、タイプ AC UNIX のすべてのホストを自動的に除外するように、「Non UNIX Hosts」という名前のホスト グループの割り当て条件を変更します。

```
editres GHNODE ("Non UNIX Hosts") criteria+(NODE_TYPE!=AC UNIX)
```

例: 割り当てられた条件の削除

この例では、事前に「All Windows Hosts」という名前のホスト グループに対して割り当ててあった NODE_TYPE 条件を削除します。

```
editres GHNODE ("All Windows Hosts") criteria-(NODE_TYPE=AC Windows)
```

注: ホストの有効な属性を表示するために、DMS 監査ファイルを表示し、ホストのハートビートを見つけることができます。DMS 監査ファイルを表示するには、seaudit -a -fn pmd.audit コマンドを使用します。

論理ホスト グループの定義

関連するエンドポイントで構成されるグループのポリシーを管理するには、それらのエンドポイントを論理ホスト グループとして定義し、グループ全体で拡張ポリシー管理アクションを実行することができます。 ホスト グループを作成するには、あらかじめエンドポイントを DMS 上で定義しておく必要があります。

注: この手順では、CA Access Control エンタープライズ管理 を使用して、DMS 上で論理ホスト グループを定義する方法について説明します。

論理ホスト グループの定義方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ホスト]サブタブを順にクリックし、左側のタスク メニューにある[ホスト グループ]ツリーを展開します。

   [ホスト グループの作成]が使用可能なタスクリストに表示されます。

2. [ホスト グループの作成]をクリックします。

   [ホスト グループの作成: ホスト グループの検索]画面が表示されます。

3. [ホスト グループ タイプの新規オブジェクトの作成]が選択されていることを確認し、[OK]をクリックします。

   [ホスト グループの作成]タスク ページが表示されます。

4. ダイアログ ボックスで以下のフィールドを完了します。

   名前

   論理ホスト グループ(GHNODE オブジェクト)の名前を定義します。

   説明

   (オプション)ホスト グループの役割説明(書式自由)を定義します。このフィールドを使用して、ホスト グループの識別に役立つ情報を記録できます。

5. [ホスト選択]をクリックし、次に[追加]をクリックします。

   [メンバの追加]ダイアログ ボックスが表示されます。

6. ホスト グループに追加するエンドポイントを選択し、[選択]をクリックします。

   [メンバの追加]ダイアログ ボックスを閉じます。選択したエンドポイントが、定義中の論理ホスト グループ用の[メンバ リスト]に追加されます。

7. [サブミット]をクリックします。

   タスクがサブミットされ、成功すると、新規ホスト グループ(GHNODE)が作成されたことを示すメッセージがすぐに表示されます。

ホスト グループのインポート

ホスト グループのインポートは、既存 PMDB 構造を拡張ポリシー管理へ移行するのに役立ちます。ホスト グループをインポートする場合、ホスト グループを作成するか、ホストをホスト グループに追加します。ホストは PMDB のサブスクライバに相当します。

注: 拡張ポリシー管理では、階層ホスト グループをサポートしていません。ホスト グループを PMDB からインポートする場合、すべてのサブスクライバを同じホスト グループに格納します。CA Access Control エンタープライズ管理 は、サブスクライバ PMDB に相当するホストを作成しません。

ホスト グループに追加する各 PMDB サブスクライバについて、CA Access Control エンタープライズ管理 は、サブスクライバに対応するホスト(HNODE オブジェクト)がすでに DMS に存在していないか確認します。対応するホストが DMS に存在すれば、CA Access Control はホスト グループにそのホストを追加します。対応するホストが DMS に存在していなければ、CA Access Control は新しいホストを作成し、ホスト グループに追加します。

ユーザにエンドポイントにアクセスする権限がなければ、エンドポイントはウィザードに表示されず、対応するホストをホスト グループに追加できません。

ホスト グループのインポート方法

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. [ポリシー管理]をクリックします。
   b. [ホスト]サブタブをクリックします。
   c. 左側のタスク メニューで[ホスト グループ]ツリーを展開します。

      [ホスト グループ インポート]タスクが使用可能なタスク リストに表示されます。
2. [ホスト グループ インポート]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。
3. ユーザ名、パスワード、および PMDB 名を入力し、[ログイン]をクリックします。

   注: PMDB 名は「*PMDB 名*@ホスト」形式で、たとえば「master_pmdb@example」のように指定します。

   [全般]タスク ステージに、ホスト グループ インポート ウィザードが表示されます。
4. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

   CA Access Control はホストをホスト グループに追加します。ホストが DMS に存在しなければ、CA Access Control はホストの HNODE オブジェクトを作成してから、ホストをホスト グループ(GHNODE)に追加します。

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

割り当てパス

A *割り当てパス*は、特定のホストまたはホスト グループへのポリシー割り当てを説明するものです。以下のパスで、ポリシーをホストに割り当てることができます。

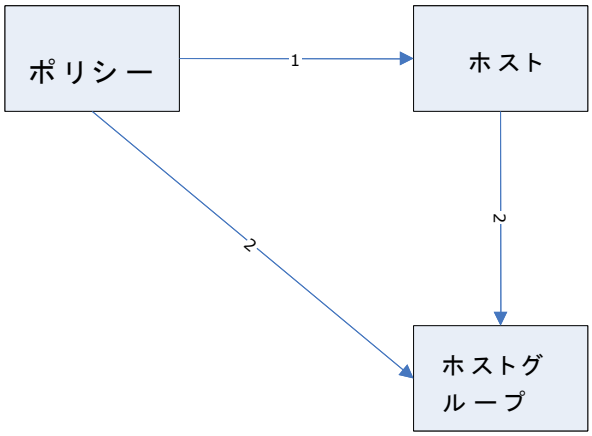
- ポリシーはホストに直接割り当てられます。
- ポリシーはホストが属するホスト グループに割り当てられます。
- ホストは、1 つ以上のポリシーが割り当てられているホスト グループに追加されます。

割り当てパスは重要です。複数の割り当てパスの存在は、拡張ポリシー管理に次のような影響を与えるからです。

- 割り当てパスを 1 つ削除しても、ホストとポリシーの間には別の割り当てパスがまだ存在するので CA Access Control はポリシーのデプロイ解除を行いません。
- 割り当てパスを追加すると、追跡および管理用にデプロイ パッケージとデプロイ タスクが作成されます。しかし、デプロイ タスクのステータスは[*アクションがありません*]となるので、*デプロイ タスクはエンドポイントでポリシーのデプロイを開始しません。*

例: ポリシー IIS の複数の割り当てパス

以下の図は、ポリシー IIS の複数の割り当てパスの例を示しています 。ホスト「host1.comp.com」はホスト グループ「Servers」のメンバです。パス 1 は、ポリシー IIS を直接ホスト「host1.comp.com」に割り当てる場合の、割り当てパスを示しています。パス 2 は、ポリシー IIS をホスト グループ「Servers」に割り当てる場合の、割り当てパスを示しています。



例: 割り当てパスの削除

前の図では、ポリシー IIS はホスト グループ「Servers」、およびホスト「host1.comp.com」に割り当てられています。「host1.comp.com」を「Servers」ホスト グループから 削除すると、パス 2 が削除されます。しかし、CA Access Control はポリシー IIS を「host1.comp.com」からデプロイ解除しません。これは、このポリシーが依然として、ホストに直接割り当てられているためです (パス 1)。

ポリシーを作成しデプロイする方法

拡張ポリシー ベース管理を使用して、ポリシーのドラフト バージョンを格納し、それを確認して必要に応じて変更してから、承認バージョンをデプロイすることができます。

承認されたポリシー バージョンを CA Access Control エンタープライズ管理 を使用してデプロイするには、以下の手順に従います。

1. ポリシー バージョンを DMS に保存します。

   ポリシー バージョンを格納したら、ポリシーを確認およびデプロイできます。

2. ポリシーを確認します。

   一旦ポリシー バージョンが格納されたら、ポリシーに関連付けられたルールを確認する必要があります。

3. ポリシーをファイナライズします。

   ポリシーをファイナライズしたら、ポリシーをデプロイさせるホストまたはホストグループにポリシーを割り当てることができます。

4. 利用可能な割り当てパスのうちの 1 つを使用して、ポリシーをエンドポイントに割り当てます。

   - 格納されたポリシーを、ホストまたはホスト グループに割り当てます。
   - ホストを、すでにポリシーが割り当てられているホストの論理グループに割り当てます。

   一旦ポリシーが割り当てられれば、CA Access Control はポリシーの最新のファイナライズされたバージョンを自動的にデプロイします。

注: UNAB ログインおよび設定ポリシーを作成しデプロイするために、異なるプロセスに従います。

詳細情報:

UNAB ログイン認証の管理 (P. 321)
UNAB ホストまたはホスト グループの設定 (P. 323)
割り当てパス (P. 94)

管理要件

ポリシーを DMS に格納、またはこれらのポリシーを割り当てるには、ユーザおよびユーザが使用しているコンピュータに適切な権限が必要です。

DMS にポリシーを格納する場合

- DMS を管理するのに使用しているコンピュータまたは *policydeploy ユーティリティを実行するのに使用しているコンピュータには、DMS に対する端末権限 (TERMINAL クラス) が必要です。*
- *ユーザには、DMS の POLICY、GPOLICY、および RULESET クラスに対するサブ管理権限が必要です。*

ポリシーをホストまたはホスト グループに割り当てる方法

- DMS を管理しているコンピュータに、DMS の端末権限 (TERMINAL クラス) がある必要があります。
- *ユーザには、DMS の DEPLOYMENT、GDEPLOYMENT、POLICY、GPOLICY、HNODE、および GHNODE (ホスト グループにポリシーを割り当てる場合) クラスに対するサブ管理権限が必要です。*

注: 端末権限およびサブ管理者権限の詳細については、「*UNIX エンドポイント管理ガイド*」および「*Windows エンドポイント管理ガイド*」を参照してください。

ポリシーの依存関係

拡張ポリシー管理では、ポリシーがデプロイおよびデプロイ解除される順序を適用できます。

ポリシーの依存関係を使用すると、1 つまたは複数の他のポリシーに依存するポリシーを定義できます。ただし、依存先のポリシーがすべてデプロイされるまで依存関係のあるポリシーをデプロイすることはできません。同様に、依存関係にある 1 つまたは複数のポリシーがデプロイされている場合、前提条件のポリシーをデプロイ解除することはできません。

ポリシーの依存関係は、ポリシーを作成または変更するときに定義します。

ポリシー検証

ポリシー検証が有効な場合、CA Access Control はポリシーをデプロイする前にポリシーにエラーが含まれていないことを確認します。CA Access Control によってポリシー デプロイメント スクリプトにエラーが検出されると、そのポリシー スクリプトはエンドポイント上で実行されません。そのため、エラーが発生するポリシーはデプロイされず、エンドポイント上のスクリプト エラーがトレース可能になります。ポリシー検証は、デフォルトで無効になっています。

ポリシー検証が有効ではなく、ポリシーのデプロイでエラーが発生した場合、他のコマンドではエラーが発生するにもかかわらず、ポリシー コマンドが実行可能な場合があります。

ポリシー検証は CA Access Control データベース コマンド（AC 環境の selang コマンド）のみを確認します。ポリシー検証では、ネイティブ環境、設定環境、または Policy Model 環境のコマンドは確認しません。ポリシーに AC 環境および他の環境のコマンドが含まれている場合、ポリシー検証は AC 環境のコマンドのみを確認します。

ポリシー検証では、デプロイ解除スクリプトを確認できません。

ポリシー検証の仕組み

ポリシー検証では、ポリシーが実際にエンドポイント上にデプロイされる前に、ポリシーがエラーなくデプロイできることを確認します。

.注: ポリシー検証はデフォルトでは有効になっていません。

以下のプロセスでは、ポリシー検証の仕組みについて説明します。

1. ポリシーをホストまたはホスト グループに割り当てます。
2. 各エンドポイントで、CA Access Control エンタープライズ管理 はポリシーを検証します。
3. 以下の*いずれか*のイベントが発生します。
   - ポリシーにエラーがない場合、CA Access Control エンタープライズ管理 はポリシーをエンドポイントにデプロイします。

     エンドポイントは、ポリシー ステータスが「*デプロイ済み*」の DMS を更新します。
   - ポリシー スクリプトにエラーがある場合、CA Access Control エンタープライズ管理 はエンドポイントにポリシーを*デプロイしません*。

     エンドポイントは、ポリシー ステータスが「*未実行*」の DMS を更新します。また、DMS は、スクリプト エラーのあるポリシーに対応する各デプロイメント タスクのステータスを「*失敗*」に更新します。

     .注: エラーのあるスクリプトを表示するには、CA Access Control エンタープライズ管理 のデプロイメント監査機能を使用できます。

ポリシー検証の有効化

ポリシー検証では、ポリシーが実際にエンドポイント上にデプロイされる前に、ポリシーがエラーなくデプロイできることを確認します。

ポリシー検証を有効にするには、policyfetcher セクションの policy_verification 環境設定値を「1」に設定します。

ポリシー検証が有効になります。

ポリシー バージョンの作成および格納

作成し DMS に格納するポリシーにはすべて、自動的にバージョン番号が付けられます。ポリシーを最初に格納する際に、バージョン番号「01」が付けられます。たとえば、ポリシー「*myPolicy*」を最初に格納するときに、CA Access Control エンタープライズ管理 によって「*myPolicy*」という名前の GPOLICY オブジェクトと「*myPolicy#01*」という名前の POLICY オブジェクトが作成されます。DMS にすでに存在するポリシーを格納するたびに、格納されているポリシーの最新バージョンに 1 を加えて新しいポリシー バージョンが作成されます。たとえば、「*myPolicy*」のバージョンを 28 回目に格納するときに、CA Access Control エンタープライズ管理 によって「*myPolicy#28*」という名前の POLICY オブジェクトが作成されます。

注: この手順では、CA Access Control エンタープライズ管理 を使用してポリシー バージョンを作成および格納する方法について説明します。この手順は UNAB のログインおよび設定ポリシーには適用されません。

ポリシー バージョンの作成および格納

1. (オプション) selang デプロイ コマンドを含む新しいスクリプト ファイルを作成します。

   これらは、企業内のエンドポイントにデプロイするポリシーを作成するために必要なコマンドです。

   重要: ポリシーのデプロイでは、ユーザ パスワードを設定するコマンドはサポートされていません。そのようなコマンドをデプロイ スクリプト ファイルに含めないでください。ネイティブ selang コマンドはサポートされていますが、偏差レポートには示されません。

2. (オプション) selang デプロイ解除コマンドを含む新しいスクリプト ファイルを作成します。

   これらは、企業内のエンドポイントからポリシーをデプロイ解除 (削除) するために必要なコマンドです。

3. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]タスクを順にクリックし、左側のタスク メニューにある[ポリシー]ツリーを展開します。

   [ポリシー]タスクが表示されます。

4. [ポリシーの作成]をクリックします。

   [ポリシーの作成: ポリシー検索]画面が表示されます。

   注: 既存のポリシーについて新しいバージョンを作成する場合は、代わりに[ポリシーの変更]をクリックし、変更するポリシーを検索します。

5. [OK]をクリックします。

   [ポリシーの作成]タスク ページが表示されます。

6. ダイアログ ボックスで以下のフィールドを完了します。

   Name

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

   説明

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

7. [ポリシー スクリプト]タブをクリックし、以下の*いずれかの方法を使用してデプロイおよびデプロイ解除スクリプトを提供します。*

   - デプロイ スクリプトおよびデプロイ解除スクリプトを適切なフィールドに入力します。

     デプロイメント コマンドでスクリプト ファイルを作成しなかった場合は、このオプションを使用します。

   - 既存の selang スクリプト ファイルからコマンドを以下の手順でロードします。

     a. [参照]をクリックし、使用する selang スクリプトが含まれるファイルの場所を特定します。

     b. [ロード]をクリックして、選択したファイルの内容をスクリプト フィールドにロードします。

8. (オプション)このポリシー バージョンに関する説明を入力します。

   これは、このポリシー バージョンに使用するデプロイ スクリプトに関する特定の情報を提供するために使用します。

9. （オプション）[サブミット時にファイナライズ]を選択します。

   このオプションにより、作成した新しいポリシー バージョンはデプロイ可能であることが指定されます。デプロイ スクリプトが完成していない場合は、このオプションをオフにします。

   注: このオプションを選択していない場合は、デプロイ スクリプトを修正するのに、新しいポリシー バージョンを作成する必要はありません。しかし、ファイナライズされていないポリシー バージョンはデプロイできません。

10. [ポリシーの依存関係]タブをクリックし、[追加]をクリックします。

    [メンバの追加]ダイアログ ボックスが表示されます。

11. ポリシーの前提条件として追加するポリシーを選択し、[選択]をクリックします。

    [メンバの追加]ダイアログ ボックスが閉じ、選択したポリシーが、作成中のポリシー用の[メンバ リスト]に追加されます。

12. [サブミット]をクリックします。

    タスクがサブミットされ、成功すると、新規ポリシー バージョンが作成されたことを示すメッセージがすぐに表示されます。UNAB のログインおよび設定ポリシーを作成しデプロイするには、異なるプロセスに従います。

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

詳細情報:

UNAB ログイン認証の管理 (P. 321)
UNAB ホストまたはホスト グループの設定 (P. 323)

変数を定義するポリシーの作成

変数を定義するポリシーを作成しデプロイすると、多くのエンドポイントで同じ変数を定義できます。

変数を定義するポリシーの作成方法

1. 変数を定義する selang デプロイメント コマンドで、スクリプト ファイルを作成します。各変数を定義するために、以下の selang コマンドを使用します。

   ```
   editres ACVAR ("variable_name") value("variable_value")
   ```

2. (オプション) 変数を使用する selang コマンドをスクリプト ファイルに追加します。

   注: ポリシーの後続ルールで変数を参照する前に、ポリシーで各変数を定義する必要があります。変数の参照は、以下の形式で指定します。"<!*変数*>"

3. ポリシーを DMS に保存します。

例: 変数を定義するポリシーの作成

この例では、以下のポリシーで、「/opt/jboss」という値を持つ「jboss_home」という名前の変数を定義し、ユーザ Mark に、JBoss を使用してアクセスする /opt ディレクトリ内の任意のリソースへのアクセスを許可するルールを作成します。

```
editres ACVAR ("jboss_home") value("/opt/jboss")
authorize FILE /opt/* uid(Mark) access(all) via(pgm("<!jboss_home>/jboss"))
```

エンドポイントがポリシーをコンパイルすると、以下のルールを作成します。

```
authorize FILE /opt/* uid(Mark) access(all) via(pgm(/opt/jboss/jboss))
```

例: 複数の変数値を定義するポリシーの作成

以下のポリシーは、「C:¥JBoss」という値を持つ「jboss_home」という名前の変数を定義し、C:¥Program Files¥JBoss 値を jboss_home 変数に追加し、アクセス ルールを作成します。

```
editres ACVAR ("jboss_home") value("C:¥JBoss")
editres ACVAR ("jboss_home") value+("C:¥Program Files¥JBoss")
editres FILE ("<!jboss_home>¥bin") defacc(none) audit(a)
```

エンドポイントがポリシーをコンパイルすると、以下のルールを作成します。

```
editres FILE ("C:¥JBoss¥bin") defacc(none) audit(a)
editres FILE ("C:¥Program Files¥JBoss¥bin") defacc(none) audit(a)
```

例: 変数を使用した、Windows と UNIX の両方のエンドポイントへの同じポリシーのデプロイ

以下の例では、Windows と UNIX で JBoss のインストール場所が異なっている場合でも、変数を使用して、同じ JBoss ポリシーを Windows と UNIX の両方のエンドポイントにデプロイする方法について説明します。この例は、各オペレーティング システムで JBoss のインストール場所を定義する 2 つの jboss_home 変数を定義します。

1. 各オペレーティング システムで JBoss のインストール場所を定義する 2 つの jboss_home 変数を定義します。
   - Windows での JBoss のインストール場所を定義するポリシーを作成し、作成したポリシーを Windows エンドポイントにデプロイします。

     ```
     editres ACVAR ("jboss_home") value("C:¥JBoss")
     ```

   - UNIX での JBoss のインストール場所を定義するポリシーを作成し、作成したポリシーを UNIX エンドポイントにデプロイします。

     ```
     editres ACVAR ("jboss_home") value("/opt/jboss")
     ```

2. jboss_home 変数を使用して JBoss のインストール場所を保護するポリシーを作成し、作成したポリシーを Windows と UNIX のエンドポイントにデプロイします。

   ```
   editres FILE "<!jboss_home>" defacc(none) audit(all)
   ```

   - Windows エンドポイントがポリシーをコンパイルする場合、以下のルールを作成します。

     ```
     editres FILE "C:¥JBoss" defacc(none) audit(all)
     ```

   - UNIX エンドポイントがポリシーをコンパイルする場合、以下のルールを作成します。

     ```
     editres FILE "/opt/jboss" defacc(none) audit(all)
     ```

ポリシーに関連付けられたルールの表示

一旦ポリシーが DMS に格納されると、各ポリシー バージョンのデプロイ スクリプトおよびデプロイ解除スクリプトで、ルールを表示できます。

ポリシーに関連付けられたルールを表示するには、以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[ポリシー]ツリーを展開します。

   [ポリシー]タスクが表示されます。

2. [ポリシーの表示]をクリックします。

   [ポリシーの表示: ポリシー検索]画面が表示されます。

3. 検索範囲を定義して、[検索]をクリックします。

   定義した検索範囲と一致したポリシーのリストが表示されます。

4. 表示するポリシーを選択し、[選択]をクリックします。

   [ポリシーの表示: *policyName*]ページが表示されます。さまざまなタブで、ポリシーのプロパティを参照できます。プロパティには、ポリシーの名前および説明、最新バージョンのデプロイメント スクリプトおよびデプロイメント解除スクリプト、このポリシーに存在するすべてのポリシー バージョンのリスト、ポリシーの作成および更新イベントに関する一般的な情報などが表示されます。

5. [バージョン履歴]タブをクリックします。

   ポリシー バージョンのリストが表示されます。各バージョンには、デプロイおよびデプロイ解除スクリプトへのリンクが設定されています。

6. 以下のいずれかの操作を行います。

   - [デプロイ スクリプト]リンクをクリックします。

     デプロイ スクリプトを示すポップアップ ウィンドウが表示されます。

   - [デプロイ解除スクリプト]リンクをクリックします。

     デプロイ解除スクリプトを示すポップアップ ウィンドウが表示されます。

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

ポリシーのインポート

ポリシーをインポートする場合、CA Access Control エンタープライズ管理 はローカル CA Access Control データベースまたは PMDB から selang ルールをエクスポートし、ルールが含まれているポリシーを作成し、DMS に格納します。これにより、1 つのエンドポイントを保護するルールを多数のエンドポイントを保護可能なポリシーに変換し、PMDB の拡張ポリシー管理への移行に役立ちます。

注: ルールのエクスポート元のエンドポイントまたは PMDB は、CA Access Control r12.0 以降がインストールされているホスト上にある必要があります。以前の CA Access Control バージョンからのポリシーをインポートするには、まず、エンドポイントをアップグレードします。

ポリシーのインポート方法

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. [ポリシー管理]をクリックします。
   b. [ポリシー]サブタブをクリックします。
   c. 左側のタスク メニューで、[ポリシー]ツリーを展開します。

      [ポリシー インポート]タスクが使用可能なタスクリストに表示されます。
2. [ポリシー インポート]をクリックします。

   [ホスト ログイン]ページが表示されます。
3. ユーザ名、パスワード、およびルールのエクスポート元の PMDB またはホストの名前を入力し、[ログイン]をクリックします。

   注: PMDB 名は「*PMDB 名*@ホスト」形式で、たとえば「master_pmdb@example」のように指定します。

   [全般]タスク ステージに、ポリシー インポート プロセス ウィザードが表示されます。

4. 以下のフィールドに入力し、[次へ]をクリックします。

   名前

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

   説明

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

   ポリシー クラス

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

   依存クラスのエクスポート

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

   [ポリシー スクリプト]ステージが表示されます。

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

   [サマリ]ステージが表示されます。

6. [完了]をクリックします。

   ポリシーが作成されます。

格納されたポリシー バージョンの割り当て

特定のホストまたはホスト グループに、最新のファイナライズされたバージョンのポリシーを割り当てることができます。割り当てられたポリシーは自動的にデプロイされます。そのステータスは DMS から監視できます。

注: この手順は、ログイン ポリシーと設定ポリシーには適用されません。

格納されたポリシー バージョンをデプロイする方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブの順にクリックし、左側のタスクメニューにある[割り当て]ツリーを展開し、[ポリシーの割り当て]をクリックします。

   [ポリシーの割り当て]ウィザードの[ポリシー選択]タスク ステージが表示されます。

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

   CA Access Control は、ポリシー割り当てタスクをサブミットします。ホストにポリシーが割り当てられると(直接的に、または論理ホスト グループ メンバシップを介して)、CA Access Control は検索対象のホストごとに DEPLOYMENT タスクを作成します。

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

ポリシーのメンテナンス

デプロイ済みのポリシーに対して、以下のアクションを実行できます。

- ポリシーを割り当てられたホストから割り当て解除する
- ホストを最新のポリシー バージョンにアップグレードする
- ホストを以前のポリシー バージョンにダウングレードする
- ポリシーがエラーなしでデプロイされていることを確認する
- ポリシーまたはポリシー バージョンを削除する

これらのアクションは、CA Access Control エンタープライズ管理 で、または policydeploy ユーティリティを使用して実行します。

割り当てられたポリシーの割り当て解除

特定のホストまたはホスト グループに割り当てられたポリシーは、割り当てを解除することができます。割り当て解除されたポリシーは、自動的にデプロイ解除されます。

割り当てられたポリシーを割り当て解除するには、以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[割り当て]ツリーを展開して、[ポリシーの割り当て解除]をクリックします。

   [ポリシー選択]タスク ステージで[ポリシーの割り当て解除]ウィザードが表示されます。

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

   CA Access Control は、ポリシー割り当てタスクをサブミットします。ホストからポリシーが割り当て解除されると(直接的に、または論理ホスト グループ メンバシップを介して)、CA Access Control は検索対象のホストごとに DEPLOYMENT タスクを作成します。

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

割り当てられたホストを最新のポリシー バージョンにアップグレード

新しいポリシー バージョンは、割り当てられたホストまたはポリシーがデプロイされているホストに対して自動的に送信されません。ポリシーがデプロイされているホストを最新のポリシー バージョンにアップグレードする処理は手動で行う必要があります。

割り当てられたホストを最新のポリシー バージョンにアップグレードするには、以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[割り当て]ツリーを展開して、[ポリシーのアップグレード]をクリックします。

   [ポリシーのアップグレード]ウィザードの[ポリシー選択]タスク ステージが表示されます。

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

   CA Access Control はポリシー アップグレード タスクをサブミットします。ホストでポリシーをアップグレードする場合、CA Access Control は検索対象のホストのために DEPLOYMENT タスクを作成します。

   注: アップグレードするホスト グループを選択すると、CA Access Control エンタープライズ管理 で、デプロイ済みのバージョンより古いバージョンのポリシーを持つホストを含むホスト グループのみから選択できるようになります。

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

割り当てられたホストを特定のポリシー バージョンにダウングレード

間違って 1 つまたは複数のホストに不正なポリシー バージョンを割り当てた場合、または特定のホストのポリシーを以前のバージョンに戻したい場合は、ポリシーのダウングレードが可能です。

割り当てられたホストを特定のポリシー バージョンにダウングレードするには、以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[割り当て]ツリーを展開して、[ダウングレード ポリシー]をクリックします。

   [ダウングレード ポリシー]ウィザードの[ポリシー選択]タスク ステージが表示されます。

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

   CA Access Control は、ポリシー ダウングレード タスクをサブミットします。ホストでポリシーをダウングレードする場合、CA Access Control は検索対象のホストのために DEPLOYMENT タスクを作成します。

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

削除ポリシー

DMS から論理ポリシー（GPOLICY オブジェクト）またはポリシー バージョン（POLICY オブジェクト）を削除できます。ユーザがポリシー バージョンを削除すると、CA Access Control エンタープライズ管理 もそのバージョンに関連付けられているデプロイメント スクリプトおよびデプロイメント解除スクリプト（RULESET オブジェクト）を解除します。論理ポリシーを削除する場合、論理ポリシーに関連付けられたすべてのポリシー バージョン、およびそれらの関連するスクリプトを削除します。

削除された論理ポリシーまたはポリシー バージョンをリストアすることができません。

削除できないポリシー

以下の場合、ポリシーを削除できません。

- 1 つ以上のポリシーのポリシー バージョンを削除できない場合。
- ポリシーが別のポリシーの前提条件になっている場合。

  ポリシーを削除する前に、それに依存するポリシーも削除する必要があります。
- ポリシーがホスト上で割り当てられているかデプロイされている場合。

  ポリシーをホストから割り当て解除するかデプロイ解除してから、ポリシーを削除する必要があります。

削除できないポリシー バージョン

以下のいずれかに当てはまる場合、ポリシー バージョンを削除することはできません。

- ポリシー バージョンがホスト上で有効になっている(割り当てられているかデプロイされている)場合。

  ポリシー バージョンをホストから割り当て解除するかデプロイ解除してから、ポリシー バージョンを削除する必要があります。
- ポリシー バージョンに DMS 上でステータスが存在する場合。

  ポリシー バージョンをホストから割り当て解除するかデプロイ解除してから、ポリシー バージョンを削除する必要があります。ポリシー バージョンを割り当て解除できない、またはデプロイ解除できない場合、ホストから手動で削除する必要があります。
- ポリシーのステータスが「デプロイ解除されたがエラーがある」となっている場合。

  ポリシー バージョンを削除する前に、このステータスを削除する必要があります。

例: 削除できないポリシー バージョン

以下は、削除できないポリシー バージョンの例です。これらは、DMS 上にはステータスがありますが、ホスト上では有効ではありません。

- デプロイされましたがエラーがあります
- 実行されていません

どちらの場合も、ポリシー バージョンを削除する前に、ホストからポリシー バージョンを手動で削除する必要があります。

注: ホスト(HNODE)上でのポリシー ステータスの詳細については、「*リファレンス ガイド*」を参照してください。ポリシー バージョンのステータスの削除の詳細については、「トラブルシューティング ガイド」を参照してください。

ポリシーの削除

ポリシーがもはやホストにもホスト グループに割り当てられていない場合、CA Access Control エンタープライズ管理 からポリシーを削除できます。

重要: ユーザがポリシー(GPOLICY オブジェクト)を削除すると、CA Access Control エンタープライズ管理 は各ポリシー バージョンに関連付けられたポリシー バージョン(POLICY オブジェクト)および RULESET オブジェクトをすべて削除します。

ポリシーを削除するには、以下の手順を実行します。

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[ポリシー]サブタブを順にクリックし、左側のタスク メニューにある[ポリシー]ツリーを展開します。

   [ポリシー]タスクが表示されます。

2. [ポリシーの削除]をクリックします。

   [ポリシーの削除: ポリシー検索]画面が表示されます。

3. 検索範囲を定義して、[検索]をクリックします。

   定義した検索範囲と一致したポリシーのリストが表示されます。

4. 削除するポリシーを選択し、[選択]をクリックします。

   ポリシー削除の確認メッセージが表示されます。

5. [はい]をクリックします。

   ポリシーは削除されます。

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

詳細情報:

削除できないポリシー (P. 112)

ポリシー バージョンの削除

もはや必要のない保存済みポリシー バージョン(POLICY オブジェクト)を削除できます。ユーザがポリシー バージョン(POLICY オブジェクト)を削除する場合、CA Access Control エンタープライズ管理 はポリシー バージョンに関連付けられたデプロイメント スクリプトおよびデプロイメント解除スクリプトをすべて削除します。

ポリシー バージョンを削除するために、以下のコマンドを実行します。

```
policydeploy -delete name#xx [-dms list]
```

-delete *name#xx*

指定されたポリシー バージョンを削除します。

-dms *list*

(オプション) 削除するポリシー バージョンがある DMS ノードを、カンマ区切りリストで指定します。DMS ノードを指定しない場合、policydeploy ユーティリティは、ローカル CA Access Control データベースで指定された DMS ノードのリストを使用します。

例: IIS 5 保護ポリシー バージョンの削除

以下の例は、DMS から割り当て解除されたポリシー バージョン IIS5#05 を削除する方法を示します。この例では、ポリシー バージョン IIS5#05 はどのホストまたはホスト グループにも割り当てられておらず、crDMS@cr_host.company.com DMS ノード上に格納されています。

IIS 5 保護ポリシー バージョンを削除し、コマンド プロンプト ウィンドウを開き、policydeploy ユーティリティを実行する場合:

```
policydeploy -delete IIS5#05
```

ポリシー バージョン IIS5#05 は crDMS@cr_host.company.com DMS ノードから削除されます。

変数

変数によって、構成およびオペレーティング システムが異なるエンドポイントに同じポリシーをデプロイできます。たとえば、Windows と Solaris で CA Access Control のインストール場所が異なる場合でも、変数を使用すると、同じポリシーを Windows と Solaris の両方のエンドポイントにデプロイできます。

変数の作成方法

変数は ACVAR クラスのオブジェクトで、1 つ以上の値を持つことができます。エンドポイント上の各変数の名前は一意である必要があります。また、ポリシー内の各変数の名前は一意である必要があります。変数を作成するには、以下のメソッドのいずれかを使用します。

- CA Access Control エンドポイント管理 を使用して、エンドポイント上の変数を定義する。
- 変数を定義するポリシーを作成して、ポリシーを多くのエンドポイントにデプロイする。

重要: 作成できるのは、ポリシー内で変数を使用するルールのみです。変数が含まれているルールで CA Access Control データベースを直接更新すると、データベースはルールをコンパイルできず、CA Access Control はルールを実行できません。ポリシー スクリプト内で変数を参照する前に、変数を定義する必要があります。

変数タイプ

CA Access Control はユーザ定義変数および組み込み変数をサポートしています。

- ユーザ定義変数は CA Access Control データベース内で定義する変数です。
- 組み込み変数は CA Access Control がインストール時に作成する変数です。組み込み変数を変更することができません。

ユーザ定義変数

CA Access Control は以下のユーザ定義変数をサポートします。

静的変数

CA Access Control エンドポイント上の固定位置を定義します。

名前が同じで値が異なる静的変数を定義できますが、各変数は別々のエンドポイント上に存在し、ポリシーも異なる必要があります。

注: 変数作成時に変数タイプを指定しないと、CA Access Control は静的変数を作成します。

レジストリ値変数

(Windows) レジストリ値をベースに、CA Access Control エンドポイント上の場所を定義します。

注: 定義できるのは、REG_SZ または REG_EXPAND_SZ レジストリ タイプをポイントするレジストリ値のみです。

例: 以下のルールでは、「jboss_home」という名前のレジストリ値を定義できます。

```
editres ACVAR ("jboss_home") value("HKLM¥Software¥Jboss¥home") type(regval)
```

ポリシーでこのルールをデプロイすると、Windows エンドポイントは、HKLM¥Software¥Jboss¥home レジストリ キーの値を使用して、変数値を解決します。

オペレーティング システム変数

オペレーティング システム環境値をベースに、CA Access Control エンドポイント上の場所を定義します。

例: 以下のルールでは、「jboss_home」という名のオペレーティング システム変数を定義します。

```
editres ACVAR (“jboss_home”) value(“JBOSS_HOME”) type(osvar)
```

ポリシーでこのルールをデプロイすると、エンドポイントは、JBOSS_HOME オペレーティング システム環境変数の値を使用して、変数値を解決します。

組み込み変数

CA Access Control は、インストール処理中に、CA Access Control データベース内に組み込み変数を作成します。 組み込み変数は変更も削除もできませんが、ポリシーで使用できます。組み込み変数は動的で、CA Access Control エンドポイントのシステム セッティングに依存します。組み込み変数の値は、対応するシステム設定が変更されると、変更されます。

注: CA Access Control データベースをエクスポートする場合、組み込み変数は出力に含まれません。DMS または PMDB を作成する場合、CA Access Control は組み込み変数を作成しません。

CA Access Control は、以下の組み込み変数をサポートします。

<!HOSTNAME>

ローカル コンピュータの完全修飾ホスト名を識別します。

<!HOSTIP>

ホストの IP アドレスまたはアドレスを識別します。

<!AC_ROOT_PATH>

CA Access Control のインストール パスを識別します。

<!AC_REGISTRY_KEY>

（Windows）CA Access Control のルート レジストリ キーを識別します。

<!USER_OS_ADMIN>

ローカル コンピュータ上のオペレーティング システムの管理者を識別します。

<!DOMAINNAME>

ローカル コンピュータの名前を識別します。

<!DNSDOMAINNAME>

ローカル コンピュータの DNS ドメイン名を識別します。

例: ポリシーでの組み込み変数の使用

この例では、ネットワークリソース ルールを作成します。

```
authorize TCP 8333 uid(*) host(<!HOSTNAME>) access(WRITE)
```

ポリシーをエンドポイント「host1.example.com」にデプロイし、エンドポイントがポリシーに準拠すると、以下のルールが作成されます。

```
authorize TCP 8333 uid(*) host(host1.example.com) access(WRITE)
```

変数使用のガイドライン

変数を使用する場合は、以下のガイドラインに準拠する必要があります。

- 別の変数またはポリシーが使用している変数を削除することはできません。
- 変数は複数の値を持つことができます。変数値は追加または削除できます。
- 変数は入れ子にすることができます。たとえば、以下のルールは、名前が「ac_data」で、組み込み変数、<!AC_ROOT_PATH> を含む変数を定義します。

  ```
  editres ACVAR ac_data value("<!AC_ROOT_PATH>¥data")
  ```

  デフォルトの CA Access Control がインストールされている Windows エンドポイントがこのルールをコンパイルすると、以下のルールが作成されます。

  ```
  editres ACVAR ac_data value("C:¥Program Files¥CA¥AccessControl¥data")
  ```

- 各変数は、タイプを 1 つのみ持つことができます。たとえば、同時に性的変数でありレジストリ値変数である変数を定義することはできません。
- 未定義の変数が含まれているポリシーはデプロイできません。未定義の変数が含まれているポリシーをデプロイすると、CA Access Control によってポリシーのデプロイメント ステータスが[デプロイの一時停止中]に変更されます。ポリシーデプロイするためには、未定義の変数を定義し、ポリシーを再デプロイする必要があります。

  注: ポリシーのどの変数が未定義か検出するには、ポリシーの DEPLOYMENT オブジェクトを確認します。ユーザがポリシー検証を有効にしたか無効にしたかどうかにかかわらず、CA Access Control は未定義の変数がないかどうかの確認を行います。

- CA Access Control は、CA Access Control の変数と Windows のシステム変数が組み合わされたルールを解決できません。たとえば、CA Access Control は、「var1」という名前の変数を定義する以下のルールを解決できません。

  ```
  editres ACVAR var1 value("%SYSTEMROOT%¥temp")
  ```

  %SYSTEMROOT% を CA Access Control 変数として定義し、%SYSTEMROOT%¥temp を保護するポリシーを作成するには、以下のルールを使用します。

  ```
  editres ACVAR var1 value("SYSTEMROOT") type(osvar)
  editres ACVAR var2 value("<!var1>¥temp")
  ```

- CA Access Control は、相互に依存する変数を解決できません。たとえば、CA Access Control は、以下の例の変数「var1」および「var2」を解決できません。

  ```
  editres ACVAR var1 value("<!var2>")
  editres ACVAR var2 value("<!var1>")
  ```

- 変数内でディレクトリを定義するためにスラッシュが使用されている場合、CA Access Control は Windows および UNIX のエンドポイントで正しい方向になるように、スラッシュを解決します。

- selang ルールを使用して変数を定義する場合、エンドポイントにルールをデプロイするポリシーを使用する必要があります。selang ルールを使用してエンドポイント上の CA Access Control データベースを直接更新すると、CA Access Control はルールをコンパイルできません。たとえば、エンドポイント上で「jboss_home」という名の変数を定義していて、以下の selang ルールでデータベースを直接更新する場合:

  ```
  editres FILE <!jboss_home> audit(all)
  ```

  CA Access Control はルールをコンパイルできませんが、代わりに、<!jboss_home> という名前の FILE オブジェクトをデータベース内に作成します。

UNIX エンドポイント上でオペレーティング システム変数を使用するためのガイドライン

UNIX で該当

CA Access Control オペレーティング システム変数（タイプ osvar の ACVAR オブジェクト）は、UNIX 環境変数の値を使用します。UNIX プロセスはそれぞれ独自の環境変数セットを持っているので、UNIX エンドポイント上ではオペレーティング システム変数を使用することはお勧めできません。

UNIX エンドポイント上でオペレーティング システム変数を使用する場合は、CA Access Control を開始する前に、必要な環境変数を設定しエクスポートする必要があります。UNIX エンドポイント上でオペレーティング システム変数を使用する場合は、以下のガイドラインを順守する必要があります。

- コンピュータの起動時に rc 起動スクリプトを使用して CA Access Control を開始する場合、このスクリプトが環境変数を設定しエクスポートしてから CA Access Control を開始することを確認します。
- ユーザが CA Access Control を停止し再起動する場合、ユーザ自身が自分のセッション内で環境変数を設定しエクスポートしてから CA Access Control を再起動する必要があります。

Windows エンドポイント上でオペレーティング システム変数を使用するためのガイドライン

Windows で該当

CA Access Control オペレーティング システム変数（タイプ osvar の ACVAR オブジェクト）は、Windows 環境変数の値を使用します。

Windows エンドポイント上でオペレーティング システム変数を使用する場合は、以下のガイドラインを順守する必要があります。

- 環境変数はシステム変数である必要があります。
- Windows 環境変数の値を変更した場合、CA Access Control を再起動するまで、CA Access Control では変更が認識されません。さらに、Windows の一部のリリースでは、任意の Windows サービスおよび CA Access Control で変更が認識されるためにコンピュータを再起動する必要があります。

エンドポイントで変数を解決する仕組み

変数によって、構成およびオペレーティング システムが異なるエンドポイントに同じポリシーをデプロイできます。以下のプロセスでは、ポリシーの作成およびデプロイ後に、CA Access Control エンドポイントがポリシー内の変数を解決する仕組みについて説明します。

1. policyfetcher がポリシーを取得すると、CA Access Control はポリシー内の変数がポリシーまたは CA Access Control データベースで定義されるかどうか確認します。*以下のいずれか*のイベントが発生します。
   - 変数がポリシーまたはデータベースで定義されていない場合、CA Access Control はポリシーのステータスを[デプロイの一時停止中]に変更します。

     注: .ポリシーをデプロイするには、未定義の変数を定義し、ポリシーを再デプロイする必要があります。
   - 変数がポリシーまたはデータベースで定義されている場合、CA Access Control はポリシーをコンパイルし、そのポリシーが含まれているルールを実行します。
2. すべてのハートビートで、policyfetcher は、CA Access Control データベース内で変数値が変更されているかどうか確認します。*以下のいずれか*のイベントが発生します。
   - 変数値が変わっていない場合、policyfetcher は手順 2 を繰り返します。
   - 変数値が変わっている場合、CA Access Control は、変更された変数を使用している、エンドポイント上の任意のポリシーのポリシー ステータスを[非同期]に変更します。

     注: ポリシーの[非同期]ステータスをクリアするには、ポリシーを再デプロイする必要があります。

ポリシーのデプロイのトラブルシューティング

ホストにポリシーを割り当てる場合、policyfetcher がデプロイメント タスクを取得し、ポリシー スクリプトを実行するまで、ポリシーは割り当てられたエンドポイント上にデプロイされません。したがって、エンドポイントでポリシーが転送されたりデプロイされたりするときに、さまざまな理由でデプロイ エラーが発生する可能性があります。

ポリシー デプロイメント エラーを解決するために、拡張ポリシー管理では以下のようなトラブルシューティング アクションが用意されています。これらのアクションは、CA Access Control エンタープライズ管理 または policydeploy ユーティリティのいずれかを使用して実行できます。CA Access Control エンタープライズ管理では、トラブルシューティング アクションは[ポリシー管理]タブの[ポリシー]サブタブにあります。

以下のようなトラブルシューティング アクションがあります。

- **Redeploy** - ポリシー スクリプトを含む新規デプロイメント タスクを作成し、作成したタスクをエンドポイントにデプロイします。

  エンドポイントでのポリシー デプロイ中にエラーが発生した場合に、このオプションを使用します。つまり、selang ポリシー スクリプトの実行に失敗した場合です。ポリシーのデプロイ解除を行うには、エンドポイントにおけるスクリプト エラーの原因を手動で解決しておく必要があります。

  注: このオプションは CA Access Control エンタープライズ管理 でのみ利用可能で、policydeploy ユーティリティではサポートされていません。

- **Undeploy** - ポリシーを対応するホストから割り当て解除せずに、指定されたエンドポイントからポリシーをデプロイ解除します。

  このオプションは、DMS 上のホストに割り当てられていないエンドポイントから任意のポリシーを削除するために使用します。

- **Reset** - エンドポイントをリセットします。CA Access Control はホスト ステータスをリセットし、有効なポリシーをすべてデプロイ解除します。また、GPOLICY、POLICY、RULESET の各オブジェクトをすべて削除します。

  このオプションを使用すると、すべてのポリシー デプロイからエンドポイントと DMS 上にあるエンドポイントのステータスを削除します。

  注: 監査に必要な場合があるため、このオプションでは DEPLOYMENT オブジェクトや GDEPLOYMENT オブジェクトはエンドポイントまたは DMS から 削除されません。dmsmgr -cleanup 機能を使用すると、エンドポイントをリセットした後に DEPLOYMENT オブジェクトと GDEPLOYMENT オブジェクトを削除することができます。エンドポイントをリセットした後、そのエンドポイントにポリシーを通常どおり割り当てることができます。

- **Restore** - 指定したホスト上のポリシーをすべてデプロイ解除します。次に、新規デプロイ タスクを作成し、そのタスクを実行するホストに送信することによって、ホスト上にデプロイする(アサインまたは直接デプロイする)必要のあるすべてのポリシーをリストアします。

  DMS がエンドポイント上で有効であることを示すポリシーをすべて再デプロイするために、CA Access Control やオペレーティング システムをエンドポイント上に再インストールする場合、またはバックアップからエンドポイントをリストアする場合には、このオプションを使用します。

使用されなくなったエンドポイントの削除方法

DMS は企業に関する情報を格納します。コンピュータから CA Access Control をアンインストールし、そのコンピュータを企業から撤去した場合でも、DMS はそのノードへの参照をまだ保持しています。定期的な保守手順として、これらの古いノードから DMS を消去する必要があります。

古くなったノードを削除するには、以下のいずれかの操作を行います。

- DMS コンピュータ上で dmsmgr ユーティリティを実行して、定期的なクリーンアップを行います。

  `dmsmgr -cleanup number_of_days -dms name`

  number_of_days

  CA Access Control ノードが使用可能でなくなってからの期間の最小日数を定義します。

- DMS コンピュータ上で以下の selang コマンドを発行して、特定のノードを手動で削除することもできます。

  `rr HNODE HNODE_name`

重要: ノードを削除すると、CA Access Control は HNODE 関連のすべてのデプロイタスクを削除し、デプロイタスクのパッケージをすべて削除(ほかのデプロイタスク メンバが含まれていない場合)してから、ようやく HNODE オブジェクトを削除します。

デプロイメント監査情報の表示

CA Access Control エンタープライズ管理 ではポリシー デプロイの監査をサポートしています。この監査では、ポリシーのデプロイメント(デプロイメント タスクの説明リスト)を表示できます。このリストには、各デプロイタスクのトリガ、各デプロイ タスクが作成された日時、必要とされたデプロイのタイプが詳細に示されます。各デプロイタスクについて、さらに探索可能な詳細として、デプロイタスクが作成されたホストおよびポリシー ペア、デプロイされたポリシーのバージョン、デプロイタスクのステータス([キューに入れられました]、[成功]、[失敗])、selang の出力(このコマンドをデプロイした結果)などが挙げられます。

デプロイメント監査情報の表示方法

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. [ポリシー管理]をクリックします。
   b. [ポリシー]サブタブをクリックします。
   c. 左側のタスク メニューで、[デプロイメント]ツリーを展開します。

      [デプロイメント監査]タスクが使用可能なタスク リストに表示されます。
2. [デプロイメント監査]をクリックします。

   [デプロイ監査]ページが表示されます。
3. デプロイ監査の範囲を定義して、[移動]をクリックします。

   CA Access Control エンタープライズ管理 は、定義された範囲内でデプロイに関する情報を取得し、しばらくしてから結果を表示します。
4. (オプション) デプロイのトリガをクリックして、関連付けされたデプロイ スクについて詳細情報を表示します。

ポリシー偏差計算のしくみ

拡張ポリシー管理では、(ポリシー デプロイの結果として)エンドポイントにデプロイする必要があるアクセス ルールと、同じエンドポイントに正常にデプロイされている実際のルールとの違いを確認できます。また、ポリシー オブジェクトに対して行われたプロパティの追加や変更についても解決します。これにより、ポリシーのデプロイに関する問題を解決できます。

エンドポイント上でポリシー偏差計算を実行すると、以下のアクションが実行されます。

1. エンドポイントにデプロイされるルールのリストをローカル ホストから取得します。

   これらは、デプロイされる各ポリシーに指定されたルールです。デプロイされる各ポリシーの POLICY オブジェクトに関連付けられたローカルの RULESET オブジェクトに指定されています。

2. これらの各ルールがエンドポイントに適用されるかどうかをチェックします。

   重要: 偏差計算では、ネイティブ ルールが適用されるかどうかはチェックされません。データベースからオブジェクト(ユーザまたはオブジェクト属性、ユーザまたはリソース権限、あるいは実際のユーザまたはリソース)を削除するルールも無視されます。たとえば、偏差計算では、以下のルールが適用されるかどうかは確認できません。
   rr FILE /etc/passwd

3. (オプション)ローカルのポリシー オブジェクトと DMS のポリシー オブジェクトを比較します。

   通常、偏差計算機能はローカル ホスト上でのみ偏差をチェックします。*-strict* オプションを指定すると、偏差計算機能はローカルの HNODE オブジェクトに関連付けられたポリシーと DMS で HNODE オブジェクトに関連付けられたポリシーも比較します。このツールでは以下の比較を実行します。

   a. ローカル ホストを表す HNODE オブジェクトに関連付けられたポリシーのリスト

   b. HNODE オブジェクトに関連付けられた各 POLICY オブジェクトのポリシーのステータス

   c. HNODE オブジェクトに関連付けられた各 POLICY オブジェクトのポリシーのシグネチャ

4. 以下の 2 ファイルが出力されます。

   - *ACInstallDir*/data/devcalc/deviation.log

     最後の偏差計算で収集されたログとエラー メッセージ。

   - *ACInstallDir*/data/devcalc/deviation.dat

     ポリシーとその偏差のリスト。このファイルの内容は、エンドポイントで selang コマンド *get devcalc* を使用することで取得できます。

   注: CA Access Control は監査イベントも送信します。監査イベントは *seaudit -a* を使用して表示できます。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。

5. 検出された偏差を DMS に通知します。

   通知は、ローカル CA Access Control データベースに指定された DH 経由で DMS に送信されます。

偏差計算機能のトリガ

DMS にポリシー偏差ステータスの最近の情報が含まれるように、偏差計算機能を定期的に実行する必要があります。エンドポイント上で拡張ポリシー管理を有効にすると、各ハートビート送信後に policyfetcher によって偏差計算機能がトリガされます。

注: デフォルトで実行される偏差計算は、エンドポイントに追加された項目を考慮しません。これらの項目を参照するには、devcalc_command 環境設定を変更し、厳密なモードで偏差計算が実行されるようにします。

ポリシー偏差計算機能がユーザ要件をサポートする間隔で実行されるように policyfetcher 設定を変更することをお勧めします。

ポリシーの偏差ログおよびエラー ファイル

ポリシー偏差計算では、各偏差計算の実行時に新しいログが作成されます。このログは、エラー メッセージも含み、*ACInstallDir*/data/devcalc/deviation.log に格納されます。

このログは、レポートに示された（DMS から取得した）偏差が、最後に偏差計算が実行された時点から収集されていない場合に使用します。このログで、偏差計算結果が DMS に送信されなかった理由を診断できます。

例: 偏差ログおよびエラー ファイル

偏差ログおよびエラー ファイルの例を以下に示します。

```
開始時刻: Mon Jan 23 13:04:48 2006
WARNING,¥"DMS ホスト名の取得に失敗しました。偏差はローカルに保存されます。¥"
ポリシー 'iis8#02' の偏差が見つかりました
終了時刻: Mon Jan 23 13:05:04 2006
```

ポリシー偏差データ ファイル

ポリシー偏差計算では、ポリシーとその偏差のリストを含むデータ ファイルが作成されます。このデータ ファイルは、*ACInstallDir*/data/devcalc/deviation.dat に格納されます。

注: データ ファイルに含まれるポリシーのリストは、偏差が計算されるポリシーに応じて異なります(デフォルトでは、すべてのポリシーと、エンドポイントのすべてのポリシー バージョン)。

重要: 偏差計算では、ネイティブ ルールが適用されるかどうかはチェックされません。データベースからオブジェクト(ユーザまたはオブジェクト属性、ユーザまたはリソース権限、あるいは実際のユーザまたはリソース)を削除するルールも無視されます。たとえば、偏差計算では、以下のルールが適用されるかどうかは確認できません。
rr FILE /etc/passwd

偏差ステータスは(偏差があってもなくても)DMS に送信されますが、実際の偏差はローカルに保存されます。レポートの作成時に、実際の偏差結果をこのファイルから取得してレポートに追加できます。

ポリシー偏差データ ファイルに以下の行が表示されることがあります。

Date

偏差計算のタイムスタンプを表示します。日付行は常に偏差レポートの最初の行となります。

形式: DATE, *DDD MMM DD hh:mm:ss YYYY*

Strict

偏差計算が -strict オプションを指定して実行されたことを示します。

形式: STRICT, *DMS@hostname*, *policy_name#xx*, [1|0]

ここで、[1|0] は、ローカルの HNODE オブジェクトに関連付けられたポリシーと、*DMS@hostname*(使用可能な最初の DMS)の HNODE オブジェクトに関連付けられたポリシーとの間に偏差が検出されたか(1)されなかったか(0)を意味します。

ポリシーの開始

このポリシー バージョンの偏差を定義するポリシー ブロックを開始します。

形式: POLICYSTART, *policy_name#xx*

違い

検出されたポリシーの偏差を示します。 偏差に対応するポリシーの名前は、この行の上の直近の*ポリシー行にあります*。

偏差には 7 つのタイプがあります。そのうち 4 つは不在要素を示し、残りの 3 つは追加された要素を示します。これらを次の表に示します。

偏差のタイプ	形式
クラスが見つからない	DIFF, -(*class_name*), (*), (*), (*)
オブジェクトが見つからない	DIFF, (*class_name*), -(*object_name*), (*), (*)
オブジェクトが追加された	DIFF, (*class_name*), +(*object_name*), (*), (*)
プロパティが見つからない	DIFF, (*class_name*), (*object_name*), -(*property_name*), (*)
プロパティが追加された	DIFF, (*class_name*), (*object_name*), +(*property_name*), (*)
プロパティ値が存在しない	DIFF, (*class_name*), (*object_name*), (*property_name*), *-(expected_value*)
プロパティ値が追加された	DIFF, (*class_name*), (*object_name*), (*property_name*), *+(value*)

注: 偏差計算は不在クラスを検出すると、不在のオブジェクト、プロパティ、および値のすべてに対して偏差行を作成します。

ポリシーの終了

このポリシーの偏差を定義するポリシー ブロックの終了です。

形式: POLICYEND, *policy_name#xx*, [1|0]

ここで、[1|0] は、偏差が検出されたか(1)されなかったか(0)を意味します。

警告

警告を示します。

形式: WARNING, "*warning_text*"

例: 偏差データ ファイル

以下の例は、偏差データ ファイルからの抜粋です。

```
Date, Sun Mar 19 08:30:00 2006
警告, "DH ホスト名の取得に失敗しました。偏差はローカルに保存されます"
POLICYSTART, iis8#02
DIFF, (USER), (iispers), (*), (*)
POLICYEND, iis8#02, 1
```

不在要素を示す偏差

偏差計算機能は、不在要素と新規要素の追加を区別します。不在要素は、指定されたポリシーでは明示的に定義されているが、ローカル ホストには存在しない CA Access Control 要素を指しています。このような不在要素になる可能性があるのは、クラス、オブジェクト、プロパティ、および値です。

不在要素の組み合わせにより、階層要件が定義されます。たとえば、Policy1 で以下のルールが定義されているとします。

```
eu mytestuser2 operator
```

この場合、以下の暗黙的な要件が満たされていることが偏差計算機能の前提になります。

- USER クラスが存在する必要がある

  このルールでは、USER クラスに属するユーザが指定されています。

- USER オブジェクト mytestuser2 が存在する必要がある

  このルールでは、USER クラスの mytestuser2 オブジェクトが明示的に参照されています。

- プロパティ OBJ_TYPE が存在する必要がある

  このルールでは、operator パラメータを使用して USER オブジェクトの OBJ_TYPE パラメータを設定します。

- Operator 値が OBJ_TYPE プロパティに割り当てられている

  このルールでは、この値を明示的に設定します。

追加要素を示す偏差

偏差計算機能は、不在要素と新規要素の追加を区別します。追加要素は、ローカルには定義されているが、指定されたポリシーには存在しない CA Access Control 要素を指しています。このような追加要素になる可能性があるのは、オブジェクト、プロパティ、および値です。

ローカル例外で以下のような追加が行われた場合、追加の偏差が取り込まれます。

- ポリシー内に記述されたオブジェクトのプロパティへの新しい値の追加
- ポリシー内に記述されたオブジェクトへの新しいプロパティの追加

注: どのポリシーにも記述されていない新規のオブジェクトは、追加と見なされません。この規則は、新規のクラスにも適用されます。

変更された要素を示す偏差

偏差データ ファイル中の偏差線行が 1 行も変更を示していない場合、変更された要素を示す偏差が発生します。変更を識別するには、同じ要素に適用される連続した削除行および追加行を探す必要があります。たとえば、偏差データ ファイルからの以下の抽出結果では、Operator 値を持っていた mytestuser が Auditor 値および Administrator 値の両方を持つように変更されています。

```
DIFF, (USER), (mytestuser2), (OBJ_TYPE), -(Operator)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Auditor)
DIFF, (USER), (mytestuser2), (OBJ_TYPE), +(Administrator)
```

第 5 章: PUPM の実装計画

このセクションには、以下のトピックが含まれています。

特権ユーザ パスワード管理

特権ユーザ パスワード管理(PUPM)は、組織が組織内の最も強力なアカウントに関連したアクティビティをすべて保護、管理、追跡するプロセスです。

PUPM は、中央の場所から、ターゲット エンドポイント上の特権アカウントに対してロール ベースのアクセス管理を行います。PUPM では、特権アカウントおよびアプリケーション ID のパスワードを安全に保管できます。また、定義したポリシーに基づいて特権アカウントおよびパスワードへのアクセスを制御します。さらに、PUPM を使用することにより、特権アカウントおよびアプリケーション パスワードのライフサイクルを管理し、環境設定ファイルとスクリプトからパスワードを削除することができます。

特権アカウントについて

特権アカウントは、個々のアカウントに割り当てられず、ミッション クリティカルなデータおよびプロセスへのアクセス権を持つアカウントです。システム管理者は特権アカウントを使用して、ターゲット エンドポイント上で管理者タスクを実行します。特権アカウントは、ユーザが操作しなくても処理が進むように、サービス ファイル、スクリプト、環境設定ファイルに埋め込まれています。。

特権アカウントは識別可能なユーザに割り当てられないので、管理が難しく、監査と追跡が難しくなります。これは、偶然および有害なアクティビティに基幹システムを露出する脆弱性です。組織は、こうした特権アカウントの数を運用上のニーズを満たす最小限に減らす必要があります。

管理者は、ほとんどの内部制御をバイパスして、制限された情報にアクセスすることができます。また、アプリケーションを削除したり、アプリケーションをアクセス不能にしたりすることによって、サービス妨害(DOS)攻撃を引き起こすことができます。さらに、特権アカウントを使用して実行されたアクティビティは、識別可能なユーザ アカウントに関連付けるのが容易ではありません。

特権アクセス ロールおよび特権アカウント

特権アクセス ロールは、各ユーザが CA Access Control エンタープライズ管理で実行できる PUPM タスクと、各ユーザがチェックインおよびチェックアウトできる特権アカウントを指定するために使用します。CA Access Control エンタープライズ管理 は、定義済みの特権アクセス ロールが用意されています。定義済みのロールを自分の組織に合わせて変更することも、または新しいロールを作成することもできます。

ユーザが CA Access Control エンタープライズ管理 にログインすると、それぞれのロールに対応するタスクと特権アカウントだけが表示されます。

詳細情報:

特権アクセス ロール (P. 25)

特権アクセス ロールの使用

企業の要件に応じて PUPM をセットアップする前に、以下のポイントを考慮する必要があります。

- ユーザ ストアとして Active Directory を使用し、各ロールのメンバ ポリシーを変更して、それぞれが Active Directory のグループを指すようにすることをお勧めします。この方法でセットアップしたロールからユーザを追加または削除するには、Active Directory グループからユーザを追加または削除します。これにより、管理上のオーバーヘッドが減少します。

- ユーザ ストアとして Active Directory を使用する場合は、CA Access Control エンタープライズ管理 を使用してユーザまたはグループを作成または削除できません。ユーザおよびグループの作成と削除は、Active Directory 内だけで行うことができます。
- あるロールに対してメンバ ポリシーが定義されている場合、PUPM ユーザ マネージャがそのロールをユーザに割り当て、ユーザがそのメンバ ポリシーに適合しないときには、CA Access Control はそのユーザにロールを割り当てません。メンバ ポリシーで定義されるルールは、PUPM ユーザ マネージャによる割り当てに優先します。
- 特権アカウント リクエストに応答するには、PUPM 承認者ロールを持っており、かつ要求ユーザのマネージャである必要があります。組み込みユーザ ストアを使用すると、CA Access Control エンタープライズ管理 では、ユーザの作成タスクおよびユーザの変更タスクでユーザのマネージャを指定できます。
- CA Access Control では、そのまま使用できる Break Glass、PUPM 承認者、特権アカウント リクエスト、および PUPM ユーザ ロールがすべてのユーザに割り当てられます。この動作を変更するには、各ロールのメンバ ポリシーを変更します。
- ロールのスコープ ルールを変更して、そのロールがアクセスできる特定のエンドポイントおよび特権アカウントを定義できます。スコープ ルールを使用すると、組織全体の特権アカウントへのアクセスを詳細に指定できます。スコープ ルールは、ロールのメンバ ポリシーで定義します。

詳細情報:

メンバ ポリシー (P. 31)

特権アクセス ロールがチェックアウトおよびチェックイン タスクに与える影響

エンドポイント上で管理タスクを実行するときには特権アクセスをチェックアウトし、エンドポイント上でのタスクが完了したら特権アクセスをチェックインします。

重要: ユーザには、エンドポイント タイプ上でタスクを実行するためのエンドポイント特権アクセスロールが必要です。エンドポイント特権アクセス ロールは、ユーザが特権アクセス アカウントを使用してタスクを実行できるエンドポイントのタイプを指定します。たとえば、Windows エージェントレス エンドポイント特権アクセス ロールをユーザに割り当てた場合、そのユーザは、Windows エンドポイント上で特権アカウントを使用するエンドポイント タスクを実行できます。ユーザに Break Glass、特権アカウント リクエスト、または PUPM ユーザ ロールを割り当てた場合は、同時にエンドポイント特権アクセスロールも割り当てる必要があります。そのようにしない場合、ユーザはタスクを完了できません。

以下のプロセスでは、ユーザが実行するチェックアウトおよびチェックイン タスクに特権アクセスロールがどのような影響を与えるかについて説明します。

1. 特権アカウントのチェックアウトは、以下のいずれかの方法で行います。
   - PUPM ユーザ ロールが割り当てられたユーザは、特権アカウントをチェックアウトします。
   - Break Glass ロールが割り当てられたユーザは、Break Glass チェックアウトを実行します。
   - アプリケーション(たとえば CLI のパスワード コンシューマ)により、CA Access Control のエンドポイント上で特権アカウントがチェックアウトされます。

   特権アカウントがチェックアウトされます。

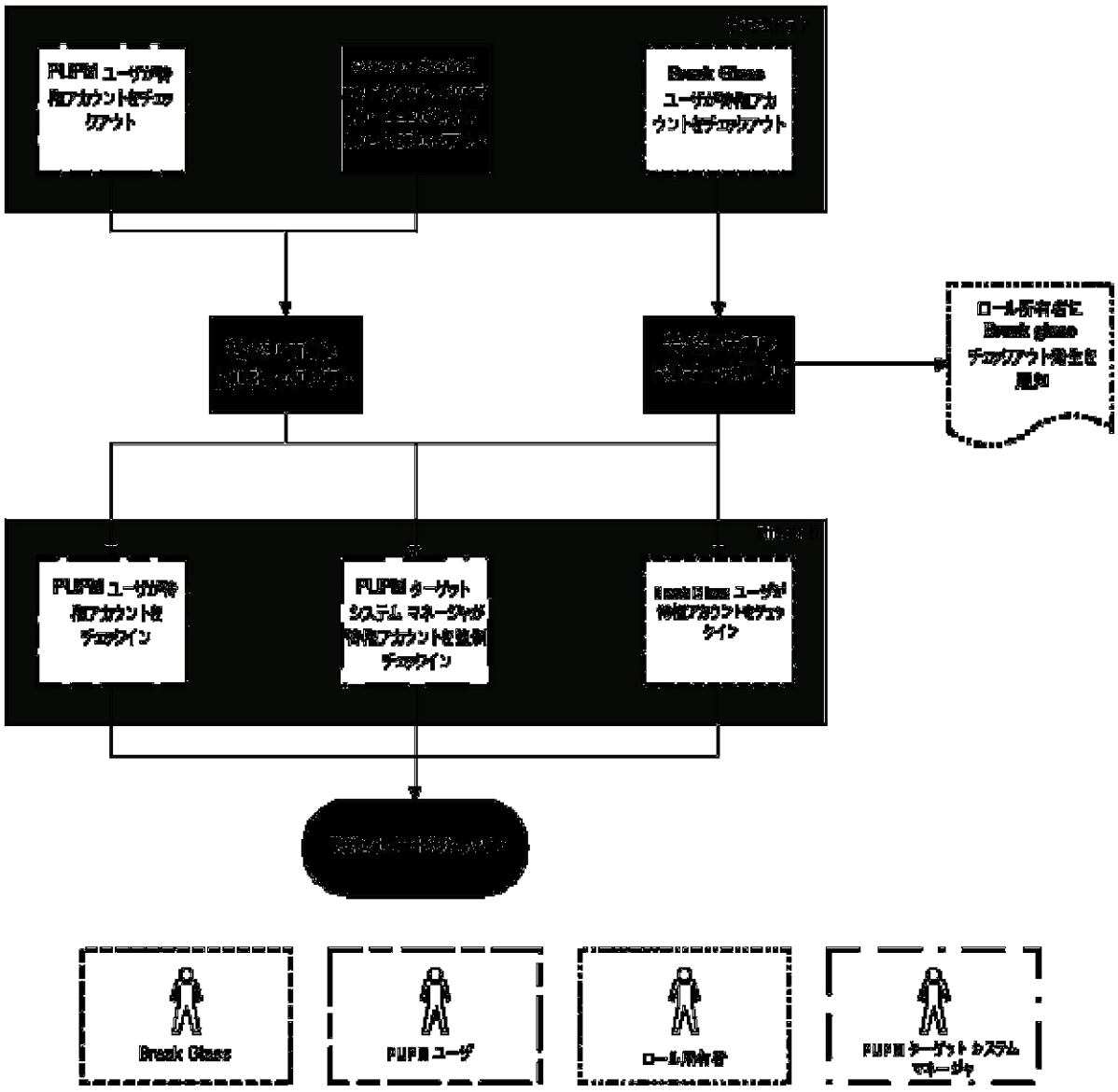
   注: Break Glass チェックアウトを実行した場合、CA Access Control はロール所有者に通知メッセージを送信します。ロール所有者は、監査目的でこのメッセージに情報を追加するように選択できます。

2. 特権アカウントのチェックインは、以下のいずれかの方法で行います。

   - PUPM ユーザ ロールが割り当てられたユーザは、特権アカウントをチェックインします。
   - Break Glass ロールが割り当てられたユーザは、特権アカウントをチェックインします。
   - CA Access Control エンドポイント上のアプリケーションは、特権アカウントをチェックインします。
   - PUPM ターゲット システム マネージャ ロールが割り当てられたユーザは、特権アカウントのチェックインを強制します。

   特権アカウントがチェックインされます。

次の図に、ユーザが実行するチェックアウトおよびチェックイン タスクに特権アクセス ロールが与える影響を示します。



例: 特権アカウントのチェックアウト

あなたはシステム マネージャ ロールを持っています。あなたは Joe に対して、PUPM ユーザ ロールおよび Windows エージェントレス接続エンドポイント特権アクセス ロールを割り当てます。CA Access Control エンタープライズ管理 にログインした Joe には、Windows エンドポイント上で特権アカウントをチェックアウトおよびチェックインするタスクだけが表示されます。

例: 特権アカウントの Break Glass

あなたはシステム マネージャ ロールを持っています。あなたは Fiona に対して、Break Glass ロールおよび Oracle Server 接続エンドポイント特権アクセス ロールを割り当てます。Fiona は、Oracle エンドポイントへの即時アクセスを必要としています。CA Access Control エンタープライズ管理 にログインした Fiona には、Oracle エンドポイント上でアカウントの Break Glass チェックアウトを実行するタスクだけが表示されます。Fiona は、Oracle 特権アカウントの Break Glass チェックアウトを実行し、CA Access Control は Break Glass ロール所有者に通知メッセージを送信します。

注: デフォルトでは、Break Glass ロール所有者はシステム マネージャ管理ロールです。

特権アクセス ロールが特権アカウント リクエスト タスクに与える影響

特権アカウントをチェックアウトできず、アカウントへの即時アクセスを必要としないユーザは、特権アカウント リクエストをサブミットできます。ユーザのマネージャは、その特権アカウント リクエストを承認または拒否できます。このトピックでは、特権アカウント リクエスト タスクを実行するために必要な特権アクセス ロールについて説明します。

重要: ユーザには、エンドポイント タイプ上でタスクを実行するためのエンドポイント特権アクセスロールが必要です。エンドポイント特権アクセス ロールは、ユーザが特権アクセス アカウントを使用してタスクを実行できるエンドポイントのタイプを指定します。たとえば、Windows エージェントレス エンドポイント特権アクセス ロールをユーザに割り当てた場合、そのユーザは、Windows エンドポイント上で特権アカウントを使用するエンドポイント タスクを実行できます。ユーザに Break Glass、特権アカウント リクエスト、または PUPM ユーザ ロールを割り当てた場合は、同時にエンドポイント特権アクセスロールも割り当てる必要があります。そのようにしない場合、ユーザはタスクを完了できません。

以下のプロセスでは、ユーザが実行できる特権アカウント リクエスト タスクに特権アクセス ロールがどのような影響を与えるかについて説明します。

1. 特権アカウント リクエスト ロールが割り当てられたユーザは、特権アカウントへのアクセスを要求できます。
2. CA Access Control は、ユーザのマネージャ（同時に PUPM 承認者ロールを持つ）に特権アカウント リクエストを送信します。

   注: 特権アカウント リクエストを受信するには、PUPM 承認者ロールが付与されており、かつユーザのマネージャである必要があります。

3. PUPM 承認者ロールを持つユーザは、特権アカウントリクエストに応えて以下のいずれかを行います。

   - 特権アカウントリクエストを拒否する。

     特権アカウントリクエスト ロールを持つユーザは、特権アカウントをチェックアウトできません。

   - 特権アカウントリクエストを保留する。

     他のユーザは、特権アカウントリクエストを承認または拒否できません。特権アカウントリクエスト ロールを持つユーザは、PUPM 承認者がリクエストの承認を選択するまで特権アカウントをチェックアウトできません。

   - 特権アカウントリクエストを承認する。

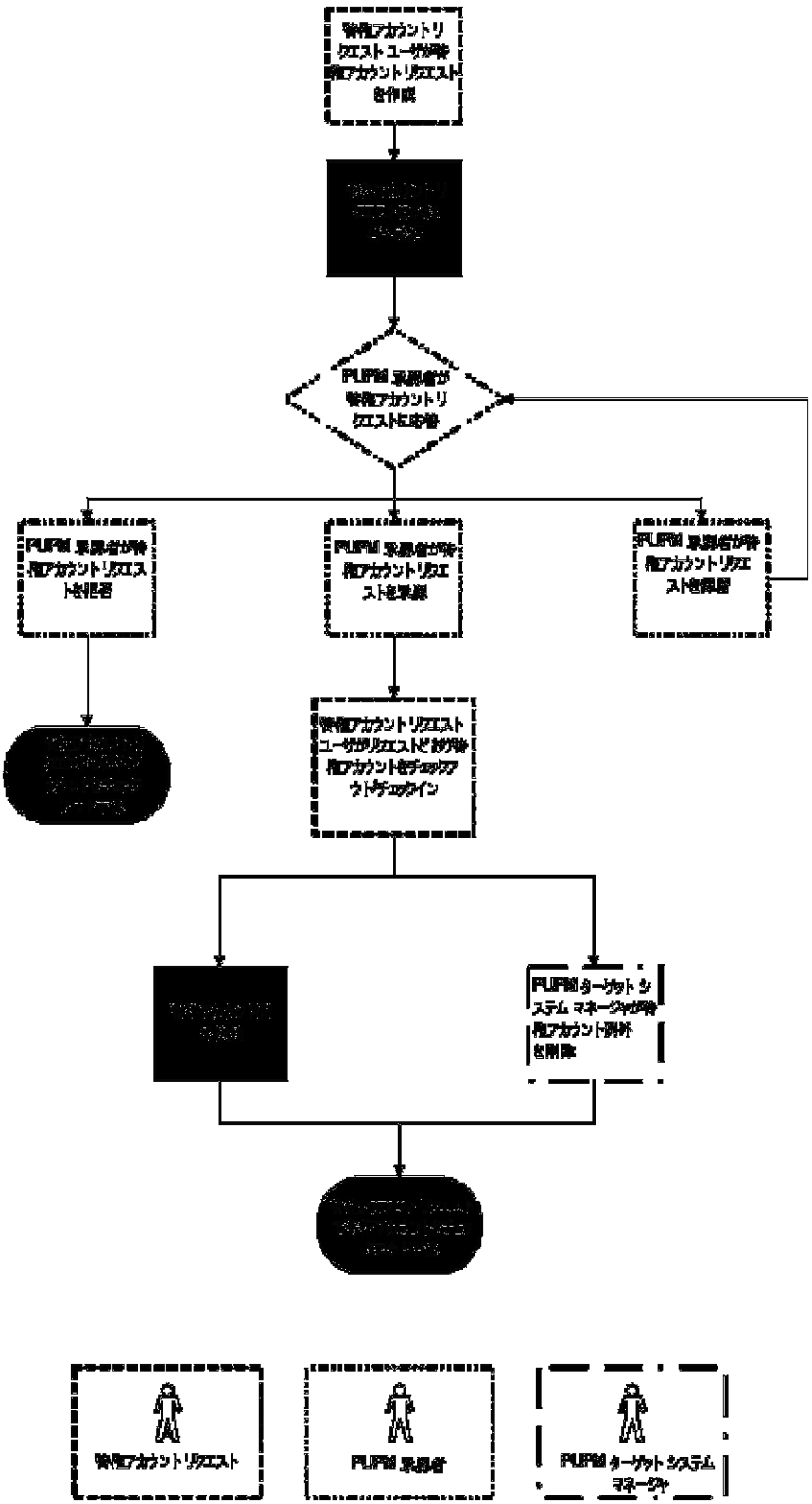
     特権アカウントリクエスト ロールを持つユーザに特権アカウント例外が付与され、そのユーザは特権アカウントをチェックアウトおよびチェックインできます。

4. 特権アカウント例外は、以下のいずれかの理由で期限切れになります。

   - 特権アカウント例外で指定された有効期限に到達した。
   - PUPM ターゲット システム マネージャ ロールが割り当てられたユーザが特権アカウント例外を削除した。

   特権アカウントリクエスト ロールを持つユーザは、特権アカウントをチェックアウトできなくなります。

以下の図に、ユーザが実行できる特権アカウントリクエスト タスクに特権アクセス ロールがどのような影響を与えるかを示します。


特権アカウントリクエスト
PUPM 承認者
PUPM ターゲット システム マネージャ

例: 特権アカウント リクエストの実行および応答

あなたはシステム マネージャ ロールを持っています。あなたは Alice に対して、特権アカウント リクエスト ロールおよび SSH Device 接続エンドポイント特権アクセス ロールを割り当てます。Bob は Alice のマネージャであり、あなたは Bob に PUPM 承認者ロールを割り当てます。

CA Access Control エンタープライズ管理 にログインした Alice には、UNIX エンドポイントで特権アカウント リクエストをサブミットするタスクだけが表示されます。Alice は、UNIX エンドポイントで example_ux アカウントの特権アカウント リクエストをサブミットします。

CA Access Control エンタープライズ管理 にログインした Bob には、特権アカウント リクエストに応答するタスクだけが表示されます。Bob は、Alice の特権アカウント リクエストを許可し、その有効期限を午後 6 時までと指定します。これで、Alice は example_ux 特権アカウントをチェックアウトできるようになりました。午後 6 時で特権アカウント例外は期限切れになり、Alice は example_ux 特権アカウントをチェックアウトできなくなります。

Break Glass プロセス中に発生するイベント

管理権限がないアカウントへの即時アクセスが必要な場合、ユーザは break glass チェックアウトを実行します。

Break Glass アカウントは、ユーザ ロールに従ってユーザに割り当てられていない特権アカウントです。しかし、必要であれば、ユーザはそのアカウント パスワードを取得することができます。

Break Glass チェックアウト プロセスでは、Break Glass チェックアウト プロセスが発生したことを管理者に伝える通知メッセージがロール管理者に送信されます。しかし、管理者はこのプロセスを承認も停止もできません。

チェックアウトされた Break Glass アカウントが、[ホーム]タブの[Break Glass]オプションにある、ユーザの[マイ チェックアウト特権アカウント]タブに追加されます。

注: Break Glass 特権アクセス ロールを持つユーザのみが、Break Glass プロセスを実行できます。

パスワード コンシューマ

*パスワード コンシューマ*はアプリケーション、Windows サービスおよび Windows スケジュール タスクであり、特権アカウントおよびサービス アカウントを使用して、スクリプトの実行、データベースへの接続、あるいは Windows サービス、スケジュール タスク、RunAs コマンドを管理します。*サービス アカウント*は、Windows サービスによって使用される内部アカウントです。たとえば、Windows サービスでは、オペレーティング システムへのログインに NT AUTHORITY¥LocalService サービス アカウントが使用されます。

パスワード コンシューマを使用すると、アプリケーション スクリプトからハードコードされたパスワードを削除したり、エンドポイントにパスワード ポリシーを適用することができます。たとえば、Windows のエンドポイント上のスケジュールされた各タスクにパスワード コンシューマを作成して、各パスワード コンシューマにより同じパスワード ポリシーが使用されるように指定できます。次に PUPM により、パスワード ポリシーで指定された間隔でスケジュールされた各タスクのパスワードが変更されます。

PUPM によりパスワード コンシューマに特権アカウント パスワードが提供される方法は、以下のとおりです。

- オンデマンド -- パスワード コンシューマにより特権アカウントに要求が送信される場合。たとえば、特権アカウントで、認証を必須とするデータベースへの接続にオープン データベース接続が使用される場合。

  注: オンデマンドでパスワードを取得するパスワード コンシューマを使用するには、PUPM 統合機能を有効にした PUPM エンドポイント上に CA Access Control をインストールする必要があります。

- パスワードの変更時 -- CA Access Control エンタープライズ管理 でパスワード コンシューマに対してパスワードの変更イベントが発生した場合。たとえば、パスワード ポリシーで、ある一定の時間が経過したらサービス アカウント用のパスワードが変更されるように指定されている場合。

  注: パスワード変更でパスワードを取得するパスワード コンシューマを使用するには、PUPM エンドポイントに CA Access Control をインストールする必要はありません。

パスワード コンシューマのタイプ

パスワード コンシューマは、PUPM エンドポイント上で実行されるアプリケーション、Windows サービス、または Windows スケジュール タスクの表現形です。ソフトウェア開発キット パスワード コンシューマを除いて、他のすべてのパスワード コンシューマでは特権アカウント パスワードが取得されますが、パスワードのチェックアウトおよびチェックインは行われません。

PUPM では以下のパスワード コンシューマに特権アカウント パスワードがオンデマンドで提供されます。

- **Software Development Kit（SDK/CLI）** -- ソフトウェア開発キット パスワード コンシューマでは、エンドポイント上のスクリプトによって実行される場合に特権アカウント パスワードが要求されます。

  スクリプト内のハードコードされたパスワードを置き換えるには、ソフトウェア開発キット パスワード コンシューマを使用します。

  注: 他のパスワード コンシューマと異なり、ソフトウェア開発キット パスワード コンシューマでは特権アカウント パスワードのチェックアウトとチェックインが可能です。

- **データベース（ODBC、JDBC、OLEDB、OCI、.NET）** -- データベース パスワード コンシューマでは、エンドポイント上で実行されているプログラムがデータベースに接続するときに特権アカウント パスワードが要求されます。

  データベースに接続するプログラム内のハードコードされたパスワードを置き換えるには、データベース パスワード コンシューマを使用します。

- **Windows 実行ユーザ** -- Windows 実行ユーザ パスワード コンシューマは、ユーザが特権アカウントの代理として特定のコマンドを実行するために RunAs アプリケーションを実行する際に、パスワードを要求します。

  ユーザが特権アカウントの代理として特権アカウント パスワードを使用せずにコマンドを実行する場合に、Windows 実行ユーザ パスワード コンシューマを使用します。

注: オンデマンドでパスワードを取得するパスワード コンシューマを使用するには、PUPM 統合機能を有効にした PUPM エンドポイント上に CA Access Control をインストールする必要があります。

PUPM では、パスワードの変更時に、以下のパスワード コンシューマに特権アカウント パスワードが提供されます。

- **Windows スケジュール タスク** -- Windows スケジュール タスク パスワード コンシューマでは、サービス アカウントを使用してスケジュールされたタスクが管理されます。CA Access Control エンタープライズ管理 で、パスワードの変更イベントが発生する場合は常に、PUPM により、タスク用パスワードが強制的に変更されます。

  パスワード ポリシーを設定しスケジュール タスク用のパスワードの変更を自動化するには、Windows スケジュール タスク パスワード コンシューマを使用します。

- **Windows サービス** -- Windows サービス パスワード コンシューマでは、Windows サービスの実行にサービス アカウントが使用されます。CA Access Control エンタープライズ管理 で、パスワードの変更イベントが発生する場合は常に、PUPM により、サービス アカウント用パスワードが強制的に変更されます。

  パスワード ポリシーを設定し Windows サービス用のパスワードの変更を自動化するには、Windows サービス パスワード コンシューマを使用します。このサービスは、パスワードを変更できるアカウント、たとえば、コンピュータの管理者アカウントまたはドメイン アカウントにより実行される必要があります。

注: パスワード変更でパスワードを取得するパスワード コンシューマを使用するには、PUPM エンドポイントに CA Access Control をインストールする必要はありません。

詳細情報:

パスワード コンシューマの作成 (P. 259)

パスワード コンシューマがパスワードをオンデマンドで取得する方法

パスワード コンシューマでは、関連付けられた特権アカウントが別のアプリケーションに対して認証する際に、PUPM からパスワードが取得されます。パスワードをオンデマンドで取得するパスワード コンシューマでは、CA Access Control エンタープライズ管理 との通信にメッセージ キューを使用する PUPM Agent にパスワード要求が転送されます。

ソフトウェア開発キット、データベース、および Windows 実行ユーザのパスワード コンシューマは、パスワードをオンデマンドで取得します。スクリプト内のハードコードされたパスワードを置き換える場合は、パスワードをオンデマンドで取得するパスワード コンシューマを使用します。アプリケーションにより認証を目的としてパスワードが提供される場合は常に、PUPM により、ハードコードされたパスワードが特権アカウント パスワードで置き換えられます。

注: オンデマンドでパスワードを取得するパスワード コンシューマを使用するには、PUPM 統合機能を有効にした PUPM エンドポイント上に CA Access Control をインストールする必要があります。

以下のプロセスでは、パスワード コンシューマにより特権アカウント パスワードがオンデマンドで取得される方法が説明されています。

1. アプリケーションでは、ユーザ認証を必須とするシステムへの接続が試みられる場合に、ハードコードされたパスワードが使用されます。
2. パスワード コンシューマにより、接続の試行がインターセプトされます。

   たとえば、OCI パスワード コンシューマでは、Oracle データベースへの接続の試行がインターセプトされます。
3. PUPM Agent によりキャッシュが確認されます。以下の*いずれか*のイベントが発生します。
   - 要求がキャッシュされる場合、PUPM Agent によりパスワード コンシューマへ特権アカウント パスワードが転送されます。パスワード コンシューマでは、ハードコードされたパスワードが特権アカウント パスワードに置き換えられます。アプリケーションでは、システムへのログインに特権アカウント パスワードが使用されます。このステップで、プロセスが終了します。CA Access Control エンタープライズ管理 では、パスワードの取得に関しては監査レコードには書き込まれません。
   - 要求がキャッシュされない場合、PUPM Agent により CA Access Control エンタープライズ管理 へパスワード要求が転送されます。

4. CA Access Control エンタープライズ管理 によりメッセージが受け取られ、パスワード コンシューマが特権アカウント パスワードを取得する権限を付与されているかどうかが確認されます。
5. 以下の*いずれか*のイベントが発生します。
   - パスワード コンシューマがパスワードを取得する権限を付与されている場合、CA Access Control エンタープライズ管理 では PUPM Agent に特権アカウント パスワードが送信されます。PUPM Agent により、ハードコードされたパスワードが特権アカウント パスワードに置き換えられます。アプリケーションでは、システムへのログインに特権アカウント パスワードが使用されます。CA Access Control エンタープライズ管理 により、イベントに関して監査レコードに書き込まれます。
   - パスワード コンシューマがパスワードを取得する権限を付与されていない場合、CA Access Control エンタープライズ管理 では PUPM Agent にエラー メッセージが送信されます。PUPM Agent ではアプリケーションにパスワードが転送されないため、アプリケーションでは、システムへのログインにハードコードされたパスワードが使用されます。

PUPM がパスワード コンシューマにパスワードの変更を通知する方法

CA Access Control エンタープライズ管理 でパスワードの変更イベントが発生した場合、たとえば、一定の時間が経過したらパスワードを変更する必要があることがパスワード ポリシーにより指定されている場合、PUPM により、パスワード コンシューマにパスワードの変更が強制されます。CA Access Control エンタープライズ管理 では、パスワードの変更時にパスワードを取得するパスワード コンシューマとの通信に JCS が使用されます。

パスワードの変更時にパスワードを取得するのは、Windows スケジュール タスクおよび Windows サービス パスワード コンシューマのみです。

注: パスワード変更でパスワードを取得するパスワード コンシューマを使用するには、PUPM エンドポイントに CA Access Control をインストールする必要はありません。

以下のプロセスでは、PUPM によりパスワード コンシューマにパスワードの変更が通知される方法が説明されています。

1. パスワードの変更イベントにより、新規パスワードが生成されます。
2. CA Access Control エンタープライズ管理 により、そのパスワードを使用するパスワード コンシューマが中央データベースで検索されます。

3. JCS では、エンドポイントの作成時に提供した管理者クレデンシャルを使用して、該当する各エンドポイントにログインされます。
4. JCS により、エンドポイントでのパスワード コンシューマのパスワード変更が試みられます。以下の*いずれか*のイベントが発生します。
   - JCS では、エンドポイントでのパスワード コンシューマのパスワードが変更され、オプションでサービスが再起動されます。

     注: パスワード コンシューマを作成する際に、JCS によりサービスが再起動されるかどうかを指定します。
   - JCS では、エンドポイントでのパスワード コンシューマのパスワード変更はできません。CA Access Control エンタープライズ管理 では、パスワードの変更イベントを開始したタスクで通知メッセージが書き込まれます。
5. CA Access Control エンタープライズ管理 により、パスワードの変更に関して監査レコードが書き込まれます。

   注: PUPM の監査レコードを表示するには[サブミット済みタスクの表示]を使用します。JCS でパスワード コンシューマのパスワード変更ができない場合は、[パスワード コンシューマの同期]を使用してパスワードの変更を再試行できます。

詳細情報:

パスワード コンシューマの同期 (P. 313)

パスワード コンシューマの実装に関する考慮事項

パスワード コンシューマを実装する前に、以下の点を考慮する必要があります。

- ソフトウェア開発キット、データベース、および Windows 実行ユーザ パスワード コンシューマを使用するには、<pump> 統合機能を有効にして、CA Access Control を PUPM エンドポイントにインストールする必要があります。
- JDBC データベース パスワード コンシューマを使用するには、データベースに接続するアプリケーションで JRE 1.5 以降を使用する必要があります。
- OCI データベース パスワード コンシューマを使用するには、データベースに接続するアプリケーションで OCI8 以降を使用する必要があります。

- デフォルト以外のドライバで ODBC または OLEDB データベース パスワード コンシューマを使用する場合は、CA Technologies のサポートにご連絡ください。

  注: デフォルトドライバは、ODBC または OLEDB プラグイン用のレジストリ サブキー内の ApplyOnProcess レジストリ エントリ内に定義されています。 詳細については、当社テクニカル サポート(http://www.ca.com/jp/support/)にお問い合わせください。

- Java PUPM SDK パスワード コンシューマを使用するには、作成する Java アプリケーションで JRE 1.5 以降を使用する必要があります。

- .NET PUPM SDK パスワード コンシューマを使用するには、.NET Framework 2.0 以降をエンドポイントにインストールする必要があります。

- Windows サービスまたは Windows スケジュール タスクのパスワード コンシューマを作成するためのサービス アカウントを検出する際に、CA Access Control で検出されるのはパスワードを変更できるアカウントで実行されているサービスのみになります。

- ドメイン アカウントであるサービス アカウントを検出するには、アカウントが存在するドメイン コントローラ(DC)を表す PUPM エンドポイントを作成する必要があります。このエンドポイントでは、以下の属性を使用する必要があります。

  - エンドポイント タイプ -- Windows エージェントレス
  - Active Directory -- True
  - ホストドメイン -- DC がメンバであるドメイン名
  - ユーザ ドメイン -- DC 上で定義されたユーザがメンバであるドメイン名

    注: アカウントが存在するドメインとは異なるドメインから管理者アカウントを使用する場合にのみ、ユーザ ドメインを指定します。

詳細情報:

サービス アカウントの検出 (P. 257)

PUPM の監査レコード

CA Access Control エンタープライズ管理 では、たとえばユーザが特権アカウント パスワードをチェックインする際に、イベントの監査データが記録されます。CA Access Control エンタープライズ管理 では、失敗したイベントについても監査データが記録されます。たとえば、特権アカウント パスワードのチェックアウトに自動ログインを選択しながら、ActiveX のダウンロードを承認しない場合、CA Access Control エンタープライズ管理 により自動ログインが失敗した理由が記録されます。CA Access Control エンタープライズ管理 では、PUPM の監査データは中央データベースに格納されます。

詳細情報:

監査データ (P. 47)
特権アカウントの監査 (P. 308)

パスワード コンシューマ監査レコード

パスワード コンシューマによりパスワード要求が作成されるたびに、さらに PUPM Agent によりエンタープライズ管理サーバからパスワードが取得されるたびに、CA Access Control エンタープライズ管理 では監査レコードが書き込まれます。CA Access Control エンタープライズ管理 では、パスワード コンシューマによるパスワードの要求が失敗した場合、たとえば、アクセス権のないパスワードがパスワード コンシューマにより要求された場合も、監査レコードが書き込まれます。

パスワード コンシューマでパスワード要求が作成され、エンドポイント上の PUPM Agent でパスワードがキャッシュから取得される場合、CA Access Control エンタープライズ管理 では監査レコードは書き込まれません。

PUPM フィーダ監査レコード

PUPM フィーダは、以下のタスクを実行します。CA Access Control エンタープライズ管理 は、PUPM フィーダが実行する各アクションに対して監査レコードを作成します。

- フィーダ フォルダのポーリング - PUPM フィーダが CA Access Control エンタープライズ管理 へのポーリング フォルダに CSV ファイルを正常にアップロードしたかどうかを指定します。
- フィーダ プロセスの csv ファイル - アップロードされた CSV ファイルが CA Access Control エンタープライズ管理 によって正常に処理されたか、また CA Access Control エンタープライズ管理 が CSV ファイル内で処理した行数を追跡する進行状況インジケータを表示するかどうかを指定します。

また、CA Access Control エンタープライズ管理 は、インポートした CSV ファイルの各行に対して監査レコードを作成します。各行は、PUPM エンドポイントまたは特権アカウントの作成または変更タスクを表わしています。監査レコードは各タスクのステータスを追跡します。これらのタスクには、以下のステータスがあります。

- **完全** - CA Access Control エンタープライズ管理 はタスクを完了しました(例: 特権アカウントの作成が完了しました)。
- **失敗** - CA Access Control エンタープライズ管理 はタスクを処理しましたが、そのタスクは完了しませんでした(例: 存在しないエンドポイント上で特権アカウントを作成できませんでした)。
- **監査** - CA Access Control エンタープライズ管理 はタスクを処理または完了しませんでした(例: ACCOUNT_NAME 属性が指定されていないため、特権アカウントを作成できませんでした)。

システム マネージャ ロールを持つユーザは、[サブミット済みタスクの表示]タスクを使用して各タスクのステータスを表示できます。

PUPM エンドポイント上の監査イベント

CA Access Control エンタープライズ管理 では、エンタープライズ管理サーバ上で発生するイベントの監査データが記録されます。CA Enterprise Log Manager に PUPM エンドポイントを統合する場合、個々の特権アカウント セッションのエンドポイントにおける監査イベントも記録できます。

ユーザが特権アカウントをチェックアウトし、そのアカウントをエンドポイントへのログインに使用すると、この統合によりユーザは、特権アカウントによりエンドポイント上で実行されたアクションを追跡できるようになります。 これらのアクションは、CA Enterprise Log Manager のレポート内に収集される監査イベントに記録されます。これらの CA Enterprise Log Manager のレポートは CA Access Control エンタープライズ管理 で表示できます。

たとえば、privileged1 という名前のアカウントがチェックアウトされた後でユーザが実行したアクションを確認するとします。CA Access Control エンタープライズ管理 で[特権アカウントの監査]タスクを使用して、privileged1 アカウントのチェックアウトに対する監査レコードを検索します。次に、この監査レコードからドリルダウンし、privileged1 アカウントがエンドポイントで実行したアクティビティ(たとえば、プログラムの開始と終了)についての CA Enterprise Log Manager のレポートを表示します。

詳細情報:

PUPM のエンドポイントでの監査イベントの表示 (P. 312)

PUPM エンドポイントを CA Enterprise Log Manager に 統合する方法

PUPM エンドポイントを CA Enterprise Log Manager に 統合すると、特権アカウント セッションごとに監査イベントをエンドポイントに記録できます。また、この統合により、CA Access Control エンタープライズ管理 で PUPM エンドポイント上の特権アカウント監査イベントの CA Enterprise Log Manager レポートを表示できます。

PUPM エンドポイントを CA Enterprise Log Manager に統合するには、以下の手順に従います。

1. CA Access Control エンタープライズ管理 内で、
   a. CA Enterprise Log Manager への接続を設定します。
   b. PUPM エンドポイントごとに、CA Enterprise Log Manager のホスト名およびイベント ログ名を指定します。

      ホスト名およびイベント ログ名を指定するには、[エンドポイントの作成] または[エンドポイントの変更]タスクの[CA Enterprise Log Manager]タブを使用します。
2. PUPM エンドポイントから継続して情報を収集するように CA Enterprise Log Manager を設定します。

注: CA Enterprise Log Manager への接続の設定方法の詳細については、「*実装ガイド*」を参照してください。CA Enterprise Log Manager の設定方法の詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

詳細情報:

エンドポイントの作成 (P. 194)
PUPM のエンドポイントでの監査イベントの表示 (P. 312)

CA Service Desk Manager 統合

PUPM は CA Service Desk Manager と通信して、チケットを特権アカウント リクエストおよび承認プロセスの一部として、受け取り、検証できます。CA Service Desk Manager と統合されると、PUPM はアクティブなチケットと照合して、特権アカウント パスワードの各リクエストを検証します。PUPM を CA Service Desk Manager と統合することにより、複数の承認プロセスを含む特権アカウント リクエストの検証プロセスを作成できます。

特権アカウント リクエストを CA Service Desk Manager に統合する方法

PUPM と CA Service Desk Manager を統合する方法を理解すると、CA Service Desk Manager への接続のセットアップや検証プロセスの実装を容易に実行できます。

PUPM と CA Service Desk Manager を統合するには、以下を実行します。

1. CA Service Desk Manager をデプロイし、設定を行います。
2. CA Access Control エンタープライズ管理 から CA Service Desk Manager への接続を設定します。
3. CA Service Desk Manager を使用し、特権アカウントへのアクセスを要求するサービス デスク チケットをオープンします。
4. CA Service Desk Manager を使用してサービス デスク リクエストを承認します。
5. CA Access Control エンタープライズ管理 で特権アカウントの要求を作成し、CA Service Desk Manager のチケット番号を指定します。
6. 特権アカウントの要求を承認または否定します。

CA Service Desk Manager への接続の設定

PUPM を CA Service Desk Manager と統合するために、CA Access Control エンタープライズ管理 から CA Service Desk Manager への接続を定義します。

CA Service Desk Manager への接続の設定方法

1. CA Access Control エンタープライズ管理 で、[システム]-[接続管理]-[CA Service Desk Manager]-[管理対象の CA Service Desk Manager 接続]を選択します。

   [管理対象の CA Service Desk Manager 接続]ウィンドウが表示されます。

2. 以下を使用して、フォームに入力します。

   接続名

   接続名を定義します。

   デフォルト: プライマリ CA Service Desk Manager 接続

   接続の種類

   接続タイプを指定します。

   デフォルト: CA Service Desk Manager

   接続の説明

   接続の説明を指定します。

   ホスト名

   CA Service Desk Manager Web サービスの URL を定義します。

   デフォルト:
   http://*host_name*:8080/axis/services/USD_R11_WebService?wsdl

   ユーザ ID

   CA Service Desk Manager への接続に使用するユーザ ID を定義します。

   注: ユーザには、Web Service API を使用してサービス デスク チケットについて問い合わせる権限が必要です。

   パスワード

   ユーザ ID のパスワードを定義します。

必須

特権アカウントへのアクセスをリクエストする際に、ユーザがチケット番号を入力する必要があるかどうかを指定します。

注: 選択されない場合、特権アカウントへのアクセスリクエスト時に、チケット番号の提供を強制されません。

有効

接続を有効にするかどうかを指定します。

注: 選択されない場合、特権アカウント リクエスト タスクで、[チケット番号]フィールドは表示されません。

詳細

ユーザが詳細設定を定義するかどうかを指定します。このオプションを選択した場合、以下のフィールドが表示されます。

チケットの種類

特権アカウント パスワードのリクエストに使用される CA Service Desk Manager チケットのタイプを定義します。

制限: cr、iss、chg

デフォルト: cr

注: このフィールドでは、大文字と小文字が区別されます。

チケット クエリ

チケットの検証に使用されるカスタム クエリを定義します。任意の有効な CA Service Desk Manager クエリを指定します。

例: active=1 AND status='OP

注: このフィールドが空のままの場合、要求者チケットを検証するために、CA Access Control エンタープライズ管理 はすべてのサービスデスク チケットを列挙します。

3. [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 は接続設定をテストし、コネクタ サーバを作成します。

注: CA Service Desk Manager の詳細については、CA Service Desk Manager のマニュアルを参照してください。

詳細情報:

特権アカウントリクエストを CA Service Desk Manager に統合する方法 (P. 155)

実装時の考慮事項

以下のトピックに、PUPM を実装する前に考慮すべき項目を一覧表示します。

特権アカウント パスワードの電子メール通知

ネットワークの遅延などが発生している場合、ユーザがパスワードをチェックアウトしようとすると、CA Access Control エンタープライズ管理 が 20 秒以上ハングすることがあります。CA Access Control エンタープライズ管理 が 20 秒以上ハングする場合、画面はタイムアウトし、パスワードはユーザに表示されません。代わりに、CA Access Control エンタープライズ管理 がパスワードをユーザに電子メール送信します。

ユーザが確実にパスワードを受け取るように、以下を実行します。

- CA Access Control エンタープライズ管理 の電子メール通知設定を行います。
- 有効な電子メール アドレスが各 PUPM ユーザのユーザ ストアに記録されていることを確認します。

注: 電子メール通知の設定の詳細については、「*実装ガイド*」を参照してください。

Windows エージェントレス エンドポイント上のドメイン ユーザに対する制限事項

ユーザがローカル コンピュータ上でドメイン ユーザを設定する場合、PUPM はそのドメイン ユーザのパスワードを変更できません。この制限は、Windows の動作に起因するものです。

Active Directory エンドポイントを管理するための最小権限

Windows で有効

Active Directory エンドポイントの管理に PUPM Windows エージェントレス エンドポイント タイプを使用し、ドメイン管理者アカウントを指定しない場合、一般ユーザ アカウントを管理するために最低限必要な権限を持つ委任ユーザ アカウントを指定することができます。

例: Active Directory ユーザに、Windows Server 2008 上の他の Active Directory ユーザを管理する権限を委任

以下の例では、Windows Server 2008 上の他の Active Directory 一般ユーザを管理するための権限を一般ユーザに委任する方法を示します。

1. [スタート]-[管理ツール]-[コンポーネント サービス]を選択します

   [コンポーネント サービス]コンソールが開きます。

2. コンポーネント サービス リストを展開して[コンピュータ]を選択し、[マイ コンピュータ]を右クリックして[プロパティ]を選択します。

   [マイ コンピュータのプロパティ]ウィンドウが表示されます。

3. [COM セキュリティ]タブに移動して以下を行います。
   a. [アクセス許可]セクションの[既定値の編集]ボタンをクリックします。
   b. [追加]をクリックし、アクセスを許可するユーザを選択します。
   c. [起動とアクティブ化のアクセス許可]セクションの[既定値の編集]を選択します。
   d. [追加]をクリックし、アクセスを許可するユーザを選択します。
   e. ローカル/リモートからの起動およびローカル/リモートからのアクティブ化に対して[許可]列を選択します。
   f. [OK]をクリックして、プロパティ ウィンドウを終了します。

4. [スタート] - [管理ツール] - [Active Directory ユーザーとコンピュータ]をクリックします。以下の手順を実行します。
   a. ユーザ リストから、ユーザ アカウントを右クリックします。
   b. [所属するグループ]タブを開き、グループへの追加を選択します。
   c. 以下のグループのメンバとしてユーザを追加し、[OK]をクリックします。
      - Domain Users
      - Distributed COM Users

委任されたユーザのセキュリティ属性が設定されました。次に、このユーザが管理するコンテナのセキュリティ属性を設定します。

5. Active Directory の[ユーザーとグループ]コンソールで[ユーザー]フォルダを右クリックし、[プロパティ]を選択します。
6. [セキュリティ]タブを開き、[ユーザーの追加]を選択して[詳細設定]をクリックします。

   セキュリティの詳細設定ウィンドウが表示されます。以下の手順を実行します。

   a. [アクセス許可]タブでユーザを選択して[編集]をクリックします。

      [アクセス許可エントリ]ウィンドウが表示されます。

   b. [適用先]リストで、子オブジェクトを選択し、以下の許可を適用します。

      - 内容の一覧表示
      - すべてのプロパティの読み取り
      - すべてのプロパティの書き込み
      - アクセス許可の読み取り
      - アクセス許可の修正
      - パスワードの変更
      - パスワードのリセット

   c. [OK]をクリックして、プロパティウィンドウを終了します。

   [ユーザー]コンテナ内のユーザのセキュリティ属性が設定されました。
7. コマンド プロンプト ウィンドウから、コマンド wmimgmt を実行し、WMI コントロール コンソールを開きます。以下の手順を実行します。

a. ［WMI コントロール］を右クリックし、［プロパティ］を選択します。

［WMI コントロールのプロパティ］ウィンドウが表示されます。

b. ［セキュリティ］タブを開き、ルート ディレクトリを展開します。

c. ディレクトリを選択して［セキュリティ］ボタンをクリックします。

d. ［追加］をクリックし、編集しているユーザ アカウントを追加して、Root 名前空間および副名前空間に対して、セキュリティの読み取りに以下の許可を追加します。

- 部分的書き込み
- プロバイダによる書き込み
- アカウントの有効化
- リモートの有効化

e. WMI コントロール コンソールを閉じます。

8. コマンド プロンプト ウィンドウで、regedit ユーティリティを実行して、以下のレジストリ エントリを開きます。

HKEY_CLASSES_ROOT¥CLSID¥{76A64158-CB41-11D1-8B02-00600806D9B6}

HKEY_CLASSES_ROOT¥CLSID¥{233664b0-0367-11cf-abc4-02608c9e7553}

9. 各レジストリ キーを右クリックして、［アクセス許可］を選択します。

［アクセス許可］ウィンドウが表示されます。

10. ユーザをリストに追加し、キーおよびすべての子オブジェクトに対してフル コントロールを割り当てます。

11. ［OK］をクリックして regedit ユーティリティを閉じます。

Active Directory 一般ユーザに対して、他の一般 Active Directory ユーザを管理する権限が委任されました。

コネクタ サーバ

CA Access Control エンタープライズ管理 はコネクタ サーバと通信し、PUPM エンドポイント上の特権アカウントの検索や管理を行います。CA Access Control エンタープライズ管理 は Java コネクタ サーバ (JCS) を使用し、PUPM エンドポイント用の CA Access Control と通信します。デフォルトでは、JCS は CA Access Control エンタープライズ管理 のインストール時に配布サーバの一部としてインストールされます。

PUPM を使用して CA Identity Manager プロビジョニング エンドポイントを管理するには、CA Access Control エンタープライズ管理 内に Identity Manager プロビジョニング タイプのコネクタ サーバを作成する必要があります。

注: コネクタ サーバの作成の詳細については、「*オンライン ヘルプ*」を参照してください。

Connector Xpress の概要

Connector Xpress は、動的コネクタの管理、エンドポイントへの動的コネクタのマッピング、およびエンドポイントのルーティング ルールの確立に使用する CA Identity Manager ユーティリティです。Connector Xpress を使用すると、SQL データベースのプロビジョニングおよび管理を行うように動的コネクタを設定できます。

Connector Xpress では、プロビジョニング マネージャによって管理されるコネクタを作成する際に必要とされる技術的専門知識がない場合でも、カスタム コネクタを作成しデプロイすることができます。

さらに、Connector Xpress を使用して、コネクタ サーバ設定 (Java と C++ の両方) をセットアップし、編集し、削除することができます。

Connector Xpress への主要入力はエンドポイント システムのネイティブ スキーマです。たとえば、RDBMS への接続、およびデータベースの SQL スキーマの取得に Connector Xpress を使用できます。ID 管理とプロビジョニングに関連するネイティブ スキーマの一部からマッピングを構築する場合も Connector Xpress を使用できます。マッピングには、プロビジョニング レイヤでネイティブ スキーマの要素が表現される方法が記述されます。

注: Connector Xpress の詳細については、「*Connector Xpress ガイド*」を参照してください。

PUPM に Connector Xpress を実装する方法

デフォルトの PUPM のエンドポイント タイプではないエンドポイントを管理するには、Connector Xpress を使用して新しいエンドポイント タイプを作成し、特権アカウント パスワードを管理できます。たとえば、Microsoft SQL Server データベース内の特権アカウント パスワードを管理するために、タイプ SQL の新しいエンドポイントを作成するとします。デフォルトの PUPM の SQL エンドポイント タイプは、SQL Server 上の特権アカウントを管理し、データベース内の個別のテーブルは管理しない設計になっています。

以下の手順に従います。

1. Connector Xpress をインストールします。

   注: Connector Xpress をインストールする方法の詳細については、CA Support の CA Identity Manager ブックシェルフから入手できる「*Connector Xpress ガイド*」を参照してください。

2. Connector Xpress で、新しいエンドポイント タイプを設定します。

3. Java コネクタ サーバに、この新しいエンドポイント タイプを登録します。

   新しいエンドポイント タイプを登録して、Java コネクタ サーバでそのエンドポイント タイプの管理を有効化します。

4. エンタープライズ管理サーバに新しいエンドポイント タイプをロードします。

   エンドポイント タイプをロードするのは、CA Access Control エンタープライズ管理 で利用できるようにするためです。

5. CA Access Control エンタープライズ管理 内の新しいエンドポイント タイプ用に PUPM のエンドポイントを作成します。

6. この新しいエンドポイント上で特権アカウント パスワードを検出します。

Connector Xpress の例: SUN ONE エンドポイントの設定

この例では、システム管理者のスティーブが、SUN ONE ディレクトリに接続するために Connector Xpress 内に SUN ONE エンドポイント タイプを作成します。

スティーブはエンタープライズ管理サーバ ホストに Connector Xpress をインストールしました。スティーブは以下の動作を実行します。

1. [スタート]メニューから[プログラム]-[CA]-[Identity Manager]-[Connector Xpress]の順に選択します。

   Identity Manager Connector Xpress のメイン メニューが表示されます。

2. [Setup Data Sources]をクリックします。

   [Setup Data Sources]ウィンドウが表示されます。

3. [Add]をクリックします。

   [Source Types]ウィンドウが開き、利用可能なソースが表示されます。

4. JNDI を選択し[OK]をクリックします。

   [Edit Source]ウィンドウが開きます。

5. 以下の詳細を入力します。

   - Name -- SUN ONE
   - Server Name -- server1
   - Port -- 389
   - Bind DN -- uid=user1,ou=cont1,ou=ldapConnector,dc=company,dc=com

     重要: ディレクトリ マネージャのアカウントではなく、既存のディレクトリ ユーザ アカウントを指定します(ディレクトリ マネージャのアカウントはベース DN の直下にはありません)。

   - Base DN -- ou=ldapConnector,dc=company,dc=com

6. [Test]をクリックして接続設定を確認します。

   [Enter password for data source]ウィンドウが開きます。

7. 管理者アカウント パスワードを入力して[OK]をクリックします。

   エラーが検出されなければ、確認メッセージが表示されます。新規のデータ ソースが作成されます。スティーブは次に新しいプロジェクトを作成します。

8. [Project]-[new]-[data source]-[Edit]の順に選択し、管理者アカウント パスワードを入力します。

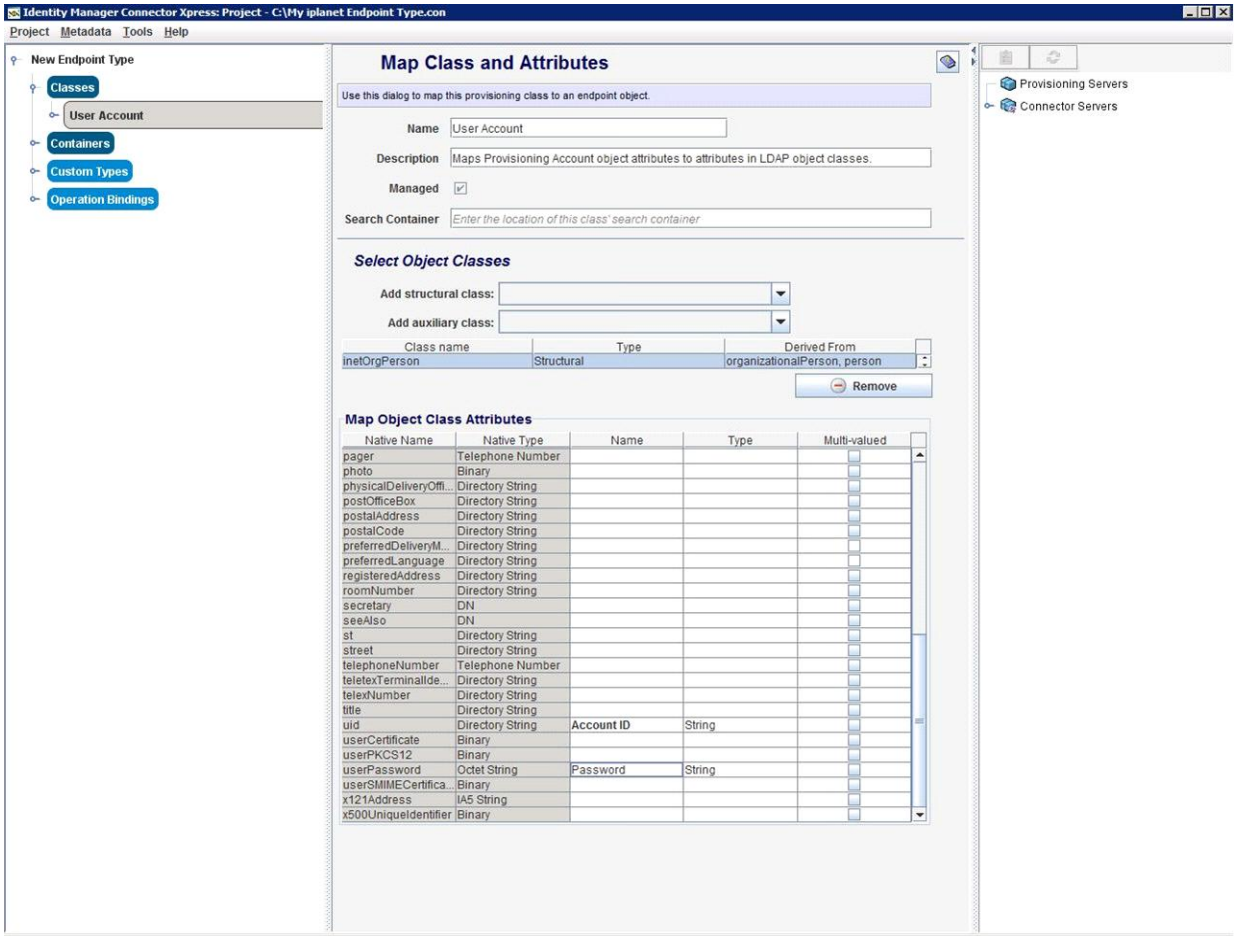
［Endpoint Type Details］画面が表示されます。

9. エンドポイント名と説明を入力し、［クラス］アイコンをダブルクリックして、［User Details］オプションを選択します。

   ［Map Class ］ウィンドウおよび［Attributes］ウィンドウが表示されます。

10. ［Select Object Classes］で、構造クラス inerOrgPerson を追加して以下の属性をマップします。

    - cn -- AccountID
    - sn -- last name
    - uid -- AccountID
    - userPassword -- ユーザ アカウント パスワード



11. プロジェクトを保存し、エンドポイント タイプの定義を保存します。

    スティーブは、Connector Xpress に新しい SUN ONE エンドポイント タイプを設定しました。スティーブは、ここで Java コネクタ サーバにエンドポイント タイプを登録します。

Connector Xpress の例: Java コネクタ サーバでの SUN ONE エンドポイントの登録

この例では、システム管理者のスティーブが Connector Xpress で作成したエンドポイント タイプを、Java コネクタ サーバで登録します。スティーブは、CA Access Control エンタープライズ管理 新しいエンドポイント タイプを表示するために、これを登録します。スティーブは以下の動作を実行します。

1. [Identity Manager Connector Xpress Project]ウィンドウの[コネクタ サーバ]オプションを右クリックし、[Add Server]を選択します。

   [Connector Server Details]ウィンドウが表示されます。

2. Java コネクタ サーバのホスト名を指定し[OK]をクリックします。

   注: Java コネクタ サーバは配布サーバの一部です。エンタープライズ管理サーバでは、デフォルトでこのサーバ上に配布サーバをインストールします。
   [Connector Server Password Required]ウィンドウが表示されます。

3. エンタープライズ管理サーバの通信パスワードを入力します。

   通信パスワードとは、エンタープライズ管理サーバをインストールした際に指定したものです。既存のエンドポイント タイプの一覧が表示されます。

4. エンドポイント タイプを右クリックし、[Create New Endpoint Type]を選択します。

   [Create New Endpoint Type]ウィンドウが表示されます。

5. エンドポイント タイプ名を入力し[OK]をクリックします。

   エラーが検出されなければ、Connector Xpress により新しいエンドポイント タイプが作成されます。

スティーブは Java コネクタ サーバに新しいエンドポイントを登録しました。スティーブは、ここでエンタープライズ管理サーバに新しいエンドポイント タイプをロードします。

詳細情報:

Connector Xpress の例: エンタープライズ管理サーバへのエンドポイント タイプのロード (P. 170)

Connector Xpress の例: JDBC エンドポイントの設定

この例では、システム管理者のスティーブが、Microsoft SQL Server に接続させるために Connector Xpress 内に JDBC エンドポイント タイプを作成します。

スティーブはエンタープライズ管理サーバ ホストに Connector Xpress をインストールしました。スティーブは以下の動作を実行します。

1. [スタート]メニューから[プログラム]-[CA]-[Identity Manager]-[Connector Xpress]の順に選択します。

   Identity Manager Connector Xpress のメイン メニューが表示されます。

2. [Setup Data Sources]をクリックします。

   [Setup Data Sources]ウィンドウが表示されます。

3. [Add]をクリックします。

   [Source Types]ウィンドウが開き、利用可能なソースが表示されます。

4. JDBC を選択し[OK]をクリックします。

   [Edit Source]ウィンドウが開きます。

5. 以下の詳細を入力します。

   - データ ソース名 -- SQL Server
   - データベースの種類 -- Microsoft SQL Server
   - ユーザ名 -- sa
   - サーバ名 -- mysql
   - ポート -- 1433
   - データベース -- ユーザ

6. [Test]をクリックして接続設定を確認します。

   [Enter password for data source]ウィンドウが開きます。

7. sa ユーザ アカウント パスワードを入力し[OK]をクリックします。

   エラーが検出されなければ、確認メッセージが表示されます。新規のデータ ソースが作成されます。次に、スティーブは新しいエンドポイント タイプを設定します。

8. ［Identity Manager Connector Xpress］のメイン メニューに戻り、［New Project］を選択します。

   ［New Project］ウィンドウに［Select Data Source］が表示されます。

9. 彼が作成したデータ ソースを選択し［OK］をクリックします。

   ［Endpoint Type Details］ウィンドウが表示されます。

10. エンドポイント名と説明を入力し、［クラス］アイコンをダブルクリックして、［User Details］オプションを選択します。

    ［Map Class ］ウィンドウおよび［Attributes］ウィンドウが表示されます。

11. ［Select Schema and Table］セクションで、以下を選択します。

    - スキーマは、dbo を選択します。
    - テーブルについては、sqlConnector テーブルを選択します。

    マップ済みの列が表示されます。

12. ［Map Columns］セクションでは、［Name］列に以下の値を入力します。

    - ［uname］行には、アカウント ID を入力します。
    - ［upassword］行には、パスワードを入力します。

13. ［Project］ - ［Save］の順に選択し、エンドポイント タイプの定義を保存します。

スティーブは、Connector Xpress に新しい JDBC エンドポイント タイプを設定しました。スティーブは、ここで Java コネクタ サーバにエンドポイント タイプを登録します。

Connector Xpress の例: Java コネクタ サーバでの JDBC エンドポイントの登録

この例では、システム管理者のスティーブが Connector Xpress で作成したエンドポイント タイプを、Java コネクタ サーバで登録します。スティーブは、CA Access Control エンタープライズ管理 新しいエンドポイント タイプを表示するために、これを登録します。スティーブは以下の動作を実行します。

1. [Identity Manager Connector Xpress Project]ウィンドウの[コネクタ サーバ]オプションを右クリックし、[Add Server]を選択します。

   [Connector Server Details]ウィンドウが表示されます。

2. Java コネクタ サーバのホスト名を指定し[OK]をクリックします。

   注: Java コネクタ サーバは配布サーバの一部です。エンタープライズ管理サーバでは、デフォルトでこのサーバ上に配布サーバをインストールします。[Connector Server Password Required]ウィンドウが表示されます。

3. エンタープライズ管理サーバの通信パスワードを入力します。

   通信パスワードとは、エンタープライズ管理サーバをインストールした際に指定したものです。既存のエンドポイント タイプの一覧が表示されます。

4. エンドポイント タイプを右クリックし、[Create New Endpoint Type]を選択します。

   [Create New Endpoint Type]ウィンドウが表示されます。

5. エンドポイント タイプ名を入力し[OK]をクリックします。

   エラーが検出されなければ、Connector Xpress により新しいエンドポイント タイプが作成されます。

スティーブは Java コネクタ サーバに新しいエンドポイントを登録しました。スティーブは、ここでエンタープライズ管理サーバに新しいエンドポイント タイプをロードします。

Connector Xpress の例: エンタープライズ管理サーバへのエンドポイント タイプのロード

この例では、システム管理者のスティーブが、作成した新しいエンドポイント タイプをエンタープライズ管理サーバにロードします。スティーブが新しいエンドポイント タイプをロードすると、CA Access Control エンタープライズ管理 からエンドポイントを設定し管理することができます。スティーブは以下の動作を実行します。

1. JBoss アプリケーション サーバを停止します。
2. 以下のいずれかを実行します。
   - (JDBC)ファイル conXpressnamespace_config.xml.template を編集します。
   - (SUN One) iplanetnamespace_config.xml を編集します。

   このファイルは以下のディレクトリ内にあります(*JBoss_HOME* は JBoss をインストールしたディレクトリです)。

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
3. <endpointType> パラメータを見つけて、デフォルト値「REPLACE_WITH_ENDPOINT_TYPE」を削除します。
4. Connector Xpress で指定したエンドポイント タイプ名を入力します。
5. このファイルを conXpress_E*Endpoint_Type*_namespace_config.xml という名前で以下のディレクトリに保存します。

   JBOSS_HOME/server/default/deploy/IdentityMinder.ear/custom/ppm/namespaceConfigs/
6. JBoss アプリケーション サーバを起動します。

スティーブは、エンタープライズ管理サーバに新しいエンドポイント タイプをロードしました。スティーブは、CA Access Control エンタープライズ管理 内にこのタイプのエンドポイントを定義し、エンドポイント上の特権アカウントを検出することができるようになりました。

Connector Xpress の制限事項

Connector Xpress に作成したエンドポイント タイプで Discovery 特権アカウント ウィザードを実行する前に、以下の内容を考慮する必要があります。

- Connector Xpress 内に作成したのと同じタイプのエンドポイント、たとえば SQL Server エンドポイントを定義し、エンドポイント管理者アカウント クレデンシャルを提供します。CA Access Control エンタープライズ管理 によりエンドポイントが作成される場合、切断された特権アカウントも作成されます。
- エンドポイント タイプのメニューから Connector Xpress に作成したエンドポイント タイプを指定します。[URL]フィールドで、以下の例のようにデータベース名を指定します。
- [ユーザ ログイン]および[パスワード]フィールドは空欄にしておきます。[Use the following privileged account]を確認し、エンドポイントに接続できる権限を持った特権アカウントを選択します。事前に定義したエンドポイント用に CA Access Control エンタープライズ管理 により作成された切断された特権アカウントを使用します。

例: エンドポイントの[URL]フィールドの SQL Server データベース名

以下の例には、SQL Server データベース名を含む[URL]フィールドが示されています。

```
jdbc:sqlserver://server.company.com:1433;database=database_name
```

PUPM SDK

PUPM SDK を使用すると、特権アカウント パスワードをチェックアウトおよびチェックインするアプリケーションを作成できます。PUPM SDK には、パスワード コンシューマ SDK と Web サービス SDK の 2 つの種類があります。

以下の表に、この 2 種類の SDK の相違の概要を示します。

機能	パスワード コンシューマ SDK	Web サービス SDK
プログラミング言語	Java .NET	Java
ユーザ認証	Yes	No
パスワード キャッシュ	Yes	No

機能	パスワード コンシューマ SDK	Web サービス SDK
エンドポイントで CA Access Control が必要	Yes	No

使用事例: PUPM SDK

PUPM SDK では、スクリプト内の特権アカウント パスワードの管理を自動化することができます。ハードコードされたパスワードを含むスクリプトを変更しない場合、スクリプト内のパスワードを定期的に置換するアプリケーションを作成できます。

たとえば、同じ特権アカウント用のハードコードされたパスワードを含むスクリプトを エンドポイントに 10 個持っているとします。スクリプトは変更しません。PUPM SDK を使用すると、適切なダウンタイムで特権アカウント パスワードをチェックアウトし、各スクリプト内のパスワードを更新し、次にパスワードをチェックインするアプリケーションを作成できます。定期的にパスワードを変更することは、特権アカウントのセキュリティの向上に役立ちます。

このタスクを実行するアプリケーションを作成する場合、CA Access Control エンタープライズ管理 がチェックアウトまたはチェックインするときに特権アカウント パスワードを変更しないことを確認します。特権アカウントの表示タスクを使用すると、この情報を確認できます。

注: CLI のパスワード コンシューマを使用しても、スクリプト内のハードコードされたパスワードを置換できます。たとえば、ファイル内のハードコードされたパスワードを手動で更新する場合は、CLI のパスワード コンシューマを使用します。

パスワード コンシューマ SDK アプリケーションがパスワードを取得する方法

パスワード コンシューマ SDK を使用すると、特権アカウント パスワードを取得、チェックイン、およびチェックアウトするアプリケーションを作成できます。パスワード コンシューマ SDK を使用するには、以下の手順に従う必要があります。

- アプリケーションが動作するエンドポイントに CA Access Control をインストールする
- アプリケーション用のパスワード コンシューマを CA Access Control エンタープライズ管理 に定義する

PUPM SDK には、次の 2 種類があります。

- Java PUPM SDK
- .NET PUPM SDK

パスワード コンシューマ SDK アプリケーションは、PUPM エージェントと通信します。PUMP エージェントは、メッセージ キューを使用して CA Access Control エンタープライズ管理 と通信します。PUPM エージェントは、SSL 通信およびポート 7243 を使用してメッセージ キューと通信します。

以下のプロセスでは、パスワード コンシューマ SDK アプリケーションがパスワードを取得する方法を示します。

1. アプリケーションは、PUPM エージェントにパスワード要求を送信します。
2. PUPM エージェントは、パスワード要求を受信します。 CA Access Control は、アプリケーションを実行するユーザの ID を検証し、キャッシュを確認します。以下の*いずれか*のイベントが発生します。
   - パスワード要求がキャッシュされる場合、PUPM エージェントは特権アカウント パスワードをアプリケーションに送信します。このステップで、プロセスが終了します。CA Access Control エンタープライズ管理 では、パスワード要求の監査レコードは書き込まれません。
   - パスワード要求がキャッシュされない場合、PUPM エージェントはパスワード要求およびアプリケーションの実行ユーザ名を CA Access Control エンタープライズ管理 に送信します。
3. CA Access Control エンタープライズ管理 は要求を受信し、アプリケーションに特権アカウント パスワードの取得権限を与えるパスワード コンシューマが存在することを確認します。

   パスワード コンシューマは、アプリケーションのパス、アプリケーションが要求できる特権アカウント、アプリケーションを実行できるユーザ、およびアプリケーションを実行できるホストを指定します。

4. 以下の*いずれか*のイベントが発生します。
   - アプリケーションにパスワード取得権限が付与されている場合、CA Access Control エンタープライズ管理 は PUPM エージェントに特権アカウント パスワードを送信します。
   - アプリケーションにパスワード取得権限が付与されていない場合、CA Access Control エンタープライズ管理 は PUPM エージェントにエラー メッセージを送信します。

   どちらの場合も、CA Access Control エンタープライズ管理 はイベントに関する監査レコードを書き込みます。
5. PUPM エージェントは、特権アカウント パスワードまたはエラー メッセージをアプリケーションに送信します。

   アプリケーションが初めて特権アカウント パスワードを取得した場合、PUPM エージェントはパスワードをキャッシュします。

注: 特権アカウント パスワードが変更された場合、CA Access Control エンタープライズ管理 はパスワード変更イベントをエンドポイントにブロードキャストします。エンドポイントがブロードキャスト メッセージを受信すると、PUPM エージェントは特権アカウント パスワードをキャッシュから削除します。

詳細情報:

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定する方法 (P. 296)

Java PUPM SDK

Java PUPM SDK は、特権アカウント パスワードを取得、チェックアウト、およびチェックインする Java アプリケーションを作成するためのパスワード コンシューマ SDK です。Java PUPM SDK は、CA Access Control がインストールされている Windows および UNIX エンドポイントで使用できます。作成する Java アプリケーションは JRE 1.5 以降を使用する必要があります。

Java PUPM SDK は以下のディレクトリ内にあります。

ACInstallDir/SDK/JAVA

このディレクトリには、以下のファイルがあります。

- PupmJavaSDK.jar -- Java アプリケーションに含まれる SDK ライブラリ。
- CAPUPMCLientCommons.jar -- アプリケーション起動時に、クラスパスに含まれる必要があるサポート ライブラリ。
- jsafeFIPS.jar -- アプリケーション起動時に、クラスパスに含まれる必要があるサポート ライブラリ。
- CAPUPM.properties.SAMPLE -- デフォルト アプリケーション プロパティを変更するために編集できるサンプル ファイル。

  このファイルを編集する場合、新規ファイルを CAPUPM.properties と命名し、アプリケーションを起動するとき、このファイル名がクラスパスに含まれる必要があります。

  注: このファイルを変更する前に CA サポート にお問い合わせください。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。
- Samples -- 特権アカウント パスワードをチェックアウトしチェックインするサンプル Java アプリケーションを含んでいるフォルダ。

アプリケーションがランタイム イベントおよび情報のログを記録する場合、さらに、log4j ライブラリがクラスパスに含まれる必要があります。アプリケーションが特権アカウント パスワードを取得、チェックアウト、およびチェックインするには、CA Access Control エンタープライズ管理 でそのアプリケーション用に Software Development Kit（SDK/CLI）パスワード コンシューマを作成する必要があります。

詳細情報:

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定する方法 (P. 296)

.NET PUPM SDK

Windows で有効

.NET PUPM SDK は、特権アカウント パスワードを取得、チェックアウト、およびチェックインする C# アプリケーションを作成するためのパスワード コンシューマ SDK です。.NET PUPM SDK は CA Access Control がインストールされている Windows エンドポイントのみで使用できますが、任意のオペレーティング システム上にある特権アカウントのパスワードを取得、チェックアウト、およびチェックインできます。.NET PUPM SDK を使用するには、エンドポイントに.NET Framework 2.0 以降をインストールする必要があります。

.NET PUPM SDK は以下のディレクトリ内にあります。

ACInstallDir¥SDK¥DOTNET

このディレクトリには、以下のファイルがあります。

- Pupmcsharpsdk.dll -- C# アプリケーションに含まれる SDK ライブラリ。
- Examples -- 特権アカウント パスワードをチェックアウトしチェックインするサンプル アプリケーションを含んでいるフォルダ。

  各サンプル アプリケーションには、コンパイルされていないサンプル（.cs ファイル）およびコンパイルされたサンプル（.exe ファイル）が含まれます。

アプリケーションが特権アカウント パスワードを取得、チェックアウト、およびチェックインするには、CA Access Control エンタープライズ管理 でそのアプリケーション用に Software Development Kit（SDK/CLI）パスワード コンシューマを作成する必要があります。

詳細情報:

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定する方法 (P. 296)

Web サービス PUPM SDK

Web サービス PUPM SDK を使用すると、特権アカウント パスワードをチェックインおよびチェックアウトする Java アプリケーションを作成できます。Web サービス PUPM SDK は、CA Access Control がインストールされていないエンドポイント（メインフレーム エンドポイントなど）で使用できます。

Web サービス PUPM SDK アプリケーションを使用して特権アカウント パスワードをチェックアウトまたはチェックインするには、アプリケーションを表すユーザを CA Access Control エンタープライズ管理 で作成し、そのユーザに適切な特権アクセス ロールを割り当てる必要があります。

Web サービス PUPM SDK を使用するには、以下のコンポーネントをエンドポイントにインストールする必要があります。

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- （オプション）Eclipse などの統合開発環境（IDE）

Web サービス PUPM SDK は以下のディレクトリにあります。

ACServerInstallDir/IAM Suite/Access Control/tools/samples/webservice/Axis

このディレクトリには、Web サービス PUPM SDK 用の以下のコンポーネントが含まれています。

- Readme.txt -- 環境を設定し、Java サンプルを作成して実行する方法について説明したファイル。
- build.xml -- Apache Ant ビルド スクリプト。
- build.properties -- build.xml にプロパティを設定するファイル。
- CheckInPrivilegedAccount.java -- 特権アカウント パスワードをチェックインするサンプル Java アプリケーション。
- CheckOutPrivilegedAccount.java -- 特権アカウント パスワードをチェックアウトするサンプル Java アプリケーション。
- client-config.wsdd -- すべての受信および送信 XML メッセージを axis.log というファイルに保存するように Axis を設定するファイル。

  注: このディレクトリには、その他の管理タスク（特権アカウントの作成、削除など）を実行できるサンプル Java アプリケーションも含まれています。

詳細情報:

Web サービス PUPM SDK アプリケーションを使用するためにエンドポイントを設定する方法 (P. 299)

Web サービス SDK アプリケーションがパスワードを取得する方法

Web サービス PUPM SDK を使用すると、特権アカウント パスワードをチェックインおよびチェックアウトする Java アプリケーションを作成できます。Web サービス PUPM SDK アプリケーションが動作するエンドポイントに CA Access Control をインストールする必要はありません。ただし、パスワード コンシューマ SDK とは異なり、Web サービス PUPM SDK はパスワードのキャッシュとユーザの認証を行いません。

Web サービス PUPM SDK アプリケーションは、SOAP (Simple Object Access Protocol) およびポート 18080 を使用してエンタープライズ管理サーバと直接通信します。

重要: アプリケーションとエンタープライズ管理サーバ間の接続の認証には、NTLM のような高度な認証プロトコルを使用することをお勧めします。

以下のプロセスでは、Web サービス PUPM SDK アプリケーションがパスワードを取得する方法を示します。

1. アプリケーションが CA Access Control エンタープライズ管理 にログインします。

   アプリケーションがログインに使用するユーザ名およびパスワードは、アプリケーションに定義されています。

2. アプリケーションは、特権アカウント用のパスワードを要求します。

3. CA Access Control エンタープライズ管理 は、アプリケーションを表すユーザに割り当てられた特権アクセス ロールを確認します。

4. 以下の*いずれか*のイベントが発生します。
   - その特権アクセス ロールを持つユーザが特権アカウント パスワードを取得できる場合、CA Access Control エンタープライズ管理 はアプリケーションにパスワードを送信します。
   - その特権アクセス ロールを持つユーザが特権アカウント パスワードを取得できない場合、CA Access Control エンタープライズ管理 はアプリケーションにエラー メッセージを送信します。
5. アプリケーションが CA Access Control エンタープライズ管理 をログアウトします。

詳細情報:

Web サービス PUPM SDK アプリケーションを使用するためにエンドポイントを設定する方法 (P. 299)

第 6 章: 特権アカウントの実装

このセクションには、以下のトピックが含まれています。

特権アカウントのセットアップ方法

特権ユーザ パスワード管理(PUPM)は、組織内で最も強力な権限を持つアカウントに関連付けられたすべてのアクティビティを保護、管理、追跡するプロセスです。特権アカウント パスワードの使用を開始する前に、CA Access Control エンタープライズ管理 を PUPM 用にセットアップするいくつかの手順を完了する必要があります。その後、定義した特権アカウントの使用を開始できます。

以下のプロセスでは、特権アカウントをセットアップするためにユーザが完了する必要があるタスクについて説明します。各プロセス手順を完了するには、指定されたロールが必要です。システム マネージャ管理ロールが割り当てられているユーザは、このプロセスのすべての CA Access Control エンタープライズ管理 タスクを実行できます。

注: このプロセスを開始する前に、電子メール通知が CA Access Control エンタープライズ管理 内で有効であることを確認します。CA Access Control エンタープライズ管理 がユーザにパスワードを表示できない場合、代わりに電子メールでユーザにパスワードを送信します。

特権アカウントをセットアップするには、以下の手順に従います。

1. PUPM ターゲット システム マネージャは、パスワード ポリシーを作成します。パスワード ポリシーは、特権アカウント パスワードのルールおよび制限事項を設定します。
2. PUPM ターゲット システム マネージャは、CA Access Control エンタープライズ管理 でエンドポイントを作成します。エンドポイントは、特権アカウントによって管理されるデバイスです。CA Access Control エンタープライズ管理 でエンドポイントを作成するか、PUPM フィーダを使用して、エンドポイントをインポートできます。
3. PUPM ターゲット システム マネージャは、各エンドポイントの特権アカウントを作成します。特権アカウントを作成することにより、CA Access Control エンタープライズ管理 はアカウントを管理できます。CA Access Control エンタープライズ管理 で特権アカウントを作成するか、PUPM フィーダを使用して、特権アカウントをインポートできます。
4. (オプション) システム マネージャはログイン アプリケーションを作成します。また、PUPM ターゲット システム マネージャは、ログイン アプリケーションを使用するために PUPM エンドポイントを変更します。ログイン アプリケーションによって、ユーザは CA Access Control エンタープライズ管理 から特権アカウントにログインできます。
5. PUPM ポリシー マネージャは、特権アクセス ロールのメンバ ポリシーを変更します。メンバ ポリシーは、ロール内のタスクを実行できるユーザを定義します。

   注: Active Directory をユーザ ストアとして使用する場合は、各メンバ ポリシーを変更して、それぞれが対応する Active Directory グループを指すようにすることをお勧めします。このようにすると、対応する Active Directory グループでユーザを追加または削除することによって、ロール内でユーザを追加または削除できます。この結果、管理上のオーバーヘッドが大幅に減少します。
6. (組み込みユーザ ストア) PUPM ユーザ マネージャは、各ユーザのマネージャを指定します。

   注: ユーザによる特権アカウント リクエストは、マネージャのみが承認できます。ユーザ ストアとして Active Directory を使用する場合は、Active Directory に各ユーザのマネージャが指定されていることを確認します。
7. (オプション) システム マネージャは、CA Service Desk Manager への接続を設定します。

   CA Service Desk Manager との統合により、特権アカウント リクエストに対して複数の承認プロセスを作成できます。

以下の図に、各プロセス手順を実行する特権アクセス ロールを示します。

特権アカウントの検出

一定の間隔で特権アカウント検出プロセスを実行して、エンドポイント上に新規特権アカウントがないかどうかスキャンすることをお勧めします。特権アカウントの検出によって、複数の特権アカウントを同時に作成できます。CA Access Control エンタープライズ管理 によって検出されたアカウントがテーブルで示されます。そのため、すでに PUPM で管理しているアカウントを容易に識別します。

エンドポイント タイプ 上で特権アカウントを初めて検出すると、CA Access Control エンタープライズ管理 は、そのエンドポイント タイプ 上で特権アカウントを使用するために、エンドポイント特権アクセス ロールを自動的に作成します。たとえば、Windows エージェントレス エンドポイント上で初めて特権アカウントを検出した場合、CA Access Control エンタープライズ管理 は Windows エージェントレス接続エンドポイント特権アクセス ロールを自動的に作成します。

特権アカウントの検出方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[アカウント]-[特権アカウント検出ウィザード]をクリックします。

   [特権アカウント検出ウィザード: 特権アカウントの選択]ページが表示されます。

2. リストから[エンドポイント タイプ]を選択します。

3. 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エンドポイントのリストが表示されます。

4. 管理する特権アカウントを選択します。

   以下のテーブル列見出しには説明が必要です。

   検出されたアカウント

   アカウントが CA Access Control エンタープライズ管理 にすでに認識されているかどうかを示します。既知のアカウントには、CA Access Control エンタープライズ管理 がすでに管理しているアカウント、および、CA Access Control エンタープライズ管理 がエンドポイントを管理するために使用する管理者アカウントなどがあります。

エンドポイント管理者

CA Access Control エンタープライズ管理 がエンドポイントを管理するために、このアカウントを使用するかどうかを指定します。

重要: エンドポイント管理者アカウントを選択する際には注意が必要です。CA Access Control エンタープライズ管理 は、管理する特権アカウントのパスワードを自動的に変更します。エンドポイント管理者アカウントを選択すると、エンドポイント上の特権アカウントにログインして管理する機能が失われます。

[次へ]をクリックします。

[特権アカウント検出ウィザード: 全般アカウントの詳細]ページが表示されます。

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。

接続解除システム

アカウントの場所を接続解除システムにするかどうかを指定します。

このオプションを選択すると、PUPM はアカウントを管理しません。代わりに、PUPM は、接続解除システムの特権アカウントのパスワード ボールトとしてのみ機能します。パスワードを変更するたびに、管理対象エンドポイント上のアカウント パスワードも手動で変更する必要があります。

パスワード ポリシー

特権またはサービス アカウントに適用するパスワード ポリシーを指定します。

チェックアウト期限

チェックアウト アカウントが失効するまでの期間を分単位で指定します。

専用アカウント

単一ユーザだけがいつでもアカウントを使用することができるかどうかを指定します。*専用アカウント*は、アカウントの使用を1 回に 1 ユーザに制限する、特権アカウントの制限事項です。

チェックアウト時にパスワードを変更

特権アカウントがチェックアウトされるたびに、CA Access Control エンタープライズ管理 でそのパスワードを変更するかどうかを指定します。

注: このオプションはサービス アカウントに適用されません。

チェックイン時にパスワードを変更

ユーザまたはプログラムによって特権アカウントがチェックインされるたび、またはチェックアウト期間の失効時に、CA Access Control エンタープライズ管理 でそのパスワードを変更するかどうかを指定します。

注: アカウントが専用ではない場合、すべてのユーザがアカウントをチェックインしている場合のみ、CA Access Control エンタープライズ管理 は新規特権アカウント パスワードを生成します。

注: このオプションはサービス アカウントに適用されません。

サービス アカウント

検出されたアカウントがサービス アカウントかどうかを指定します。

注: さらに、サービス アカウント検出ウィザードを使用して、サービス アカウントを検出できます。

[完了]をクリックします。

エラーがない場合、CA Access Control エンタープライズ管理 はタスクをサブミットし、選択された特権アカウントを作成します。

詳細情報:

サービス アカウントの検出 (P. 257)

特権またはサービス アカウントの作成

管理対象および接続解除システム上でアカウント パスワードを管理するために、特権およびサービス アカウントを作成します。特権およびサービス アカウントは、異なる目的で使用します。

- ユーザに特権アカウント パスワードをチェックアウトおよびチェックインさせるために、特権アカウントを作成します。
- CLI、データベースまたは Windows RunAs パスワード コンシューマをセットアップするには、特権アカウントを作成します。
- Windows サービスよび Windows スケジュール タスク パスワード コンシューマをセットアップするには、サービス アカウントを作成します。

  注: サービス アカウント パスワードはチェックアウトおよびチェックインできません。

複数のアカウントを作成するには、特権アカウント検出ウィザードおよびサービス アカウント検出ウィザードを使用して、エンドポイント上の特権およびサービス アカウントを検索します。単一のアカウントを作成するには、このウィンドウに特権またはサービス アカウントの詳細を入力します。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[アカウント]-[特権アカウントの作成] をクリックします。

   [特権アカウントの作成: 特権アカウントの選択]ページが表示されます。
2. (オプション)既存の特権アカウントを選択して、パスワード ポリシーをそのコピーとして、以下のように作成します。
   a. [特権アカウント 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特権アカウントのリストが表示されます。
   c. 新規特権アカウントのベースとして使用するオブジェクトを選択します。
3. [OK]をクリックします。

   [特権アカウントの作成]タスク ページの[全般]タブが表示されます。特権アカウント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ロードされています。

4. ［全般］タブで以下のフィールドに入力します。

アカウント名

ユーザがこの特権アカウントを参照するために使用する名前を定義します。

注: RACF、ACF、および Top Secret などのメインフレーム システムには、大文字小文字を区別するユーザ名を使用します。大文字でアカウント名を入力します。

切断アカウント

アカウントの場所を接続解除システムにするかどうかを指定します。

このオプションを選択すると、PUPM はアカウントを管理しません。代わりに、PUPM は、接続解除システムの特権アカウントのパスワード ボールトとしてのみ機能します。パスワードを変更するたびに、管理対象エンドポイント上のアカウント パスワードも手動で変更する必要があります。

アカウント タイプ

アカウントが共有（特権）アカウントかサービス アカウントかを指定します。

注: サービス アカウントの作成時に、PUPM はアカウント パスワードの変更を試行しません。

エンドポイント名

特権またはサービス アカウントが存在する、定義済みのエンドポイントの名前を指定します。CA Access Control エンタープライズ管理 は、指定したタイプのエンドポイントのみをリスト表示します。

エンドポイント タイプ

特権またはサービス アカウントが存在するエンドポイントのタイプを指定します。

コンテナ

特権またはサービス アカウントのコンテナの名前を指定します。*コンテナ*は、そのインスタンスが他のオブジェクトの集合であるクラスです。コンテナは、特定のアクセス ルールに従って、整理された方法でオブジェクトを格納するために使用されます。

パスワード ポリシー

特権またはサービス アカウントに適用するパスワード ポリシーを指定します。

パスワード

ユーザが新しい特権アカウントで使用するパスワードを定義します。

注: 新しいパスワードは、指定するパスワード ポリシーに準じる必要があります。

チェックアウト期限

チェックアウト アカウントが失効するまでの期間を分単位で指定します。

専用アカウント

単一ユーザだけがいつでもアカウントを使用することができるかどうかを指定します。 *専用アカウント*は、アカウントの使用を1 回に 1 ユーザに制限する、特権アカウントの制限事項です。

チェックアウト時にパスワードを変更

特権アカウントがチェックアウトされるたびに、CA Access Control エンタープライズ管理 でそのパスワードを変更するかどうかを指定します。

注: このオプションはサービス アカウントに適用されません。

チェックイン時にパスワードを変更

ユーザまたはプログラムによって特権アカウントがチェックインされるたび、またはチェックアウト期間の失効時に、CA Access Control エンタープライズ管理 でそのパスワードを変更するかどうかを指定します。

注: アカウントが専用ではない場合、*すべて*のユーザがアカウントをチェックインしている場合のみ、CA Access Control エンタープライズ管理 は新規特権アカウント パスワードを生成します。

注: このオプションはサービス アカウントに適用されません。

ログイン アプリケーション チェックアウトのみ

エンドポイントに対してログイン アプリケーションが定義されている場合にのみ、パスワードのチェックアウトを許可するかどうかを指定します。

注: このオプションを有効に設定すると、ユーザはパスワードの表示やクリップボードへのコピーを実行できません。

5. (オプション) [パスワード コンシューマ]タブに移動します。

   設定されている場合、CA Access Control エンタープライズ管理 は特権アカウントを使用するパスワード コンシューマを表示します。

6. (オプション) [情報]タブをクリックして、タブ内のフィールドに値を入力します。

   このタブでエンドポイント固有の属性を指定すると、特権アクセス ロールを定義または変更するときにその属性を使用することができます。

   特権アクセス ロールのメンバが CA Access Control エンタープライズ管理 にログインする際に、そのユーザは特権アクセス ロールに定義された属性に従って特権アクセス アカウントへのアクセスを取得します。

   所有者

   エンドポイント所有者の名前を指定します。

   部署

   部門の名前を指定します。

   例: Development

   Custom 1...5

   エンドポイント固有のカスタム属性を指定します(最大 5 つ)。

   注: 特権アクセス ロールのカスタム属性は、[メンバ]タブ、[メンバ ポリシー]セクション、[メンバ ルール]ウィンドウ内で指定します。

7. [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 は新しい特権またはサービス アカウントを作成します。

パスワード ポリシーの作成

特権アカウントのパスワード ポリシーは、許容可能な特権アカウント パスワードを決定するルールおよび制限事項のセットです。たとえば、長さが 8 文字以上で、1 つの数字と 1 つの文字を含むパスワードを要求するポリシーを設定できます。また、パスワード ポリシーによって、CA Access Control エンタープライズ管理 がアカウントの新規パスワードを自動的に作成する間隔を決定します。

注: CA Access Control エンタープライズ管理 には使用可能な事前定義済みパスワード ポリシーが最初から用意されています。各エンドポイントに対して適切であり、セキュリティ要件に準拠したパスワード ポリシーを定義することをお勧めします。

パスワード ポリシーの作成方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[パスワード ポリシー]-[パスワード ポリシーの作成]をクリックします。

   [パスワード ポリシーの作成: 標準検索画面の設定]ページが表示されます。

2. (オプション)既存のパスワード ポリシーを選択して、パスワード ポリシーをそのコピーとして、以下のように作成します。

   a. [特権アカウント パスワード ポリシー タイプのオブジェクトのコピーの作成]を選択し、[検索]をクリックします。

      パスワード ポリシーのリストが表示されます。

   b. 新規パスワード ポリシーのベースとして使用するオブジェクトを選択します。

3. [OK]をクリックします。

   [パスワード ポリシーの作成]タスク ページが表示されます。パスワード ポリシー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ロードされています。

4. パスワード ポリシーの名前とオプションの説明を入力します。

5. (オプション) [有効化]をクリアします。

   デフォルトでは、新しいパスワード ポリシーは有効です。作成しているポリシーがまだ承認されない場合、このチェック ボックスをクリアし、ポリシーを無効にしておくことを選択できます。

6. パスワード構成ルールを定義します。

7. （オプション）パスワード失効間隔を定義します。

   これは CA Access Control エンタープライズ管理 がパスワードを自動的に変更する通常の間隔です。デフォルトでは、失効間隔は無効になっています（ゼロに設定）。

8. （オプション）CA Access Control エンタープライズ管理 がパスワードを変更できる時間を、24 時間形式で定義します。

   たとえば、サービス アカウントのパスワード ポリシーを作成する場合、CA Access Control エンタープライズ管理 がアカウントのパスワードを変更できるのは、日曜日の午後 10 時から午後 11 時 59 分（22:00-23:59）であると指定できます。

9. ［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 によってパスワード ポリシーが作成されます。

詳細情報:

パスワード構成ルール (P. 192)

パスワード構成ルール

パスワード ポリシーを作成する場合、新規パスワードの内容に関する要件を定義できます。

重要: パスワード構成ルールを設定する場合、要件設定時に、パスワードの最大長を考慮します。必要な文字の合計数が最大パスワード長を超えると、すべてのパスワードが拒否されます。

CA Access Control エンタープライズ管理 では、特権アカウントに関して、以下のパスワード構成ルールが用意されています。

パスワードの最小文字数

パスワードで使用する必要がある文字の最小数を指定します。

パスワードの最大文字数

パスワードで使用する必要がある文字の最大数を指定します。

最大繰り返し文字数

パスワードに含めることができる繰り返し文字の最大数を指定します。

たとえば、この値を「3」に設定すると、文字列「aaa」はパスワードに使用できませんが、「aa」は使用できます。

大文字 (パターンの場合は u)

パスワードに大文字を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある大文字の最小数を定義します。

小文字 (パターンの場合は c)

パスワードに小文字を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある小文字の最小数を定義します。

文字 (パターンの場合は l)

パスワードに英字を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある英字の最小数を定義します。

数字 (パターンの場合は d)

パスワードに数字を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある数字の最小数を定義します。

文字または数字 (パターンの場合は a)

パスワードに英数字を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある英数字の最小数を定義します。

句読点 (パターンの場合は p)

パスワードに句読点を含めることができるかどうかを指定します。できる場合は、パスワードに含める必要がある句読点の最小数を定義します。

任意 (パターンの場合は *)

パスワードに任意の文字を含めることができることを指定します。このオプションを選択すると、CA Access Control エンタープライズ管理 は自動的に他のすべての文字コンテンツ定義を選択します。

パターンの使用

文字コンテンツを定義するのではなく、パスワードが使用する必要があるパターンを定義することを指定します。

例:

- **uuuuu** - ASDKF または IUTYE に一致
- **ucdddp** - Rv671* または Uc194^ に一致

- ******** - lkI&5Jj@ または sffIU*&1 に一致
- **llllaaaa** - yuUI1Uo3 または qWcV1Er6 に一致

禁止文字

特権アカウント パスワードの作成または変更時に、使用できない文字を定義します。

PUPM エンドポイントと特権アカウントの作成

以下のトピックでは、CA Access Control エンタープライズ管理 でのエンドポイントの作成、特権アカウントの作成および検出、ログイン アプリケーションの作成方法について説明しています。

複数の PUPM のエンドポイントまたは特権アカウントを作成または変更する場合は、PUPM フィーダを使用することを検討します。PUPM フィーダを使用すると、ユーザは 1 つのステップで多くのエンドポイントまたは特権アカウントをインポートし、PUPM のエンドポイントと特権アカウントの管理を自動化できます。

エンドポイントの作成

CA Access Control エンタープライズ管理 でエンドポイント定義を作成すると、エンドポイントの管理、およびエンドポイント上の特権およびサービス アカウントの検出を実行できます。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[エンドポイント]-[エンドポイントの作成]をクリックします。

   [エンドポイントの作成: エンドポイントの選択]ページが表示されます。

2. (オプション)既存のエンドポイントを選択して、エンドポイントをそのコピーとして、以下のように作成します。

   a. [エンドポイント 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エンドポイントのリストが表示されます。

   c. 新規エンドポイントのベースとして使用するオブジェクトを選択します。

3. [OK]をクリックします。

   [エンドポイントの作成]タスク ページの[全般]タブが表示されます。エンドポイント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ロードされています。

4. このタブのフィールドにデータを入力します。以下のフィールドについて説明します。

   名前

   エンドポイントの論理名を定義します。

   注: このフィールドは、エンドポイントの名前が CA Access Control エンタープライズ管理 でどのように表示されるかを定義します。エンドポイント タイプの選択時に、接続情報を指定します。

   説明

   (オプション)エンドポイントに関して、記録する情報を定義します(書式自由)。

   エンドポイント タイプ

   特権またはサービス アカウントが存在するエンドポイントのタイプを指定します。

   注: エンドポイント タイプの選択時に、追加のダイアログ ボックスが開きます。ここで、そのタイプのエンドポイント上の特権アカウントを管理するために PUPM が必要とするクレデンシャルを指定できます。選択するエンドポイント タイプは、提供する必要がある接続情報に影響します。

5. (オプション)[ログイン アプリケーション]タブをクリックし、タブ内のフィールドに値を入力します。

   ログイン アプリケーション

   このエンドポイントに割り当てるログイン アプリケーションを指定します。

   注: ログイン アプリケーションをエンドポイントに割り当てる前に、まず、ログイン アプリケーションを作成します。複数のログイン アプリケーションを同じエンドポイントに割り当てることができます。

6. （オプション）CA Enterprise Log Manager タブをクリックし、タブ内のフィールドに値を入力します。

   このタブでは、CA Access Control エンタープライズ管理 の PUPM エンドポイント上での特権アカウント監査イベントの CA Enterprise Log Manager レポートを表示できます。CA Enterprise Log Manager への接続を設定していない場合、このタブは表示されません。

   ホスト名

   CA Enterprise Log Manager に指定したようにホスト名を定義します。

   このフィールドに値を入力しない場合、CA Access Control エンタープライズ管理 は［全般］タブの［名前］フィールドに指定したホスト名を使用します。

   イベント ログ名

   CA Enterprise Log Manager に指定したようにイベント ログ名を定義します。たとえば、Windows エージェントレス エンドポイントのイベント ログ名は、「NT-Security」になります。

   このフィールドに値を入力しない場合、CA Access Control エンタープライズ管理 で特権アカウント監査イベントのレポートを表示すると、すべてのエンドポイント タイプの監査イベントが表示されます。

   注: イベント ログ名の詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

7. （オプション）［情報］タブをクリックして、タブ内のフィールドに値を入力します。

   このタブでエンドポイント固有の属性を指定すると、特権アクセス ロールを定義または変更するときにその属性を使用することができます。

   特権アクセス ロールのメンバが CA Access Control エンタープライズ管理 にログインする際に、そのユーザは特権アクセス ロールに定義された属性に従って特権アクセス アカウントへのアクセスを取得します。

   所有者

   エンドポイント所有者の名前を指定します。

   部署

   部門の名前を指定します。

   例: Development

Custom 1...5

エンドポイント固有のカスタム属性を指定します(最大 5 つ)。

注: 特権アクセス ロールのカスタム属性は、[メンバ]タブ、[メンバ ポリシー]セクション、[メンバ ルール]ウィンドウ内で指定します。

8. [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、ユーザーが提供するクレデンシャルを使用して、エンドポイントへの接続を試行します。接続に成功した場合、エンドポイントが作成されます。成功しなかった場合は、接続エラーを受信します。

関連項目:

PUPM 接続情報用の Access Control (P. 198)
MS SQL Server 接続情報 (P. 201)
Oracle Server 接続情報 (P. 203)
VMware ESX/ESXi 接続情報 (P. 208)
Windows エージェントレス接続情報 (P. 209)
SSH Device 接続情報 (P. 219)
SAP R3 接続情報 (P. 227)
CA Identity Manager プロビジョニング接続情報 (P. 229)
接続解除されたエンドポイント接続情報 (P. 233)
ログイン アプリケーションの作成 (P. 233)

PUPM 接続情報用の Access Control

PUPM エンドポイント タイプ用の Access Control では、特権 Access Control アカウントを管理できます。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

ホスト ドメイン

このホストがメンバであるドメインの名前を指定します。

例: Domain.com

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

IBM AS/400 接続情報

IBM AS/400 エンドポイント タイプによって、IBM AS/400 の管理対象アカウントを管理できます。

IBM AS/400 エンドポイントに対して指定した管理者ユーザは、以下の権限を持っている必要があります。

- 他のユーザ アカウントの表示
- 自身のユーザ アカウントの表示
- 他のユーザ アカウント パスワードの表示

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

名前

エンドポイントの名前を指定します。

重要: エンドポイント名はホスト名と一致する必要があります。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

注: CA Access Control がエンドポイントにインストールされている場合、この属性に CA Access Control ホスト名を指定することをお勧めします。エンドポイントの CA Access Control ホスト名を表示するために、ワールド ビューを使用できます。

重要: ホスト名はエンドポイント名と一致する必要があります。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

MS SQL Server 接続情報

MS SQL Server エンドポイント タイプを使用して、Microsoft SQL Server 特権アカウントを管理できます。

MS SQL Server のエンドポイントに対して指定される管理者ユーザは、以下を満たしている必要があります。

- securityadmin サーバ ロールを保持している

注: securityadmin サーバ ロールを持つユーザは serveradmin および sysadmin サーバ ロールを変更することができません。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

URL

エンドポイントに接続するために CA Access Control エンタープライズ管理 が使用できる URL を定義します。URL は特定のタイプのデータベース サーバを指定します。

構文: jdbc:sqlserver://*servername*:*port*

例: jdbc:sqlserver://localhost:1433

注: URL の形式の詳細については、エンドポイントのドキュメントを参照してください。

ホスト

エンドポイントのホスト名を定義します。

注: CA Access Control がエンドポイントにインストールされている場合、この属性に CA Access Control ホスト名を指定することをお勧めします。エンドポイントの CA Access Control ホスト名を表示するために、ワールド ビューを使用できます。

Port

(オプション) サーバのリスニング ポート番号を指定します。指定するポート番号は、URL で指定するポート番号と一致する必要があります。

例: 1433

インスタンス名

(オプション) データベース インスタンス名を指定します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

Oracle Server 接続情報

Oracle Server エンドポイント タイプを使用すると、Oracle データベース 特権アカウントを管理できます。

Oracle Server のエンドポイントに対して指定した管理者ユーザは ALTER USER および SELECT ANY DIRECTORY のシステム権限を保持している必要があります。

このタイプのエンドポイントを作成する場合、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

URL

エンドポイントに接続するために CA Access Control エンタープライズ管理 が使用できる URL を定義します。URL は特定のタイプのデータベース サーバを指定します。

形式: jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

例: jdbc:oracle:thin:@ora.comp.com:1521:orcl

注: URL の形式の詳細については、エンドポイントのドキュメントを参照してください。

ホスト

エンドポイントのホスト名を定義します。これは完全修飾ホスト名です。

注: CA Access Control がエンドポイントにインストールされている場合、この属性に CA Access Control ホスト名を指定することをお勧めします。エンドポイントの CA Access Control ホスト名を表示するために、ワールド ビューを使用できます。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

Sybase Server 接続情報

Sybase Server エンドポイント タイプを使用すると、Sybase Server 特権アカウントを管理できます。

重要: データベースが適切に設定され、ポート 2638 が開いていて接続可能であることを確認してください。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

URL

エンドポイントに接続するために CA Access Control エンタープライズ管理 が使用できる URL を定義します。URL は特定のタイプのデータベース サーバを指定します。

形式: jdbc:sybase:Tds:*servername*:*port*

例: jdbc:sybase:Tds:localhost:2638

注: URL の形式の詳細については、エンドポイントのドキュメントを参照してください。

ホスト

エンドポイントのホスト名を定義します。

注: CA Access Control がエンドポイントにインストールされている場合、この属性に CA Access Control ホスト名を指定することをお勧めします。エンドポイントの CA Access Control ホスト名を表示するために、ワールド ビューを使用できます。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

RACF 接続情報

RACF タイプを使用すると、RACF 特権アカウントを管理できます。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、[assign the value for eACVPM in your book] がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

例: *cn=user1,host=RACF,o=company,c=com*

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

注: CA Access Control がエンドポイントにインストールされている場合、この属性に CA Access Control ホスト名を指定することをお勧めします。エンドポイントの CA Access Control ホスト名を表示するために、ワールド ビューを使用できます。

ベース DN

LDAP ディレクトリ内の検索開始ポイントを指定します。

例: *host=RACF,o=company,c=com*

URL

エンドポイントに接続するために CA Access Control エンタープライズ管理が使用できる URL を定義します。URL は特定のタイプのデータベース サーバを指定します。

例: ldap://*host_name.company.com:5*91

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

注: 自分自身および他のユーザ アカウントに対する管理権限を持つユーザ アカウントを指定します。

VMware ESX/ESXi 接続情報

VMware ESX/ESXi エンドポイント タイプによって、VMware ESX/ESXi 特権アカウントを管理できます。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、[assign the value for eACVPM in your book] がエンドポイントに接続できるようにします。

ユーザ名

エンドポイントの管理ユーザの名前を定義します。CA Access Control エンタープライズ管理 はこのアカウントを使用して、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクを実行します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

Windows エージェントレス接続情報

Windows エージェントレス エンドポイント タイプを使用すると、Windows 特権アカウントを管理できます。

注: ローカル コンピュータ上でドメイン ユーザを設定すると、PUPM はそのドメイン ユーザのパスワードを変更できません。この制限は、Windows の動作に起因するものです。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

例: myhost-ac-1

ホストドメイン

このホストがメンバであるドメイン名を指定します。

注: ホストドメイン名には接頭辞だけを指定します。たとえば、完全なドメイン名が company.com である場合、接頭辞の company のみを入力します。

Active Directory

ユーザ アカウントが Active Directory アカウントかどうかを指定します。

ユーザ ドメイン

このユーザがメンバであるドメイン名を指定します。

注: ユーザ ドメイン名は接頭辞だけを指定します。たとえば、完全なドメイン名が company.com である場合、接頭辞の company のみを入力します。

重要: PUPM 自動ログインを使用してエンドポイントにログインする場合、ホストドメイン名を指定することを確認します。エンドポイントがワークグループのメンバである場合は、ワークグループ名ではなくホスト名を指定します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

Windows エージェントレス エンドポイントの PUPM 用の設定

以下のトピックでは、PUPM を実装する前に Windows エージェントレス エンドポイントで必要な場合がある追加設定手順を説明します。

詳細情報:

Windows エージェントレス エンドポイント上のドメイン ユーザに対する制限事項 (P. 158)

Windows エージェントレス エンドポイントのファイアウォール設定

Windows Server 2008 および Windows 7 Enterprise で有効

PUPM Windows エージェントレス コネクタは、Windows エージェントレス エンドポイントとの接続にポート 135 (DCOM ポート)を使用します。PUPM Windows エージェントレス コネクタは JCS の一部です。コネクタは、エンドポイントとの接続後、動的ポート(1001 以上)を使用して WMI(Windows Management Instrumentation)サービスと通信します。

Windows エージェントレス エンドポイントで Windows ファイアウォールが有効化されていると、ポート 135 および動的ポートへの接続がファイアウォールによってブロックされる場合があります。Windows ファイアウォールがこれらの接続をブロックした場合、エンタープライズ管理サーバはエンドポイントと通信できません。そのため、Windows エージェントレス エンドポイントを作成できないか、またはエンドポイント上のサービス アカウントとスケジュールされたタスクを検出できません。

Windows ファイアウォールを有効にしている場合、PUPM Windows エージェントレス コネクタがエンドポイントに接続できるように、ファイアウォールを設定する必要があります。ファイアウォールの設定ではポート 135 を開き、動的な RPC ポートから WMI サービスに送られるすべてのトラフィックがファイアウォールによって許可されるように指定します。

詳細情報:

Windows ファイアウォールを PUPM 用に設定する方法 (P. 211)

Windows ファイアウォールを PUPM 用に設定する方法

Windows エージェントレス エンドポイントに該当

PUPM Windows エージェントレス コネクタは、Windows エージェントレス エンドポイントとの接続にポート 135 (DCOM ポート)を使用します。コネクタは、エンドポイントとの接続後、動的ポート(1001 以上)を使用して WMI(Windows Management Instrumentation)サービスと通信します。

Windows ファイアウォールを有効化にしている場合、PUPM Windows エージェントレス コネクタがエンドポイントに接続できるように、ファイアウォールを設定する必要があります。ファイアウォールを設定しないと、エンタープライズ管理サーバはエンドポイントと通信できません。

Windows ファイアウォールを PUPM 用に設定するには、以下の手順に従います。

1. ポート 135 を開きます。
2. 動的な RPC ポートから WMI サービスに送られるすべてのトラフィックが許可されるように、ファイアウォール ルールを作成します。

   以下の例を参考に、ユーザの Windows ファイアウォールを設定してください。

例: ポート 135 を開く

以下の例では、Windows Server 2008 コンピュータ上でポート 135 を開く方法を示します。

1. [スタート] - [コントロール パネル] - [Windows ファイアウォール]の順にクリックします。

   [Windows ファイアウォール]ダイアログ ボックスが表示されます。
2. [設定の変更]をクリックします。

   [Windows ファイアウォールの設定]ダイアログ ボックスが表示されます。
3. [例外]タブをクリックし、[ポートの追加]をクリックします。

   [ポートの追加]ダイアログ ボックスが開きます。
4. 以下のようにダイアログに入力します。
   - [名前]フィールドに「**DCOM_TCP135**」と入力します。
   - [ポート番号]フィールドに「**135**」と入力します。
   - [プロトコル]セクションで、[TCP]を選択します。

   [OK]をクリックします。

   [例外]タブに[DCOM_TCP135]ルールが表示されます。
5. [OK]をクリックします。

   [Windows ファイアウォールの設定]ダイアログ ボックスが閉じます。ポート 135 が開きました。

例: 動的 RPC ポートから WMI サービスに送られるトラフィックを許可するファイアウォール ルールの作成

以下に、Windows Server 2008 コンピュータ上でファイアウォール ルールを作成する場合の例を示します。このファイアウォール ルールは、動的 RPC ポートから WMI サービスに送られるトラフィックを許可します。

1. [スタート] - [管理ツール] - [セキュリティが強化された Windows ファイアウォール]の順にクリックします。

   [セキュリティが強化された Windows ファイアウォール]ダイアログ ボックスが開きます。

2. 左ペインの[受信の規則]を右クリックし、[新しい規則]をクリックします。

   [新規の受信の規則ウイザード]が表示されます。

3. [新規の受信の規則ウイザード]を終了します。以下を*除く*すべてのページで、デフォルトの設定を使用します。

   a. [規則の種類]ページでは、[カスタム]を選択します。

   b. [プログラム]ページでは、以下の手順に従います。

      - すべてのプログラムを選択します。
      - [カスタマイズ]をクリックします。

        [サービス設定のカスタマイズ]ダイアログ ボックスが表示されます。

      - [このサービスに適用] - [Windows Management Instrumentation]を選択し、[OK]をクリックします。

   c. [スコープ]ページの[この規則はどのリモート IP アドレスに一致しますか?]セクションで以下のように指定します。

      - [これらの IP アドレス]を選択し、[追加]をクリックします。

        [IP アドレス]ダイアログ ボックスが表示されます。

      - [IP アドレスまたはサブネット]に配布サーバの IP アドレスを入力し、[OK]をクリックします。

   d. [名前]ページの[名前]フィールドに新しいルールの名前を入力します。

   ウィザードが終了すると、動的 RPC ポートから WMI サービスに送られたすべてのトラフィックが、ファイアウォールによって許可されるファイアウォール ルールが作成されています。

詳細情報:

Windows エージェントレス エンドポイントのファイアウォール設定 (P. 211)

Windows Server 2008 R2 x64 エンドポイントの PUPM 用の設定

Windows Server 2008 に該当

Windows Server 2008 R2 x64 エンドポイント上で PUPM を使用するには、エンドポイント上で追加の設定手順を実行します。

以下の手順に従います。

1. Windows レジストリを開きます。
2. 以下のレジストリ キーに移動し、各キーについて手順 3 ～ 6 を実行します。

   HKEY_CLASSES_ROOT¥CLSID¥{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT¥CLSID¥{233664b0-0367-11cf-abc4-02608c9e7553}

   注: [編集]メニューの[検索]オプションを使用して、このレジストリ キーを検索できます。
3. 各キーを右クリックして、[アクセス許可]を選択します。

   アクセス許可ダイアログ ボックスが表示されます。
4. [詳細]をクリックします。

   セキュリティの詳細設定ダイアログ ボックスが表示されます。
5. [所有者]タブをクリックし、[所有者の変更]フィールドで[管理者]をクリックし、[適用]をクリックし、[OK]をクリックします。

   セキュリティの詳細設定ダイアログ ボックスが閉じます。
6. アクセス許可ダイアログ ボックスの[グループ名またはユーザ名]ウィンドウで[管理者]を選択し、アクセス許可ウィンドウの[許可]列で[フル コントロール]チェックボックスを選択します。
7. [OK]をクリックします。
8. [スタート]、[管理ツール]、[ローカル セキュリティ ポリシー]をクリックします。

   [ローカル セキュリティ ポリシー]コンソールが開きます。

9. [ローカル ポリシー]-[セキュリティ オプション]を選択します。

   使用可能なセキュリティ オプションのリストが表示されます。

10. 以下のセキュリティ ポリシーを確認します。

    - ネットワーク セキュリティ: NTLM SSP ベース(セキュア RPC を含む)のサーバー向け最小セッション セキュリティ
    - ネットワーク セキュリティ: NTLM SSP ベース(セキュア RPC を含む)のサーバー向け最小セッション セキュリティ

11. 各ポリシーを右クリックして、[プロパティ]を選択します。

    [ローカル セキュリティの設定]タブが表示されます。

12. [128 ビット暗号化が必要]オプションが選択されていないことを確認します。

13. [OK]をクリックして終了します。

    これで、Windows Server 2008 R2 x64 エンドポイントが PUPM 用に設定されました。さらに、ファイアウォールを設定し、DCOM への許可を追加する必要がある場合があります。

ログイン アプリケーションを使用するための Windows Server 2008 エンドポイントの変更

Windows Server 2008 で有効

Microsoft は、Windows Server 2008 コンピュータにおける ActiveX コントロール オプションに対する自動ダイアログのデフォルト値を変更しました。Windows Server 2008 コンピュータで、このオプションのデフォルト値は無効になっています。以前のバージョンの Windows では、このオプションのデフォルト値は有効になっていました。 このオプションは、ローカル イントラネットのセキュリティ設定、および信頼できるサイト ゾーンに影響します。

Windows Server 2008 エンドポイントを、ログイン アプリケーションを使用するように変更するには、ActiveX コントロール オプションの自動ダイアログの値をローカル イントラネットおよび信頼できるサイト ゾーンに対して有効にします。

注: このオプションの値を変更しない場合、Windows Server 2008 コンピュータ上で自動ログインを使用することができません。

詳細情報:

ログイン アプリケーションの作成 (P. 233)

PUPM 用の Windows 7 エンタープライズ エンドポイントの設定

Windows 7 Server で該当

Windows 7 エンドポイント上で PUPM を使用するには、エンドポイント上で追加の設定手順を実行する必要があります。

以下の手順に従います。

1. Windows レジストリを開きます。
2. 以下のレジストリ キーに移動し、各キーについて手順 3 ～ 6 を実行します。

   HKEY_CLASSES_ROOT¥CLSID¥{76A64158-CB41-11D1-8B02-00600806D9B6}

   HKEY_CLASSES_ROOT¥CLSID¥{233664b0-0367-11cf-abc4-02608c9e7553}

   注: [編集]メニューの[検索]オプションを使用して、このレジストリ キーを検索できます。
3. このキーを右クリックして、[アクセス許可]を選択します。

   アクセス許可ダイアログ ボックスが表示されます。
4. [詳細設定]をクリックします。

   セキュリティの詳細設定ダイアログ ボックスが表示されます。
5. [所有者]タブをクリックし、[所有者の変更]フィールドで[管理者]をクリックし、[適用]をクリックし、[OK]をクリックします。

   セキュリティの詳細設定ダイアログ ボックスが閉じます。
6. アクセス許可ダイアログ ボックスの[グループ名またはユーザ名]ウィンドウで[管理者]を選択し、アクセス許可ウィンドウの[許可]列で[フル コントロール]チェックボックスを選択します。
7. [OK]をクリックして、Windows レジストリを閉じます。
8. Windows の[コントロール パネル]-[管理ツール]-[サービス]を開きます。

   [Windows サービス]コンソールが開きます。
9. [Remote Registry]サービスを右クリックし、[プロパティ]を選択します。

   [プロパティ]ダイアログ ボックスが開きます。
10. [スタートアップの種類]を[自動]に変更し、[開始]を選択します。

    [Remote Registry]サービスが開始します。

11. [ファイル名を指定して実行]コマンドライン ウィンドウから DCOMCNFG コマンドを実行します。

    [コンポーネント サービス]ウィンドウが開きます。

12. [コンソール ルート]-[コンポーネント サービス]-[コンピュータ]を選択します。

13. [マイ コンピュータ]を右クリックして[プロパティ]を選択します。

    [プロパティ]ダイアログ ボックスが開きます。

14. [COM セキュリティ]タブをクリックし、[アクセス許可]セクションの下で[既定値の編集]をクリックします。

    [既定のセキュリティ]ダイアログ ボックスが開きます。

15. [グループ名またはユーザー名]ウィンドウで Administrators を選択し、[ローカル アクセス]および[リモート アクセス]の[許可]チェック ボックスをオンにします。

16. [OK]をクリックし、[起動とアクティブ化のアクセス許可]セクションで手順 14 と 15 を繰り返します。

17. [OK]をクリックして、[コンポーネント サービス]コンソールを閉じます。

    これで、PUPM 用に Windows 7 エンタープライズ エンドポイントを設定しました。ファイアウォールも設定する必要があります。

管理者承認モードの変更

Windows Server 2008 および Windows 7 で有効

PUPM エンドポイント管理タスクは、バックグラウンドで実行され、ネイティブ管理者アカウントのアクセス権限を必要とします。PUPM エンドポイント管理者にこのネイティブ管理者アカウントのアクセス権がない場合、すべてのエンドポイント管理者に対して管理者承認モードでの実行を許可する必要があります。

重要: ポリシー設定が無効になっている場合、セキュリティ センターは、オペレーティング システムの全体的なセキュリティが低下していることをユーザに通知します。

以下の手順に従います。

1. [コントロール パネル]-[管理ツール]-[ローカル セキュリティ ポリシー]を選択します。

   [ローカル セキュリティ ポリシー]ウィンドウが表示されます。

2. [ローカル ポリシー]-[セキュリティ オプション]を選択します。

   [ポリシー]ペインが開きます。

3. [ユーザー アカウント制御: 管理者承認モードですべての管理者を実行する]を右クリックし、[プロパティ]を選択します。

   プロパティ ダイアログ ボックスが表示されます。

4. オペレーション モードを[無効]に変更して[OK]をクリックします。

   プロパティ ダイアログ ボックスが閉じます。

5. 変更を適用するためコンピュータを再起動します。

   バックグラウンドのエンドポイント管理タスクが正常に実行されるようになりました。

チャレンジ/レスポンス認証プロトコルの制限事項

Windows エージェントレス エンドポイントに該当

ネットワーク ログインのチャレンジ/レスポンス認証プロトコルは、認証プロトコルのレベル、およびエンドポイントがクライアント/サーバ通信に使用するセッション セキュリティに影響します。ネットワーク ログインに使用する Windows チャレンジ/レスポンス認証プロトコルには、3 タイプあります。

- LM - LAN Manager チャレンジ/レスポンス
- NTLM - Windows NT チャレンジ/レスポンス
- NTLMv2 - NTLM のバージョン 2

LAN Manager 認証レベル設定では、エンドポイントが使用するチャレンジ/レスポンス認証プロトコルが制御されます。この設定のデフォルト値は[LM と NTLM 応答を送信する]です。エンタープライズ管理サーバは、LAN Manager 認証レベル設定の値が[LM と NTLM 応答を送信する]の場合にのみ、Windows エンドポイントと通信できます。たとえば、この設定の値が、[NTLMv2 応答のみ送信(LM を拒否する)]の場合、エンタープライズ管理サーバは、Windows エンドポイントと通信できません。

エンドポイントでの LAN Manager 認証レベル設定が[LM と NTLM 応答を送信する]である場合にのみ、Windows エージェントレス エンドポイントを作成できます。Windows エージェントレス エンドポイントを作成できない場合、エンドポイントでのチャレンジ/レスポンス認証プロトコルの変更が必要な場合があります。

SSH Device 接続情報

SSH Device タイプを使用すると、UNIX 特権アカウントを管理できます。

重要: PUPM SSH エンドポイントを設定する前に、エンドポイント上のトンネル化されたクリア テキスト パスワードを無効にしてから、エンドポイントを設定します。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がデバイスに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。操作管理者アカウントを指定すると、PUPM は、そのアカウントを使用してエンドポイント上で管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

Telnet の使用

SSH デバイスへの接続に、SSH ではなく Telnet を使用するように指定します。

操作管理者ユーザ ログイン

(オプション)エンドポイントの操作管理ユーザの名前を定義します。PUPM は、このアカウントを使用してエンドポイントに対する管理タスクを実行します。たとえば、特権アカウントのパスワードを検出し、変更します。ユーザが操作管理者ユーザを指定しない場合も、PUPM はユーザ ログイン アカウントを使用して、エンドポイントに対する管理タスクを実行します。

Check Point ファイアウォールを使用する SSH エンドポイントに対して操作管理者ユーザを指定する場合、エキスパート ユーザを指定します。ただし、PUPM を使用してエンドポイント上のエキスパート アカウントのパスワードを変更することはできません。この制限は、エキスパート アカウントが PUPM 内の接続解除されたアカウントである必要があることを意味します。

操作管理者パスワード

(オプション) 操作管理者ユーザのパスワードを定義します。

環境設定ファイル

SSH Device XML 設定ファイルの名前を指定します。ニーズに合わせて XML ファイルをカスタマイズできます。

注: このフィールドの値を指定しない場合、CA Access Control エンタープライズ管理 は ssh_connector_conf.xml ファイルを使用します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

PUPM で UNIX エンドポイントに接続する方法

エンドポイントを作成する際、PUPM でのエンドポイントへの接続、特権アカウントのパスワードの検出や変更などの管理者タスクの実行に使用する管理者アカウントを指定します。UNIX アカウントでは、最も適切な管理者アカウントは root です。PUPM は SSH を使用して UNIX エンドポイントに接続しますが、組織によってはユーザやアプリケーションが root ユーザとして SSH 接続を行うのを禁じている場合があります。

この問題を解決するために、SSH Device エンドポイントを作成する際に、接続アカウントと操作管理者アカウントの両方を指定できます。(PUPM では UNIX エンドポイント用のエンドポイント タイプとして SSH Device が使用されます)。2 つのアカウントを使用することにより、さらにユーザに、操作管理者アカウントより少ない権限しか持たない接続アカウントも使用できるようになります。

以下のプロセスでは、PUPM がこれらのアカウントを使用して SSH Device エンドポイントに接続する方法について説明します。

1. PUPM は、接続アカウントのクレデンシャルを使用してエンドポイントに接続します。
2. PUPM では、そのアカウントへの su の実行に、操作管理者アカウントのクレデンシャルが使用されます。

   たとえば、操作管理者アカウントが root の場合、PUPM では、su を使用した root アカウントの使用に、root のクレデンシャルが使用されます。
3. PUPM では、操作管理者として管理タスクが実行されます。

   たとえば、操作管理者アカウントが root の場合、PUPM では、root として管理タスクが実行されます。

SSH Device エンドポイント上の特権アカウントを表示すると、接続アカウントおよび操作管理者アカウントの両方がエンドポイント管理者としてリストされます。

カスタマイズした SSH Device エンドポイントを作成する方法

特権アカウントを検出するために PUPM が使用するデフォルト設定が SSH Device エンドポイントに適用されない場合は、カスタマイズした SSH Device エンドポイントを作成できます。

カスタマイズした SSH Device エンドポイントを作成するには、以下の手順に従います。

1. SSH Device XML ファイルをカスタマイズします。
2. CA Access Control エンタープライズ管理 で SSH Device エンドポイントを作成します。 (P. 194) 作成した XML ファイルの名前を[環境設定ファイル]フィールドに入力します。

   SSH Device エンドポイントがカスタム設定を使用して作成されます。
3. 作成したエンドポイント上で特権アカウント検出ウィザード (P. 184)を実行します。

   CA Access Control エンタープライズ管理 は、XML ファイルに定義したパラメータを使用して、エンドポイントの特権アカウントを検索します。

4. JCS コネクタ ログ ファイル(jcs_stdout.log)および JCS コネクタ エラー ファイル(jcs_sterr.log)を確認します。ファイルは以下の場所にあります。

   ACServerInstallDir/Connector Server/logs

5. 必要な場合は、XML ファイルを修正してログ ファイルに表示されるエラーを解決します。

注: SSH デバイス XML ファイルの形式の詳細については、「*リファレンス ガイド*」を参照してください。

SSH Device XML 構成ファイルのタイプ

CA Access Control では、以下の SSH Device XML 構成ファイルが提供されます。これらのファイルをカスタマイズして、企業の要件に適合させます。

- **aix_connector_conf.xml** -- AIX エンドポイントである SSH デバイス用の環境設定を定義します。
- **checkpoint_connector_conf.xml** -- Check Point ファイアウォールを使用する SSH デバイス用の環境設定を定義します。
- **Cisco-UCS_connector_conf.xml** -- Cisco UCS エンドポイントである SSH デバイス用の環境設定を定義します。
- **device_connector_conf.xml** -- ルータなどのデバイス用の環境設定を定義します。
- **nis_connector_conf.xml** -- NIS サーバと一緒に動作する SSH デバイス用の環境設定を定義します。

  注: 接続済みユーザとしてローカル root アカウントを使用します。以下の手順を実行します。

  a. NIS エンドポイント(nis_endpoint_1)を作成し、デフォルトの XML ファイル(ssh_connector_conf.xml)を使用して、root アカウントを定義します 。

  b. 別の NIS エンドポイント(nis_endpoint_2)を作成し、[詳細]オプションを使用して、最初の NIS エンドポイントの root アカウントを定義します。

- **ssh_connector_conf.xml** -- アカウント パスワードを変更するために passwd コマンドを使用する SSH デバイスの環境設定時に、このファイルを使用します。

  注: 接続済みユーザとして、ローカル ユーザ、たとえば、root を指定します。

- **sudo_connector_conf.xml** - sudo および passwd コマンドを使用する SSH Device の環境設定時に、このファイルを使用します。

SSH Device XML ファイルのカスタマイズ

SSH Device XML ファイルは、PUPM が SSH Device エンドポイントに接続し、ユーザ アカウントを検出し、エンドポイント上の特権アカウント パスワードを変更する方法を定義します。CA Access Control には複数の SSH Device XML ファイルが用意されています。これらのファイルには、SSH Device エンドポイントのさまざまなタイプに接続するために PUPM が使用するデフォルト設定が含まれています。

SSH Device エンドポイントが別の方法を使用してエンドポイント上の特権アカウント パスワードを変更する場合は、SSH Device XML ファイルをカスタマイズしてデフォルト以外の設定を指定します。たとえば、SSH Device XML ファイルをカスタマイズして、標準以外の方法でユーザ アカウントを検出して特権アカウント パスワードを変更するエンドポイントをルータ、スイッチ、またはファイアウォール用に作成します。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 上でカスタマイズする XML ファイルを探します。これらのファイルは、以下のディレクトリにあります。

   ACServerInstallDir/Connector Server/conf/override/sshdyn

2. カスタマイズするファイルをコピーし、新しいファイルを編集用に開きます。

   注: 新しいファイルは同じディレクトリに保存します。

3. 自社の要件に合わせてファイル内のパラメータを変更します。

   ファイル内の各 <item> 要素は、特定のコマンドのパラメータを定義します。PUPM は、これらのコマンドを使用してエンドポイント上のユーザを取得し、パスワードを変更します。<item> 要素を変更して、PUPM がエンドポイントに送信するコマンドを定義します。また、エンドポイントに接続するために PUPM が使用する設定を変更することもできます。

4. ファイルを保存して閉じます。

   これで、SSH Device XML ファイルがエンドポイント用にカスタマイズされました。

注: SSH デバイス XML ファイルの形式の詳細については、「*リファレンス ガイド*」を参照してください。

注: 中国語、日本語、または韓国語を含むファイルをカスタマイズしている場合は、UTF-8 エンコーディングを使用してファイルを保存する必要があります。

例: SSH Device XML ファイルで PUPM コマンドを定義する方法

この例では、SSH Device XML ファイルのセクションで PUPM が SSH Device エンドポイント上で実行するコマンドを定義する方法について説明します。このセクションの各 <item> 要素は、特定のアクションのパラメータを定義します。すべての <item> 要素が一体となって、PUPM がエンドポイントと対話する方法を定義する 1 つのスクリプトが作成されます。

各 <item> 要素は、sCommand パラメータで始まります。sCommand パラメータは、PUPM がエンドポイント上で実行するコマンドを定義します。sCommand パラメータの後のパラメータは、PUPM がそのコマンドの後に実行する他のアクションを定義します。

この例では、Cisco-UCS_connector_conf.xml ファイルのセクションで、Cisco スイッチ上の特権アカウント パスワードを変更するために PUPM が使用するコマンドを定義する方法を示します。Cisco-UCS_connector_conf.xml ファイルは以下のディレクトリにあります。

ACServerInstallDir/Connector Server/conf/override/sshdyn

この例では、Cisco-UCS_connector_conf.xml ファイルの 1 つのセクションのみを示します。ファイル内の追加の要素では、Cisco スイッチへの接続を設定し、PUPM がユーザを取得するために実行するコマンドを指定します。

注: SSH デバイス XML ファイルの形式の詳細については、「*リファレンス ガイド*」を参照してください。

以下のプロセスでは、Cisco スイッチ上の特権アカウント パスワードを変更するために PUPM が実行するコマンドを示します。PUPM が実行するコマンドを <item> 要素で 設定する方法を示すために、対応する <item> 要素を各手順の最後に示します。

1. PUPM は、特権アカウントのパスワードの変更を指定します。PUPM は、この手順を完了するために以下のアクションを実行します。

   a. PUPM は以下のコマンドを発行します。

      ```
      set password
      ```

   b. PUPM は 500 ミリ秒待機します。

   c. PUPM は **word:** という文字列を受信するまで待機します。この文字列を受信すると、次の手順に進みます。

   この手順で PUPM が実行するアクションは、以下の <item> 要素で指定されます。

   ```
   <item>
   <param name="sCommand" value="set password" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="word:" />
   </item>
   ```

2. PUPM は、特権アカウントの新しいパスワードを指定します。PUPM は、この手順を完了するために以下のアクションを実行します。

   a. PUPM はエンドポイントに新しいパスワードを送信します。

      PUPM はログ ファイルに新しいパスワードを書き込みません。

   b. PUPM は 500 ミリ秒待機します。

   c. PUPM は **word:** という文字列を受信するまで待機します。この文字列を受信すると、次の手順に進みます。

   このコマンドのパラメータは、以下の <item> 要素で指定されます。

   ```
   <item>
   <param name="sCommand" value="[%%password%%]" />
   <param name="bHideSentLog" value="true" />
   <param name="iWait" value="500" />
   <param name="sWaitForText" value="word:" />
   </item>
   ```

3. PUPM は、特権アカウントの新しいパスワードを確認します。PUPM は、この手順を完了するために以下のアクションを実行します。

   a. PUPM はエンドポイントに新しいパスワードを再送信します。

      PUPM はログ ファイルに新しいパスワードを書き込みません。

   b. PUPM は 500 ミリ秒待機します。

   c. PUPM は **local-user* #** という文字列を受信するまで待機します。この文字列を受信すると、次の手順に進みます。

      PUPM が **failure**、**invalid**、または **error** という文字列を受信した場合、パスワード変更は失敗しました。

   このコマンドのパラメータは、以下の <item> 要素で指定されます。

```
<item>
<param name="sCommand" value="[%%password%%]" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="local-user* #" />
<param name="sFailureResult" value="failure;invalid;error" />
</item>
```

4. PUPM は、特権アカウントの新しいパスワードをコミットします。PUPM は、この手順を完了するために以下のアクションを実行します。

   a. PUPM は以下のコマンドを発行します。

      ```
      commit-buffer
      ```

      PUPM はログ ファイルにこのコマンドを書き込みません。

   b. PUPM は 500 ミリ秒待機します。

   c. PUPM は **local-user #** という文字列を受信するまで待機します。この文字列を受信すると、パスワード変更は完了します。

      PUPM が **Error: Update failed:** という文字列を受信した場合、パスワード変更は失敗しました。

   このコマンドのパラメータは、以下の <item> 要素で指定されます。

```
<item>
<param name="sCommand" value="commit-buffer" />
<param name="bHideSentLog" value="true" />
<param name="iWait" value="500" />
<param name="sWaitForText" value="local-user #" />
<param name="sFailureResult" value="Error: Update failed:" />
</item>
```

   パスワード変更が完了しました。

SAP R3 接続情報

PUPM SAP R3 エンドポイント タイプによって、SAP R3 の特権アカウントを管理できます。SAP R3 エンドポイントを PUPM 内に作成する前に、SAP R3 コネクタを設定する必要があります。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がデバイスに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。PUPM は、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行にこのアカウントを使用します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

システム ID

SAP R3 システム ID を定義します。

システム番号

SAP R3 システム番号を定義します。

クライアント番号

SAP R3 システム クライアント番号を定義します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

注: システム ID、システム番号、およびクライアント番号の詳細については、SAP R3 のドキュメントを参照してください。

SAP R3 コネクタの環境設定

PUPM を使用して SAP R3 エンドポイント上の特権アカウントを管理できるようにするには、SAP R3 コネクタを設定する必要があります。

SAP R3 コネクタを設定するには、エンタープライズ管理サーバまたは Java コネクタ サーバ（JCS）がインストールされているすべてのサーバに SAP JCo ライブラリをインストールします。

ご使用の SAP ログイン情報を使用すると、SAP マーケットプレースから SAP JCo ライブラリをダウンロードできます。ご使用のシステム プラットフォームに適した SAP JCo ライブラリを選択したことを確認してください。

例: Windows 上での SAP JCo ライブラリのインストール

以下の例では、x86 版の Windows 2003 Server に SAP JCo ライブラリをインストールする方法について説明します。

1. sapjco-ntamd64-2.1.9.zip を一時ディレクトリに抽出します。
2. sapjcorfc.dll および librfc32.dll ファイルを Windows system32 ディレクトリにコピーします。

   注: メッセージが表示されたら、このディレクトリにある既存のファイルを上書きします。
3. sapjco.jar ファイルを Java Connector Server extlib ディレクトリにコピーします。このディレクトリは、以下の場所にあります。

   ```
   [set the Access Path variable]¥Connector Server¥extlib
   ```
4. CA Identity Manager - コネクタ サーバー サービスを再起動します。

   PUPM を使用して SAP R3 エンドポイント上の特権アカウントを管理できるようになりました。

詳細情報:

SAP R3 接続情報 (P. 227)

CA Identity Manager プロビジョニング接続情報

CA Identity Manager プロビジョニング コネクタを使用すると、プロビジョニング サーバで定義した CA Identity Manager エンドポイントを管理できます。PUPM 内で CA Identity Manager のエンドポイントを作成する前に、Identity Manager プロビジョニング タイプ コネクタ サーバを作成する必要があります。

注: コネクタ サーバの作成方法の詳細については、オンライン ヘルプを参照してください。

注: CA Identity Manager プロビジョニング コネクタ サーバの設定時に、etaadmin の完全識別名を指定します。

以下に例を示します。

```
eTGlobalUserName=etaadmin,eTGlobalUserContainerName=Global
Users,eTNamespaceName=CommonObjects,dc=ProvisioningDomainName,dc=eta
```

CA Identity Manager は、ターゲット システム上で設定されているパスワード ポリシーとは異なるパスワード ポリシーを強制できます。がターゲット システムに対してパスワード ポリシーを強制すると、PUPM はユーザ パスワードを変更します。ただし、ユーザはエンドポイント上で変更されたパスワードを使用することはできません。ターゲット システム上のパスワード ポリシーが PUPM のパスワード ポリシーに準拠していることを確認してください。CA Identity Manager パスワード ポリシー強制オプションの詳細については、「*CA Identity Manager 管理ガイド*」を参照してください。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

エンドポイント

CA Identity Manager プロビジョニング サーバで定義したとおりに、エンドポイント名前を定義します。

CA Access Control エンタープライズ管理 が CA Identity Manager エンドポイント タイプを表示するのは、ユーザがプロビジョニング サーバで接続設定を行った後のみです。

ホスト

エンドポイントのホスト名を定義します。これは、エンドポイントに割り当てる論理名です。CA Access Control エンタープライズ管理 は、ワールド ビュー内でのエンドポイントの表示にこの名前を使用します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

詳細情報:

PUPM 用の CA Identity Manager プロビジョニング マネージャの設定 (P. 230)

PUPM 用の CA Identity Manager プロビジョニング マネージャの設定

PUPM を使用して、プロビジョニング サーバで定義する CA Identity Manager r12.5 および r12.5 SP1 のエンドポイントの管理を開始する前に、PUPM 用の CA Identity Manager プロビジョニング マネージャを設定する必要があります。

PUPM 用の CA Identity Manager プロビジョニング マネージャの設定方法

1. CA Identity Manager プロビジョニング マネージャにログインします。
2. [システム]タブをクリックします。
3. 設定するドメインを選択し、左ペインにある[ドメイン設定]をクリックします。

   ドメイン設定ツリーが表示されます。
4. [パスワード]ツリーを展開し、[アカウント パスワードを強制的に同期]を選択します。

   [アカウント パスワードを強制的に同期]パラメータの[ドメイン設定]タブが表示されます。

5. ［編集］をクリックし、値を［いいえ］に変更して、［OK］をクリックします。
6. ［適用］をクリックします。

   ［アカウント パスワードを強制的に同期］パラメータの値が変更されます。
7. CA Identity Manager - プロビジョニング サーバおよび CA Identity Manager - コネクタ サーバ（Java）サービスを再開します。

   CA Identity Manager プロビジョニング マネージャが PUPM 用に設定されます。

CA Identity Manager プロビジョニング コネクタ検索制限の変更

特権アカウント検出ウィザードを実行する際に、CA Identity Manager プロビジョニング コネクタは CA Identity Manager 接続マネージャで設定したエンドポイントごとに最大 1000 件の結果を返します。 このデフォルト検索制限を変更すると、各クエリ内でより多くの結果を表示することができます。

CA Identity Manager プロビジョニング コネクタ検索制限の変更

1. エンタープライズ管理サーバで、Java コネクタ サーバを停止します。以下の*いずれか*の操作を実行します。

   a. Windows では、[サービス]ウィンドウを開き、[CA Identity Manager]-[Connector Server (Java) service]を選択し、[Stop]をクリックします。

   b. UNIX では、以下のディレクトリに移動します。ここで *ACServerInstallDir* はエンタープライズ管理サーバがインストールされているディレクトリを示します。

   ```
   ACServerInstallDir/Connector_Server/bin
   ```

   c. 以下のコマンドを実行します。

   ```
   ./im_jcs stop
   ```

   Java コネクタ サーバが停止します。

2. im_connector_conf.xml ファイルを開いて、編集します。このファイルは以下のディレクトリにあります。

   ```
   ACServerInstallDir/Connector_Server/conf/override/imdyn
   ```

3. トークン「I_SEARCH_SIZE_LIMIT」を見つけて、値として検索制限を指定します。以下に例を示します。

   ```
   <param name="I_SEARCH_SIZE_LIMIT" value="1500" />
   ```

4. ファイルを保存して閉じます。

5. Java コネクタ サーバを起動します。

重要: デフォルトより高い検索制限値を指定すると、システム パフォーマンスが低下する場合があります。

接続解除されたエンドポイント接続情報

接続解除されたエンドポイント タイプによって、接続解除されたエンドポイント上に存在する特権アカウントのパスワードを格納できます。

PUPM は、接続解除されたエンドポイント上のアカウントへのログイン、またはアカウントの管理を行いません。代わりに、PUPM は、エンドポイント上の特権アカウントのパスワード ボールトとしてのみ機能します。CA Access Control エンタープライズ管理 で、接続解除されたエンドポイント上の特権アカウントのパスワードを変更するたびに、管理対象エンドポイント上のアカウントを手動で変更する必要があります。

接続解除されたエンドポイント上で、接続解除されたアカウントのみを作成できます。接続解除されたアカウントは PUPM が管理しないアカウントです。たとえば、PUPM は、接続解除されたアカウントのパスワードを変更しません。さらに、特権アカウント検出ウィザードまたはサービス アカウント検出ウィザードを使用して、接続解除されたエンドポイント上のアカウントを検出できません。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ホスト名

エンドポイントのホスト名を定義します。

ログイン アプリケーションの作成

ログイン アプリケーションは、スクリプトを使用して、エンドポイント上でアプリケーションを実行します。このアプリケーションによって、ユーザが特権アカウント パスワードをチェックアウトした後に、ユーザを特権アカウントに自動的にログインさせます。ログイン アプリケーションによって、PUPM 自動ログインを設定できます。

以下のタイプのログイン アプリケーションを作成できます。各タイプのログイン アプリケーションは Visual Basic スクリプトです。

- ORACLE_10G_WEB.vbs -- Oracle 10g データベースの Enterprise Manager Web インターフェースに自動的にログインします。
- ORACLE_10XE_WEB.vbs -- Oracle XE データベースの Database Home Page Web インターフェースに自動的にログインします。
- ORACLE_11G_WEB.vbs -- Oracle 11g データベースの Enterprise Manager Web インターフェースに自動的にログインします。

- PUTTY.vbs -- SSH Device エンドポイントに自動的にログインします。

  注: PuTTY ログイン アプリケーションを使用するには、PuTTY Release 0.60 をコンピュータにインストールします。

- RDP.vbs -- Windows エンドポイントに自動的にログインします。

自動ログインを使用して Windows エージェントレス エンドポイント上で特権アカウント パスワードをチェックアウトする場合、CA Access Control エンタープライズ管理 はホストドメインを特権アカウント名の前に付けます。Windows エージェントレス エンドポイント用のログイン アプリケーションを作成する前に、以下を確認します。

- エンドポイントがワークグループの一部である場合は、コンピュータ名が[ホストドメイン]フィールドで指定されていることを確認します。
- エンドポイントがドメインの一部である場合は、ドメイン名が[ホストドメイン]フィールドで指定されていることを確認します。

  注: [エンドポイントの変更]タスクを使用して[ホストドメイン]フィールドを変更できます。

デフォルトでは、ログイン アプリケーションを作成するには「システム マネージャ」ロールが必要です。ログイン アプリケーションを使用できるのは、Microsoft Internet Explorer ブラウザ内のみです。

ログイン アプリケーションの作成方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[ログイン アプリケーション]-[ログイン アプリケーションの作成]タスクをクリックします。

   [ログイン アプリケーションの作成: ログイン アプリケーション検索]画面が表示されます。

2. (オプション)既存のアプリケーションを選択して、以下のようにして、ログイン アプリケーションをそのコピーとして作成できます。

   a. [ログイン アプリケーション 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ログイン アプリケーションのリストが表示されます。

   c. 新規ログイン アプリケーションのベースとして使用するオブジェクトを選択します。

3. [OK]をクリックします。

   [ログイン アプリケーションの作成]タスク ページが表示されます。アプリケーションを既存のオブジェクトから作成している場合、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ロードされています。

4. 以下のフィールドに値を入力します。

   名前

   ユーザがこのアプリケーションを参照するために使用する名前を定義します。

   説明

   (オプション)ログイン アプリケーションに関して、記録する情報を定義します(書式自由)。

   スクリプト

   ログイン アプリケーションの起動に使用する Visual Basic スクリプトを定義します。

   注: 提供されているこれらのスクリプトはカスタマイズしないことをお勧めします。

   有効

   このログイン アプリケーションが有効であると指定します。

   [サブミット]をクリックします。

   CA Access Control エンタープライズ管理 はログイン アプリケーションを作成します。ユーザがログイン アプリケーションを使用できるようになるには、ログイン アプリケーションを使用するように CA Access Control エンタープライズ管理 内のエンドポイントを変更する必要があります。端末統合を使用し、Windows Server 2008 上でユーザ ログイン アプリケーションを使用するには、エンドポイント上で追加の設定手順を実行する必要があります。

詳細情報:

端末統合の設定 (P. 300)
ログイン アプリケーションを使用するための Windows Server 2008 エンドポイントの変更 (P. 215)

PUPM エンドポイントおよび特権アカウントのインポート方法

PUPM のエンドポイントおよび特権アカウント管理を自動化するには、PUPM フィーダを使用します。PUPM フィーダを使用すると、1 回の手順で多くの PUPM エンドポイントおよび特権アカウントを CA Access Control エンタープライズ管理 にインポートできます。また、PUPM フィーダを使用して、PUPM エンドポイントおよび特権アカウントの作成または変更を行うことができます。

注: PUPM フィーダを使用して PUPM エンドポイントおよび特権アカウントを削除することはできません。

重要: 処理中のエラーを回避するために、特権アカウント CSV ファイルをインポートする前に、エンドポイント CSV ファイルを PUPM にインポートしてください。

PUPM エンドポイントおよび特権アカウントを CA Access Control エンタープライズ管理 にインポートするには、以下の手順に従います。

1. フィーダのプロパティ ファイルを設定します。

   このフィーダのプロパティ ファイルによって、ポーリング間隔、およびポーリング フォルダ、処理済みファイルのフォルダ、およびエラー ファイルのフォルダの名前と場所を指定します。

2. (オプション) ポーリング フォルダ、処理済みファイル フォルダ、およびエラー ファイル フォルダへのアクセスを制限する CA Access Control ルールを書き込みます。

   これらのフォルダへのアクセスを制限することによって、不正なユーザがエンドポイントおよび特権アカウント CSV ファイル内の平文パスワードにアクセスするのを阻止します。

3. 以下のいずれか、または両方の手順を実行します。

   - エンドポイント CSV ファイルを作成します。
   - 特権アカウント CSV ファイルを作成します。

   CSV ファイルの各行は、PUPM エンドポイントまたは特権アカウントの作成または変更タスクを表わします。個別のエンドポイントおよび特権アカウント CSV ファイルを作成する必要があります。

   注: 別のアプリケーションで自動化プロセスを設定して、CSV ファイルを作成できます。

4. (オプション) ポーリング タスクを開始します。

   ポーリング タスクが開始されると、PUPM フィーダはポーリング フォルダにある CSV ファイルを CA Access Control エンタープライズ管理 にアップロードし、CA Access Control エンタープライズ管理 で CSV ファイルが処理されます。

   注: ポーリング タスクを手動で開始していない場合、PUPM フィーダはフィーダのプロパティ ファイルに指定された時間に、ポーリング フォルダ内にファイルがあるかどうか確認します。

5. CA Access Control エンタープライズ管理 による CSV ファイルの処理が完了したら、エラー ファイル フォルダ内の CSV ファイル フォルダに失敗タスクがないかどうか確認してください。

   このファイルは、失敗したタスク、および CA Access Control エンタープライズ管理 が処理できなかったタスクをリスト表示します。

6. ファイルのエラーを修正し、修正したファイルをポーリング フォルダに保存します。

7. ポーリング タスクを開始します。

8. PUPM エンドポイントおよび特権アカウントがすべてインポートされるまで、手順 5 から 7 までを繰り返します。

PUPM フィーダの動作の仕組み

PUPM フィーダを使用することにより、多くの PUPM エンドポイントまたは特権アカウントを一度に作成または変更できます。PUPM フィーダの動作の仕組みを理解することは、ユーザの企業において PUPM をもっとも最適な状態に設定し、発生する可能性のある問題のトラブルシューティングを行う際に役立ちます。

以下のプロセスでは、PUPM フィーダの動作の仕組みについて説明します。

1. ユーザまたは自動プロセスによって、1 つ以上の CSV ファイルが作成され、ポーリング フォルダに保存されます。

   CSV ファイルの各行は、PUPM エンドポイントまたは特権アカウントの作成または変更タスクを表わします。エンドポイント用と特権アカウント用に、別々の CSV ファイルを作成します。

2. ポーリング タスクが開始されると、PUPM フィーダはポーリング フォルダにある CSV ファイルを CA Access Control エンタープライズ管理 にアップロードします。指定された時間に実行されるように、ポーリング タスクを設定できます。また、ポーリング タスクを手動で開始することもできます。

   注: PUPM フィーダがファイル名を変更できない場合、ファイルを処理できません。未処理の CSV ファイルはポーリング フォルダ内に残ります。

3. CA Access Control エンタープライズ管理 は CSV ファイルの名前を「*original_timestamp*.csv」に変更し、処理済みファイル フォルダに移動します。

   注: *original* は元の CSV ファイルの名前で、*timestamp* はファイルの処理時間を示すタイムスタンプです。たとえば、元の CSV ファイルの名前「endpoints.csv」の場合、CA Access Control エンタープライズ管理 は処理済みファイル フォルダ内のファイルに「endpoints_091209130256.csv」という名前を付けます。

4. CA Access Control エンタープライズ管理 は、CSV ファイルの各行を順番に処理します。CSV ファイルの各行で、以下のイベントが発生します。

   - CA Access Control エンタープライズ管理 がタスクを完了できる場合、CA Access Control エンタープライズ管理 は、
     - そのタスクを完了します。たとえば、エンドポイントを作成します。
     - そのタスク用の監査レコードを作成します。

- CA Access Control エンタープライズ管理 がタスクを完了できない場合、CA Access Control エンタープライズ管理 は、
  - CSV ファイルのその行をエラー ファイル フォルダ内の CSV ファイルにコピーします。
  - 「FAILURE_REASON」という名前の列を、エラー ファイル フォルダ内の CSV ファイルにコピーします。
  - タスクが失敗した理由を「FAILURE_REASON」列に追加します。
  - そのタスク用の監査レコードを作成します。

エラー ファイル フォルダ内の CSV ファイルによって、失敗タスクを容易に確認することができます。このファイルの名前も「*original_timestamp*.csv」です。

注: 処理済みファイル フォルダ内の CSV ファイルにすべての処理済みタスクが一覧されますが、各タスクのステータスは指定されません。つまり、タスクが完了したか失敗したかは指定されません。

5. CA Access Control エンタープライズ管理 は、CSV ファイル内の各行で手順 4 を繰り返します。

フィーダのプロパティ ファイルの設定

このフィーダのプロパティ ファイルによって、ポーリング間隔、およびポーリング フォルダ、処理済みファイルのフォルダ、およびエラー ファイルのフォルダの名前と場所を指定します。JBoss は、起動するたびにフィーダのプロパティ ファイルを読み取ります。

フィーダのプロパティ ファイルの設定方法

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. テキスト エディタでフィーダのプロパティ ファイルを開きます。このファイルは、以下の場所にあります。ここで、「*JBoss_home*」は JBoss のインストール場所です。

   ```
   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/default/feeder.properties
   ```

3. 以下の*いずれか*のパラメータを有効にします。

   FOLDER_POLLING_INTERVAL_IN_MINUTES

   間隔を分単位で定義します。ここで指定した間隔で、PUPM フィーダはポーリング フォルダをポーリングします。このパラメータは、デフォルトで有効になっています。

   制限:1 ～ 60

   デフォルト: 60

   FOLDER_POLLING_CRON_EXPR

   PUPM フィーダがポーリング フォルダをポーリングする時間を指定します。このパラメータは、cron 式として指定します。

   重要: このパラメータを使用する場合は、FOLDER_POLLING_CRON_EXPR 行からコメント記号(#)を削除し、FOLDER_POLLING_INTERVAL_IN_MINUTES 行の先頭にコメント記号を追加して、このパラメータを無効にします。

   例: FOLDER_POLLING_CRON_EXPR=0 0 23 ? * MON-FRI

   この例では、PUPM フィーダが月曜日から金曜日まで午後 11 時にポーリング フォルダをポーリングするように指定しています。

   ポーリング間隔が設定されます。

4. (オプション)以下のパラメータを編集します。

   FOLDER_FOR_POLLING

   ポーリング フォルダの定義 -- PUPM フィーダが CSV ファイルがあるかどうかポーリングするフォルダ。

   デフォルト:
   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

   注: このフォルダは、エンタープライズ管理サーバ コンピュータ上に配置される必要があります。このフォルダの絶対ファイル パスを指定する必要があります。

FOLDER_FOR_PROCESSED_FILES

処理済みファイル フォルダの定義 -- PUPM フィーダが CSV ファイルを処理した後に、処理済みの CSV ファイルを移動するフォルダ。

デフォルト:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/processed

注: このフォルダは、エンタープライズ管理サーバ コンピュータ上に配置される必要があります。このフォルダの絶対ファイル パスを指定する必要があります。

FOLDER_FOR_ERROR_FILES

エラー ファイル フォルダの定義 -- PUPM フィーダが処理できない CSV ファイルを移動するフォルダ。

デフォルト:
JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/failedToSubmit

注: このフォルダは、エンタープライズ管理サーバ コンピュータ上に配置される必要があります。このフォルダの絶対ファイル パスを指定する必要があります。

ポーリング フォルダの名前が設定されます。

5. ファイルを保存して閉じます。

   フィーダのプロパティ ファイルが設定されます。

6. JBoss アプリケーション サーバを再起動します。

例: フィーダのプロパティ ファイル

以下の例では、ポーリング フォルダを 30 分間隔でポーリングするように PUPM フィーダを設定し、ポーリング フォルダ、処理済みファイル フォルダ、およびエラー ファイル フォルダの場所を定義します。

```
# feeder folder polling job configuration
# folder specified as FOLDER_FOR_POLLING will be checked every
FOLDER_POLLING_INTERVAL_IN_MINUTES minutes e.g. 60 equals every 1 hour (max value is
every hour)
FOLDER_POLLING_INTERVAL_IN_MINUTES=30
# if cron expression is supplied remark the FOLDER_POLLING_INTERVAL_IN_MINUTES key
# FOLDER_POLLING_CRON_EXPR=
FOLDER_FOR_POLLING=C:¥feeder¥waitingToBeProcessed
FOLDER_FOR_PROCESSED_FILES=C:¥feeder¥processed
FOLDER_FOR_ERROR_FILES=C:¥feeder¥failedToSubmit
```

エンドポイント CSV ファイルの作成

エンドポイント CSV ファイル内の各行について、ヘッダ行の次にある行は CA Access Control エンタープライズ管理 でエンドポイントの作成や変更を行うタスクを表します。

重要: CSV ファイルを作成する際に、他にそのファイルを使用するアプリケーションがないこと、およびファイル名が変更できることを確認します。PUPM フィーダは、名前を変更できる CSV ファイルのみを処理します。

以下の手順に従います。

1. CSV ファイルを作成して、適切な名前を付けます。

   注: エンドポイント CSV ファイルのサンプルのコピーを作成することをお勧めします。サンプル ファイルは以下のディレクトリにあります。この *ACServer* はエンタープライズ管理サーバをインストールしたディレクトリです。

   ACServer/IAM Suite/Access Control/tools/samples/feeder

2. エンドポイント属性の名前を指定するヘッダ行を作成します。

   エンドポイント属性の名前は以下のとおりです。いくつかのエンドポイント属性は、特定のエンドポイント タイプにのみ有効です。

   OBJECT_TYPE

   インポートするオブジェクトのタイプを指定します。

   値: ENDPOINT

   ACTION_TYPE

   実行するアクションのタイプを指定します

   値: CREATE、MODIFY、DELETE

   %FRIENDLY_NAME%

   CA Access Control エンタープライズ管理 内でこのエンドポイントを参照するために使用する名前を定義します。

   DESCRIPTION

   このエンドポイント用に記録する情報を定義します。

ENDPOINT_TYPE

エンドポイントのタイプを指定します。

注: 利用可能なエンドポイント タイプを CA Access Control エンタープライズ管理 に表示できます。CA Identity Manager プロビジョニング タイプのエンドポイントを作成する場合は、CA Access Control エンタープライズ管理 内に Identity Manager プロビジョニング タイプのコネクタ サーバを作成しておきます。

HOST

エンドポイントのホスト名を定義します。

LOGIN_USER

エンドポイントの管理ユーザの名前を定義します。この属性は、CA Identity Manager プロビジョニング エンドポイント タイプに対しては有効では*ありません*。ただし、その他のすべてのエンドポイント タイプに対して有効です。

SSH Device 以外のすべての有効なエンドポイント タイプ:

- 特権管理アカウント(IS_ADVANCE 属性)を指定しない場合、PUPM では LOGIN_USER を使用してエンドポイントに接続され、エンドポイントに対する管理タスク(たとえば、アカウントの検出やパスワードの変更)が実行されます。
- 特権管理アカウントを指定する場合、PUPM では LOGIN_USER のすべての値が無視されます。

SSH Device エンドポイント:

- 操作管理者(OPERATION_ADMIN_USER_NAME)および特権管理アカウントを指定しない場合、PUPM では LOGIN_USER を使用してエンドポイントに接続され、エンドポイントに対する管理タスクが実行されます。
- 操作管理者を指定する場合、PUPM では LOGIN_USER を使用してエンドポイントに接続され、操作管理者を使用してエンドポイントに対する管理タスクが実行されます。
- 特権管理アカウントを指定する場合、PUPM では LOGIN_USER のすべての値が無視されます。

PASSWORD

LOGIN_USER のパスワードを定義します。この属性は CA Identity Manager プロビジョニング エンドポイント タイプ対しては有効では*ありません*。ただし、その他のすべてのエンドポイント タイプ対しては有効です。

URL

エンドポイントに接続するために CA Access Control エンタープライズ管理 が使用する URL を定義します。この属性は、MS SQL Server および Oracle Server のエンドポイント タイプに有効です。

形式: (MS SQL Server) jdbc:sqlserver://*servername*:*port*

形式: (Oracle Server) jdbc:oracle:*drivertype*:@*hostname*:*port*:*service*

DOMAIN

このエンドポイントがメンバであるドメインの名前を指定します。この属性は Access Control for PUPM および Windows エージェントレス エンドポイント タイプに有効です。

IS_ACTIVE_DIRECTORY

ユーザ アカウントが Active Directory アカウントかどうかを指定します。この属性は Windows エージェントレス エンドポイント タイプのみに有効です。

制限: TRUE、FALSE

USER_DOMAIN

LOGIN_USER がメンバであるドメインの名前を指定します。この属性は Windows エージェントレス エンドポイント タイプに有効です。

CONFIGURATION_FILE

定義する SSH Device XML 環境設定ファイルの名前を指定します。この属性は SSH Device エンドポイント タイプに有効です。

注: この属性の値を指定しない場合、CA Access Control エンタープライズ管理 は デフォルト設定ファイル（ssh_connector_conf.xml）ファイルを使用します。

OPERATION_ADMIN_USER_NAME

(オプション)エンドポイントの操作管理者ユーザの名前を定義します。PUPM は、このアカウントを使用してエンドポイントに対する管理タスクを実行します。たとえば、特権アカウントのパスワードを検出し、変更します。この属性は、以下のように、SSH Device エンドポイント タイプに有効です。

- 特権管理アカウント(IS_ADVANCE 属性)および操作管理者を指定する場合、PUPM では特権管理アカウントを使用してエンドポイントに接続され、操作管理者を使用してエンドポイントに対する管理タスクが実行されます。
- LOGIN_USER および操作管理者アカウントを指定する場合、PUPM では LOGIN_USER を使用してエンドポイントに接続され、操作管理者を使用してエンドポイントに対する管理タスクが実行されます。

Check Point ファイアウォールを使用する SSH エンドポイントに対して操作管理者を指定する場合、エキスパート ユーザを指定する必要があります。ただし、PUPM を使用してエンドポイント上のエキスパート アカウントのパスワードを変更することはできません。この制限は、エキスパート アカウントが PUPM 内の接続解除されたアカウントである必要があることを意味します。

OPERATION_ADMIN_USER_PASSWORD

(オプション)エンドポイントの操作管理者ユーザのパスワードを定義します。この属性は SSH Device エンドポイント タイプに有効です。

ENDPOINT

CA Identity Manager のプロビジョニング サーバで定義したとおりに、エンドポイント名を定義します。この属性は CA Identity Manager プロビジョニング エンドポイント タイプに有効です。

IS_ADVANCE

(オプション)エンドポイントに接続し、エンドポイントに対する管理タスク(たとえば、アカウントの検出やパスワードの変更)を実行するのに、特権管理アカウントを使用するかどうかを指定します。この属性はすべてのエンドポイント タイプに有効です。

SSH Device 以外のすべての有効なエンドポイント タイプに対し、特権管理アカウント(IS_ADVANCE は TRUE)を指定する場合、PUPM では特権管理のアカウントを使用してエンドポイントに接続され、エンドポイントに対する管理タスクが実行されます。

SSH Device エンドポイント:

- 特権管理アカウントおよび操作管理者（OPERATION_ADMIN_USER_NAME）を指定する場合、PUPM では特権管理アカウントを使用してエンドポイントに接続され、操作管理者を使用してエンドポイントに対する管理タスクが実行されます。
- 特権管理アカウントのみを指定する場合、PUPM では特権管理アカウントを使用して、エンドポイントに接続され、エンドポイントに対する管理タスクが実行されます。

制限: TRUE、FALSE

注: この属性の値を TRUE に設定した場合は、LOGIN_USER には値を指定しません。ただし、PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE、PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME、PROPERTY_ADMIN_ACCOUNT_CONTAINER、および PROPERTY_ADMIN_ACCOUNT_NAME は指定する必要があります。

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_TYPE

（オプション）特権管理アカウントが定義されるエンドポイントのタイプを定義します。

注: 特権管理アカウントを使用するには、IS_ADVANCE を TRUE に指定する必要があります。

PROPERTY_ADMIN_ACCOUNT_ENDPOINT_NAME

（オプション）特権管理アカウントが定義されるエンドポイントの名前を定義します。エンドポイントは CA Access Control エンタープライズ管理 内に存在する必要があります。

注: 特権管理アカウントを使用するには、IS_ADVANCE を TRUE に指定する必要があります。

PROPERTY_ADMIN_ACCOUNT_CONTAINER

（オプション）特権管理アカウントが定義されるコンテナを定義します。コンテナは、そのインスタンスが他のオブジェクトの集合であるクラスです。

値:（Windows エージェントレスおよび Oracle Server）: Accounts

（SSH Device）: SSH Accounts

（MS SQL Server）: MS SQL Logins

注: 特権管理アカウントを使用するには、IS_ADVANCE を TRUE に指定する必要があります。

PROPERTY_ADMIN_ACCOUNT_NAME

(オプション) PUPM によりエンドポイントに対する管理タスク(たとえば、アカウントの検出やパスワードの変更)の実行に使用される特権管理アカウントの名前を定義します。特権アカウントは CA Access Control エンタープライズ管理 内に存在する必要があります。

注: 特権管理アカウントを使用するには、IS_ADVANCE を TRUE に指定する必要があります。

LOGIN_APPLICATION

エンドポイントと関連付けるログイン アプリケーションの名前を指定します。

OWNER_INFO

エンドポイントの所有者を指定します。

DEPARTMENT_INFO

部門の名前を指定します。

CUSTOM1....5_INFO

カスタマ固有の属性を 5 つまで指定します。

3. エンドポイント タスクの行を CSV ファイルに追加します。

   各行はエンドポイントを作成または変更するタスクを表します。また、ヘッダと同じ属性が必要です。この属性はヘッダと同じ順にする必要があります。行に属性の値がない場合は、フィールドを空にしておきます。

4. ファイルをポーリング フォルダに保存します。

   エンドポイント CSV ファイルは、PUPM フィーダにより処理される準備が完了しています。

   注: デフォルトのポーリング フォルダは以下の場所にあります。この *JBoss_home* は JBOSS をインストールしたディレクトリです。

   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waitingToBeProcessed

例: エンドポイント CSV ファイル

以下は、エンドポイント CSV ファイルのサンプルです。それ以外のサンプル エンドポイント CSV ファイルは、*ACServer*/IAM Suite/Access Control/tools/samples/feeder directory にあります。

```
OBJECT_TYPE,%FRIENDLY_NAME%,DESCRIPTION,ENDPOINT_TYPE,HOST,LOGIN_USER,
PASSWORD,URL,CONFIGURATION_FILE,DOMAIN,IS_ACTIVE_DIRECTORY,USER_DOMAIN,ENDPOINT

ENDPOINT,Oracle1,oracle 10g,Oracle Server,TEST10,
ORAADMIN1,ORAADMIN1,jdbc:oracle:thin:@TEST10:1521:RNDSRV,,,,,

ENDPOINT,local MSSQL1,local SQL server,MS SQL Server,
localhost,testAdmin,Password1@,jdbc:sqlserver://localhost:1433,,,,,

ENDPOINT,SSH_Device2,unix machine,SSH Device,TEST84,root,Password1@,,,,,,

ENDPOINT,IM_Access Control,Access Control via provisioning,Access
Control,TEST1,,,,,,,,TEST1
```

詳細情報:

SSH Device XML 構成ファイルのタイプ (P. 222)
カスタマイズした SSH Device エンドポイントを作成する方法 (P. 221)

特権アカウント CSV ファイルの作成

特権アカウント CSV ファイルにおける各行では、ヘッダ行の後で、CA Access Control エンタープライズ管理 で特権アカウントの作成や変更を行うタスクを表します。

重要: CSV ファイルを作成する際に、他にそのファイルを使用するアプリケーションがないこと、およびファイル名が変更できることを確認します。PUPM フィーダは、名前を変更できる CSV ファイルのみを処理します。

以下の手順に従います。

1. CSV ファイルを作成して、適切な名前を付けます。

   注: エンドポイント CSV ファイルのサンプルのコピーを作成することをお勧めします。サンプル ファイルは以下の場所にあります。このパスの *ACServer* はエンタープライズ管理サーバをインストールしたディレクトリです。

   ACServer/IAMSuite/AccessControl/tools/samples/feeder

2. 特権アカウント属性の名前を指定するヘッダ行を作成します。

   特権アカウント属性の名前は以下のとおりです。

   OBJECT_TYPE

   インポートするオブジェクトのタイプを指定します。

   値: ACCOUNT_PASSWORD

   ACTION_TYPE

   実行するアクションのタイプを指定します

   値: CREATE、MODIFY、DELETE

   ACCOUNT_NAME

   CA Access Control エンタープライズ管理 上の特権アカウントを表わす名前を指定します。

   注: RACF、ACF、Top Secret、SSH Device などのエンドポイント タイプのメインフレーム システムでは、大文字と小文字を区別してユーザ名を使用します。これらのエンドポイント タイプには、大文字と小文字が正しいアカウント名を入力します。メインフレーム システムおよび Oracle Server 上のエンドポイント上の特権アカウントには、アカウント名を大文字で入力します。

   ENDPOINT_NAME

   特権アカウントが存在するエンドポイントの名前を定義します。エンドポイントで任意の特権アカウントを作成できるようにするには、CA Access Control エンタープライズ管理 でエンドポイントを定義する必要があります。

   NAMESPACE

   エンドポイントのエンドポイント タイプを指定します。

   注: 利用可能なエンドポイント タイプを CA Access Control エンタープライズ管理 に表示できます。CA Identity Manager プロビジョニング タイプのエンドポイントを作成する前に、CA Access Control エンタープライズ管理 内に Identity Manager プロビジョニング タイプのコネクタ サーバ を作成する必要があります。

CONTAINER

特権アカウント用のコンテナの名前を指定します。コンテナは、そのインスタンスが他のオブジェクトの集合であるクラスです。コンテナは、特定のアクセス ルールに従って、整理された方法でオブジェクトを格納するために使用されます。

値:（Windows エージェントレスおよび Oracle Server のエンドポイント）: Accounts

（SSH Device エンドポイント）: SSH Accounts

（MS SQL Server エンドポイント）MS SQL Logins

DISCONNECTED_SYSTEM

特権アカウントを接続解除システムから実行するどうかを指定します。

TRUE を指定すると、PUPM はアカウントを管理しません。代わりに、PUPM は、接続解除システムの特権アカウントのパスワード ボールトとしてのみ機能します。PUPM でパスワードを変更するたびに、管理対象エンドポイント上のアカウントのパスワードも手動で変更されます。

値; TRUE、FALSE

EXCLUSIVE_ACCOUNT

単一ユーザのみがいつでもアカウントをチェックアウトできるかどうかを指定します。

TRUE を指定すると、PUPM では単一ユーザのみがいつでもアカウントをチェックアウトできます。

値: TRUE、FALSE

NEW_PASSWORD

特権アカウントのパスワードを定義します。この属性の値を指定しない場合、CA Access Control エンタープライズ管理 は指定したパスワード ポリシーに準拠したパスワードを生成します。

注: パスワードは指定したパスワード ポリシーに準拠している必要があります。

PASSWORD_POLICY

特権アカウントのパスワード ポリシーを指定します。

注: 存在しないパスワード ポリシーを指定するとタスクが失敗します。また、CA Access Control エンタープライズ管理 によって特権アカウントが作成されません。

OWNER_INFO

アカウント所有者の名前を指定します。

DEPARTMENT_INFO

部門の名前を指定します。

CUSTOM1....5_INFO

カスタマ固有の属性を 5 つまで指定します。

3. タスクの行を CSV ファイルに追加します。

   各行は特権アカウントを作成または変更するタスクを表します。また、ヘッダと同じ数の属性値が必要です。行に属性の値がない場合は、フィールドを空にしておきます。

4. ファイルをポーリング フォルダに保存します。

   特権アカウント CSV ファイルは、PUPM フィーダによってインポートされる準備が完了しています。

   注: デフォルトのポーリング フォルダは以下の場所にあります。この *JBoss_home* は JBOSS をインストールしたディレクトリです。

   ```
   JBoss_home/server/default/deploy/IdentityMinder.ear/custom/ppm/feeder/waiting
   ToBeProcessed
   ```

例: 特権アカウント CSV ファイル

以下は、特権アカウント CSV ファイルのサンプルです。*ACServer*/IAMSuite/AccessControl/tools/samples/Feeder ディレクトリに複数の特権ファイルのサンプルがあります。

```
OBJECT_TYPE,ACCOUNT_NAME,ENDPOINT_NAME,NAMESPACE,CONTAINER,
DISCONNECTED_SYSTEM,EXCLUSIVE_ACCOUNT,NEW_PASSWORD,PASSWORD_POLICY

ACCOUNT_PASSWORD,demo1,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,Password1@,default password policy

ACCOUNT_PASSWORD,demo2,local windows 2003,Windows Agentless,
Accounts,FALSE,FALSE,,default password policy

ACCOUNT_PASSWORD,disconnected1,local windows 2003,Windows Agentless,
Accounts,TRUE,FALSE,Password1@,default password policy
```

手動でのポーリング タスクの開始

ポーリング タスクが開始されると、PUPM フィーダはポーリング フォルダにある CSV ファイルをアップロードします。 CA Access Control エンタープライズ管理 は、次に CSV ファイル内の各行を処理します。

注: ポーリング タスクを手動で開始していない場合、PUPM フィーダは、フィーダのプロパティ ファイルで指定された時間にポーリング フォルダを確認します。ポーリング タスクを開始するには、システム マネージャまたは PUPM ターゲット システム マネージャのロールを持っている必要があります。

手動でのポーリング タスクの開始方法

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. [特権アカウント]をクリックします。
   b. [アカウント]サブタブをクリックします。

      [フィーダ フォルダのポーリング]タスクが使用可能なタスク リストに表示されます。
2. [フィーダ フォルダのポーリング]をクリックします。

   [フィーダ フォルダのポーリング]画面が表示されます。
3. [サブミット]をクリックします。

   PUPM フィーダは、ポーリング フォルダにある CSV ファイルをポーリングします。

パスワード コンシューマのセットアップ方法

パスワード コンシューマは、アプリケーション、Windows サービス、および Windows スケジュール タスクです。特権アカウントおよびサービス アカウントを使用したスクリプトの実行、データベースへの接続、または Windows サービス、スケジュール済みタスク、または RunAS コマンドの管理を行います。パスワード コンシューマによって、ハードコードされたパスワードをアプリケーション スクリプトから削除し、サーバ アカウントにパスワード ポリシーを強制的に適用します。

パスワード コンシューマには 2 つのグループがあります。

- オン デマンドでパスワードを取得するパスワード コンシューマ -- データベース、Windows 実行ユーザ、Software Development Kit
- パスワード変更時にパスワードを取得するパスワード コンシューマ -- Windows スケジュール タスク、Windows サービス

Software Development Kit パスワード コンシューマは特権アカウント パスワードを取得、チェックアウト、およびチェックインします。他のすべてのタイプのパスワード コンシューマは特権アカウント パスワードを取得しますが、パスワードをチェックアウトまたはチェックインしません。

以下のプロセスでは、パスワード コンシューマをセットアップするために組織内のユーザが完了する必要があるタスクについて説明します。各プロセス手順を完了するには、指定されたロールが必要です。システム マネージャ管理ロールが割り当てられているユーザは、このプロセスのすべての CA Access Control エンタープライズ管理 タスクを実行できます。

パスワード コンシューマをセットアップするには、以下の手順に従います。

1. システム管理者は、以下のようにエンドポイントを設定します。

   a. CA Access Control を、データベース、Windows 実行ユーザ、および Software Development Kit パスワード コンシューマを使用するエンドポイントにインストールします。

      システム管理者は、インストール処理中に PUPM の統合機能を有効にできます。

      注: Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを使用するのに、CA Access Control をエンドポイントにインストールする必要はありません。

   b. 以下のパスワード コンシューマを使用するエンドポイント上で、追加の設定手順を実行します。

      - データベース(JDBC) -- データベース(JDBC)パスワード コンシューマを使用するために、エンドポイントを準備します (P. 282)。
      - データベース(ODBC、OLEDB、OCI) -- データベース(ODBC、OLEDB、OCI)パスワード コンシューマを使用するために、エンドポイントを設定します (P. 289)。
      - データベース(.NET) -- データベース(.NET)パスワード コンシューマを使用するために、エンドポイントを設定します (P. 291)。
      - Software Development Kit (CLI) -- CLI パスワード コンシューマを使用するために、エンドポイントを設定します (P. 293)。
      - Software Development Kit (SDK) -- PUPM SDK を使用するために、エンドポイントを設定します (P. 296)。

   エンドポイントはパスワード コンシューマを使用するように設定されます。

2. PUPM ターゲット システム マネージャ ロールは、CA Access Control エンタープライズ管理 でパスワード ポリシーを作成します。パスワード ポリシーによって、特権およびサービス アカウント用のパスワード ルールおよびパスワード失効間隔を設定します。

3. PUPM ターゲット システム マネージャは、CA Access Control エンタープライズ管理 でエンドポイントを作成します。エンドポイントは、特権およびサービス アカウントによって管理されるデバイスです。CA Access Control エンタープライズ管理 でエンドポイントを作成するか、PUPM フィーダを使用して、エンドポイントをインポートできます。

   注: 特権アカウントのセットアップ時にすでにエンドポイントを作成している場合は、この手順を完了しません。

4. データベース、Windows 実行ユーザ、または Software Development Kit パスワード コンシューマを作成するには、以下の手順に従います。

   a. PUPM ターゲット システム マネージャは、CA Access Control エンタープライズ管理 内の特権アカウントを検出または作成します。

      このユーザは、CA Access Control エンタープライズ管理 内での特権アカウントを検出および作成、または PUPM フィーダを使用して特権アカウントをインポートできます。

   b. システム マネージャは、CA Access Control エンタープライズ管理 内で、データベース、Windows 実行ユーザおよび Software Development Kit パスワード コンシューマを作成します。

      システム マネージャは、パスワード コンシューマ 作成タスクの一部として、データベース、Windows 実行ユーザおよび Software Development Kit パスワード コンシューマを特権アカウントに関連付けます。

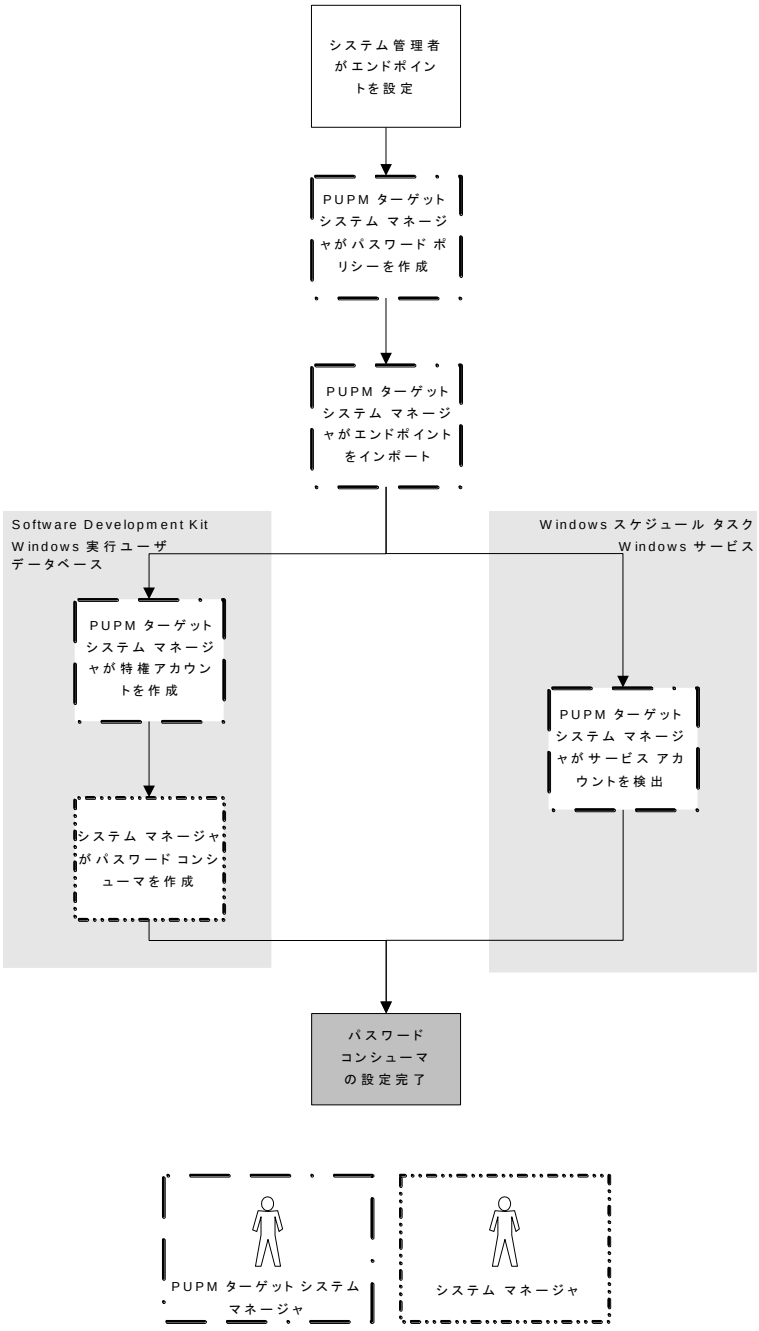
5. Windows スケジュール タスクまたは Windows パスワード コンシューマを作成するには、PUPM ターゲット システム マネージャがサービス アカウントを検出します。

   CA Access Control エンタープライズ管理 は、検出する各サービスおよびスケジュール済みタスクについて、パスワード コンシューマを作成します。

   注: CA Access Control エンタープライズ管理 は、ユーザがパスワード変更可能なアカウントによって実行されるサービスのみを検出します。たとえば、CA Access Control エンタープライズ管理 は、ユーザのコンピュータの Administrator アカウントまたはドメイン アカウントによって実行されるサービスを検出しますが、NT AUTHORITY¥Local Service アカウントによって実行されるサービスは検出しません。

   これで、ユーザの組織のパスワード コンシューマがセットアップされます。

以下の図に、各プロセス手順を実行する特権アクセス ロールを示します。



サービス アカウントの検出

*サービス アカウント*は、Windows サービスによって使用される内部アカウントです。これらのサービスは、オペレーティング システムの中核的およびその他の機能をコンピュータに提供します。CA Access Control エンタープライズ管理 からサービス アカウント パスワードを管理することによって、潜在的な攻撃からこれらのサービスを保護できます。

Windows エージェントレス エンドポイント上のサービスおよびスケジュール済みタスクを管理するサービス アカウントを検出できます。サービス アカウントの検出により、CA Access Control エンタープライズ管理 内に複数のサービス アカウントを同時に作成し、パスワード コンシューマをサービス アカウントに割り当てることができます。サービス アカウントのパスワード コンシューマを作成しない場合は、[特権またはサービス アカウントの作成]タスクを使用してサービス アカウントを作成します。

注: 特権アカウントを検出するには、特権アカウント検出ウィザードを使用します。

サービス アカウント検出ウィザードによってエンドポイント上のすべてのサービスが検出されるわけではありません。このウィザードによって検出されるのは、ユーザがパスワード変更可能なアカウントによって実行されているサービスのみです。たとえば、CA Access Control エンタープライズ管理 は、ユーザのコンピュータの Administrator アカウントまたはドメイン アカウントによって実行されるサービスを検出しますが、NT AUTHORITY¥Local Service アカウントによって実行されるサービスは検出しません。

サービス アカウントの検出方法

1. (オプション)ドメイン アカウントであるサービス アカウントを検出するには、アカウントが存在するドメイン コントローラ(DC)が CA Access Control エンタープライズ管理 内で、以下の属性で定義されていることを確認します。
   - エンドポイント タイプ -- Windows エージェントレス
   - Active Directory -- True
   - ホストドメイン -- DC がメンバであるドメイン名
   - ユーザ ドメイン -- DC 上で定義されたユーザがメンバであるドメイン名

     注: アカウントが存在するドメインとは異なるドメインから管理者アカウントを使用する場合にのみ、ユーザ ドメインを指定します。

   サービス アカウント検出ウィザードは、ドメイン アカウントであるサービス アカウントを検出できるようになりました。

2. CA Access Control エンタープライズ管理 で、[特権アカウント]-[アカウント]-[サービス アカウント検出ウィザード]をクリックします。

   [サービス アカウント検出ウィザード]ウィンドウが表示されます。

   注: [エンドポイント タイプ]フィールドの値は、「Windows Agentless」です。これは、PUPM が Windows Agentless エンドポイント上でのみサービス アカウントを管理するためです。

3. 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サービス アカウントのリスト、そのサービス アカウントを使用する Windows サービスおよびスケジュール済みタスクのリストが表示されます。ウィザード検出したアカウントのドメインが不明な場合、警告メッセージが表示されます。

   注: このプロセスは完了するまで、ある程度の時間がかかる場合があります。サービスおよびスケジュール済みタスクは、[パスワード コンシューマ]列にリスト表示されます。この列のアイコンによって、どのパスワード コンシューマがサービスであり、どのパスワード コンシューマがスケジュール済みタスクであるかが一目で分かります。

4. パスワード コンシューマを使用して管理するサービスおよびスケジュール済みタスクを選択し、[次へ]をクリックします。

   [一般アカウント プロパティ]ウィンドウが表示されます。

5. サービスおよびスケジュール済みタスクに割り当てるパスワード ポリシーを選択し、[次へ]をクリックします。

   [サマリ]ウィンドウが表示されます。

6. サマリを確認してから、[完了]をクリックします。

   エラーがない場合、CA Access Control エンタープライズ管理 はタスクをサブミットし、サービス アカウントを追加します。CA Access Control エンタープライズ管理 は、サービス アカウントを追加した後に、ユーザが選択した各サービスおよびスケジュール済みタスクについてパスワード コンシューマを自動的に作成します。パスワード コンシューマを表示および変更するために、適切なパスワード コンシューマ タスクを使用できます。

詳細情報:

特権またはサービス アカウントの作成 (P. 187)
特権アカウントの検出 (P. 184)

パスワード コンシューマの作成

パスワード コンシューマは、アプリケーション、Windows サービス、および Windows スケジュール タスクです。特権アカウントおよびサービス アカウントを使用したスクリプトの実行、データベースへの接続、または Windows サービス、スケジュール済みタスク、または RunAS コマンドの管理を行います。

パスワード コンシューマには 2 つのグループがあります。

- オンデマンドでパスワードを取得するパスワード コンシューマ -- Software Development Kit、データベース、Windows 実行ユーザ

  注: オンデマンドでパスワードを取得するパスワード コンシューマを使用するには、PUPM 統合機能を有効にした PUPM エンドポイント上に CA Access Control をインストールする必要があります。

- パスワード変更時にパスワードを取得するパスワード コンシューマ -- Windows スケジュール タスク、Windows サービス

各グループからパスワード コンシューマを作成するには、異なる情報を提供します。デフォルトでは、パスワード コンシューマを作成するには、「システム マネージャ」ロールが必要です。

注: Software Development Kit、データベース、および Windows 実行ユーザ タイプのパスワード コンシューマを作成する場合は、このタスクを完了します。サービス アカウント検出ウィザードを使用して、Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成することをお勧めします。

パスワード コンシューマの作成方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[パスワード コンシューマ]-[パスワード コンシューマの作成]をクリックします。

   [パスワード コンシューマの作成: パスワード コンシューマ検索]画面ページが表示されます。

2. (オプション)既存のパスワード コンシューマを選択して、以下のようにして、そのコピーとしてパスワード コンシューマを作成します。

   a. [パスワード コンシューマ 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パスワード コンシューマのリストが表示されます。

   c. 新規パスワード コンシューマのベースとして使用するオブジェクトを選択します。

3. [OK]をクリックします。

   [パスワード コンシューマの作成]タスク ページが表示されます。パスワード コンシューマ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ロードされています。

4. [全般]タブで以下のフィールドに入力します。

   名前

   このパスワード コンシューマの参照に使用する名前を定義します。

   説明

   (オプション)パスワード コンシューマに関して、記録する情報を定義します(書式自由)。

   コンシューマ タイプ

   パスワード コンシューマのタイプを指定します。

アプリケーション パス

(Software Development Kit、データベース、Windows 実行ユーザ、Windows スケジュール タスク) エンドポイント上のパスワード コンシューマの完全パス名を定義します。

- Software Development Kit パスワード コンシューマについては、パスワード リクエストを実行するアプリケーションのパス名を指定します。
- データベース パスワード コンシューマについては、データベースに接続するアプリケーションのパス名を指定します。
- Windows 実行ユーザ パスワード コンシューマについては、ユーザが実行するアプリケーションのパス名を指定します。
- Windows スケジュール タスク パスワード コンシューマについては、スケジュール タスクのパス名を指定します。

注: パラメータで、ワイルドカード (*) および CA Access Control 変数を使用します。たとえば、「<!AC_ROOT_PATH>¥bin¥acpwd.exe」のようになります。

サービス名

(Windows サービス) Windows サービスのパス名を定義します。[Windows サービス] プロパティ ページに表示される通りに、パス名を正確に指定します。

有効

パスワード コンシューマの有効化、つまり、PUPM がこのコンシューマからのリクエストを受け取るか、このコンシューマにパスワードの変更を強制するように指定します。

ステータス

(Windows スケジュール タスクまたは Windows サービス) 前回のパスワード変更が成功したか失敗したかを示します。

最終同期日

(Windows スケジュール タスクまたは Windows サービス) 前回の成功したパスワード同期を表示します。

再起動

(Windows サービス) パスワード変更後に、Windows サービスを再起動するかどうかを指定します。

5. [特権アカウント]タブをクリックして、パスワード コンシューマに関連付けられている特権アカウントを指定します。

   Software Development Kit、データベースまたは Windows 実行ユーザ パスワード コンシューマを作成する場合、パスワード コンシューマは指定する特権アカウントのパスワードを取得できます。

   Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成する場合、これらの特権アカウントのパスワード変更時に、PUPM はパスワード コンシューマのパスワード変更を強要します。

6. パスワード コンシューマを使用できるエンティティを指定します。以下の*いずれか*の操作を実行します。

   - Software Development Kit、データベースまたは Windows 実行ユーザ パスワード コンシューマを作成するには、以下の手順に従います。

     a. [ホスト]タブをクリックしてパスワード コンシューマが特権アカウント パスワードを取得可能なホストまたはホスト グループを指定するか、[すべてのホスト]を選択してすべてのホストまたはホスト グループに特権アカウント パスワードへのアクセスを許可します。

        注: [名前]フィールドにホストまたはホスト グループ名を入力するか、「...」をクリックして CA Access Control ホストまたはホスト グループ (HNODE または GHNODE オブジェクト) を検索します。

     b. [ユーザ]タブをクリックして特権アカウント パスワードをリクエストできるユーザまたはユーザ グループを指定するか、[すべてのユーザ]を選択して各ユーザが特権アカウント パスワードを要求することを許可します。

        ユーザまたはグループの名前をエンドポイントに表示されているように指定します。たとえば、「DOMAIN¥user1」のように指定します。CA Access Control エンタープライズ管理 ユーザまたはグループは指定しません。

   - Windows スケジュール タスクまたは Windows サービス パスワード コンシューマを作成するには、[エンドポイント]タブをクリックし、パスワード コンシューマを作成するエンドポイントを指定します。

7. [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 によってパスワード コンシューマが作成されます。

詳細情報:

パスワード コンシューマのタイプ (P. 145)

パスワード コンシューマの例: Windows 実行ユーザ

Windows 実行ユーザ アプリケーションを使用すると、特定のタスクを実行するために特権アカウントから権限を借用することができます。 RunAs を実行する際に、PUPM Agent により RunAs アプリケーションに特権アカウント パスワードが直接供給されるように、Windows 実行ユーザ パスワード コンシューマを作成できます。 Windows 実行ユーザ パスワード コンシューマにより、管理タスクを実行する場合に特権アカウント パスワードを知る必要がなくなります。

Windows 実行ユーザ パスワード コンシューマは、Windows エージェントレス エンドポイント上でのみ作成できます。

以下の例では、バックアップ タスクは週単位で実行されるようにスケジュールされています。このタスクは C:¥backup¥backup.exe にあり、Administrator によって実行されます。スケジュールされたバックアップが失敗する場合、システム管理者 Steve はユーザ John にバックアップを手動で開始させたいと考える場合があります。Steve は、Windows 実行ユーザ パスワード コンシューマを使用して、John に Administrator パスワードなしでバックアップ タスクを開始させることができます。

以下のプロセスでは、win123_PUPM という名前のエンドポイント上で Windows 実行ユーザ パスワード コンシューマを作成および使用するために、Steve と John が実行する手順について説明します。

1. Steve は、PUPM 統合機能を有効にして、CA Access Control を win123_PUPM にインストールします。
2. スティーブは 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. win123_PUPM という名前の Windows エージェントレス エンドポイントを作成します。
   b. win123_PUPM エンドポイントで管理者特権アカウントを検索します。

c. 以下のパラメータを使用して、Windows 実行ユーザ パスワード コンシューマを作成します。

- 名前 -- win123_PUPM Backup RunAs
- コンシューマ タイプ -- Windows 実行ユーザ
- アプリケーション パス -- C:¥backup¥backup.exe
- アカウント -- 管理者
- ホスト -- win123_PUPM
- ユーザ -- Domain1¥John

  注: Steve は John のユーザ名を、エンドポイントで表示されるとおりに入力します。

Windows Run As パスワード コンシューマが作成されます。

3. スケジュールされたバックアップ タスクが失敗すると、John は win123_PUPM にログオンして、手動でバックアップを開始します。John は、以下のパラメータを使用して、バックアップ タスクを開始する RunAs コマンドを実行します。

- アカウント -- 管理者
- パスワード -- なし

  注: PUPM Agent では、ジョンがパスワードに指定するすべての値が無視されます。

PUPM Agent では、John による前回のバックアップ タスク開始の要求がキャッシュで確認されます。ジョンによるこの要求は初めてのものだったので、要求はキャッシュされていません。PUPM Agent では、CA Access Control エンタープライズ管理 から特権アカウント パスワードが取得され、これが RunAs アプリケーションに提供されます。バックアップ タスクが開始します。

パスワード コンシューマの例: Windows スケジュール タスク

Windows スケジュール タスクおよび Windows サービス パスワード コンシューマは、サービス アカウント用のパスワードの変更の自動化に役立ちます。 サービス アカウントは Windows サービスによって使用される内部アカウントです。たとえば、ソフトウェアの更新を定期的にチェックするスケジュール タスクを設定する場合、スケジュール タスクではサービス アカウントを使用してエンドポイントにログインし、タスクが実行されます。

Windows スケジュール タスクと Windows サービスのパスワード コンシューマは、Windows エージェントレス エンドポイント上でのみ作成できます。Windows サービスと Windows スケジュール タスク パスワード コンシューマを使用するために、エンドポイントに CA Access Control をインストールする必要はありません。

パスワードを変更できるアカウントにより実行されるサービスに対してのみ、Windows サービス パスワード コンシューマを作成できます。たとえば、コンピュータの管理者アカウントにより実行されるサービスに対してはパスワード コンシューマを作成できますが、NT AUTHORITY¥Local Service アカウントにより実行されるサービスに対してパスワード コンシューマを作成することはできません。

以下に、システム管理者のスティーブが、win456 という名前の Windows エンドポイント上のソフトウェア更新を確認するスケジュール タスクに対するパスワード コンシューマを作成する例を示します。スケジュール タスクでは、win456¥ServiceAdmin アカウントを使用してエンドポイントにログインされます。

スティーブは 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。

1. スティーブは、30days という名前のパスワード ポリシーを作成します。このパスワード ポリシーにより、CA Access Control エンタープライズ管理 がサービス アカウントのパスワードを 30 日ごとに変更すること、パスワードは日曜日の午前 1 時から午前 3 時の間しか変更できないことが指定されています。
2. スティーブは、win456 という名前の Windows エージェントレス エンドポイントを作成します。
3. スティーブは、サービス アカウント検出ウィザードを使用して win456 エンドポイント上の win456¥ServiceAdmin アカウントを検出し、30days パスワード ポリシーをサービス アカウントに適用します。

4. CA Access Control エンタープライズ管理 により、以下のパラメータを使用して Windows スケジュール タスク パスワード コンシューマが作成されます。
   - 名前 -- win456 の UpdateTask（C:¥WINDOWS¥Tasks¥UpdateTask.bat）
   - コンシューマ タイプ -- Windows スケジュール タスク
   - アプリケーション パス -- C:¥WINDOWS¥Tasks¥UpdateTask.bat
   - 特権アカウント -- win456¥ServiceAdmin
   - エンドポイント -- win456

   スティーブはパスワード コンシューマを作成しました。CA Access Control エンタープライズ管理 により win456¥ServiceAdmin アカウント用のパスワードが変更されるたびに、JCS では win456 エンドポイントにログインして、ソフトウェア更新のスケジュール タスクで使用するパスワードが変更されます。パスワードの変更が成功しない場合、スティーブは、パスワードの変更を再試行するために[パスワード コンシューマの同期]タスクを使用できます。

詳細情報:

パスワード コンシューマの同期 (P. 313)

PUPM の自動ログイン

PUPM 自動ログインにより、ユーザは 1 ステップで特権アカウント パスワードをチェックアウトして、PUPM のエンドポイントにログインできます。PUPM の自動ログインでは、チェックアウト後にパスワードは表示されませんが、このパスワードを使用して、エンドポイント上の特権アカウントに自動的にユーザがログインされます。チェックアウト後は、CA Access Control エンタープライズ管理 でパスワードを表示できます。

重要: PUPM の自動ログインは、Microsoft Internet Explorer ブラウザのみで使用できます。

自動ログインを管理するため、CA Access Control エンタープライズ管理 でログイン アプリケーションを作成します。ログイン アプリケーションでは、スクリプトを使用してユーザのコンピュータ上でウィンドウが開かれ、チェックアウト済みの特権アカウントにユーザがログインされます。たとえば、SSH Device エンドポイント上のルート アカウントをチェックアウトするために PuTTY ログイン アプリケーションを使用する場合、CA Access Control エンタープライズ管理 により、ユーザのコンピュータ上に[PuTTY]ウィンドウが開かれて、エンドポイント上のルート アカウントにユーザがログインされます。

自動ログインが機能するしくみ

PUPM 自動ログインにより、ユーザは 1 ステップで特権アカウント パスワードをチェックアウトして、PUPM のエンドポイントにログインできます。

以下のプロセスでは、PUPM により、エンドポイントにユーザを自動的にログインさせる方法が説明されています。このプロセスを開始する前に、CA Access Control エンタープライズ管理 でログイン アプリケーションを作成し、PUPM エンドポイントにアプリケーションを割り当てる必要があります。

1. 特権アカウント パスワードをチェックアウトし、CA Access Control エンタープライズ管理 によりエンドポイントへのログインに使用されるログイン アプリケーションを選択します。

2. ActiveX がユーザのコンピュータにインストールされていない場合、以下の手順が発生します。

   a. CA Access Control エンタープライズ管理 により、お使いのコンピュータに ActiveX パッケージが送信されます。

   b. ActiveX をインストールします。

      ActiveX をインストールしないと、エンドポイントに自動的にログインできません。

3. ActiveX がインストールされると、ログイン アプリケーション内に定義されたスクリプト ファイルが、ActiveX により、エンタープライズ管理サーバからユーザのコンピュータにダウンロードされます。

   このスクリプト ファイルには特権アカウント パスワードが含まれています。スクリプト ファイルが実行され、エンドポイントに接続されて、特権アカウントのクレデンシャルが自動的に入力されます。

   注: ActiveX では、ユーザのコンピュータ上にスクリプト ファイルが保存されることはありません。

4. 端末、Windows リモート デスクトップ、またはインターネット ブラウザのウィンドウが開かれます。

   エンドポイント上の特権アカウントへのログインが完了します。

5. ユーザがセッションを完了すると、以下の *いずれか* のイベントが発生します。

   - リモート ウィンドウを閉じる前に、ユーザが特権アカウント パスワードをチェックインすると、PUPM により、猶予期間後にウィンドウが閉じられるという通知が送信されます。猶予期間が経過すると、PUPM によってウィンドウが閉じられ、セッションが終了されます。

     注: 猶予期間はスクリプト ファイルで定義されています。スクリプト ファイルをカスタマイズして、猶予期間を延長または短縮できます。

   - ユーザがリモート ウィンドウを閉じていて、特権アカウント パスワードをチェックインしない場合、PUPM から、ユーザがパスワードをチェックインするかどうかを尋ねる通知が送信されます。

詳細情報:

ログイン アプリケーションの作成 (P. 233)

PUPM 自動ログイン アプリケーション スクリプトをカスタマイズする方法

PUPM 自動ログイン アプリケーション スクリプトをカスタマイズすることによって、PUPM 自動ログイン機能を拡張できます。PUPM 自動ログイン SDK を使用してカスタム スクリプトを作成し、ユーザがエンドポイントに自動的にログインできるようにします。

以下のプロセスでは、自動ログイン アプリケーション スクリプトをカスタマイズする方法について説明します。

1. Visual Basic スクリプトを作成します

   スクリプトの作成には、標準の COM オブジェクトまたは ACLauncher ActiveX メソッドを使用できます。

2. CA Access Control エンタープライズ管理 でログイン アプリケーションを設定し、作成したスクリプトをアプリケーションに関連付けます。
3. ログイン スクリプトとエンドポイントを関連付けます

詳細情報:

PUPM 自動ログイン アプリケーション Visual Basic スクリプト (P. 269)

PUPM 自動ログイン アプリケーション Visual Basic スクリプト

PUPM 自動ログイン アプリケーションでは、Visual Basic スクリプトを使用して自動ユーザ ログインを有効にします。新しいログイン アプリケーションを作成または既存のログイン アプリケーションを変更するために Visual Basic スクリプトをカスタマイズできます。

PUPM 自動ログイン アプリケーション スクリプトには、エンタープライズ管理サーバからクライアント マシン上へのダウンロード時に ActiveX によって値が置換される変数が含まれています。エンタープライズ管理サーバによりスクリプトが処理され、キーワードが値に置換されます。次に、ActiveX によりクライアント マシン上でスクリプトが実行されます。

PUPM 自動ログイン アプリケーション スクリプトは以下のディレクトリにあります。

JBOSS_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

要素

PUPM ログイン アプリケーション スクリプトには以下のキーが含まれます。

#host#

ユーザが自動的にログインするエンドポイントの名前を指定します。

#username#

チェックアウトされた特権アカウントを指定します。

#password#

チェックアウトする特権アカウントのパスワードを指定します。

#userdomain#

（Active Directory）特権アカウントドメイン名を指定します。

#isActiveServletUrl#

ACLauncher ActiveX でアカウント パスワード チェックイン イベントを確認するために使用する URL を指定します。

#CheckinUrl#

ACLauncher ActiveX で、ユーザがエンドポイントからログアウトした場合にアカウント パスワードをチェックインするために使用する URL を指定します。

#SessionidUrl#

ACLauncher ActiveX で、セッションが ObserverIT Enterprise に記録された場合に記録されたセッション ID を送信するために使用する URL を指定します。

PUPM 自動ログイン アプリケーションの以下のコードの一部は、変数がどのように表示されるかを示しています。

```
Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#¥#userName#", "#password#")
' Set window close event
pupmObj.SetWindowCloseEvent(hwnd)
' Set server checkin event
pupmObj.SetServerCheckinEvent("#isActiveServletUrl#")
' Wait until one of the events signaled
rc = pupmObj.WaitForEvents()
If rc = 1 Then 'user has closed the window - notify the server side
        pupmObj.SendCheckinEvent("#CheckinUrl#")
ElseIf rc = 2 Then 'timeout elapsed - close the window
    call pupmObj.CloseWindow(hwnd, 0)
ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
    call pupmObj.CloseWindow(hwnd, 120)
End If
```

構造

PUPM の自動ログイン アプリケーション スクリプトの構造は以下のとおりです。

- COM オブジェクトの初期化

  ```
  Set pupmObj = CreateObject("ACLauncher.ACWebLauncher")
  ```

- 自動ログイン アプリケーションの実行

  ```
  hwnd = pupmObj.LauncheRDP("#host#", "#userDomain#¥#userName#", "#password#")
  ```

- 実行後タスク -- パスワード チェックイン、対話型ログイン、またはタイムアウト

  ```
  ' Wait until one of the events signaled
  rc = pupmObj.WaitForEvents()
  If rc = 1 Then 'user has closed the window - notify the server side
      pupmObj.SendCheckinEvent("#CheckinUrl#")
  ElseIf rc = 2 Then 'timeout elapsed - close the window
      call pupmObj.CloseWindow(hwnd, 0)
  ElseIf rc = 3 Then 'the account was checkedin at the server side - close the window
      call pupmObj.CloseWindow(hwnd, 120)
  End If
  ```

ログイン アプリケーション セッションを記録するには、スクリプトに記録命令を、以下に従って追加します。

- 初期化セクションで、以下の作業を実行します。以下を追加します。

```
Set observeIT = CreateObject("ObserverIT.AgentAPI.Proxy")
```

- アプリケーション実行セクションで、以下を追加します。

```
'Get application processid
processID = pupmObj.GetWindowProcessID(hwnd)
'Start recording
sessionid = observeIT.StartByProcessID(processID, true)
'Send the sessions if to the ENTM server
pupmObj.AssignSessionID "#SessionidUrl#" ,sessionId
```

- 実行後セクションで、以下を追加します。

```
'Stop recording

observeIT.StopBySessionId sessionId, true
```

メソッド

ACLauncher ActiveX では以下のメソッドを使用します。

```
LaunchеRDP (BSTR bsHostName, BSTR bsUserName, BSTR bsPassword, VARIANT *phWindow);
```

入力クレデンシャルでリモート デスクトップ セッションを開始し、リモート デスクトップ ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеRDP("hostname.com", "hostname¥administrator", "password")

```
LaunchePUTTY  (BSTR bsHostName,  BSTR bsUserName, BSTR bsPassword,  VARIANT *phWindow);
```

入力クレデンシャルで PuTTY セッションを開始し、PuTTY ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test. LaunchePUTTY ("hostname.ca.com", "root", "password")

```
LaunchеProcessAsUser (BSTR bsApplication, BSTR bsCommandline, BSTR bsUsername, BSTR bsPassword, VARIANT *phWindow);
```

入力クレデンシャルでプロセスを開始し、プロセス ウィンドウ ハンドルを返します。

例: Dim test Set test = CreateObject("ACLauncher.ACWebLauncher") Hwnd = test.LaunchеProcessAsUser("cmd.exe", "/k echo This console is run under %USERNAME% account...", "administrator" , "password")

```
GetWindowProcessID(VARIANT *phWindow, LONG *pProcessID);
```

指定されたウィンドウ ハンドルのプロセス ID を返します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") id = test.GetWindowProcessID(hwnd) test.Echo "Process ID = " & id

```
GetWindowTitle(VARIANT *phWindow, BSTR *pbsTitle);
```

指定されたウィンドウ ハンドルのタイトルを返します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") title = test.GetWindowTitle(hwnd)

```
CloseWindow(VARIANT *phWindow, LONG Seconds);
```

ウィンドウが X 秒後に閉じることを通知するメッセージを含むダイアログ ボックスを表示し、指定されたウィンドウ ハンドルのウィンドウを閉じます。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.Sleep(5000) test.CloseWindow(hwnd, 60)

```
SetTimeoutEvent(LONG seconds);
```

"WaitForEvents" メソッドのタイムアウトを指定します。タイムアウト値に達すると、WaitForEvents メソッドは、タイムアウトに達したことを示す戻り値で、ブロックしているコールから戻ります。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetTimeoutEvent(10)

```
SetWindowCloseEvent(VARIANT *phWindow);
```

"WaitForEvents" メソッドに対してウィンドウを閉じるイベントを指定します。ウィンドウが閉じられた後、"WaitForEvents" メソッドは、ブロックしているコールから戻り、ウィンドウが閉じられたことを示す戻り値を表示します。

例: Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetWindowCloseEvent(hwnd)

```
SetServerCheckinEvent(BSTR bsURL);
```

PUPM チェックイン イベントを、実行ブロック条件として設定します。ActiveX は 5 秒ごとに PUPM をクエリします。

例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb") (replace with variable)

```
WaitForEvents(VARIANT *pRetVal);
```

レジスタ条件の 1 つに該当するまで、スクリプトの実行をブロックします。

オプション： 1 -- ユーザによってウィンドウが閉じられました、2 -- タイムアウトが経過しました、3 -- がサーバ側でチェックインされました

例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SetServerCheckinEvent("http://server.com/__azy?djfhwek5jy34brfhwkeb")

test.SetWindowCloseEvent(hwnd) test.SetTimeoutEvent(360) rc = test.WaitForEvents() If rc = 3 Then call test.CloseWindow(hwnd, 10) End If

```
SwitchToThisWindow(VARIANT *phWindow);
```

ウィンドウを Z 順の最前面に移動させます

例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password") test.SwitchToThisWindow(hwnd)

```
SendCheckinEvent(BSTR bsURL);
```

ユーザがウィンドウを閉じたら、チェックイン イベントを送信します。

例： Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.LauncheRDP("hostname", "administrator", "password")

```
Sleep(LONG milliseconds);
```

スクリプトの実行を一時停止します。

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Sleep(2000)

```
Echo(VARIANT* pArgs);
```

メッセージを画面に出力します、

Set test = CreateObject("ACLauncher.ACWebLauncher") hwnd = test.Echo("Password Checkin")

拡張ログイン

拡張ログインは自動ログイン タイプの 1 つであり、これによりユーザは、あるエンドポイント上で定義されている特権アカウントをチェックアウトし、そのアカウントを使用して他のエンドポイントにログインできます。拡張ログインでは、自動ログインを使用して、Active Directory で定義されている特権アカウントをチェックアウトできます。

たとえば、Active Directory に example1 という名前の UNAB のエンドポイントを定義し、example1 のユーザとグループ（ルートを含む）を Active Directory に移行するとします。CA Access Control エンタープライズ管理 でルートを特権アカウントとして定義します。ルートをチェックアウトする際に自動ログインを使用する場合は、ルート アカウントが定義されているエンドポイント、つまり Active Directory ドメイン コントローラにログインします。ルートをチェックアウトする際に拡張ログインを使用する場合は、example1 のエンドポイントへのログインを選択できます。

CA Access Control エンタープライズ管理 により、ログイン アプリケーションを割り当てた各エンドポイント用の拡張ログイン オプションが表示されます。エンドポイントにログイン アプリケーションを割り当ててあれば、拡張ログインを設定する追加の手順を実行する必要はありません。

端末統合

端末統合により、特権アカウントを使用するユーザのアクティビティを追跡するために、ユーザの CA Access Control のエンドポイントを PUPM に統合できます。端末統合が動作するのは、ユーザが特権アカウント パスワードをチェックアウトして、CA Access Control のエンドポイントへのログインに自動ログインを使用する場合のみです。

端末統合により、以下のようにユーザのセキュリティとアカウンタビリティが強化されます。

- セキュリティを強化するため、ユーザが PUPM の自動ログインを使用してエンドポイントにログインするように指定できます。
- アカウンタビリティを強化するため、CA Access Control による監査レコードの書き込みと許可の判断の際に、特権アカウント ユーザ名ではなく元のユーザ名が使用されるように指定できます。

CA Access Control による監査レコードの書き込みと許可の判断の際に、元のユーザ名が使用されするように指定すると、CA Access Control では、ログイン セッション用の監査モードが蓄積されます。蓄積された監査モードにより、元のユーザ用の監査モードと特権アカウント用の監査モードが使用されます。元のユーザが CA Access Control のデータベースに定義されていない場合、CA Access Control では、デフォルト ユーザ用の監査モードと特権アカウント用の監査モードが蓄積されます。

たとえば、1 つのエンドポイント用に端末統合を設定します。そのエンドポイントで、user1（元のユーザ）用の監査モードは失敗で、privileged_user という名前の特権アカウント用の監査モードは成功です。user1 が privileged_user としてエンドポイントへのログインに自動ログインを使用する場合、CA Access Control により、ログイン セッション用の監査モードが失敗、成功に設定されます。

端末統合を使用できるのは、CA Access Control がインストールされている Windows エージェントレス エンドポイントと SSH Device エンドポイント上でのみです。さらに、ユーザは特権アカウント パスワードのチェックアウトに自動ログインを使用する必要があります。

PUPM の統合機能を有効にして CA Access Control をインストールすると、端末統合はデフォルトで有効になります。 CA Access Control をインストールしてから、CA Access Control エンドポイント管理 を使用して、エンドポイント上で端末統合を設定します。

例: ログイン イベントの監査レコード

以下の例では、端末統合を設定したアカウントのログイン イベント監査レコードが示されています。エンドポイントへのログインに、ユーザが PUPM の自動ログインを使用する必要があると指定されています。

```
Event type: Login attempt
Status: Denied
User name: example1¥administrator
Terminal: example1.domain.com
Program: Terminal services
Date: 27 May 2010
Time: 17:35
Details: Automatic login is required for this account
User Logon Session ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
Audit flags: OS user
```

例: リソース アクセス監査レコード

以下の例では、端末統合を設定したアカウント用のリソース アクセス監査レコードが示されています。CA Access Control による監査レコードの書き込みと許可の判断の際に、特権アカウント ユーザ名ではなく元のユーザ名が使用されるように指定しています。元のユーザ名 (user1) は[ユーザ名]フィールド内に一覧表示されています。また、特権アカウント(管理者)は[有効なユーザ名]フィールドに一覧表示されています。

```
Event type: Resource access
Status: Denied
Class: FILE
Resource: C:¥tmp¥core.txt
Access: Exec
User name: domain¥user1
Terminal: example1.domain.com
Program: C:¥WINDOWS¥system32¥cmd.exe
Date: 02 Feb 2010
Time: 14:20
Details: No Step that allowed access
User Logon Session ID: 7dd2b3dc-8a1a-4ffa-8e7d-f9bc20d2b341
Audit flags: OS user
Effective user name: example1¥administrator
```

詳細情報:

端末統合の設定 (P. 300)
端末統合の実装に関する考慮事項 (P. 279)

端末統合の動作のしくみ

端末統合により、セキュリティとアカウンタビリティを強化するため、ユーザの CA Access Control のエンドポイントを PUPM に統合できます。

以下のプロセスでは、端末統合の動作のしくみが説明されています。

1. ユーザは、CA Access Control エンタープライズ管理 で特権アカウント パスワードのチェックアウトに自動ログインを使用します。
2. CA Access Control エンタープライズ管理 では、DMS からエンドポイントの詳細が取得され、プレ ログイン メッセージがメッセージ キューに送信されます。メッセージには、特権アカウントの名前、アカウントをチェックアウトしたユーザの名前、およびエンドポイントの名前が含まれています。

3. CA Access Control エンドポイント上の PUPM Agent では、メッセージ キューからプレ ログイン メッセージが取得されます。
4. ユーザがエンドポイントへのログインに特権アカウントを使用する際、CA Access Control 許可エンジンにより特権アカウントのローカル データベース レコードが確認され、以下のアクションが実行されます。
   a. このエンジンにより、アカウントがログインの前にアカウントのチェックアウトを必要とするかどうか、つまり、ユーザがエンドポイントにログインするために自動ログインを使用する必要があるかどうかが確認されます。*以下のいずれか*のイベントが発生します。
      - アカウントのチェックアウトが必要で、PUPM Agent では特権アカウント用のプレ ログイン メッセージが受け取られていない場合、エンジンによりログイン試行が拒否されます。
      - アカウント チェックアウトが必要で、PUPM Agent で特権アカウント用のプレ ログイン メッセージが受け取られている場合、ログインを阻止する追加の制限、たとえば TERMINAL 制限が存在しないならば、エンジンによりログインが許可されます。
      - アカウントのチェックアウトが必要ではなく、追加の制限が存在しない場合、エンジンによりログインが許可されます。
   b. エンジンにより、許可の判断を下すためにユーザの元の ID を使用する必要があるかどうかが確認されます。*以下のいずれか*のイベントが発生します。
      - ユーザの元の ID を使用する必要がある場合、エンジンでは元のユーザ名を使用してリソース アクセス要求が評価され、監査レコードが書き込まれます。
      - ユーザの元の ID が使用されない場合、エンジンでは特権アカウント名を使用してリソース アクセス要求が評価され、監査レコードが書き込まれます。

詳細情報:

端末統合の設定 (P. 300)
端末統合の実装に関する考慮事項 (P. 279)

端末統合の実装に関する考慮事項

端末統合を実装する前に、以下の点を考慮してください。

- 端末統合は、CA Access Control がインストールされている Windows エージェントレスおよび SSH エンドポイント タイプに設定できます。他のエンドポイント タイプには端末統合を設定できません。
- （UNIX）CA Access Control は、エンドポイントへの接続に使用されるログイン プログラムに対して、PAM ログイン インターセプトを使用する必要があります。たとえば、ユーザが SSH を使用してエンドポイントに接続する場合、CA Access Control は PAM ログイン インターセプトを使用して SSH ログインをインターセプトする必要があります。

  CA Access Control がログイン プログラムに対して PAM ログイン インターセプトを使用するように指定するには、ログイン プログラムの LOGINAPPL レコードで loginflags（pamlogin）フラグを設定します。以下に例を示します。

  ```
  editres loginappl SSH loginflags(pamlogin)
  ```

- 端末統合は、特権アカウント ログインに対してのみ有効化できます。ログイン統合は、サービス アカウント ログインに対しては機能しません。
- 端末統合は、特権アカウントのチェックアウトに自動ログインを使用する場合にのみ機能します。
- （UNIX）端末統合は、SSH ログインにのみ使用できます。端末統合が機能するのはユーザが特権アカウント パスワードのチェックアウト、および CA Access Control のエンドポイントへのログインに PUPM の自動ログインを使用する場合のみであり、PUPM では SSH 用のログイン スクリプトのみが提供されるために、この制限が存在します。

  他のログイン タイプ用にログイン アプリケーションを作成するためにカスタマイズしたスクリプトを記述し、他のログイン タイプの端末統合を有効にする場合は、適切なログイン プログラムの LOGINAPPL レコードの loginflags（pamlogin）プロパティを設定します。

詳細情報:

端末統合の設定 (P. 300)

第 7 章: PUPM エンドポイントの設定

このセクションには、以下のトピックが含まれています。

データベース(JDBC)パスワード コンシューマを使用するための JBoss アプリケーションの準備

JDBC データベース パスワード コンシューマを使用すると、データベースへの接続に JDBC を使用するアプリケーション内のハードコードされたパスワードを置き換えることができます。アプリケーションが認証を目的としてパスワードを提供する場合は常に、PUPM Agent により CA Access Control エンタープライズ管理 から特権アカウント パスワードが取得され、ハードコードされたパスワードが特権アカウント パスワードに置き換えられます。

パスワード コンシューマが使用するデータベースを設定する前に、JDBC パスワード コンシューマを使用するためのエンドポイントの準備を行うべきです。

データベース(JDBC)パスワード コンシューマを使用するために JBoss アプリケーションを準備する方法

1. PUPM 統合機能が有効になっているエンドポイントに CA Access Control がインストールされていること、そして、データベースに接続するアプリケーションが JRE 1.5 以降を使用することを確認します。

   注: データベースに接続するアプリケーションがインストールされるエンドポイントに、CA Access Control をインストールします。データベース ホストに CA Access Control をインストールする必要はありません。

2. データベースに接続しているアプリケーションがある場合は停止します。
3. 以下のディレクトリに移動します(*ACInstallDir* は CA Access Control をインストールしたディレクトリです)。

   ACInstallDir/SDK/JDBC

4. 以下のファイルを探します。
   - CAJDBCService.sar
   - CAJDBCDriver.jar
   - CAPUPMClientCommons.jar
   - jsafeFIPS.jar

5. 以下のディレクトリに CAJDBCService.sar をコピーします。ここで *JBOSS_HOME* は JBoss をインストールしたディレクトリです。

   JBOSS_HOME/server/default/deploy

6. 以下のディレクトリに、ファイル CAJDBCDriver.jar、CAPUPMClientCommons.jar、および jsafeFIPS.jar をコピーします。

   JBOSS_HOME/server/lib

7. エンタープライズ管理サーバで、パスワード コンシューマ用に定義したデータ ソース XML ファイルを検索します。

8. ファイルを編集用に開きます。以下の*いずれか*の操作を実行します。

   - Microsoft SQL Server 用のデータ ソース設定ファイルのカスタマイズ (P. 284)
   - Oracle 用のデータ ソース設定ファイルのカスタマイズ (P. 284)

   データ ソース設定ファイルをカスタマイズするのは、データベース接続設定およびデータ ソース クラスを指定するためです。

9. CA Access Control を起動します。

   パスワード コンシューマを使用するエンドポイントが設定できました。次に、CA Access Control エンタープライズ管理 でアプリケーション用のパスワード コンシューマを作成する必要があります。パスワード コンシューマを作成した後、アプリケーションを起動します。

詳細情報:

パスワード コンシューマの例: JDBC データベース (P. 285)
パスワード コンシューマの作成 (P. 259)

Microsoft SQL Server 用のデータ ソース設定ファイルのカスタマイズ

JDBC データベース パスワード コンシューマを設定すると、Microsoft SQL Server データベースへの接続に JDBC を使用するアプリケーション内のハードコードされたパスワードを置き換えることができます。エンドポイントを準備した後、以下の手順に従って、JDBC パスワード コンシューマを使用します。

Microsoft SQL Server 用のデータ ソース設定ファイルのカスタマイズ

1. <driver-class> タグを見つけて、デフォルト値を JDBC ドライバ クラス プロパティで置き換えます。以下に例を示します。

   ```
   <driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
   ```

2. <connection-url> タグを見つけて、デフォルト値をデータベース接続設定で置き換えます。以下に例を示します。

   ```
   <connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
   ```

3. CA Access Control を起動します。

   これで、Microsoft SQL Server 用にデータ ソース設定ファイルをカスタマイズしました。次に、CA Access Control エンタープライズ管理 でアプリケーション用のパスワード コンシューマを作成する必要があります。パスワード コンシューマを作成した後、アプリケーションを起動します。

Oracle 用のデータ ソース設定ファイルのカスタマイズ

JDBC データベース パスワード コンシューマを設定すると、Oracle データベースへの接続に JDBC を使用するアプリケーション内のハードコードされたパスワードを置き換えることができます。エンドポイントを準備した後、以下の手順に従って、JDBC パスワード コンシューマを使用します。

Oracle 用のデータ ソース設定ファイルのカスタマイズ

1. <xa-datasource-class> タグを見つけて、デフォルト値を JDBC ドライバ クラス プロパティで置き換えます。以下に例を示します。

   ```
   <xa-datasource-class>com.ca.ppm.clients.jdbc.CAJDBCDataSource</xa-datasource-class>
   ```

   重要: プロパティ名の大文字と小文字はデフォルト値と同じである必要があります。

2. <xa-datasource-property name=> タグをすべて見つけます。以下に例を示します。

```
<xa-datasource-property
name="URL">jdbc:oracle:oci8:@tc</xa-datasource-property>
<xa-datasource-property name="User">scott</xa-datasource-property>
<xa-datasource-property name="Password">tiger</xa-datasource-property>
```

3. これらのプロパティを単一の文字列にまとめます。以下に例を示します。

```
<xa-datasource-property
name="CAJDBCProperties">CAJDBCPropertyRealDatasourceClass="oracle.jdbc.xa.cli
ent.OracleXADataSource";URL="jdbc:oracle:oci8:@tc";User="scott";Password="tig
er";</xa-datasource-property>
```

4. CA Access Control を起動します。

これで、Oracle 用にデータ ソース設定ファイルをカスタマイズしました。次に、CA Access Control エンタープライズ管理 でアプリケーション用のパスワード コンシューマを作成する必要があります。パスワード コンシューマを作成した後、アプリケーションを起動します。

パスワード コンシューマの例: JDBC データベース

ここでは、システム管理者の Steve が JBoss アプリケーション サーバを使用して、クリア テキストのパスワードを含むアプリケーションを起動する例を示します。アプリケーションは、Microsoft SQL Server データベースへの接続を認証するためにクリア テキストのパスワードを使用します。Steve は、アプリケーションがデータベースに接続するたびに PUPM から特権アカウント パスワードを取得するように JBoss アプリケーション サーバを変更しようとしています。

Steve は Windows エンドポイント上に、JBoss アプリケーション サーバ バージョン 4.2.3.GA および Java Development Kit (JDK) 1.6.0_19 をインストールしました。エンドポイントの名前は JBossEndpoint です。JBossEndpoint¥Administrator という名前のユーザが run.bat ファイルを使用して JBoss アプリケーション サーバを起動し、このサーバが Microsoft SQL Server データベースに接続するアプリケーションを実行します。そのアプリケーションは、sa アカウントを使用してデータベースに接続します。

1. Steve は JBossEndpoint 上で以下の手順を実行します。
   a. JBoss を停止します。
   b. PUPM 統合機能を有効にして CA Access Control をインストールします。
   c. 以下のディレクトリに移動します。

```
C:¥Program Files¥CA¥AccessControl¥¥SDK¥JDBC
```

d. 以下のファイルを見つけます。
   - CAJDBCService.sar
   - CAJDBCDriver.jar
   - CAPUPMClientCommons.jar
   - jsafeFIPS.jar

e. 以下のディレクトリにファイル CAJDBCService.sar をコピーします。

```
C:¥jboss-4.2.3.GA¥server¥default¥deploy
```

f. 以下のディレクトリにファイル CAJDBCDriver.jar、CAPUPMClientCommons.jar、および jsafeFIPS.jar をコピーします。

```
C:¥jboss-4.2.3.GA¥server¥default¥lib
```

g. 以下のディレクトリに移動します。

```
C:¥jboss-4.2.3.GA¥server¥default¥deploy
```

h. 以下のファイルを開いて、編集します。
   - imworkflowdb-ds.xml
   - objectstore-ds.xml
   - reportsnapshot-ds.xml
   - userstore-ds.xml

i. <driver-class> タグを見つけて、デフォルト値を JDBC ドライバ クラス プロパティで置き換えます。以下に例を示します。

```
<driver-class>com.ca.ppm.clients.jdbc.CAJDBCDriver</driver-class>
```

j. <connection-url> タグを見つけて、デフォルト値をデータベース接続設定で置き換えます。以下に例を示します。

```
<connection-url>>@@@com.microsoft.sqlserver.jdbc.SQLServerDriver@@@jdbc:sqlserver://SQLServer1:1433;selectMethod=cursor;DatabaseName=tempdb</connection-url>
```

k. 保存してファイルを閉じます。

l. CA Access Control を起動します。

2. Steve は 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. JBossEndpoint_PUPM という名前の Windows エージェントレス エンドポイントのタイプを作成します。

   b. JBossEndpoint_PUPM エンドポイント上で sa 特権アカウントを検出します。

c. 以下のパラメータを使用して、データベース パスワード コンシューマを作成します。

- 名前 -- JBossEndpoint MS SQL connection
- コンシューマ タイプ -- データベース（ODBC/JDBC/OLEDB/OCI）
- アプリケーション パス -- C:¥jboss-4.2.3.GA¥bin¥run.bat
- アカウント -- sa
- ホスト -- JBossEndpoint
- ユーザ -- JBossEndpoint¥Administrator

3. JBossEndpoint¥Administrator ユーザが、run.bat ファイルを実行するとエンドポイント上の JBoss アプリケーション サーバが起動されます。

   JBoss アプリケーション サーバが起動され、アプリケーションは、SQL Server への接続を試行します。PUPM Agent は、接続試行をインターセプトし、アプリケーションに特権アカウント パスワードを提供します。

4. Steve は、以下のディレクトリにある JBoss ログ ファイルでエラーがないか確認します。

   ```
   C:¥jboss-4.2.3.GA¥server¥default¥log
   ```

Oracle データベース向け追加情報

tnsnames.ora ファイルは、Oracle のデータベースに接続する場合のデータベース アドレスを定義する、クライアント向けの Oracle 構成ファイルです。tnsnames.ora ファイルには複数のホスト名、ポート、サービス名、インスタンス名または SID が含まれる場合があります。

PUPM Agent では、$ORACLE_HOME と $TNS_ADMIN の環境変数を解決して、tnsnames.ora ファイルの完全パスを解決します。環境変数は以下のレジストリ エントリ内に定義されています。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns¥plugin¥EnvironmentVariables
```

プラグイン

接続の試行をインターセプトするプラグインの名前を指定します。

値: OCIPlg、ODBCPlg、OLEDBPlg

PUPM Agent は Oracle データベースへの接続の試行をインターセプトするたびに、tnsnames.ora ファイルを解析します。ファイルに、これらすべての属性の複数の値が含まれている場合、PUPM Agent により、可能な属性の各組み合わせに対して個別のネットワーク セットが作成されます。PUPM Agent は、ネットワーク セットと最も一致する特権アカウントのパスワードを取得した CA Access Control エンタープライズ管理 にネットワーク セットをすべて送信します。

例: tnsnames.ora ファイル内のネットワーク セット

以下は tnsnames.ora ファイルの例です。

```
SAMPLE_INSTANCE=
 (DESCRIPTION=
   (SOURCE_ROUTE=yes)
   (ADDRESS=(PROTOCOL=tcp)(HOST=host1)(PORT=1630))    # hop 1
   (ADDRESS_LIST=
     (FAILOVER=on)
     (LOAD_BALANCE=off)                                # hop 2
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2a)(PORT=1630))
     (ADDRESS=(PROTOCOL=tcp)(HOST=host2b)(PORT=1630)))
   (ADDRESS=(PROTOCOL=tcp)(HOST=host3)(PORT=1521))    # hop 3
   (CONNECT_DATA=(SERVICE_NAME=Sales.example.com)))
```

PUPM Agent はこの tnsnames.ora ファイルを解析すると、CA Access Control エンタープライズ管理 に以下のネットワーク セットを送信します。

- HOST=host1、PORT=1630
- HOST=host2a、PORT=1630
- HOST=host2b、PORT=1630
- HOST=host3、PORT=1521、SERVICE_NAME= Sales.example.com

データベース（ODBC、OLEDB、OCI）パスワード コンシューマを使用するためのエンドポイントの設定

Windows エージェントレス エンドポイントで有効。

ODBC、OLEDB または OCI データベース パスワード コンシューマを使用して、データベースへの接続に ODBC、OLEDB または OCI を使用するアプリケーション内のハードコードされたパスワードを置き換えることができます。アプリケーションがデータベースに接続を試みる場合、PUPM Agent は接続の試行をインターセプトし、ハードコードされたパスワードを CA Access Control エンタープライズ管理 から取得する特権アカウント パスワードに置き換えます。

アプリケーションは、CA Access Control がインストールされている Windows エージェントレス エンドポイント上に存在する必要があります。OCI データベース パスワード コンシューマを作成する場合、アプリケーションが OCI8 以降を使用することを確認します。

PUPM は別のプラグインを使用して、各タイプの接続の試行をインターセプトします。たとえば、OCI プラグインは OCI を使用する接続の試行をインターセプトします。以下のレジストリ キーが、CA Access Control プラグインの動作をコントロールします。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥PlugIns
```

各プラグインの設定は以下のサブキー内に格納されています。

- OCI -- Instrumentation¥PlugIns¥OCIPlg
- ODBC -- Instrumentation¥PlugIns¥ODBCPlg
- OLEDB -- Instrumentation¥PlugIns¥OLEDBPlg

データベース（ODBC、OLEDB、OCI）パスワード コンシューマを使用するためのエンドポイントを設定する方法

1. PUPM の統合機能が有効になっているエンドポイントに CA Access Control がインストールされていることを確認します。

   注: データベースに接続するアプリケーションがインストールされるエンドポイントに、CA Access Control をインストールします。データベース ホストに CA Access Control をインストールする必要はありません。

2. エンドポイントで CA Access Control を停止します。

3. 接続の種類に対して適切なレジストリ サブキーで、以下の手順に従います。

   - OperationMode レジストリ エントリの値が 1 であることを確認します。

     このレジストリ エントリはプラグインを有効にします。

   - アプリケーションを起動するプロセスの名前が ApplyOnProcess レジストリ エントリの値であることを確認します。

     このレジストリ エントリは、プラグインが適用されるプロセスを指定します。たとえば、IIS アプリケーション用のパスワード コンシューマを作成している場合は、w3wp.exe が レジストリ エントリの値であることを確認します。

     注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート（http://www.ca.com/jp/support/）にお問い合わせください。

4. CA Access Control を起動します。

   データベース パスワード コンシューマを使用するためのエンドポイントを設定しました。次に、CA Access Control エンタープライズ管理 内にアプリケーション用のデータベース パスワード コンシューマを作成する必要があります。

   注: IIS アプリケーション用のパスワード コンシューマを作成する場合、特権アカウント パスワードの取得にパスワード コンシューマを使用できる NT_AUTHORITY¥NETWORK SERVICE および *hostname*¥IUSR_*hostname* ユーザを指定する必要があります。ここで、*hostname* はエンドポイントの名前を表します。

データベース(.NET)パスワード コンシューマを使用するためのエンドポイントの設定

Windows エージェントレス エンドポイントで有効

.NET データベース パスワード コンシューマを使用すると、データベースへの接続に .NET を使用するアプリケーション内のハードコードされたパスワードを置き換えることができます。 アプリケーションがデータベースへの接続を試行すると、PUPM エージェントは接続の試行をインターセプトし、ハードコードされたパスワードを、CA Access Control エンタープライズ管理 から取得する特権アカウントパスワードに置き換えます。

注: アプリケーションは、CA Access Control がインストールされている Windows エージェントレス エンドポイントに存在する必要があります。

PUPM は、各接続の試行をインターセプトするプラグインをロードするためにプロファイラを使用します。.NET プラグインは、.NET を使用する接続の試行をインターセプトします。CA Access Control .NET の動作は、以下のレジストリ キーによって制御されます。

```
HKEY_LOCAL_MACHINE¥SOFTWARE¥ComputerAssociates¥AccessControl¥Instrumentation¥.NET¥
```

プロファイラとプラグイン用の設定は、以下のサブキーに存在します。

- プロファイラ -- Instrumentation¥.NET¥Profiler¥
- プラグイン -- Instrumentation¥.NET¥Profiler¥Plugin

.NET データベース パスワード コンシューマを使用するためにエンドポイントを設定する方法

1. PUPM の統合機能が有効になっているエンドポイントに CA Access Control がインストールされていることを確認します。

   注: データベースに接続するアプリケーションがインストールされるエンドポイントに、CA Access Control をインストールします。データベース ホストに CA Access Control をインストールする必要はありません。

2. エンドポイントで CA Access Control を停止します。

3. 接続の種類に対して適切なレジストリ サブキーで、以下の手順に従います。

   - OperationMode レジストリ エントリの値が 1 であることを確認します。

     このレジストリ エントリはプラグインを有効にします。

     重要: プロファイラとプラグイン用の OperationMode レジストリ エントリが 1 に設定されていることを確認します。

   - アプリケーションを起動するプロセスの名前が ApplyOnProcess レジストリ エントリの値であることを確認します。

     このレジストリ エントリは、プラグインが適用されるプロセスを指定します。たとえば、IIS アプリケーション用のパスワード コンシューマを作成している場合は、w3wp.exe が レジストリ エントリの値であることを確認します。

     注: ユーザ自身がこのレジストリ エントリの値を変更しすることはお勧めできません。 詳細については、当社テクニカル サポート (http://www.ca.com/jp/support/) にお問い合わせください。

4. CA Access Control を起動します。

   データベース パスワード コンシューマを使用するためのエンドポイントを設定しました。次に、CA Access Control エンタープライズ管理 内にアプリケーション用のデータベース パスワード コンシューマを作成する必要があります。

   注: IIS アプリケーション用のパスワード コンシューマを作成する場合、特権アカウント パスワードの取得にパスワード コンシューマを使用できるユーザとして NT_AUTHORITY¥NETWORK SERVICE および *hostname*¥IUSR_*hostname* を指定します(*hostname* はエンドポイント名を表します)。

CLI パスワード コンシューマを使用するためのエンドポイントの設定

CLI パスワード コンシューマはソフトウェア開発キット パスワード コンシューマの一種です。CLI のパスワード コンシューマを使用して、スクリプト内のハードコードされたパスワードを特権アカウント パスワードに置き換えることができます。CLI のパスワード コンシューマは、特権アカウント パスワードを取得し、特権アカウント パスワードをチェックアウトまたはチェックインするスクリプトの表現形です。このスクリプトは、CA Access Control エンタープライズ管理 から特権アカウント パスワードを取得する PUPM Agent を呼び出します。

他のファイルまたはスクリプトを変更する機能に制限がある .bat または .sh スクリプトを書き込むには、CLI のパスワード コンシューマを使用します。たとえば、手動でファイル内のハードコードされたパスワードを更新するために acpwd ユーティリティを使用するスクリプトに書き込むことができます。また、CLI のパスワード コンシューマを使用して、ユーザにエンドポイント上のコマンド ラインから acpwd ユーティリティを実行させることもできます。

注: スクリプト内のハードコードされたパスワードを特権アカウント パスワードに置き換えるには、PUPM SDK を使用することもできます。たとえば、複数のファイル内のパスワードを置き換えるカスタマイズされたスクリプトに書き込むには、PUPM SDK を使用します。

CLI のパスワード コンシューマを使用するためにエンドポイントを設定する方法

1. PUPM の統合機能が有効になっているエンドポイントに CA Access Control がインストールされていることを確認します。
2. スクリプトに以下のコマンドを追加します。

   ```
   acpwd {-checkout | -get} -account name -ep name -eptype type [-container name] -nologo
   ```

   注: acpwd ユーティリティの構文の詳細については、「*リファレンス ガイド*」を参照してください。
3. コマンド(特権アカウント パスワード)の出力を使用するように、ユーザのスクリプトを変更します。

   CLI のパスワード コンシューマを使用するためにエンドポイントを設定しました。次に、CA Access Control エンタープライズ管理 内のスクリプト用の Software Development Kit (SDK/CLI) パスワード コンシューマを作成する必要があります。

詳細情報:

パスワード コンシューマの作成 (P. 259)

CLI のパスワード コンシューマのしくみ

CLI のパスワード コンシューマを使用して、スクリプト内のハードコードされたパスワードを特権アカウント パスワードに置き換えることができます。CLI のパスワード コンシューマは、特権アカウント パスワードの取得、特権アカウント パスワードをチェックアウト、またはチェックインするために acpwd ユーティリティを使用するスクリプトの表現形です。また、CLI のパスワード コンシューマを使用して、ユーザにエンドポイント上のコマンド ラインから acpwd ユーティリティを実行させることもできます。CLI のパスワード コンシューマが acpwd ユーティリティの使用に役立つしくみを把握します。

注: スクリプト内、またはコマンド ラインから acpwd ユーティリティを使用するには、まず CA Access Control エンタープライズ管理 内にスクリプトまたはユーティリティを Software Development Kit (SDK/CLI) パスワード コンシューマとして定義する必要があります。パスワード コンシューマは、特権アカウント パスワードの取得を許可されているユーザのリストを定義します。

以下のプロセスに、CLI のパスワード コンシューマが動作するしくみを説明します。

1. エンドポイント上の acpwd ユーティリティは以下のいずれかの方法で呼び出されます。
   - ユーザは、コマンド プロンプト ウィンドウからユーティリティを実行します。
   - スクリプトまたはアプリケーション サーバが実行され、ユーティリティを呼び出します。
2. acpwd ユーティリティは特権アカウント パスワードを要求します。PUPM エージェントは認可のために CA Access Control エンタープライズ管理 へリクエストを転送します。
3. CA Access Control エンタープライズ管理 はエンドポイントに特権アカウント パスワードを送信します。PUPM Agent はパスワードを表示するか元のプログラムに転送し、確認メッセージを記録します。

4. ユーザ、スクリプト、アプリケーション サーバ、または CA Access Control エンタープライズ管理 は、アカウント パスワードにチェックインし直します。また、PUPM Agent は確認メッセージを記録します。
5. PUPM エージェントは、チェックインが正常に行われたことを示す確認メッセージをログに記録します。

   注: ゼロ(0)を含む確認メッセージは、PUPM Agent によるパスワードの取得の成功、チェックアウト、またはチェックインを示します。acpwd ユーティリティの構文の詳細については、「*リファレンス ガイド*」を参照してください。

例: パスワードを取得するスクリプト

以下に、Windows 上の特権アカウント パスワードを取得するスクリプトの例の抜粋を示します。この例では、PUPM Agent が CA Access Control エンドポイントにインストールされていると仮定します。

このサンプル スクリプトは、CA Access Control エンタープライズ管理 から取得した特権アカウント パスワードを使用して、Windows レジストリのエントリの追加および削除を試行します。

```
set AdminUser=PowerUser
FOR /F "tokens=*" %%i IN ('"C:¥Program Files¥AccessControl¥bin¥acpwd.exe" -get
-account PowerUser
 -ep comp1_123 -eptype "Windows Agentless" -container "Windows Accounts" -nologo')
DO SET AdminPassword=%%i
set runasadmin="C:¥utils¥psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM¥SOFTWARE¥PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM¥SOFTWARE¥PUPM Registry" /F
```

この例では、スクリプトが PUPM Agent を実行して特権アカウント パスワードを取得します。このスクリプトには、アカウント名(*PowerUser*)、エンドポイント名(*comp1_123*)、エンドポイント タイプ(*Windows Agentless*)、ユーザのコンテナ名(*Windows Accounts*)が含まれています。このスクリプトは、パスワードだけを表示するように PUPM エージェントに指示し、そのパスワードを使用して、レジストリ エントリを追加および削除する管理者ユーザとして PsExec プログラムを実行します。

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定する方法

パスワード コンシューマ SDK を使用すると、CA Access Control エンドポイント用のアプリケーションを作成できます。これらのアプリケーションは、特権アカウント パスワードを取得、チェックアウト、およびチェックインし、パスワードキャッシュおよびユーザ認証を行います。

アプリケーションは、実行時に PUPM エージェントをコールします。このエージェントは、CA Access Control エンタープライズ管理 から特権アカウント パスワードを取得、チェックアウト、およびチェックインします。

PUPM SDK には、次の 2 種類があります。

- Java PUPM SDK -- Windows と UNIX のエンドポイント用の Java アプリケーションを作成するときには、この SDK を使用します。

  作成する Java アプリケーションは JRE 1.5 以降を使用する必要があります。
- .NET PUPM SDK -- Windows エンドポイント用の C# アプリケーションを作成するときには、この SDK を使用します。

  .NET PUPM SDK を使用するには、エンドポイントに.NET Framework 2.0 以降をインストールする必要があります。

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定するには、以下の手順に従います。

1. PUPM の統合機能が有効になっているエンドポイントに CA Access Control がインストールされていることを確認します。
2. パスワード コンシューマ SDK サンプルを使用してアプリケーションを作成します。サンプルの場所は以下のとおりです。
   - Java PUPM SDK -- *ACInstallDir*/SDK/JAVA/Samples/PUPMJavaSDK/src/cpm/ca/pupm/javasdk/Tester.java
   - .NET PUPM SDK -- *ACInstallDir*/SDK/DOTNET/Examples

   パスワード コンシューマ SDK アプリケーションを使用するためのエンドポイントを設定しました。次に、CA Access Control エンタープライズ管理 内のアプリケーション用に Software Development Kit（SDK/CLI）パスワード コンシューマを作成する必要があります。

詳細情報:

パスワード コンシューマ SDK アプリケーションがパスワードを取得する方法 (P. 173)
Java PUPM SDK (P. 174)
.NET PUPM SDK (P. 176)
パスワード コンシューマの作成 (P. 259)

Java PUPM SDK アプリケーションの実行

パスワード コンシューマ SDK アプリケーションを使用するためにエンドポイントを設定したら、アプリケーションを実行して特権アカウント パスワードを取得、チェックアウト、およびチェックインできます。

Java PUPM SDK アプリケーションを実行する方法

1. CA Access Control エンタープライズ管理 にアプリケーション用のパスワード コンシューマを作成したことを確認します。
2. コマンド プロンプト ウィンドウを開き、アプリケーションがインストールされたフォルダに移動します。
3. 以下のコマンドを実行します。

```
java -cp PupmJavaSDK.jar;CAPUPMClientCommons.jar;jsafeFIPS.jar;[log4jLib];.
applicationName {explicit | keyvalues} {checkout | checkin} "endpointType"
"endpointName" "accountName" "accountContainer" flags
```

log4jLib

(オプション) ランタイム イベントおよび情報をログに記録するためにアプリケーションが使用する log4j ライブラリの名前を定義します。

applicationName

Java PUPM SDK アプリケーションの名前を定義します。

explicit

コマンドが各パラメータの明示的な値を提供することを指定します。

keyvalues

コマンドがキー/値ペアを使用することを指定します。

checkout

アプリケーションが特権アカウント パスワードを取得（取得またはチェックアウト）することを指定します。

注：*flags* パラメータは、アプリケーションが実行する取得またはチェックアウト アクションを指定します。

checkin

アプリケーションが特権アカウント パスワードをチェックインすることを指定します。

endpointType

特権管理アカウントが定義されるエンドポイントのタイプを定義します。

注：CA Access Control エンタープライズ管理 の［エンドポイントの表示］タスクを使用して使用可能なエンドポイント タイプのリストを確認できます。 エンドポイント タイプは、CA Access Control エンタープライズ管理に表示されるとおりに定義します（「SAP R3 via Provisioning」など）。

endpointName

特権管理アカウントが定義されるエンドポイントの名前を定義します。

accountName

特権アカウントの名前を定義します。

accountContainer

特権管理アカウントが定義されるコンテナの名前を定義します。

特権アカウントがコンテナに定義されていない場合は、このパラメータ用のアカウントを指定します。

flags

アプリケーションが特権アカウント パスワードをチェックアウトするか、または取得するかを指定します。

値： 0 -- 特権アカウント パスワードをチェックアウトまたはチェックインします（GetOnly フラグが false）。1 -- 特権アカウント パスワードを取得します（GetOnly フラグが true）。

アプリケーションは、特権アカウント パスワードに対して指定されたアクションを実行し、結果を表示します。

注：semsgtool ユーティリティを使用すると、数値の PUPM SDK エラー コードの説明を表示できます。semsgtool 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

Web サービス PUPM SDK アプリケーションを使用するためにエンドポイントを設定する方法

Web サービス PUPM SDK を使用すると、特権アカウント パスワードをチェックアウトおよびチェックインする Java アプリケーションを作成できます。アプリケーションはエンタープライズ管理サーバと直接通信するので、アプリケーションが動作するエンドポイントに CA Access Control をインストールする必要はありません。

Web サービス PUPM SDK を使用するには、以下のコンポーネントをエンドポイントにインストールします。

- Apache Ant 1.7
- Apache Axis 1.4
- Java SDK 1.4.2
- （オプション）統合開発環境（IDE）

重要：アプリケーションとエンタープライズ管理サーバ間の接続の認証には、NTLM のような高度な認証プロトコルを使用することをお勧めします。

Web サービス PUPM SDK を使用するためにエンドポイントを設定するには、以下の手順に従います。

1. Web サービス PUPM SDK Readme を参照します。

   Readme では、環境を設定し、Java サンプルを作成して実行する方法について説明されています。Readme は以下に格納されています。

   ACServerInstallDir/IAM Suite/Access Control/tools/samples/webservice/Axis

2. Java サンプルを使用して SDK アプリケーションを作成します。

   Web サービス PUPM SDK アプリケーションを使用するためのエンドポイントを設定しました。次に、CA Access Control エンタープライズ管理 にアプリケーションを表すユーザを作成し、適切な特権アクセス ロールを割り当てる必要があります。

詳細情報:

Web サービス SDK アプリケーションがパスワードを取得する方法 (P. 178)
Web サービス PUPM SDK (P. 177)

端末統合の設定

端末統合では、特権アカウントをチェックアウトするユーザのアクティビティを追跡するために、ユーザの CA Access Control エンドポイントを PUPM に統合することができます。端末統合は、特権アカウントを持つ CA Access Control エンドポイントへのログインには、自動ログインを使用する必要があることを指定することもできます。

端末統合を設定する前に、以下の点を確認します。

- 端末統合を設定する特権アカウントが CA Access Control エンタープライズ管理 内に存在すること。
- 端末統合がエンドポイント上で有効であること。つまり、PUPMAgent セクション内の EnableLogonIntegration 環境設定の値が 1 であること。

  注: PUPM 統合機能が有効な CA Access Control をインストールする場合、端末統合はデフォルトで有効です。 端末統合を有効にしていながら設定していない場合、CA Access Control はどのアカウントに対しても端末統合を強制しません。
- （UNIX）CA Access Control は、エンドポイントに接続するために使用されるログイン プログラムに対して、PAM ログイン インターセプトを使用します。

  たとえば、ユーザが SSH を使用してエンドポイントに接続する場合、CA Access Control が PAM ログイン インターセプトを使用して SSH ログインにインターセプトすることを確認します。

  注: PAM ログイン インターセプトおよび LOGINAPPL クラスの詳細については、「*selang リファレンス ガイド*」を参照してください。

次の手順では、単一の特権アカウント用の端末統合を設定する方法について説明します。複数のエンドポイント上の同じ名前の特権アカウントには、端末統合を設定するポリシーを使用できます。

端末統合を設定する方法

1. CA Access Control エンドポイント管理 で、[ユーザ]タブ、[ユーザ]サブタブの順にクリックし、端末統合を設定する特権アカウントを検索します。

   注: CA Access Control エンドポイント管理 におけるユーザの管理方法の詳細については、*オンライン ヘルプ*を参照してください。
2. 特権アカウントを選択します。

   [ユーザの変更]タスク ページに[全般]タブが表示されます。

3. [アカウント]セクションで以下のオプションのいずれか、または両方を選択します。

   元の ID の使用

   監査レコードの書き込みおよび許可に関する決定を行う際に、CA Access Control が特権アカウント ユーザ名ではなく、特権アカウントをチェックアウトしたユーザの名前を使用するように指定します。

   ログイン前にアカウントのチェックアウトが必要です。

   この特権アカウントでエンドポイントにログインするために、ユーザが自動ログインを使用する必要があることを指定します。自動ログインによって、ユーザはパスワードをチェックアウトし、CA Access Control エンタープライズ管理 からエンドポイントに自動的にログインできます。

4. [Save]をクリックします。

   特権アカウント用の端末統合を有効にして設定しました。

例: 端末統合を設定するポリシー

以下のポリシーは、administrator という名前のアカウント用の端末統合を設定します。ポリシーは CA Access Control が監査レコードを書き込み、許可の判断を下す際に、元のユーザ名を使用することを指定します。また、管理者としてエンドポイントにログインするには自動ログインを使用する必要があることも指定します。

```
editusr administrator pupm_flags(use_original_identity)
editusr administrator pupm_flags(required_checkout)
```

詳細情報:

端末統合 (P. 275)
端末統合の動作のしくみ (P. 277)
端末統合の実装に関する考慮事項 (P. 279)

第 8 章: 特権アカウントの管理

このセクションには、以下のトピックが含まれています。

特権アカウント パスワードの強制チェックイン

現在、1 つ以上のユーザによってチェックアウトされている特権アカウント パスワードを強制的にチェックインできます。

特権アカウント パスワードの強制チェックイン方法

1. [特権アカウント]-[アカウント]-[強制チェックイン]をクリックします。

   [強制チェックイン: 特権アカウントの選択]ページが表示されます。

2. 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特権アカウントのリストが表示されます。[ユーザ別チェックアウト]列は、特権アカウントがチェックアウトされたかどうかおよび誰によってチェックアウトされたかをユーザに通知します

3. チェックインする特権アカウントを選択して、[選択]をクリックします。

   確認のメッセージが表示されます。

4. [はい]をクリックして、変更を確認します。

   CA Access Control エンタープライズ管理 はタスクをサブミットして、アカウントをチェックインします。

特権アカウント パスワードの自動リセット

自動パスワード リセット タスクを使用して、選択した特権アカウントのパスワードをリセットします。開始時に、CA Access Control エンタープライズ管理 は、アカウントに割り当てられたパスワード ポリシーをベースに、選択したアカウントの新しいパスワードを生成します。

重要: アカウントのパスワードをリセットすると、前のパスワードは使用できなくなります。前のパスワードを使用しているユーザは、管理対象デバイスへのログインを継続するために、アカウントをチェックインしてからチェックアウトする必要があります。

注: このオプションは接続解除されたアカウントには有効ではありません。

特権アカウント パスワードの自動リセット方法

1. [特権アカウント]-[アカウント]-[自動アカウント リセット]をクリックします。

   [自動アカウント リセット: 特権アカウントの選択]ページが表示されます。
2. 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特権アカウントのリストが表示されます。
3. リセットする特権アカウント パスワードを選択して、[選択]をクリックします。

   確認メッセージが表示されます。
4. [はい]をクリックして、変更を確認します。

   CA Access Control エンタープライズ管理 は、タスクをサブミットして、アカウント パスワードをリセットします。

特権アカウント パスワードの手動リセット

手動パスワード リセット タスクは、特権アカウントのアカウント パスワードをリセットし、新規パスワードを手動で生成するために使用します。新規パスワードは、選択された特権アカウントに割り当てられたパスワード ポリシーに準拠する必要があります。

重要: アカウントのパスワードをリセットすると、前のパスワードは使用できなくなります。前のパスワードを使用しているユーザは、管理対象デバイスへのログインを継続するために、アカウントをチェックインしてからチェックアウトする必要があります。

手動パスワード リセットの使用は、接続解除されたエンドポイントの特権アカウントを管理する場合のみにすることを強くお勧めします。接続解除されたエンドポイント上でパスワードを変更するたびに、CA Access Control エンタープライズ管理 に格納されているパスワードを変更します。

特権アカウント パスワードの手動リセット方法

1. [特権アカウント]-[アカウント]-[手動パスワード リセット]をクリックします。

   [手動パスワード リセット: 特権アカウントの選択]ページが表示されます。

2. 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特権アカウントのリストが表示されます。

3. パスワードを変更する特権アカウントを選択し、[選択]をクリックします。

   [手動パスワード リセット]ページが表示されます。

4. 新しいパスワードを入力し、確認のために再度入力してから、[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 はタスクをサブミットして、アカウント パスワードを変更します。

特権アカウント例外の削除

*特権アカウント例外*を使用すると、ユーザは、通常はチェック アウトする権限がない特権アカウントをチェック アウトできるようになります。PUPM 承認者が特権アカウント アクセス要求を承認すると、要求者はその要求が有効な期間に特権アカウントをチェック アウトすることができます。例外が適用されるアカウントをユーザがチェック アウトできないように、特権アカウント例外を削除することができます。特権アカウント例外を削除するには、削除するユーザのアカウントにデフォルトの特権アカウント要求権限があるか、PUPM ターゲット システム マネージャ ロールが割り当てられているか、または、このタスクを含む同等のロールである必要があります。

特権アカウント要求を削除するには以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[例外]-[特権アカウント例外の削除]をクリックします。

   [特権アカウント例外の削除: 特権アカウント例外の選択]ページが表示されます。

2. 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特権アカウント例外のリストが表示されます。

3. 削除する特権アカウント例外を選択し、[選択]をクリックします。

   選択した特権アカウント例外を削除するかどうかを尋ねる確認メッセージが表示されます。

4. [はい]をクリックします。

   特権アカウント要求が削除されます。

手動パスワード抽出

アプリケーション サーバが実行されておらず、PUPM が利用できない場合、PUPM を使用して特権アカウントをチェックアウトできません。代わりに、PUPM のパスワード抽出ユーティリティである pwextractor を使用して、データベースから特権アカウント パスワードを抽出できます。次に、それらのパスワードを使用して特権アカウントに通常のユーザとしてログインして、特権アカウント パスワードをバックアップできます。

PUPM が利用できないのでデータベースから特権アカウント パスワードを抽出する場合は、PUPM のリストア時に実行するリカバリ後の手順はありません。

pwextractor のインストールは、エンタープライズ管理サーバのインストール時に行います。デフォルトでは、CA Access Control ルールは pwextractor を保護しませんが、pwextractor を保護するルールは作成できます。

pwextractor を使用するには、以下が必要になります。

- データベース テーブルへのアクセス権
- データベースにアクセスするために PUPM で使用するアカウントのユーザ名およびパスワード

  注: これらのクレデンシャルは、エンタープライズ管理サーバをインストールする際に使用します。

CA Access Control エンタープライズ管理 が実行しているか停止しているかに関わらず、また、アプリケーション サーバが実行しているか停止しているかに関わらず、pwextractor を使用できます。また、pwextractor をリモートで実行することもできます。

注: pwextractor 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: Oracle Database からの特権アカウント パスワードの抽出

以下の例では、Oracle データベースから特権アカウント パスワードを抽出し、ファイル C:¥tmp¥pwd.txt. へ出力を書き込みます。スキーマ名は orcl です。また、データベースはホスト myhost.example.com に配置されています。エンタープライズ管理サーバは Windows コンピュータ上にインストールされています。

```
pwextractor.bat -h myhost.example.com -d orcl -t oracle -l joesmith -p P@ssw0rd -f
C:¥tmp¥pwd.txt
-k
C:¥jboss-4.2.3.GA¥server¥default¥deploy¥IdentityMinder.ear¥config¥com¥netegrity¥c
onfig¥keys¥FipsKey.dat
```

特権アカウントの監査

CA Access Control エンタープライズ管理 が実行する特権アカウント操作に関する高度な詳細情報を検索、表示することができます。詳細画面によって、各タスクおよびイベントに関する追加情報が提供されます。タスクのステータスに応じて、タスクのキャンセルまたは再サブミットを実行できます。

特権アカウントの監査方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[監査]をクリックします。

   [特権アカウントの監査]タスクが使用可能なタスクリストに表示されます。

2. [特権アカウントの監査]を選択します。

   [特権アカウントの監査]タスクが開きます。

3. 検索条件 (P. 308)を指定し、表示する行数を入力して、[検索]をクリックします。

   検索条件に適合するタスクが表示されます。

特権アカウントを監査するための検索属性

処理用にサブミットされたタスクを確認するには、[特権アカウントの監査]で検索機能を使用します。以下の条件に基づいて、タスクを検索できます。

開始者

検索条件となるタスクを開始したユーザの名前を識別します。このユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

承認者

検索条件としてタスク承認者の名前を識別します。このユーザ名に基づいて検索が実行されます。有効なユーザ名を入力したことを確認するには、[検証]ボタンを使用します。

注: タスクのフィルタとして[承認タスク実行者]条件を選択した場合は、デフォルトにより[承認タスクの表示]条件も有効になります。

タスク名

検索条件としてタスク名を識別します。［タスク名］フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を指定し、テキスト フィールドに「エンドポイントの作成」と入力すると、「タスク名 = エンドポイントの作成」という検索条件を指定できます。

アカウント名

検索条件としてアカウント名を識別します。［アカウント名］フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を選択し、テキスト フィールドに「管理者」と入力すると、「アカウント名 = 管理者」という検索条件を指定できます。

エンドポイント タイプ

検索条件としてエンドポイント タイプを識別します。［エンドポイント タイプ］フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を選択し、テキスト フィールドに「Windows エージェントレス」と入力すると、「エンドポイント タイプ = Windows エージェントレス」という検索条件を指定できます。

エンドポイント名

検索条件としてエンドポイント名を識別します。［エンドポイント名］フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。 たとえば、「=」条件を選択し、テキスト フィールドに「exampleHost」と入力すると、「エンドポイント名 = exampleHost」という検索条件を指定できます。

イベント名

検索条件としてイベント名を識別します。［イベント名］フィールドの値として「=」、「以下を含む」、「以下で開始」、「以下で終了」などの条件を指定すると、検索を絞り込むことができます。たとえば、「=」条件を選択し、テキスト フィールドに「CheckInAccountPasswordEvent」と入力すると、「イベント名 = CheckInAccountPasswordEvent」という検索条件を指定できます。

タスクのステータス

検索条件となるタスク ステータスを識別します。タスクのステータスを選択するには、「タスク スタータス =」を有効にし、条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

- 完了
- 実行中
- 失敗
- 拒否
- 一部完了
- キャンセル済み
- スケジュール済み

タスク優先度

検索条件としてタスクの優先度を識別します。 タスク優先度を選択するには、[タスク優先度の条件]を有効にして条件を選択します。以下の条件に基づいて、タスクをさらに絞り込むことができます。

低

このオプションを指定すると、低優先度のタスクを検索できます。

中

このオプションを指定すると、中優先度のタスクを検索できます。

高

このオプションを指定すると、高優先度のタスクを検索できます。

対象期間

サブミット済みタスクの検索範囲を識別します。 サブミット期間フィールドに、[開始日]と[終了日]を指定する必要があります。

サブミットされていないタスクの表示

監査済み状態のタスクを識別します。他のタスクを開始したタスクや、サブミットされていないタスクが識別されます。このチェックボックスを選択した場合、そのようなタスクがすべて監査および表示されます。

承認タスクの表示

ワークフローの一部として承認すべきタスクを識別します。

詳細情報:

タスク ステータスの説明 (P. 51)

タスク ステータスの説明

サブミット済みタスクのステータスは、以下のいずれかになります。タスクのステータスに基づいて、タスクのキャンセルや再サブミットなどのアクションを実行できます。

注: タスクをキャンセルまたは再サブミットするには、タスク ステータスに基づいてキャンセル ボタンと再サブミット ボタンが表示されるように[サブミット済みタスクの表示]を設定する必要があります。

実行中

以下のいずれかが発生した場合に表示されます。

- ワークフローが開始されたが、まだ完了していない場合
- 現在のタスクの前に開始されたタスクが実行中の場合
- ネスト タスクが開始されたが、まだ完了していない場合
- プライマリ イベントが開始されたが、まだ完了していない場合
- セカンダリ イベントが開始されたが、まだ完了していない場合

この状態のタスクはキャンセルすることができます。

注: タスクをキャンセルすると、現在のタスクに関する未完了のネスト イベントとタスクがすべてキャンセルされます。

キャンセル済み

実行中のタスクまたはイベントのいずれかをキャンセルした場合に表示されます。

拒否

CA Access Control エンタープライズ管理 がワークフロー プロセスの一部であるイベントまたはタスクを拒否した場合に表示されます。. 拒否されたタスクは再サブミットすることができます。

注: タスクを再サブミットすると、CA Access Control エンタープライズ管理 によって失敗または拒否されたネスト タスクとイベントがすべて再サブミットされます。

一部完了

一部のイベントまたはネスト タスクをキャンセルした場合に表示されます。一部完了したイベントまたはネスト タスクは再サブミットすることができます。

完了

タスクが完了した場合に表示されます。現在のタスクのネスト タスクとネスト イベントがすべて完了すると、タスクが完了します。

失敗

現在のタスクに含まれるタスク、ネスト タスク、またはネスト イベントが無効の場合に表示されます。このステータスは、タスクが失敗した場合に表示されます。失敗したタスクは再サブミットすることができます。

スケジュール済み

タスクを後で実行するようスケジュール設定されている場合に表示されます。この状態のタスクはキャンセルすることができます。

PUPM のエンドポイントでの監査イベントの表示

PUPM のエンドポイントを CA Enterprise Log Manager と統合すると、個々の特権アカウント セッションについて、エンドポイントでの監査イベントを記録できます。監査イベントは CA Enterprise Log Manager レポートに収集され、ユーザは CA Access Control エンタープライズ管理 からその情報を表示できます。このレポートを使用すると、ユーザが特権アカウントをチェック アウトした後に、そのアカウントが実行するアクションを追跡できます。

CA Enterprise Log Manager レポートを表示できるのは、CheckOutAccountPasswordEvent または CheckInAccountPasswordEvent のイベントに対してのみです。

PUPM エンドポイントの監査イベントを表示する方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[監査]をクリックします。

   [特権アカウントの監査]タスクが使用可能なタスク リストに表示されます。

2. [特権アカウントの監査]を選択します。

   [特権アカウントの監査]タスクが開きます。

3. 検索条件 (P. 308)を指定し、表示する行数を入力して、[検索]をクリックします。

   検索条件に合致するタスクが表示されます。

4. 選択されたタスクについては、[特権アカウントの監査]ページの[セッション詳細]列のアイコンをクリックします。

   注: アイコンが表示されるのは、CheckOutAccountPasswordEvent または CheckInAccountPasswordEvent のイベントに対してのみです。

   CA Enterprise Log Manager レポートが表示されます。このレポートには、選択した特権アカウント セッションの監査イベントが含まれています。

5. [プレビュー]をクリックします。

   レポートが閉じて、CA Access Control エンタープライズ管理 により、対象のタスク リストが示された[特権アカウントの監査]ページが表示されます。

詳細情報:

PUPM エンドポイント上の監査イベント (P. 153)
PUPM エンドポイントを CA Enterprise Log Manager に 統合する方法 (P. 154)

パスワード コンシューマの同期

CA Access Control エンタープライズ管理 でサービス アカウントのパスワードが変更されると、JCS はサービス アカウントに関連付けられている各パスワード コンシューマのパスワード変更を試行します。JCS がパスワード コンシューマのパスワードを変更しない場合、[パスワード コンシューマの同期]を使用してパスワード変更を再試行できます。

パスワード コンシューマの同期方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[パスワード コンシューマ]-[パスワード コンシューマの同期]をクリックします。

   [パスワード コンシューマの同期]タスク ページが表示されます。

2. 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パスワード コンシューマのリストが表示されます。

   注: [エンドポイント タイプ]フィールドの値は、「Windows Agentless」です。これは、PUPM が Windows Agentless エンドポイント上でのみサービス アカウントを管理するためです。

3. 同期するパスワード コンシューマを選択し、[サブミット]をクリックします。

   JCS は、選択されたパスワード コンシューマのパスワードの更新を試行します。

   注: JCS は、パスワード コンシューマの更新を 5 回試行します。JCS がパスワード コンシューマを更新できなかった場合、パスワード コンシューマは非同期としてマークされるので、手動で同期する必要があります。

詳細情報:

PUPM がパスワード コンシューマにパスワードの変更を通知する方法 (P. 148)
パスワード コンシューマの例: Windows スケジュール タスク (P. 265)

エンドポイント管理者パスワードのリストア

管理者パスワードが変更されるたびに、PUPM は、パスワード変更の日時にしたがって、旧パスワードをデータベースに格納します。エンドポイントをバックアップからリストアした場合、エンドポイントでエラーが発生する場合は、現在の管理者パスワードがエンドポイント上で設定されている管理者パスワードと異なります。エンドポイントに接続しログインするには、使用したバックアップの期間と一致するように管理者パスワードをリストアする必要があります。

エンドポイント管理者パスワードのリストア方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]、[エンドポイント]、[エンドポイント パスワード リストア ポイント]タスクを選択します。

   [エンドポイント パスワード リストア ポイント: エンドポイント検索]画面が表示されます。

2. 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。

   検索条件に一致するエンドポイントのリストが表示されます。

3. リストからエンドポイントを選択し、[選択]をクリックします。

   エンドポイントおよび管理者アカウントの詳細が表示されます。

4. [パスワード日付]メニューから、リストアする管理者パスワードを選択します。

   [パスワード日付]メニューには、各パスワードの変更日時がリスト表示されます。使用したバックアップの日付に一番近いパスワードを選択します。

5. [確認]をクリックします。

   PUPM は、パスワードの確認を試行します。成功する場合、確認メッセージが表示されます。

6. (オプション)リセットする追加の特権アカウント パスワードを選択します。

7. [サブミット]をクリックします。

   PUPM は選択されたパスワードをリストアし、そのパスワードを現在の管理者パスワードに設定します。追加の特権アカウントを選択している場合、PUPM はそれらのアカウント パスワードもリストアします。

前の特権アカウント パスワードの表示

エンドポイント エラーの結果として、バックアップからエンドポイントをリストアした場合、エンドポイント上の管理者アカウント パスワードは PUPM データベースに格納されているパスワードと同期されません。エンドポイントにログインまたは接続するには、使用したバックアップ期間からの管理者パスワードを持っている必要があります。

パスワード変更のたびに、PUPM は旧パスワードを格納します。これによって、ユーザは以前使用したパスワードのいずれかを使用して、リストアしたエンドポイントに接続できます。

前の特権アカウント パスワードを表示する方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]、[アカウント]、[以前のアカウント パスワードの表示]を選択します。

   [以前のアカウント パスワードの表示: 特権アカウントの選択]検索画面が開きます。

2. 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エンドポイントおよび特権アカウントのリストが表示されます。

3. リストから特権アカウントを選択し、[選択]をクリックします。

   日付順に並べ替えられたアカウントの詳細およびパスワード履歴が表示された画面が表示されます。

4. リストからエントリを選択し、[パスワードの表示]をクリックします。

   CA Access Control エンタープライズ管理 の画面の最上部に、特権アカウント パスワードが表示されます。これで、パスワードを使用してエンドポイントにログインできるようになりました。

5. [閉じる]をクリックします。

第 9 章: UNAB の使用

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 コンポーネント

UNIX 認証ブローカ(UNAB)は、Active Directory ユーザによる UNIX ホストへのアクセスを管理および制御する、いくつかのコンポーネントで構成されています。

- **UNAB 認証エージェント** -- UNAB 認証エージェント(uxauthd)デーモンは、Active Directory との接続を提供し、ユーザの認証およびログイン権限付与、Active Directory へのホスト登録、ユーザおよびグループの移行、ローカル アクセス ファイルの管理などに関して、Active Directory との安全な接続を保持します。
- **uxconsole** -- xconsole は、Active Directory に UNIX ホストを登録し、ユーザとグループを移行し、UNAB を登録およびアクティブにするために使用する UNAB 管理コンソールです。
- **uxpreinstall** -- uxpreinstall ユーティリティは、UNIX コンピュータが UNAB システム要件に準拠していることを検証します。uxpreinstall ユーティリティは、考えられる問題を診断し、それらの解決方法を提示します。
- **CA Access Control エンタープライズ管理** - CA Access Control エンタープライズ管理 によって、中央の場所から UNAB ホストを管理できます。CA Access Control エンタープライズ管理 を使用すると、Active Directory ユーザによる企業内の各 UNAB ホストへのアクセスの制御、ホスト ログイン権限付与の管理、ホスト移行の競合の解決、およびレポートの生成ができます。

UNAB の設定方法

UNAB（UNIX Authentication Broker）が UNIX ホストへのアクセスを制御する仕組みを理解しておくと、実装および設定プロセス中に役立つ情報を活用することができます。

UNAB を UNIX ホストにインストールしたら、UNAB を Active Directory に登録し、UNAB を起動して、UNIX エンドポイントへのエンタープライズ ユーザの認証を有効にします。次に、移行プロセスを開始して、ローカル ユーザおよびグループを Active Directory に移行します。

1. Active Directory に UNIX ホストを登録します。

   この段階では、UNAB はログイン要求をインターセプトしません。

2. UNIX ホストへのアクセスを許可および拒否するエンタープライズ ユーザを定義します。そのためには、CA Access Control エンタープライズ管理 からログイン認証ポリシーを作成します。

3. UNAB を有効にして、UNIX ホストへのユーザ アクセスを認証できるようにします。

4. UNAB ログイン認証ポリシーにエンタープライズ ユーザおよびグループを追加して、新しいユーザがログインできるようにします。

   この段階で、ローカル ユーザ ストア（etc/passwd など）に定義されたユーザおよび UNAB ログイン認可ポリシーによって許可されたエンタープライズ ユーザのログインが許可されます。

5. ユーザおよびグループを Active Directory へ移行します。

UNAB のユーザ認証の仕組み

UNAB を UNIX ホスト上にインストールして設定した後、ユーザは Active Directory ユーザ アカウントまたはローカル ユーザ アカウントでログインできます（選択した統合モードに従う）。

UNAB が実行されている UNIX ホストにユーザがログインを試みると、以下のイベントが発生します。

1. Active Directory またはローカル アカウントのユーザ名およびパスワードの入力を促すダイアログ ボックスが表示されます。
2. UNAB は、Active Directory、ログイン認証ポリシー、またはローカル ホストのアクセス ファイルでユーザのクレデンシャルを認証し、ユーザのアカウントから取得された追加情報を確認します。
3. ユーザが認証されると、UNAB はユーザに UNIX ホストへのアクセス権限を付与します。認証されない場合、UNAB は、ホストへのユーザ アクセスをブロックします。

UNAB エンドポイント上に格納された情報

UNAB がユーザを認証した後、UNAB はエンドポイント上に以下の情報を格納します。

- ユーザ名
- SHA-1 を使用してハッシュされたパスワード
- ユーザ クラス属性
- ユーザ アカウント コントロール
- 正常な最終ログイン時刻
- 不正な最終ログイン時刻
- 正常な最終ログイン後の不正なログイン回数

NSS データベースが nss.db ファイルにユーザとグループの属性を保存するのに対し、UNAB は logon.db ファイルにユーザの詳細を保存します。両方のファイルは以下のディレクトリにあります。

```
/opt/CA/uxauth/etc
```

ホスト アクセス制御および UNAB 設定の仕組み

CA Access Control エンタープライズ管理 から、UNIX ホストへのユーザおよびグループのアクセスを制御し、UNAB を設定できます。UNIX ホストへのユーザおよびグループのアクセス制御は、ホストへのログインが許可されたユーザおよびグループにのみアクセス権を付与することで行います。

UNAB ホストの設定方法は、ホストへのアクセスを制御する場合と同じです。CA Access Control エンタープライズ管理 を使用して、企業内の UNAB ホストの機能を制御し、それをすべてのホストに適用します。

ユーザおよびグループのログイン権限の付与、またはトークン値の定義を行った後、CA Access Control エンタープライズ管理 は情報をポリシーに変換し、以下の操作を行います。

1. CA Access Control エンタープライズ管理 は、ユーザおよびグループのリストまたは設定パラメータが含まれたデプロイメント パッケージを作成し、そのパッケージを、ポリシーが適用されるホストまたはホスト グループへ割り当てます。
2. CA Access Control エンタープライズ管理 は、ホストに配布するため、パッケージを配布サーバに転送します。
3. UNAB は配布サーバからパッケージを取得し、ポリシーをインストールし、CA Access Control エンタープライズ管理 に確認メッセージを送信します。

注: エンタープライズ ログイン ポリシーおよび UNAB ログイン ポリシーの両方をホストにデプロイした場合、エンタープライズ ログイン ポリシーは UNAB ログイン ポリシーよりも優先されます。

UNAB ログイン認証の管理

UNAB ホストまたはホスト グループへのログインを制御するために、アクセスが許可されたユーザまたはグループのリストを作成します。次に、このリストは、CA Access Control エンタープライズ管理 が選択したホストまたはホスト グループに割り当てデプロイするポリシーへ変換されます。ログイン ポリシー名は「ログイン@*ホスト名*」形式で指定されます。

注: ポリシーのデプロイメント ステータスを表示するには、[デプロイメント監査] タスクを使用できます。

UNAB ログイン認証の管理方法

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. [ポリシー管理]をクリックします。
   b. [UNIX 認証ブローカ]サブタブをクリックします。
   c. 必要に応じて、左側のタスク メニューで[ホスト]または[ホスト グループ]ツリーを展開します。

      使用可能なタスクのリストが表示されます。
2. 以下の*いずれか*の操作を実行します。
   - [ホスト ログイン認証の管理]をクリックします。

     [ホスト ログイン認証の管理: ホスト検索]画面が表示されます。
   - [ホスト グループ ログイン認証の管理]をクリックします。

     [ホスト グループ ログイン認証の管理: ホスト検索]画面が表示されます。
3. 変更するホストまたはホスト グループの名前を入力し、[検索]をクリックします。

   フィルタ条件に一致するホストまたはホスト グループのリストが表示されます。
4. 変更するホストまたはホスト グループを選択し、[選択]をクリックします。

   [ホスト ログイン認証の管理: *ホスト名*]または[ホスト グループ ログイン認証の管理: *ホスト グループ名*]ページが表示されます。

5. （オプション）以下のようにして、ユーザを追加します。
   a. プルダウン メニューから[ユーザ]を選択します。
   b. ユーザの名前を「*ドメイン*/*ユーザ*」の形式で入力します。
   c. ［追加］をクリックします。

      追加したユーザは、[許可されたユーザおよびグループ]リストに表示されます。
6. （オプション）以下のようにして、グループを追加します。
   a. プルダウン メニューから[グループ]を選択します。
   b. 追加するグループの名前を入力します。
   c. ［追加］をクリックします。

      追加したグループは、[許可されたユーザおよびグループ]リストに表示されます。
7. （オプション）以下のようにして、ユーザおよびグループを削除します。
   a. 認証済みユーザおよびグループ リストから、削除するユーザおよびグループを選択します。
   b. ［削除］をクリックします。

      選択したユーザおよびグループは、認証済みユーザおよびグループ リストから削除されます。
8. ［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、ユーザおよびグループの更新済みリストを指定されたホストまたはホスト グループに割り当てます。

UNAB ホストまたはホスト グループの設定

UNAB ホストおよびホスト グループを管理する構成設定を定義できます。CA Access Control エンタープライズ管理 は、UNAB 環境設定ファイル (uxauth.ini) または CA Access Control 環境設定ファイル (accommon.ini) 内の設定値の設定に役立ちます。構成設定の値の設定終了後、CA Access Control エンタープライズ管理 は、更新済み設定値を含む構成ポリシーを作成し、それをホストまたはホスト グループに割り当てます。ポリシーは、「config@ホスト名」形式で命名されます。

注: ポリシーのデプロイメント ステータスを表示するには、[デプロイメント監査] タスクを使用できます。

UNAB ホストまたはホスト グループの設定方法

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. [ポリシー管理]をクリックします。
   b. [UNIX 認証ブローカ]サブタブをクリックします。
   c. 必要に応じて、左側のタスク メニューで[ホスト]または[ホスト グループ]ツリーを展開します。

      使用可能なタスクのリストが表示されます。
2. 以下の*いずれか*の操作を実行します。
   - [UNAB ホストの設定]をクリックします。

     [UNAB ホストの設定: ホストの検索]画面が表示されます。
   - [UNAB ホスト グループの設定]をクリックします。

     [UNAB ホストの設定: ホスト グループの検索]画面が表示されます。
3. 変更するホストまたはホスト グループの名前を入力し、[検索]をクリックします。

   フィルタ条件に一致するホストまたはホスト グループのリストが表示されます。
4. 変更するホストまたはホスト グループを選択し、[選択]をクリックします。

   [UNAB 設定: *ホスト名*]または[UNAB 設定: *ホスト グループ名*]画面が表示されます。
5. 変更するセクションとトークンを選択し、[トークンの追加]をクリックします。

   選択した環境設定トークンが表示されます。

6. 環境設定トークンの値を変更します。

   注: 環境設定トーク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。

7. (オプション) 変更する別のセクションおよびトークンを選択し、[トークンの追加]をクリックし、必要に応じて、環境設定トークンの値を変更します。

8. [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、選択された UNAB ホストまたはホスト グループ上の環境設定トークンの値を設定します。

CA Access Control エンタープライズ管理 のホストへのポリシーのコミットの確認

権限リストと設定リストの作成後、[デプロイメント監査] オプションで、CA Access Control エンタープライズ管理 が変更を UNAB ホストにコミットしたことを確認できます。

CA Access Control エンタープライズ管理のホストへのポリシーのコミットの確認方法

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]タスクを順に選択して、[デプロイメント]オプションを展開します。

   [デプロイメント]オプション メニューが開きます。

2. [デプロイメント監査]オプションを選択します。

   [デプロイメント監査]検索画面が開きます。

3. ホストおよび表示するポリシーを選択して、[実行]をクリックします。

   クエリの検索結果が表示されます。

   注: ログイン ポリシーには、プレフィックス「**login@**」が含まれています。

4. 結果行をクリックして、デプロイメント ステータスを表示します。

   CA Access Control エンタープライズ管理 はデプロイメント タスクのステータスおよび出力を表示します。

ユーザおよびグループを Active Directory に移行する方法

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。

ユーザおよびグループを Active Directory に移行するには、以下の手順に従います。

1. 移行プロセスをエミュレーション モードで実行します。

   エミュレーション モードでは、UNAB はユーザおよびグループを Active Directory に移行しません。見つかった場合、UNAB は競合をログ ファイルに記録します。ログ ファイルは、ユーザおよびグループ属性の競合の可能性について報告します。デフォルトでは、UNAB 競合ファイル（migrate.conflicts）は以下のディレクトリに存在します。

   ```
   /opt/CA/uxauth/log
   ```

2. 競合ファイルをダウンロードします。

   競合ファイルは、CA Access Control エンタープライズ管理 から CVS 形式でホストからダウンロードします。

   注: CSV をダウンロードするには、スケジュールされた次のレポート スナップショットが完了するまで待機する必要があります。

3. Active Directory に移行する各ローカル アカウントに対応する Active Directory アカウントを作成します。

   UNAB は、既存の Active Directory ユーザ アカウントを持っているユーザのみを移行します。

   注: ユーザ アカウントを作成するときに UNIX 属性を指定する必要はありません。Active Directory 内にグループを作成する必要はありません。グループは移行処理中に移行ツールによって作成されます。

4. 競合を解決する CSV ファイルをホストにアップロードします。

   UNAB は移行プロセスを再開し、解決されたアカウントおよびグループを移行します。

5. 移行終了後に移行ファイルを再度確認して、ファイルで前回報告されていたアカウントおよびグループが正常に移行されたことを確認します。

移行競合の解決

UNAB は、移行処理中に検出された競合を競合ファイルに記録します。このファイルには、ローカル ホストから Active Directory へのユーザとグループの移行を妨害した競合の原因の詳細が記録されます。

競合ファイルを CSV ファイルへエクスポートし、スプレッドシートをコンピュータにダウンロードし、競合を調査して解決します。変更したスプレッドシートは、後で再び CA Access Control エンタープライズ管理 にアップロードできます。CA Access Control エンタープライズ管理 はアップロードされたスプレッドシートをメッセージ キューに送信します。UNAB はこのファイルを取得し、移行プロセスを再実行して移行されなかったユーザおよびグループを移行します。

注: ホスト グループを移行すると、競合ファイルをダウンロードできません。しかし、修正された競合ファイルをアップロードして、移行プロセスにおける競合を解決することができます。

移行競合の解決方法

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. [ポリシー管理]をクリックします。
   b. [UNIX 認証ブローカ]サブタブをクリックします。
   c. 必要に応じて、左側のタスク メニューで[ホスト]または[ホスト グループ]ツリーを展開します。

      使用可能なタスクのリストが表示されます。
2. 以下の*いずれか*の操作を実行します。
   - [ホスト移行競合の解決]をクリックします。

     [ホスト移行競合の解決: ホスト検索]画面が表示されます。
   - [ホスト グループ移行競合の解決]をクリックします。

     [ホスト グループ移行競合の解決: ホスト グループ検索]画面が表示されます。
3. 競合を解決するホストまたはホスト グループの名前を入力し、[検索]をクリックします。

   フィルタ条件に一致するホストまたはホスト グループのリストが表示されます。

4. 競合を解決するホストまたはホスト グループを選択し、[選択]をクリックします。

   [UNAB 移行: *ホスト名*]または[UNAB 移行: *ホスト グループ名*] ページが」表示されます。

5. (オプション) ホスト移行用の競合ファイルをダウンロードし、以下の手順で、競合を解決します。

   a. [UNAB 移行競合詳細のダウンロード]セクションで、[エクスポートとダウンロード]リンクを選択します。

      ダイアログ ウィンドウが開きます。

   b. ファイルの保存場所に移動し、[保存]を選択します。

      CSV ファイルが指定された場所へダウンロードされます。

   c. CSV ファイルを開き、ファイル内で報告されている競合を解決し、ファイルを保存して閉じます。

6. (オプション) ホスト グループ移行に関して、競合を解決する CSV ファイルを作成し、保存します。

7. ホストまたはホスト グループの移行の競合を解決する CSV ファイルを、以下のようにしてアップロードします。

   a. [UNAB 移行ソリューションのアップロード]セクションで、[参照]ボタンを選択します。

      ダイアログ ウィンドウが開きます。

   b. ファイルを参照して[開く]をクリックします。

   c. [アップロード]をクリックします。

      ファイルがアップロードされます。

8. [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 はファイルをメッセージ キューに送信します。UNAB はキューからファイルを取得し、移行プロセスを再開して、解決されたアカウントおよびグループの移行を試行します。

9. 移行終了後に移行ファイルを再度確認して、ファイルで前回報告されていたアカウントおよびグループが正常に移行されたことを確認します。

注: Active Directory に同じ名前のユーザまたはグループが存在する場合、ユーザまたはグループを移行することはできません。たとえば、g1 という名前のグループを移行しようとしている場合、Active Directory に g1 という名前のユーザが存在すると、UNAB はそのグループを移行することはできません。

例: UNAB 競合ファイルの出力

以下の例は、移行処理中に作成された UNAB 競合ファイル出力の一部です。

```
*** Conflict Details as found by the CA Access Control UNAB Migration tool at 10/12/29
10:49 ***

***  CRITICAL
Conflicts:
                                                                                ***
***     The next found  conflicts prevent the user/group migration and need the
intervention    ***
***     of the system administrator as they cannot be solved by the migration
tool.                           ***

User 'John' conflicts:
    User 'John' from domain 'development.computer.com' is assigned id '47670' and Unix
id is '300821'
    User 'John' from domain 'development.computer.com' is assigned primary group
'47670' and Unix primary group is '1011'
    User 'John' from domain 'development.computer.com' is assigned home directory
'/home/aletestu' and Unix home directory is '/home/john1'
    User 'John' from domain 'development.computer.com' is assigned shell
'/sbin/nologin' and Unix shell is '/bin/bash'

***  AUTOMATIC
Conflicts:
                                                                              ***
***     Migration tool will try to solve the next found conflicts when run in
"administrative mode",
***
***      if not solved this conflicts will prevent the user/group
migration
Group 'alegcheck' conflicts:
    Cannot add members to Active Directory group 'dev_users' because UNIX group
'dev_users' contains member[s] that do not exist in domain
'development.computer.com'.
      UNIX group 'alegcheck' members: aleucheck1;aleucheck2
User 'John1' conflicts:
    User 'John1' from domain 'development.computer.com' has no UNIX attributes.

***  IGNORED
Conflicts:
                                                                                ***
***     The next found Conflicts are shown for informational purpose,  they will be
ignored for
***      while migration the
user/group
                                                  ***
```

```
User 'John' conflicts:
    User 'John' from domain 'development.computer.com' is assigned gecos '' and Unix
gecos is 'gecos of John'
    User 'John' primary group '1011' was not migrated
```

この例では、UNAB によって以下の重大な競合が報告されました。

- ユーザ 'john' には以下の属性が存在しない
  - ユーザ ID (47670) が UNIX ユーザ ID (300821)と競合する
  - ユーザ プライマリ グループ (47670) が Active Directory グループ (1011)と競合する
  - ユーザ ホーム UNIX ディレクトリ (home/john1) が Active Directory ホーム ディレクトリ設定 (/home/john)と競合する
  - ユーザ UNIX シェル (/bin/bash) が Active Directory シェル属性 (/sbin/nologin)と競合する

UNAB によって以下の競合が報告されました。UNAB は、次回移行プロセス実行時にこれらの競合を解決します。

- UNIX グループ (dev_users) が Active Directory に存在しない
- ユーザ 'john1' に対して UNIX 属性が設定されていない

<una> によって以下のマイナー競合が報告されました。移行プロセス中、<una> はこれらの競合を無視します。

- ユーザ gecos ("") が UNIX 割り当て gecos (john の gecos)と競合する
- ユーザ プライマリ グループ (1011) が移行されていない

例: UNAB 競合解決ファイル

以下の例は、UNAB が競合ファイルで報告した競合を解決するために作成する UNAB 競合解決 CSV ファイルの一部です。CSV ファイルを UNAB ホストに サブミットするには、CA Access Control エンタープライズ管理 を使用します。

ソリューション エンティティ タイプ	ソリューション エンティティ名	ソリューション操作	ソリューション AD マッピング名	競合	UID	ホーム ディレクトリ	GID	所属先	メンバ	GECOS
USER	superuser		root	Group Migration,NO AD	1	/home/superuser/	1			

この例では、競合解決 CSV ファイルには以下が含まれます。

- ソリューション エンティティ タイプ -- USER
- ソリューション エンティティ名 -- superuser
- ソリューション AD マッピング名 -- root
- 競合 -- ユーザ グループが Active Directory に見つからない
- UID -- 1
- ホーム ディレクトリ -- /home/superuser/
- GID --1

注: ユーザの移行の詳細については、「*実装ガイド*」を参照してください。

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、アカウントの詳細情報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入力します。

   ```
   ./uxconsole –manage –find –user <filter>
   ```

   ```
   ./uxconsole –manage –show -detail –user <filter>
   ```

   UNAB は、指定されたオプションに従ってユーザ詳細を表示します。

   注: ワイルドカード文字 (*) を使用できます。

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。

UNAB の停止

UNAB の新バージョンをインストールするか、オペレーティング システムを更新する場合、UNAB を停止する必要があります。

uxauthd.sh スクリプトを停止して、UNAB を停止します。

UNAB の停止方法

1. UNIX コンピュータに root 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。
3. 以下のコマンドを入力します。

   ```
   ./uxauthd.sh -stop
   ```

   UNAB デーモンが停止します。

UNAB ステータスの表示

UNAB の現在のステータスを表示するためにこのオプションを使用します。

UNAB ステータスの表示方法

1. そのコンピュータの管理権限を持っているユーザとして UNIX コンピュータにログインします。
2. UNAB bin ディレクトリに移動します。
3. 以下のコマンドを実行します。

   ```
   ./uxconsole -status -detail
   ```

   UNAB の現在のステータス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。

UNAB デバッグ ファイル

UNAB 環境設定ファイル（uxauth.ini ファイル内の）のエージェント セクションは、実行時にエージェントによって収集されるデバッグ情報を定義します。デフォルトでは、UNAB は以下のファイル内にあるデバッグ情報を収集します。ここで、「*UNABInstallDir*」は UNAB をインストールしたディレクトリです。

UNABInstallDir/log/debug/agent_debug

UNAB 設定ファイルでデバッグ メカニズムが 有効になっている場合、UNAB エージェントは uxauthd デーモンが起動したときにデバッグ メッセージをデバッグ ファイルに記録します。

-debug オプションを使用して UNAB を起動すると、デバッグ メッセージがユーザ コンソールに表示されます。

第 10 章: レポートの作成

このセクションには、以下のトピックが含まれています。

セキュリティ基準

企業の業務環境が紙ベースから電子媒体中心に移行した現在では、電子データは社内と社外の双方から攻撃を受けるという、深刻な状況に直面しています。このような問題に対処するために、いくつものセキュリティ対策が幅広い分野において導入されています。たとえば、一般的なグローバル セキュリティ、財務の正確性と財務報告、個人の資金に関する情報や個人の識別情報の保護、福祉に関する情報の保護、および米国政府機関のセキュリティのベスト プラクティスの標準化などの分野です。

CA Access Control レポート サービスによって実行されているベスト プラクティス レポートの基盤であるセキュリティ基準、法律、および要求事項の概要を以下に説明します。

Payment Card Industry Data Security Standards（PCI DSS、ペイメント カード業界データ セキュリティ標準）

PCI DSS は、詐欺やハッキングなどのセキュリティに関する問題の発生を防止する目的で、大手クレジット カード会社によって策定された業界標準です。クレジット カードやデビット カードのデータの受け付け、記録、保存、送信、または処理を行う企業は、PCI DSS に準拠する必要があります。

Health Insurance Portability and Accountability Act（HIPAA、医療保険の相互運用性と説明責任に関する法律）

HIPAA は、労働者が転職または失業した際にも健康保険を利用できるように保護する米国連邦法です。HIPAA はまた、保健医療関連のデータのセキュリティおよびプライバシーにも対処しています。

Sarbanes-Oxley Act（SOX、サーベンス オクスリー法）

SOX は、財務報告の基準を規定した米国連邦法です。この法律は、すべての米国公開企業の役員会に適用されます。

レポート タイプ

CA Access Control のデータおよびイベントに関する情報は、2 種類の異なるレポートで表示できます。

- CA Access Control レポート - ユーザおよびユーザが実行できるアクションについて記述します。

  CA Access Control レポートは、各エンドポイント上の CA Access Control データベース内のデータ、すなわち、エンドポイント上にデプロイするルールおよびポリシー、およびポリシー偏差に関する情報を提供します。CA Access Control レポートは、CA Business Intelligence および CA Access Control エンタープライズ管理 で参照します。

- 監査レポート - ユーザおよびユーザが実行したアクションについて記述します。

  監査レポートは、各エンドポイント上の監査ログ ファイル（seos.audit）のデータ、すなわち、エンドポイント上でどのユーザがどんなアクションを実行したかに関する情報を提供します。監査レポートは、CA Enterprise Log Manager および CA Access Control エンタープライズ管理 に表示されます。

  注：CA Enterprise Log Manager での監査レポートの表示の詳細については、「*CA Enterprise Log Manager Overview Guide*」を参照してください。

注：CA Access Control レポートおよび CA Access Control 監査レポートを表示するには、追加コンポーネントをインストールし、設定する必要があります。詳細については、「*実装ガイド*」を参照してください。

レポート サービス

CA Access Control レポート サービスを使用すると、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 ステータスを一括して確認できます。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 は、一度の設定だけで各エンドポイントからデータの収集および中央のサーバへのデータのレポートを独立して実行します。また、手動による操作を必要とせず、エンドポイントのステータスを継続的にレポートします。

CA Access Control レポート サービスは、BS 7799/ISO 17799、Sarbanes-Oxley (SOX)、Payment Card Industry (PCI)、Health Insurance Portability and Accountability Act (HIPAA)、Federal Information Security Management Act (FISMA)などの環境で役立ちます。レポート サービスは、何千ものエンドポイントにわたるユーザ、グループ、およびリソースのアクセスにおけるエンドポイントステータスの正確な確認を可能にするソリューションです。

レポート サービスの構造では、各エンドポイントから収集されたデータを問い合わせて取得することが可能です。さまざまな目的に応じてカスタム レポートを作成することも、CA Access Control が独自に提供する既存のレポートを使用することもできます。レポート サービスはサーバに基づくサービスであるため、レポート ストレージを集中させて一元的に管理し、レポートへの安全なアクセス(SSL)を確保することができます。レポート サービスは可用性が高くなるように構成することができます。レポート サービス コンポーネントは単一サーバ上へのインストール、または分散構成のインストールが可能です。

注: レポート サービス コンポーネントは CA Access Control コア機能の外部にあるので、既存の実装を再構成しなくても機能を強化することができます。

レポート サービス コンポーネント

レポート サービスは、以下のコア コンポーネントで構成されています。

- *レポート エージェント*は、CA Access Control または UNAB の各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、配布サーバ上にある設定されたメッセージ キューのキューに情報を送信します。
- *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。レポート用に、メッセージ キューにより、中央データベースとの間で、エンドポイント データベースのスナップショットの双方向の転送が行われます。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。
- *中央データベース*は、レポートなどの CA Access Control エンタープライズ管理 機能の情報を保持するリレーショナル データベース管理システム（RDBMS）です。さまざまなツールを使用することで、データベースに格納された CA Access Control 実装に関するデータを問い合わせて取得できます。
- *レポート ポータル*は、CA Access Control レポートを提供するアプリケーション サーバです。このサーバでは、BusinessObjects InfoView ポータルを使用することで、中央データベースに格納されたレポート情報を対話式で操作できるようにしています。
- CA Access Control エンタープライズ管理 サーバは、メッセージ キューからレポート データを読み取り、中央データベースにデータを格納します。
- 一般的なレポート シナリオ用に、データを簡単に表示できるレポートが組み込まれています。
- Web ブラウザを実行して、レポートの表示と管理を行うコンピュータ。

注: CA Access Control レポート サービスの実装およびアーキテクチャの詳細については、「*実装ガイド*」を参照してください。

レポート サービスの機能

レポート サービスを使用して、CA Access Control および UNAB の各エンドポイント、ユーザ ストア、PUPM ポリシー ストアから収集されたデータを検証することができます。レポート サービスを正しく設定するには、レポート サービスがデータを収集および格納してそのデータからレポートを生成するメカニズムを把握しておく必要があります。

レポート サービスは、以下の処理を行います。

- CA Access Control および UNAB の各エンドポイントからデータを収集します。

  各エンドポイントは、配布サーバ上のメッセージ キューにレポート データを送信します。

- 中央データベースにデータを格納します。

  CA Access Control エンタープライズ管理 は、メッセージ キューからレポート データを取得し、中央データベースに格納します。

- レポート データのスナップショットをキャプチャし、それを中央データベースに格納します。

  CA Access Control エンタープライズ管理 は、スナップショットの一部として PUPM レポート データをキャプチャします。

- 格納されたデータからレポートを生成します。

  中央データベースに利用可能なデータがあれば、レポート ポータルを使用してレポートを生成し、保存されたデータを照会できます。レポート ポータルは、BusinessObjects InfoView ポータルの CA Technologies バージョンです。中央データベースに接続するために設定され、標準の CA Access Control レポートにバンドルされています。

注: レポート サービス アーキテクチャの詳細については、「*実装ガイド*」を参照してください。

各エンドポイントからレポート用のデータを収集する方法

レポートを生成するには、各エンドポイントからデータを収集する必要があります。レポート サービスは、CA Access Control および UNAB の各エンドポイントにインストールされたレポート エージェントを使用して、スケジュールされた時刻に、またはオンデマンドでエンドポイントからデータを収集します。

注: レポート エージェントは、CA Enterprise Log Manager と統合するために、監査データを収集してルーティングする必要もあります。このプロセスでは、レポート エージェントが CA Access Control エンドポイントに関してレポートするために実行するアクションについてのみ説明します。

レポート エージェントは、各エンドポイントで以下のアクションを実行します。

1. 偏差計算を実行し、結果を配布サーバに送信します。

   重要: レポート エージェントが定期的に実行するように設定され、DMS の更新が必要ない場合は、ポリシー偏差計算を別途スケジュールする必要はありません。

2. CA Access Control エンドポイント上で CA Access Control データベース（seosdb）および各 Policy Model データベース（PMDB）のコピーを作成するか、または UNAB エンドポイント上で UNAB データベースのコピーを作成します。

   これはレポート エージェントが使用する一時コピーです。このコピーを使用することで CA Access Control のパフォーマンスに影響を及ぼすことなくデータを処理できます。

3. 各データベースからのデータを XML 構造体にダンプします。

   データベース内のすべてのオブジェクトをダンプします。つまり、データベース インターフェース ユーティリティ（selang など）を介して確認できるデータだけでなくすべてのデータがキャプチャされます。

4. データベースの XML バージョンを配布サーバに送信します。

   レポート エージェントは、配布サーバ上のレポート キューにデータを送信します。

注: レポートのデータは PUPM エンドポイントからは収集されません。

各エンドポイントからのデータを処理および格納する方法

データが各エンド ポイント上で収集されると、そのデータは処理するために配布サーバに送信されます。処理されたデータは、レポートの生成のために中央データベースのストレージに送信されます。

配布サーバは、以下のアクションを実行します。

1. 各エンドポイント上のレポート エージェントから、エンドポイントのデータベース全体の XML ダンプを受信します。
2. データベース スキーマに従って、メッセージ ドリブン ビーン（MDB）を使用して XML ダンプを処理します。

   受信した各 XML ダンプは、中央データベースに配置できるように Java オブジェクトに変換されます。
3. 各 Java オブジェクトを中央データベースに挿入します。

   これで、各エンドポイントからのデータを中央データベースから取得できるようになりました。

注: エンドポイント データは、レポート ポータルから取得する必要があります。つまり、レポートで使用する前に、スナップショットでキャプチャする必要があります。

CA Access Control エンタープライズ管理 でのスナップショットのキャプチャ方法

CA Access Control エンタープライズ管理 では、レポートでデータを使用する前に、エンドポイントのダンプを含むレポート データをスナップショットでキャプチャする必要があります。CA Access Control エンタープライズ管理 でスナップショットをキャプチャしたら、CA Access Control レポートを生成および表示できます。

スナップショット定義で指定された時間に、CA Access Control エンタープライズ管理 では、スナップショットをキャプチャするため以下のアクションを実行します。

- ユーザ ストアから中央データベースへデータを抽出する。
- PUPM ポリシー ストアから中央データベースへデータを抽出する。
- 中央データベース内に存在する最新のエンドポイント スナップショットにフラグを付け、スナップショットに含まれるようにする。

配布サーバへのエンドポイント スナップショットの送信

レポート用にエンドポイントを設定する場合、レポート エージェントがローカル CA Access Control データベースのスケジュール済みスナップショットおよびエンドポイント上の PMDB を収集し、配布サーバ上のレポート キューにスナップショットを送信する時間を指定します。スケジュールされた時間まで待たずに、配布サーバにエンドポイント スナップショットをすぐに送信することもできます。

注: accommon.ini ファイルの ReportAgent セクションまたは CA Access Control レジストリ キーでスケジュール設定を変更することにより、レポート エージェントのスケジュールを変更できます。

必要時に配布サーバにエンドポイント スナップショットを送信する方法

1. エンドポイントでコマンド プロンプト ウィンドウを開きます。
2. (UNIX)ライブラリ パス環境変数を以下のように設定します。
   a. su コマンドで root になります。
   b. *ACSharedDir*/lib にライブラリ パス環境変数を設定します。デフォルトでは、*ACSharedDir* は以下のディレクトリです。

      ```
      /opt/CA/AccessControlShared
      ```

   c. ライブラリ パス環境変数をエクスポートします。
3. (UNIX)以下のディレクトリに移動します。

   ```
   ACSharedDir/bin
   ```

4. エンドポイント上でレポート エージェントを実行します。以下の*いずれか*の操作を実行します。
   - (Windows)以下のコマンドを入力します。

     ```
     ReportAgent - レポート スナップショット
     ```

   - (UNIX)以下のコマンドを入力します。

     ```
     ./ReportAgent -report snapshot
     ```

   レポート エージェントは、CA Access Control データベースのスナップショットおよびローカル PMDB を配布サーバ上のレポート キューに送信します。

注: レポート用にエンドポイントを設定する詳細については、「*実装ガイド*」を参照してください。ReportAgent 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。ライブラリ パス環境変数の詳細については、「*トラブルシューティング 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 にレポートを表示する方法

このプロセスでは、CA Access Control レポートを作成および表示する方法について説明します。これらのレポートでは、PUPM、CA Access Control および UNAB のエンドポイント、ユーザ ストアに関する情報を提供します。また、CA Access Control レポートを CA Business Intelligence に表示することもできます。

CA Access Control エンタープライズ管理 にレポートを表示するには、以下の手順に従います。

1. スナップショット定義を作成します。

   スナップショット定義では、CA Access Control が収集するレポート データを指定し、スナップショットのスケジュールを定義します。

2. レポート用に CA Access Control および UNAB のエンドポイントを設定したことを確認します。

3. (オプション) スナップショット データをキャプチャします。

   スケジュールしたスナップショットが実行されるまで待たない場合、[スナップショットのキャプチャ]を使用すると、スナップショットをすぐに収集できます。

4. レポートを実行します。

   レポートが作成されます。

5. レポートを表示します。

注: スナップショットの定義の作成方法およびレポート用にエンドポイントを設定する方法の詳細については、「実装ガイド」を参照してください。

スナップショット データのキャプチャ

通常、レポート データは、スケジュールされた間隔でスナップショット内にキャプチャされます。スナップショット データ をオンデマンドでキャプチャする場合、[スナップショット データのキャプチャ]タスクを使用し、データをすぐに中央データベースにエクスポートします。

重要: エクスポートするデータが大きい場合、スナップショット データのエクスポートは、処理に時間を要することがあります。レポートするスナップショットに大量のデータが含まれる場合、スナップショット定義を作成し、スナップショットをスケジュールすることをお勧めします。

注: デフォルトでは、スナップショット データをキャプチャするには「システム マネージャ」ロールが必要です。

スナップショット データをキャプチャする方法

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. [レポート]をクリックします。
   b. [タスク]サブタブをクリックします。
   c. [スナップショット データのキャプチャ]をクリックします。

      [スナップショット データのキャプチャ]ページが表示されます。
2. キャプチャ対象とするスナップショット定義の名前を選択し、[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、スナップショット データを中央データベースにエクスポートします。

注: [サブミット済みタスクの表示]を使用すると、タスクの進捗状況を確認できます スナップショット定義を作成する方法の詳細については、「実装ガイド」を参照してください。

CA Access Control エンタープライズ管理 でのレポートの実行

CA Access Control レポートによって、PUPM、CA Access Control および UNAB エンドポイントに関する情報、およびユーザ ストアにあるデータが提供されます。

レポートは、CA Access Control エンタープライズ管理 がスナップショットで取得するデータで構成されています。CA Access Control エンタープライズ管理 がスナップショットを取得した後に、スナップショットのデータがレポートで利用可能になります。レポートを表示するには、まず実行する必要があります。デフォルトでは、レポートを実行するために[システム マネージャ]または[レポート]ロールが必要です。実行するレポート固有の[レポート]ロールが必要です。

注: CA Access Control エンタープライズ管理 では、繰り返されるレポートはスケジュールできません。ただし、CA Business Intelligence では、繰り返されるレポートをスケジュールできます。CA Business Intelligence でレポートをスケジュールする場合、CA Access Control エンタープライズ管理 でそのレポートを表示できません。ただし、CA Access Control エンタープライズ管理 でレポートを実行すると、CA Business Intelligence でそのレポートを表示できます。

CA Access Control エンタープライズ管理 でのレポートの実行方法

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. [レポート]をクリックします。
   b. [言語]サブタブをクリックします。

      [言語]サブタブは、CA Access Control エンタープライズ管理 のインストール言語の名前です。たとえば、CA Access Control エンタープライズ管理 を英語でインストールした場合、英語のサブタブが表示されます。
   c. 左側にあるタスク メニューで、実行するレポート タイプのツリーを展開します。

      レポートのリストが表示されます。
2. 実行するレポートを選択します。

   [パラメータ]画面が表示されます。

3. 必要なパラメータ情報を入力します。

   パラメータ情報を入力する際に、以下を考慮してください。

   - 数値のパラメータを指定し、そのパラメータに数値ではない値を入力すると、レポートは失敗します。
   - パラメータを指定し、中央データベースにそのパラメータの値がない場合、レポートは空になります。

     たとえば、ユーザが 1 つ以上のユーザに関するレポートを定義し、中央データベースにユーザ データが何もない場合、レポートするユーザ データがないので、レポートは空になります。

   注: 複数のパラメータを選択する場合は、Ctrl キーを押しながら、クリックします。

4. [サブミット]をクリックします。

   レポートがレポート サーバにサブミットされます。

詳細情報:

レポートのスケジュール (P. 348)

レポートの表示

CA Access Control レポートでは、PUPM、CA Access Control および UNAB のエンドポイント、ユーザ ストアに存在するデータに関する情報が提供されます。レポートを表示するには、まず CA Access Control を実行する必要があります。

注: CA Access Control エンタープライズ管理 でレポートを表示するには、ユーザのブラウザでサードパーティのセッション Cookie を有効にしてください。デフォルトでは、レポートを表示するには[システム マネージャ]または[レポート]ロールが必要です。

レポートの表示方法

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. [レポート]をクリックします。
   b. [タスク]サブタブをクリックします。
   c. [マイ レポートの表示]タブをクリックします。

      [マイ レポートの表示: レポートの管理画面の設定]が表示されます。

2. 表示するレポートを検索します。

   検索条件に一致するレポートのリストが表示されます。

3. 表示するレポートを選択します。

   レポートが表示されます。

4. (オプション)[Export this report](左上隅)をクリックし、レポートを以下の形式にエクスポートします。

   - Crystal Reports
   - Excel
   - PDF
   - Word
   - RTF

   レポートがエクスポートされます。

スナップショットの管理

CA Access Control エンタープライズ管理 では、スナップショット定義を表示、変更、および削除できます。スナップショット定義を表示または変更する際、[プロファイル]、[反復]、および[メンテナンス]タブが表示されます。[メンテナンス]タブが表示されるのは、スナップショットがいったんキャプチャされた後です。

重要: 複数のスナップショット定義を有効にしないでください。複数のスナップショット定義が有効に設定されている場合、CA Access Control エンタープライズ管理 ではすべてのレポートを正常に実行できません。

スナップショット定義を表示、変更、および削除するには、[レポート]-[タスク]-[スナップショット定義の管理]を選択し、実行するタスクをクリックします。

注: スナップショット定義がレポート データベースにデータをエクスポートするために使用されている場合、このスナップショット定義は削除できません。使用中のスナップショット定義を削除すると、中央データベースへのデータのエクスポートは停止されますが、スナップショット定義は引き続き使用できます。

BusinessObjects InfoView レポート ポータル

*レポート ポータル*は、CA Access Control レポートを提供するアプリケーション サーバです。このサーバでは、BusinessObjects InfoView ポータルを使用することで、中央データベースに格納されたレポート情報を対話式で操作できるようにしています。

レポートを使用するための InfoView の起動

BusinessObjects InfoView を使用して CA Access Control レポートにアクセスします。以下の手順は、レポート インターフェース(BusinessObjects InfoView)にアクセスする方法について説明します。

レポートを使用できるように InfoView を起動するには、以下の手順に従います。

1. 以下の*いずれか*の方法で、InfoView を起動します。
   - BusinessObjects InfoView がインストールされているコンピュータで、[スタート]-[プログラム]-[BusinessObjects XI Release 2]-[BusinessObjects Enterprise]-[BusinessObjects Enterprise Java InfoView]を選択します。
   - 任意のコンピュータのブラウザから、次の URL にアクセスします。

     `http://ACRPTGUI_host:ACRPTGUI_port/businessobjects/enterprise115`

     ACRPTGUI_host は、InfoView がインストールされているコンピュータの名前または IP アドレスです(レポート ポータル)。

     ACRPTGUI_port は、InfoView へのアクセスに使用するポート番号(デフォルトは 9085)です。

   [InfoView Log On]ページが表示されます。
2. InfoView のインストール時に設定したクレデンシャルを入力し、[Log On]をクリックします。

   [InfoView Home]ページが表示されます。

注: BusinessObjects InfoView の使用方法の詳細については、「*BusinessObjects Enterprise XI Release 2 InfoView User's Guide*」を参照してください。

レポートの実行

レポート インターフェース（BusinessObjects InfoView）を開いたら、レポートを選択し、それを実行できるようになります。

レポートを実行するには、以下の手順に従います。

1. InfoView を開きます。

   ［InfoView Home］ページが表示されます。

2. ［Home］-［Public Folders］-［CA Reports］を展開し、左側のフレームにある［CA Access Control］をクリックします。

   CA Access Control ページが表示されます。

3. 表示するレポートのリンク付けされたタイトルをクリックします。

   レポートのページが表示され、表示するレポートの範囲を定義する値を入力できるようになります。

4. フォーム フィールドに値を入力して取得するレポートの範囲を定義し、［OK］をクリックします。

   レポートの出力ページが表示されます。

   追加のクエリを実行して、レポート生成に反映させることができます。たとえば、すべてを含めるように指定したり、特定のホストを選択したりして、既知のすべてのホストまたは単一のホストに基づくレポートを作成できます。さらに、日付範囲を指定して、すべての履歴データを表示したり、特定の日付のデータのみを表示したりできます。

   注：%（パーセント）記号を使用して、ワイルドカード値を指定できます。% の用法は SQL の標準的な選択表記記号で、通常、ワイルドカードを指定する場合のように単一の文字を表すものでは*ありません*。

注：BusinessObjects InfoView の使用方法の詳細については、「*BusinessObjects Enterprise XI Release 2 InfoView User's Guide*」を参照してください。

レポートのスケジュール

レポートを実行するには、さまざまな方法があります。レポート タイトルをクリックし値を指定してレポートを実行することも、さまざまなオプションから選択してレポートをスケジュールすることも可能です。

レポートのスケジュール方法

1. InfoView を開きます。

   [InfoView Home]ページが表示されます。

2. [Home]-[Public Folders]-[CA Reports]を展開し、左側のフレームにある[CA Access Control]をクリックします。

   CA Access Control ページが表示されます。

3. スケジュールするレポートのタイトルの下にある[Schedule]をクリックします。

   選択したレポート用の[Schedule]ページが表示されます。

4. [Run object]ドロップダウン リストの選択内容を修正して、スケジュール対象のレポートをいつ実行するかを指定します。

5. [Parameters]セクションを展開して、レポートを実行するための値を以下のように指定します。

   a. [Empty]をクリックして、パラメータごとに値を定義します。

      [Enter prompt values]セクション フィールドが表示されます。

   b. 必要に応じて値を定義し、[OK]をクリックします。

      定義した値は、レポートの実行時に使用するよう保存されます。

6. 選択したスケジュール オプションに従ってレポートを実行するには、[Schedule]をクリックします。

   設定したレポート スケジュールのインスタンスを確認する[History]ページが表示されます。

注: BusinessObjects InfoView の使用方法の詳細については、「*BusinessObjects Enterprise XI Release 2 InfoView User's Guide*」を参照してください。

作成済みレポートの表示

レポートが生成されると、以下のいずれかの操作を行うことにより、CA Access Control レポートリストから該当するレポートを表示することができます。

- 表示するレポートの[View Latest Instance]をクリックします。
- [History]をクリックし、日付と時刻をクリックして、表示するレポート インスタンスを選択します。

注: BusinessObjects InfoView の使用方法の詳細については、「*BusinessObjects Enterprise XI Release 2 InfoView User's Guide*」を参照してください。

レポート ステータスの表示

スケジュールしたレポートが正常に実行されたかどうかは、レポートのステータスで確認できます。

レポートのステータスを表示するには、以下の手順に従います。

1. InfoView を開きます。

   [InfoView Home]ページが表示されます。

2. [Home]-[Public Folders]-[CA Reports]を展開し、左側のフレームにある[CA Access Control]をクリックします。

   CA Access Control ページが表示されます。

3. 表示するレポートの[History]リンクをクリックします。

   そのレポートの[History]ページが表示され、レポートが実行した日付と時刻のリストを表示できるようになります。

   リスト内の各エントリには、以下の内容が表示されます。

   - [Instance Time]: レポートが実行された日付と時刻
   - [Title]: レポートのタイトル
   - [Run By]: レポートを実行したユーザの名前
   - [Parameters]: 実行したパラメータのために選択されたパラメータ
   - [Format]: レポートの出力形式
   - [Status]: レポートの現在のステータス(成功など)
   - [Reschedule]: レポートを再度実行できるようにするためのリンク

注: BusinessObjects InfoView の使用方法の詳細については、「*BusinessObjects Enterprise XI Release 2 InfoView User's Guide*」を参照してください。

標準レポート

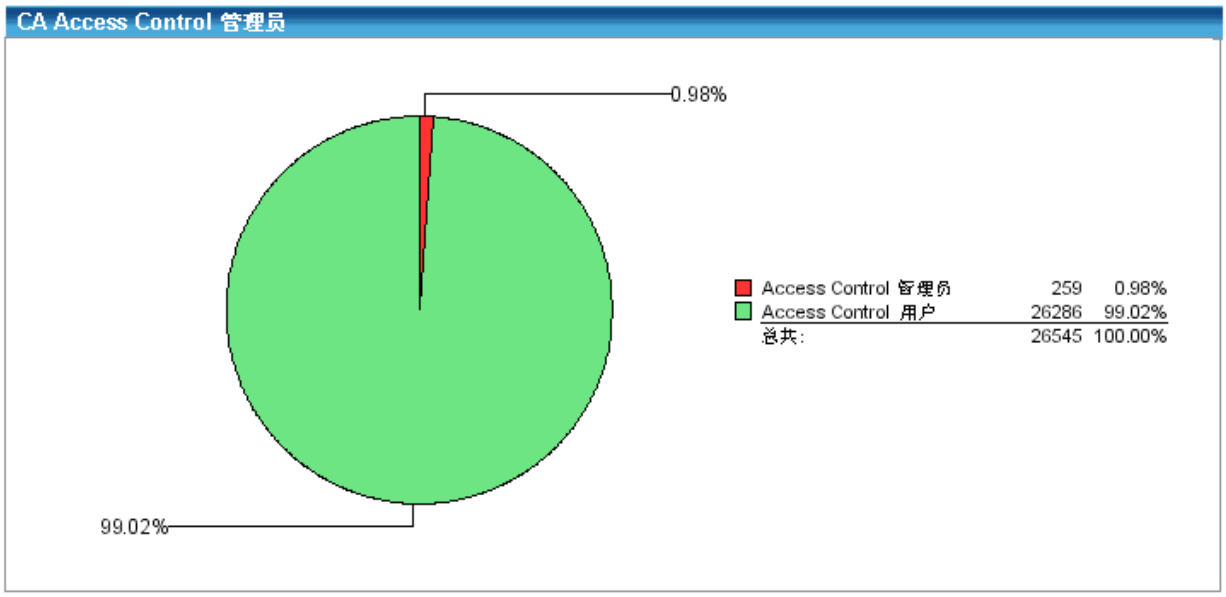
標準では、CA Access Control レポート サービスには、レポート ポータルのインストールの一部としてデプロイされる標準レポートが用意されています。このレポートは、以下のカテゴリに分類されます。

- アカウント管理レポート (P. 352)
- 権限レポート (P. 357)
- その他のレポート (P. 359)
- ポリシー管理レポート (P. 362)
- パスワード ポリシー レポート (P. 366)
- 特権アカウント管理レポート (P. 367)
- UNIX 認証ブローカ レポート (P. 373)

提供されている標準レポートのほかに、レポートをカスタマイズしてさまざまな特長を持つ類似のレポートを作成したり、まったく新しいレポートを生成したりできます。

レポートの表示内容

レポート出力には、適宜、表や図表が使用されます。たとえば、サポートの詳細情報を提供する一方で、一部のレポートにはひとめでわかる円グラフが含まれています。下図に示すように、CA Access Control 管理者レポートには、エンドポイント ユーザの何人が CA Access Control 管理者であるかが円グラフで示されています。一般ユーザに対して管理者の比率が高い場合、セキュリティ上のリスクを招く恐れがあるので、図表によりセキュリティ上の脅威が存在するかどうかが迅速に表示されます。この例では、グラフ内の細長い赤色の V 字形の部分は、現在のエンタープライズ ユーザ ベースのほぼ 1% が CA Access Control 管理を実行できることを示しているため、非常に重要です。



各レポートには、図表に加えて、実際のエンドポイント値を関連付けしたリストも含まれます。CA Access Control の管理者レポートによるこの表のサンプルを以下に示します。

CA Access Control 管理者

ユーザ名	フル ネーム	ホスト ID	管理者モードあり	パスワード管理者モードあり	オペレータ モードあり
_seagent					
		SYSTEMA	はい		
		SYSTEMB	はい		
		SYSTEMC	はい		

アカウント管理レポート

標準的なアカウント管理レポートには、ユーザ アカウントの概要が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なアカウント管理レポートのリストを以下に示します。

CA Access Control 管理者

CA Access Control 管理者レポートには、CA Access Control 管理者権限を持つすべてのユーザのリストが表示されます。これには、ADMIN、PWMANAGER、または OPERATOR 属性を持つユーザが含まれます。レポートには、サマリ データが円グラフで表示され、ユーザ名別の詳細なリストが表形式で表示されます。

CA Access Control を管理できるユーザが多くなると、企業はセキュリティ面でリスクにさらされる恐れがあります。もちろん、評価対象のエンドポイントが開発環境またはテスト環境にある場合、システムのユーザの大部分が CA Access Control 管理者であることはまったく正常であると考えられます。

CA Access Control グループ ユーザ メンバシップ

CA Access Control グループ ユーザ メンバシップ レポートには、ユーザ グループとそのメンバが表示されます。レポートには、詳細が表形式で表示されます。

管理を簡略化するために、CA Access Control 環境内の各ユーザを、現在定義されている 1 つまたは複数の CA Access Control グループのメンバとして取り込むことができます。通常はリソース アクセスがグループに適用されるため、グループ メンバシップは定期的に確認する必要があります。

CA Access Control グループ

CA Access Control グループ レポートには、グループが存在する定義済みホスト、グループの説明、およびネストされたグループと呼ばれる子グループがグループの中に存在するかどうかが表示されます。

企業全体で、どのホストにどのグループが存在しているかを理解しておくと、環境を管理するうえで役に立ちます。さらに、どのグループがほかのグループを含んでいるかを把握しておけば、特定のユーザまたはグループが特定のリソースになぜアクセスできるかを特定する際に役立ちます。

CA Access Control 非アクティブ日

CA Access Control 非アクティブ日レポートには、指定された期間中（たとえば、90 日の間）にログオンしなかったユーザが表示されます。このレポートには、そのようなユーザが一時停止されたかどうか、まだシステムにアクセスできる状態にあるかどうかについても表示されます。レポートには、アカウントが非アクティブで一時停止されているユーザ、およびアカウントが非アクティブで一時停止されていないユーザを強調表示するサマリ円グラフが含まれています。

どのような企業環境であっても、監査において重要なポイントは、環境に対するアクセス権を持っているのはどのユーザか、また最後にアクセスを行ったのはいつかを把握しておくことです。ユーザが最後にリソースにアクセスした日時（たとえばエンドポイントにログインした日時など）に加え、アカウントが非アクティブになっている期間を表示することも必要です。このレポートは、サービス アカウントのアクセス周期を判別する場合や、まだ開いているアカウントのうち、特定の期間アクセスがないものを識別する場合に役立ちます。

CA Access Control パスワード変更

CA Access Control パスワード変更レポートには、指定された期間内にパスワードを変更する必要があるユーザ アカウントのリストが表示されます。レポートにはサマリ円グラフが表示され、パスワードを変更する必要のないユーザ アカウント、パスワードを更新する必要があるユーザ アカウント、パスワードが期限切れになっているユーザ アカウントが示されます。レポートにはまた、ホスト ID およびユーザ アカウントのパスワードの有効期限切れまでの残日など、詳細なデータが表示されます。

しばらく変更されていないパスワードの状態を把握することと同様に、監査では、パスワードの変更が保留になっているユーザのリストを把握する必要もあります。この情報を使用すると、まもなく古くなると考えられるアカウントから、懸案のセキュリティ脅威を特定できます。

CA Access Control パスワード失効

CA Access Control パスワード失効レポートには、指定された日数以内にパスワードを更新していないユーザ アカウントが表示されます。レポートにはサマリ円グラフが表示され、パスワードを更新したユーザ アカウント、パスワードの有効期限切れが原因でシステム アクセスが一時停止されているユーザ アカウント、およびパスワードの有効期限が切れているのに、まだシステムにアクセスしているユーザが示されます。レポートには、過去 X 日にわたりパスワードを変更していないユーザ アカウントに関する詳細が表示されます。たとえば、ホスト ID、最後のパスワード変更日、ユーザ アカウントがまだシステムにアクセスしている理由などが表示されます。

CA Access Control は、パスワードの追加の品質チェック、そして以前のパスワード履歴の保持による、頻繁なパスワードの再使用禁止によって、エンドポイントのパスワード セキュリティの強化が可能です。このコンポーネントの一部として、最後のパスワード変更日が保持されます。このようなパスワード品質モデルのコンポーネントを使用することにより、CA Access Control は企業内のどのユーザが指定の期間内にパスワードを変更していないかを識別できます。このレポートの重要な点は、このレポートを使用することで、しばらく変更されていないパスワードが原因で企業のログイン環境に生じる可能性のある弱点を明らかにできることです。

CA Access Control パスワード ポリシー準拠（アカウント）

CA Access Control パスワード ポリシー準拠（アカウント）レポートには、パスワード長や数字および英字の最低文字数などを規定したパスワード ポリシーに準拠していないパスワードを持つユーザ アカウントが表示されます。レポートにはサマリ円グラフが表示され、ポリシーに準拠しているユーザ アカウント数とポリシーに準拠していないユーザ アカウント数が示されます。レポートにはまた、ポリシーに準拠していないユーザ アカウントの詳細が表形式で表示されます。

CA Access Control パスワード ポリシー準拠（ホスト）

CA Access Control パスワード ポリシー準拠（ホスト） レポートには、パスワード長や数字および英字の最低文字数などを規定したパスワード ポリシーに準拠していないパスワードを持つユーザ アカウントが存在するホストが表示されます。レポートにはサマリ円グラフが表示され、ポリシーに準拠しているホスト数とポリシーに準拠していないホスト数が示されます。レポートにはまた、ポリシーに準拠していないホストおよびそのようなホスト上のユーザ アカウントに関する詳細が表形式で表示されます。

CA Access Control 職務分掌

CA Access Control 職務分掌レポートには、職務分掌のポリシー（たとえば、「ユーザは管理者ユーザ グループと監査担当者ユーザ グループの両方に属することはできない」など）に違反しているユーザ アカウントが表示されます。レポートには、ポリシーに準拠するユーザ メンバとポリシーに準拠しないユーザ メンバとを比較するサマリ円グラフが表示されます。レポートにはまた、ポリシーに準拠しないユーザ アカウントに関する詳細、ホスト ID などが含まれます。

あらゆる企業環境のエンドポイントはすべて、ユーザによる保守を必要とします。この保守作業では、OS およびアプリケーション コンポーネントに対するアクセス権が必要となります。一般的に、システム管理者は OS の観点からコンピュータの保守を行い、アプリケーション管理者はアプリケーションの観点からコンピュータの保守を行います。たとえば、Solaris システム管理者は UNIX ホスト ファイル内のエントリを更新し、Oracle DBA は Oracle データベース内のテーブルの保守を行うなどのケースです。

このモデルの利点は、システム管理者の側からアプリケーションを攻撃することが困難になり、アプリケーション管理者の側からの OS への攻撃も困難となることにあります。システム管理者にアプリケーション管理者も兼任させるというやり方は、一般的に適切ではありません。

このレポートは、ユーザが、異なるロールを表す 2 つのグループに属している場合の潜在的な競合を特定するのに役に立ちます。 このグループ論理積検出は、ISO7799、SOX、PCI、HIPAA、および DoD 用の主要な監査ポイントの 1 つを満たすのに非常に有利です。

CA Access Control ユーザ グループ メンバシップ

CA Access Control のユーザ グループ メンバシップレポートには、環境内の各ホストに対するユーザおよびグループのメンバシップが示されます。このレポートでは、ユーザおよびユーザが属しているグループのホスト別に詳細が表示されます。

CA Access Control ユーザ作成日

CA Access Control のユーザ作成日レポートには、指定されたホストまたは環境内のすべてのホスト上で特定の期間内に作成されたユーザ アカウントが表示されます。このレポートには、ユーザ アカウントが作成された日付の詳細が、ホストおよびユーザ アカウント別に表示されます。

CA Access Control ユーザー時停止日

CA Access Control のユーザー時停止日レポートには、指定されたホストまたは環境内のすべてのホスト上で特定の期間内に一時停止したユーザ アカウントが表示されます。このレポートには、ユーザ アカウントが一時停止された日付の詳細が、ホストおよびユーザ アカウント別に表示されます。

CA Access Control ユーザ更新日

CA Access Control のユーザ更新日レポートには、指定されたホストまたは環境内のすべてのホスト上で特定の期間内に更新されたユーザ アカウントが表示されます。このレポートには、ユーザ アカウントが更新された日付の詳細が、ホストおよびユーザ アカウント別に表示されます。

権限レポート

標準的な権限レポートには、ユーザ権限およびリソース権限の概要が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的な権限レポートのリストを以下に示します。

CA Access Control ベースライン リソース コンプライアンス(ホスト) (P. 357)
CA Access Control グループ権限 (P. 358)
CA Access Control グループ別リソース アクセス (P. 358)
CA Access Control ユーザ別リソース アクセス (P. 358)
CA Access Control ユーザ権限 (P. 359)

CA Access Control ベースライン リソース コンプライアンス(ホスト)

CA Access Control ベースライン リソース コンプライアンス(ホスト)レポートには、指定されたリソースに対してデフォルト以外のアクセスを行うユーザ アカウントが表示されます。レポートには、サマリ円グラフが表示され、デフォルト以外のアクセスが許可されたホストの個数およびデフォルト以外のアクセスを行うユーザ アカウントの総数を示します。レポートにはまた、デフォルト以外のアクセスを行う各ユーザ アカウントについて、アクセス許可の詳細がホスト別に表示されます。

CA Access Control グループ権限

CA Access Control グループ権限レポートには、ユーザ グループがアクセスできるすべてのリソースのリストが表示されます。レポートでは、リソース名別に以下の情報が表形式で詳細に表示されます。

- ホスト ID
- アクセス権限
- アクセスがデフォルトで許可されているか、プログラムを使用することでアクセスが許可されるか
- あらゆる制限。たとえば、カレンダやほかの時間に関する適用可能な制限
- ユーザ グループがリソースを所有しているのでアクセスが許可されるかどうか

このレポートを使用すると、企業全体にわたる定義リソースまたは特定のホストに対する定義リソースにアクセスするユーザ グループを特定することができます。確認後、セキュリティ ポリシーに準拠するようにアクセス権限に変更を加えることができます。

CA Access Control グループ別リソース アクセス

CA Access Control グループ別リソース アクセス レポートには、指定されたリソースについて、ユーザ グループに付与されたアクセス権限が表示されます。レポートには、指定のリソースにアクセスするすべてのユーザ グループに関する詳細なリストが表示されます。たとえば、ホスト ID、アクセス権限、デフォルト アクセスが許可されているかどうか、そのほかの任意の制限(日時指定など)が表示されます。

CA Access Control ユーザ別リソース アクセス

CA Access Control ユーザ別リソース アクセス レポートには、指定されたリソースについて、ユーザ アカウントに付与されたアクセス権限が表示されます。レポートには、指定のリソースにアクセスするすべてのユーザ アカウントに関する詳細なリストが表示されます。たとえば、ホスト ID、アクセス権限、デフォルト アクセスが許可されているかどうか、そのほかの任意の制限(日時指定など)が表示されます。

CA Access Control ユーザ権限

CA Access Control ユーザ権限レポートは、ユーザのアクセス権限をリソース別に表示します。このレポートでは、ユーザがアクセスできる各リソースに対して、ユーザのアクセス タイプ、デフォルト アクセス、リソースにアクセスするためにユーザが使用可能なプログラム、およびユーザのリソースへのアクセスに対する時間帯制限の情報が提供されます。また、ユーザがリソース所有者かどうかも表示されます。

その他のレポート

標準的なその他のレポートには、監視対象ファイル、監視対象プログラム、およびシステムを再起動せずに CA Access Control カーネルをアンロードする UNIX ホストの対応状況に関する情報が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なその他のレポートのリストを以下に示します。

CA Access Control 監視対象ファイル (P. 359)
CA Access Control 監視対象プログラム (P. 360)
アンロードに関する考慮事項がある CA Access Control UNIX ホスト (P. 360)
CA Access ControlUNIX アンロード対応 (P. 361)

CA Access Control 監視対象ファイル

CA Access Control 監視対象ファイル レポートには、企業内のホストにある重要なシステム ファイルの状態が表示されます。レポートには、ファイルが監視されていないホスト、監視状態にあるファイルが変更されているホスト、ファイルが監視状態にあり、かつ信頼状態にあるホストがサマリ円グラフに表示されます。また、ホスト ID など、ファイルに関する詳細も表示されます。これにより、該当するホスト上のファイルに対するポリシーを確認したり、ファイルに対する修正が権限のあるユーザによって行われたかどうかを確認したりできます。

重要なシステム ファイルが確実に監視されるようにすることは、データの整合性を保護するための必須条件です。ファイルに対する変更が行われた日時を把握することで監査証跡が可能になります。結果として、権限のあるユーザが所定のセキュリティ ポリシーに従って変更を行ったことを検証できます。

CA Access Control 監視対象プログラム

CA Access Control 監視対象プログラム レポートには、企業内のホストにある重要なプログラムの状態が表示されます。このレポートには、プログラムが監視されていないホスト、監視状態にあるプログラムが変更されているホスト、およびプログラムが監視され信頼状態にあるホストがサマリ円グラフに表示されます。また、ホスト ID など、プログラムに関する詳細も表示されます。これにより、該当するホスト上のプログラムに対するポリシーを確認したり、プログラムに対する修正が権限のあるユーザによって行われたかどうかを確認したりできます。

重要なプログラムが確実に監視されるようにすることは、データの整合性を保護するための必須条件です。プログラムに対する変更が行われた日時を把握することで監査証跡が可能になります。結果として、権限のあるユーザが所定のセキュリティ ポリシーに従って変更を行ったことを検証できます。

アンロードに関する考慮事項がある CA Access Control UNIX ホスト

アンロードに関する考慮事項がある CA Access Control UNIX ホスト レポートは、CA Access Control カーネルのアンロードを妨げる可能性のある、インターセプトされたシステム コールを持つ UNIX ホストを表示します。これらのホストでは、カーネルのアンロードや CA Access Control のアップグレードを実行する前に、コンピュータを再起動する必要があります。

このレポートでは、アンロードに関する考慮事項がある各ホストに対して、プロセスおよび親プロセス ID、プログラム名、ブロック時間およびしきい値時間がリストされます。また、各システム コールがブロック中かどうかを表示します。

このレポートでは、ホストを以下のカテゴリにまとめます。

- **Not ready（overflow）** - システム コール テーブルはそのサイズを超えます。また、カーネルをアンロードする場合、再起動する必要があります。
- **Not ready（blocking system calls）** - ブロック中のインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動する必要があります。
- **Probable（non-blocking system calls）** - ブロック中ではないインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動は必要ありません。

CA Access ControlUNIX アンロード対応

CA Access ControlUNIX アンロード対応レポートは、システムを再起動せずに CA Access Control カーネルのアンロードおよび CA Access Control のアップグレードを実行する UNIX ホストの対応状況を表示します。

このレポートでは、カーネルをアンロードする準備が完了したホスト、カーネルをアンロードする準備ができた可能性のあるホスト、カーネルをアンロードする準備ができていないホストの割合を示すサマリ円グラフが提供されます。また、各ホストに対してインターセプトされ、かつブロックされていないシステム コールの数を提供します。

このレポートでは、ホストを以下のカテゴリにまとめます。

- **Not ready（overflow）** - システム コール テーブルはそのサイズを超えます。また、カーネルをアンロードする場合、再起動する必要があります。
- **Not ready（blocking system calls）** - ブロック中のインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動する必要があります。
- **Probable（non-blocking system calls）** - ブロック中ではないインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動は必要ありません。
- **Ready** - インターセプトされたシステム コールは存在しません。また、カーネルをアンロードする場合、再起動する必要はありません。
- **Not applicable** - 対象のホストは、UNIX ホストではありません。
- **Unknown status** - ホスト情報が取得できません。

ポリシー管理レポート

標準的なポリシー管理レポートには、ユーザの CA Access Control エンタープライズ管理 ポリシーに関する情報が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なポリシー管理レポートのリストを以下に示します。

CA Access Control ポリシー割り当て

CA Access Control ポリシー割り当てレポートでは、ホストおよびホスト グループ上にデプロイされたポリシー割り当てに関する詳細情報を表示します。このホストおよびホストグループは指定された DMS 上に定義されています。レポートには、以下の情報が提供されます。

- ポリシー名
- 割り当てタイプ (ホストまたはホスト グループ)
- ポリシーをデプロイするホストおよびホスト グループの名前

CA Access Control ポリシー デプロイメント スコアカード

CA Access Control ポリシー デプロイメント スコアカード レポートは、特定のポリシーのデプロイメント情報を表示します。このレポートには、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートではポリシー デプロイメントに関する問題の詳細をホスト別に提供します。

CA Access Control ホスト別ポリシー デプロイメント スコアカード

CA Access Control ホスト別ポリシー デプロイメント スコアカード レポートは、ポリシーのデプロイメント情報をホスト別に表示します。このレポートには、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストまたはホスト グループに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートではポリシー デプロイメントに関する問題の詳細をホスト別に提供します。

CA Access Control ホスト グループ別ポリシー デプロイメント スコアカード

CA Access Control ホスト グループ別ポリシー デプロイメント スコアカード レポートでは、ポリシーのデプロイメント情報をホスト グループ別に表示します。このレポートには、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストまたはホスト グループに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートでは、ポリシー デプロイメントに関する問題の詳細をホスト グループ別に提供します。

CA Access Control ホスト別ポリシー デプロイメント ステータス

CA Access Control ホスト別ポリシー デプロイメント ステータス レポートでは、ポリシーのステータス情報をホスト別に表示します。このレポートには、以下のような各ポリシーのバージョン情報が提供されます。

- 偏差ステータス
- デプロイメント日時
- ポリシーをデプロイしたユーザ名

CA Access Control ホスト グループ別ポリシー デプロイメント ステータス

CA Access Control ホスト グループ別ポリシー デプロイメント ステータス レポートは、ポリシーのステータス情報をホスト グループ別に表示します。このレポートには、以下のような各ポリシーのバージョン情報が提供されます。

- 偏差ステータス
- デプロイメント日時
- ポリシーをデプロイしたユーザ名

また、このレポートではポリシーがデプロイされたホスト グループに存在するホストを一覧表示します。

CA Access Control ポリシー インベントリ

CA Access Control ポリシー インベントリ レポートは、以下のような DMS に格納されたポリシーのスナップショットを表示します。

- 各ポリシーが最後に更新された時間
- ポリシーを最後に更新したユーザ名
- ポリシーがデプロイされたバージョンの数
- 最後にポリシーが確定されたバージョン
- 依存先のポリシー名

注: ポリシーが他のポリシーに依存している場合、依存先のポリシーがデプロイされるまでそのポリシーはデプロイできません。

CA Access Control ポリシー ルール

CA Access Control ポリシー ルール レポートは、ポリシーにある各ルールのデプロイ スクリプトおよびデプロイ解除スクリプトをポリシー名別に表示します。このレポートには、ルールの最終更新日およびルールの最終更新ユーザ名が提供されます。さらに、ポリシーが確定されデプロイメントの準備ができているか、またポリシーのバージョン番号を表示します。

CA Access Control ポリシー バージョン

CA Access Control ポリシー バージョン レポートは、各ポリシーのバージョン情報をポリシー名別に表示します。レポートには、各ポリシーに対して以下の情報が提供されます。

- 現在のバージョン番号
- 現在のバージョンのデプロイ日
- 現在のバージョンをデプロイしたユーザ名

また、このレポートでは現在のバージョンが最終バージョンかどうかを表示します。

CA Access Control ホスト別ルール偏差

CA Access Control ホスト別ルール偏差レポートは、ポリシー ステータスおよびルール偏差をホスト別に表示します。このレポートには、各ホストに存在するポリシーの一覧、および各ポリシーのステータス、バージョン、偏差ステータスが提供されます。このポリシーにルール偏差が存在する場合、レポートには偏差の詳細、つまり偏差の適用先となるリソースおよびプロパティの詳細が提供されます。

CA Access Control ホスト グループ別ルール偏差

CA Access Control ホスト グループ別ルール偏差レポートは、ポリシー ステータスおよびルール偏差をホスト グループ別に表示します。このレポートには、各ホストに存在するポリシーの一覧、および各ポリシーのステータス、バージョンおよび偏差ステータスが提供されます。 このポリシーにルール偏差が存在する場合、レポートにはホスト グループの各ホスト メンバに対する偏差の詳細、つまり偏差の適用先となるリソースおよびプロパティの詳細が提供されます。

パスワード ポリシー レポート

パスワード ポリシー レポートは、CA Access Control で定義されたパスワード ポリシーに関する情報を提供します。

以下は標準パスワード ポリシー レポートのリストです。

パスワード ポリシーによる CA Access Control 特権アカウント (P. 366)
CA Access Control PUPM パスワード ポリシー (P. 367)

パスワード ポリシーによる CA Access Control 特権アカウント

このレポートは、システム内のすべての特権アカウントのリスト、およびそれに対応するパスワード ポリシーを表示します。このレポートを使用すると、どの特権アカウントがどのパスワード ポリシーに関連付けられているかが分かります。レポートを確認した後で、パスワード ポリシーが正しく割り当てられているかどうかを判断し、必要に応じて修正措置を取ることができます。

レポートには、以下の情報が提供されます。

- スナップショット作成日時
- パスワード ポリシー名
- エンドポイントのタイプおよび名前
- アカウント名
- 前回のチェックアウト日
- 前回のパスワード変更

CA Access Control PUPM パスワード ポリシー

このレポートは、その複雑性に従って、現在のパスワード ポリシーを表示します。このレポートを使用すると、既存パスワード ポリシーの最小長および最大長、その他のポリシー パラメータがユーザのセキュリティ基準に適合しているかどうか判断できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日
- パスワード ポリシーの名前および説明
- 最大長
- 最小長
- パスワード ポリシー パラメータ

特権アカウント管理レポート

特権アカウント管理レポートは、特権アカウント管理の詳細を表示します。

以下に、標準的な特権アカウント管理レポートのリストを示します。

エンドポイント別 CA Access Control 特権アカウント (P. 368)
ユーザ別 CA Access Control PUPM ロールおよび特権アカウント (P. 368)
エンドポイント別 CA Access Control 特権アカウント リクエスト (P. 369)
承認者別 CA Access Control 特権アカウント リクエスト (P. 370)
要求者別 CA Access Control 特権アカウント リクエスト (P. 371)
特権アカウント別 CA Access Control PUPM ユーザ (P. 372)
ロール別 CA Access Control PUPM ユーザ (P. 372)

エンドポイント別 CA Access Control 特権アカウント

このレポートでは、エンドポイントのタイプおよびエンドポイント名別に、特権アカウントが一覧表示されます。このレポートを使用することによって、エンドポイントのタイプおよび名前順に、特権アカウントを表示できます。レポートを確認した後で、各エンドポイントに関連付けられている特権アカウントの数を特定できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- エンドポイントのタイプおよび名前
- アカウント名
- 前回のチェックアウト ユーザ
- 前回のチェックアウト
- 前回のパスワード変更

ユーザ別 CA Access Control PUPM ロールおよび特権アカウント

このレポートは、ユーザ アカウントに応じて、特権アクセスロールおよび特権アカウントのリストを表示します。このレポートを使用すると、関連付けられたロールおよびユーザ アカウントに応じて、特権アカウントを確認できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- ユーザ ID
- エンドポイントの時間および名前
- ロールの名前および説明
- アカウント名
- 例外
- 前回のパスワード変更

エンドポイント別 CA Access Control 特権アカウント リクエスト

このレポートは、特権アカウント リクエストのリストが、エンドポイント タイプおよびエンドポイント名別に表示されます。このレポートを使用すると、特権アカウントおよびそれに対応するエンドポイントのタイプおよび名前のチェックアウト リクエストを確認できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- エンドポイントのタイプおよび名前
- ホスト名
- アカウント
- 要求者
- 要求の説明
- 要求時間
- 承認時間
- 有効期間（開始）
- 有効期限
- 承認者
- 承認者コメント

注: レポートにはアクティブな特権アカウントのリクエストのみが表示されます。

承認者別 CA Access Control 特権アカウント リクエスト

このレポートは、承認者に基づいて、特権アカウントリクエストのリストを表示します。このレポートを使用すると、特定のユーザによって承認された特権アカウントリクエストを確認できます。レポート確認し後、承認者ロールを変更するか、ロールにユーザを追加するか、ロールからユーザを削除できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- 承認者ユーザ ID
- エンドポイントのタイプおよび名前
- ホスト名
- アカウント
- 要求者の名前と ID
- 要求の説明
- 要求時間
- 承認時間
- 有効期間（開始）
- 有効期限
- 承認者コメント

注: レポートにはアクティブな特権アカウントのリクエストのみが表示されます。

要求者別 CA Access Control 特権アカウント リクエスト

このレポートは、特権アカウント パスワードを要求したユーザに基づいて、特権アカウントリクエストを表示します。このレポートを使用すると、特権アカウントをチェックアウトするために、ユーザによって作成されたリクエストを確認できます。このレポートの確認後、チェックアウトリクエストの数、およびリクエストを作成したユーザを特定できます。

このレポートには、以下の情報が表示されます。

- スナップショット名
- 承認者ユーザ ID
- エンドポイントのタイプおよび名前
- ホスト名
- アカウント
- 要求の説明
- 要求時間
- 承認時間
- 有効期間(開始)
- 有効期限
- 承認者
- 承認者コメント

注: レポートにはアクティブな特権アカウントのリクエストのみが表示されます。

特権アカウント別 CA Access Control PUPM ユーザ

このレポートでは、エンドポイントのタイプおよび名前に従って、特権アカウントへのアクセス権を持つユーザが一覧表示されます。このレポートを使用すると、ユーザが特権アカウントにアクセスする方法、および各特権アカウントが属しているエンドポイントのタイプと名前を特定できます。

このレポートには、以下の情報が表示されます。

- スナップショット タイプ
- エンドポイントのタイプおよび名前
- 特権アカウント名
- ユーザ名
- ユーザ ID
- リクエスト

ロール別 CA Access Control PUPM ユーザ

このレポートは、ユーザおよびそれらに関連付けられた特権アカウント ロールのリストを表示します。このレポートを使用すると、ユーザが特権アカウント ロールにどのように関連付けられるか特定し、現在のステータスがユーザのセキュリティ条件に適合しているかどうか判断できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- ロール名
- メンバ数
- ユーザ名
- ユーザ ID
- 電子メール アドレス

UNIX 認証ブローカ レポート

UNAB レポートは、UNAB 管理タスクの詳細を表示します。

以下は、標準的な UNIX 認証ブローカ レポートのリストです。

CA Access Control UNAB ホスト別エンタープライズ ユーザ アクセス

このレポートでは、UNAB ホストにアクセスしたエンタープライズ ユーザのリストをホスト別に表示します。レポートには、各ホストにアクセスしたエンタープライズ ユーザ、前回のログイン試行、および誰がホストへのアクセスを許可されたか (ユーザまたはグループ) についての情報が提供されます。このレポートを確認した後、エンタープライズ ユーザがホストに対して持っているアクセス権限を変更できます。

CA Access Control UNAB エンタープライズ ユーザ別ホストへのアクセス

このレポートでは、UNAB ホストにアクセスしたエンタープライズ ユーザのリストをユーザ別に表示します。レポートには、各ホストにアクセスしたエンタープライズ ユーザ、前回のログイン試行、および誰がホストへのアクセスを許可されたか (ユーザまたはグループ) についての情報が提供されます。このレポートを確認した後、エンタープライズ ユーザがホストに対して持っているアクセス権限を変更できます。

CA Access Control UNAB エンタープライズ ユーザ

このレポートでは、ホストへのアクセスが許可されているエンタープライズ ユーザの一覧が表示されます。このレポートには、現在のエンタープライズ ユーザ アカウント、ユーザ ID、ホーム ディレクトリ、およびシェル タイプが表示されます。このレポートを確認した後で、ユーザ パラメータの変更、エンタープライズ ユーザの追加または削除ができます。

CA Access Control UNAB エンタープライズ ユーザ アクティビティ

このレポートには、移行および一部移行されたエンタープライズ ユーザ アカウントのアクティビティリストが表示されます。このレポートを使用すると、UNIX ホスト上でのエンタープライズ ユーザのアクティビティを参照できます。このレポートによって、ユーザごとに前回の成功ログインおよび失敗ログイン、前回の成功パスワード変更などの情報を確認できます。

CA Access Control UNAB エンタープライズ グループ

このレポートには、エンタープライズ グループの属性が表示されます。このレポートは、エンタープライズ グループの詳細（グループ ID など）を提供します。

ホスト グループ別 CA Access Control UNAB ホスト

このレポートでは、UNAB のホストがホスト グループ別に表示されます。このレポートを使用すると、UNAB ホストの現在のグループの概要を把握できます。

このレポートには、以下の情報が含まれています。

- ホスト グループ
- ホスト名
- 合計数

CA Access Control UNAB ローカル グループ移行ステータス

このレポートでは、各グループのエンドポイントでの移行プロセスのステータスが表示されます。このレポートを使用すると、各ホスト上の移行プロセスの現在のステータスを確認できます。

このレポートには、以下の情報が表示されます。

- ホスト名
- 移行ステータス
- グループ名
- グループ ID
- 名前の競合
- GID の競合
- メンバの競合
- Active Directory グループの競合なし
- エントリ数

CA Access Control UNAB ローカル グループの概要

このレポートでは、ローカル グループ プロパティの概要が表示されます。このレポートを使用すると、各 UNAB のホストで同じグループのインスタンスがいくつあるかを把握できます。

このレポートには、以下の情報が表示されます。

- ホスト数
- グループ名
- グループ ID
- インスタンス数

CA Access Control UNAB ローカル ユーザ

このレポートは、ローカル ユーザ パラメータの概要を表示します。このレポートの情報では、単一ユーザアカウントが UNIX ホストに表示されるインスタンスの数が表示されます。

このレポートには、以下の情報が表示されます。

- ホスト数
- ユーザ名
- ユーザ ID
- グループ ID
- ホーム ディレクトリ
- ログイン シェル
- エントリ数

グループ別 CA Access Control UNAB ローカル グループ移行ステータス

このレポートは、ローカル グループの移行ステータスを、グループ別に表示します。このレポートを使用すると、各グループの移行プロセスの現在のステータスを確認できます。

ホスト別 CA Access Control UNAB ローカル グループ移行

このレポートは、ローカル グループの移行ステータスを、ホスト別に表示します。このレポートを使用すると、グループの移行ステータスの詳細をホスト別に表示できます。

CA Access Control UNAB ローカル ユーザ移行ステータス

このレポートは、ローカル ユーザの移行ステータスを表示します。このレポートを使用すると、各ユーザの移行ステータスを表示し、ローカル ユーザ属性とエンタープライズ ユーザ属性を比較できます。

ホスト別 CA Access Control UNAB ローカル ユーザ移行テータス

このレポートは、ローカル ユーザの移行ステータスをホスト別に表示します。このレポートを使用すると、ユーザの移行ステータスをホスト別に表示できます。

ユーザ別 CA Access Control UNAB ローカル ユーザ移行テータス

このレポートは、ローカル ユーザの移行ステータスをユーザ別に表示します。このレポートを使用すると、各ローカル ユーザの移行ステータスを表示できます。

グループ別 CA Access Control UNAB 非標準ローカル グループ

このレポートでは、非標準のローカル グループの情報がグループ別に表示されます。このレポートを使用すると、ローカル属性がエンタープライズ属性と異なるローカル グループの詳細を表示できます。

ユーザ別 CA Access Control UNAB 非標準ローカル ユーザ

このレポートでは、非標準のローカル ユーザの情報がユーザ別に表示されます。このレポートを使用すると、ローカル属性がエンタープライズ属性と異なるユーザの情報を表示できます。

CA Enterprise Log Manager レポート

CA Enterprise Log Manager レポートは、CA Access Control および UNAB のアカウント アクティビティ、リソース管理などに関する詳細情報を表示します。

CA Enterprise Log Manager レポー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。

カスタム レポート

CA Access Control レポートはすべて、Crystal Reports Designer XI を使用して作成されています。これらのレポートは BusinessObjects InfoView を介して Web ベースの形式で提供されます。提供されたレポートをカスタマイズするには、Crystal Reports Designer XI が必要です。

注: 本書の手順説明では、レポートのカスタマイズを開始する際に役立つヒントをいくつか説明します。Crystal Reports Designer XI の詳細については、「*BusinessObjects Enterprise XI Release 2 Designer's Guide*」を参照してください。

CA Access Control Universe for BusinessObjects

CA Access Control Universe for BusinessObjects は、CA Access Control レポート サービスの中央データベースの簡略化ビューを表します。Universe は意味を表すレイヤーであり、データベース内のデータに該当します。このレイヤーは、データベースの複雑な構造からエンド ユーザを分離します。Universe は、クラスおよびオブジェクトの集まりです。

Universe は BusinessObjects Enterprise Designer を使用して作成されます。CA Access Control Universe は、CA Access Control レポート サービスの中央データベースに基づくレポートの作成を簡略化するために、CA Technologies によって提供されています。CA Technologies により開発された CA Access Control Universe は修正しないでください。必要ならば、固有の universe の基礎としてコピーを作成します。

CA Access Control Universe の表示

BusinessObjects Designer を使用して、CA Access Control Universe を表示できます。

CA Access Control Universe を表示するには、以下の手順に従います。

1. [スタート]-[プログラム]-[BusinessObjects XI Release 2]-[BusinessObjects Enterprise]-[Designer]を選択します。

   [User Identification]ダイアログ ボックスが表示され、BusinessObjects Designer にログインできるようになります。

2. クレデンシャルを入力し、[OK]をクリックします。

   Quick Design ウィザードの開始画面が表示されます。

3. [Run this Wizard at Startup]チェック ボックスをオフにし、[Cancel]をクリックします。

   空の Designer セッションが開きます。タイトル バー内にユーザ名およびリポジトリ名が表示されます。

4. [File]-[Open]をクリックし、CA Access Control Universe を含んでいるディレクトリを参照して *CA Access Control.unv* ファイルを選択し、[Open]をクリックします。

   現在の Designer ウィンドウで CA Access Control Universe が開きます。

   注: CA Access Control Universe は、デフォルトの universe ファイル ストアとして指定されたディレクトリ内で *CA Universe¥CA Access Control* の下に格納されています。

標準レポートのカスタマイズ

標準レポートはいずれもカスタマイズすることができます。たとえば、タイトル、色、ロゴ、およびフォントを必要に応じて変更できます。変更を行うには、レポートを Crystal Reports Designer XI で開く必要があります。どのレポートもそれぞれ対応する .rpt ファイルを使用しています。このファイルを開いて、レポートをカスタマイズします。

標準レポートをカスタマイズするには、以下の手順に従います。

1. カスタマイズする .rpt ファイルを Designer で開きます。

   レポートのデザイン ビューが表示されます。

2. 以下の*いずれかの操作を行います*。

   - レポートのタイトルを変更するには、[File]-[Summary Info]をクリックし、[Title]フィールドにタイトルを入力します。
   - テキストをカスタマイズするには、デザイン ビュー内の希望のテキストを強調表示し、それをダブルクリックして編集を行います。
   - テキストの表示方法を変更するには、開いているレポート内のテキストを右クリックして[Format text]を選択し、必要に応じてプロパティを変更します。

3. custom .rpt ファイルを保存します。

   新しいカスタム レポートが保存され、いつでも公開できるようになります。

カスタム レポートの公開

カスタム レポートは、BusinessObjects InfoView を使用して公開する必要があります。

カスタム レポートを公開するには、以下の手順に従います。

1. BusinessObjects InfoView を開き、管理者権限でログインします。

   [InfoView Home]ページが表示されます。

2. [New]-[Folder]をクリックし、[Public Folders]の下に新しいフォルダを作成します。

   [Create A New Folder]タスク ページが表示されます。

3. カスタム レポート フォルダの名前および説明を入力し、[OK]をクリックします。

   新しいフォルダが作成されます。

4. 作成したフォルダで、[New]-[Document from local computer]-[Crystal Report]をクリックします。

   [Add a document from your local computer]タスク ページが表示されます。

5. レポートのタイトルとカスタマイズされた rpt ファイルへのパス名を入力し、[OK]をクリックします。

   カスタム レポートが公開され、BusinessObjects InfoView から表示できるようになりました。カスタム レポートは、ほかの任意のレポートと同様にスケジュールすることもできます。

第 11 章: サンプル ポリシーとベスト プラクティス ポリシーのデプロイ

このセクションには、以下のトピックが含まれています。

サンプル ポリシー

CA Access Control とともに提供されるサンプル ポリシーでは、オペレーティング システムおよびアプリケーション ソース保護のために推奨される、職務分掌およびベスト プラクティスをご紹介しています。各ポリシーは selang スクリプトになっており、その中のコメントによって、ポリシーの目的と含まれているルールが説明されています。

これらのサンプル ポリシーでは、CA Access Control でユーザのシステムを保護するためのベースラインが提供されます。サンプル ポリシーを自分のポリシーのベースとして使用すると、組織のポリシーを作成するプロセスが簡単になります。サンプル ポリシーは、自分のセキュリティ ポリシーおよび環境(インストールされている実際の OS パッケージによって異なるオペレーティング システム ポリシー)に合わせてカスタマイズする必要があります。

サンプル ポリシーをカスタマイズした後で、CA Access Control エンタープライズ管理 を使用してポリシーをエンドポイントへデプロイします。

サンプル ポリシーは以下の共通アプリケーションならびにオペレーティング システムで使用可能です。

- アプリケーション:
  - Apache
  - JBoss アプリケーション サーバ

- CA Access Control Web サービス
- Microsoft SQL Server 2005
- Oracle Database 10g

- オペレーティング システム:
  - AIX
  - HP-UX
  - Red Hat Enterprise Linux
  - SuSE Linux Enterprise Server
  - Sun Solaris
  - Windows 2003
- 仮想化システム:
  - VMware ESX Server
  - Hyper-V
  - Solaris 10 ゾーン

サンプル ポリシーの保存場所

CA Access Control は、サンプル ポリシーを以下のディレクトリにインストールします。

ACInstallDir/samples/Policies/

ACInstallDir

CA Access Control のインストール先ディレクトリを定義します。

この場所には 3 つのサブディレクトリがあります。

- **Applications** - アプリケーション特有のポリシーが含まれています。
- **OS** - オペレーティング システムのポリシーが含まれています。
- **Virtualization** - 仮想システムのポリシーが含まれています。

CA Access Control は、ポリシーをテキスト ファイルとして提供します。このファイルには、ポリシーを実行する selang スクリプトが含まれています。また、各ポリシーには保護ポリシーのデプロイ解除に使用できる一致ポリシーが含まれています。CA Access Control エンタープライズ管理 に対するポリシーのデプロイとデプロイ解除を行います。

サンプル ポリシーの命名規則は *OS_ACTION* です。

OS

ポリシーの設計対象となるオペレーティング システムを定義しています。

ACTION

スクリプトが実行するポリシー アクションを定義しています。

値: deploy または undeploy

たとえば、ファイル「_LINUX40_deploy.txt」の場合、Red Hat Enterprise Linux 4.0 用のサンプル デプロイメント ポリシーが含まれています。

注: アプリケーション ポリシーにデプロイ解除スクリプトはありません。

サンプル ポリシー スクリプト

各ポリシーは selang スクリプトになっており、その中のコメントによって、ポリシーの目的と含まれているルールが説明されています。サンプル ポリシー スクリプトはベスト プラクティスの実例を示すために提供されます。

- コメント

  サンプル ポリシーには注釈が追加されているため、サンプル ポリシーの各セクションで何が実行されるのかを理解するのに役立ちます。

- コンテナ

  サンプル ポリシーでは、関連するリソースを 1 つのコンテナ リソースにまとめています。この方法により、共通のポリシーが関連するすべてのリソースに一度で適用されます。ポリシー ルール(ACL)を個々のリソースに適用する必要はありません。たとえば、ポリシーで 1 つのコンテナを使用して、すべてのシステム環境設定ファイルをまとめることができます。

  ポリシー コンテナでは、命名規則 POL_*container_name* を使用します。これらのコンテナをサブポリシーと見なすことができます。たとえば、OS サンプル ポリシーでは、POL_SYS_CONF コンテナを使用して OS 環境設定ファイルを保護します。

- ロール

  ユーザの管理を簡略化するために、サンプル ポリシーではロールに ACL を適用します。各ロールでは CA Access Control のユーザ グループが使用され、このグループに、実際のユーザを追加できます。

  ポリシー ロールでは、命名規則 ROL_*role_name* を使用します。たとえば、サンプル ポリシーは、adm および lp のような組み込みのシステム ユーザに対して ROL_SYSTEM グループを使用します。多くのポリシーでは、ユーザに(適切なシステム操作に必要な)幅広い権限を割り当てていますが、ユーザがログインに使用できないように権限を無効にすることができます。

- 変数

  デプロイ時に適用する変更を最小限に抑える必要があるため、サンプル ポリシーでは CA Access Control 変数を使用します。サンプル ポリシーは、組み込み変数を使用してローカルのシステム リソース(例えば、ローカル ホストの端末ルール)を保護します。また、ポリシーの変更を簡略化するためにユーザ定義の変数も使用します。たとえば、ユーザ定義の変数に管理者ユーザのホーム ディレクトリを含めることができます。管理者ユーザが別のホーム ディレクトリを使用する場合、ユーザ定義の変数を一度書き換えるだけで、影響を受けるすべてのルールが自動的に変更されます。

例: ポリシー スクリプト コメント

以下の Solaris SPARC 9 サンプル ポリシーのコードの抜粋では、サンプル ポリシーにどのようにコメントが追加されているかを示しています。selang 構文ルールを使用しているため、ハッシュ記号 (#) から始まる行がコメントです。

```
#
# * Home Directories Protection Policy *
#**************************************
#
# This policy uses the FILE class to protect the home
# directories of sensitive users so that only the owner
# of each directory can access it.
#
# Prerequisites:
#□□□□□None
#
# Roles:
#□□□□□None
#
# Containers:
#□□□□□POL_HOME_DIR□□□□□□- home directories of sensitive users
#
```

```
# define container POL_HOME_DIR
# Protect home directories
editres   CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC Sample - Protect home directories")
authorize CONTAINER POL_HOME_DIR uid(* _undefined)   access(NONE)
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr  < ! (USER_OS_ADMIN> )
# define specific FILE resources and connect them with POL_HOME_DIR
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE>  comment("AC Sample")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

例: サンプル ポリシーのコンテナ

以下の selang 出力は、POL_SYS_FILES のプロパティを示しています。AIX サンプル ポリシーには、システム ファイルを保護するこのサブポリシーが含まれています。

```
AC> sr container POL_SYS_FILES
Data for CONTAINER 'POL_SYS_FILES'
------------------------------------------------------------------------
ACLs□□□□□□□□□□□□□□□□:
□□□□Accessor□□□□□□□□□□□□□□□□□□□□Access
□□□□ROL_SYSADMIN□□(GROUP□□)□All
□□□□ROL_SYSTEM□□□□(GROUP□□)□All
□□□□*□□□□□□□□□□□□□□(USER□□□)□R, Chdir
□□□□_undefined□□□□(USER□□□)□R, Chdir
Members□□□□□□□□□□□□:
□□□□/boot/*□□□□□□□(FILE□□)
□□□□/dev/kmem□□□□□(FILE□□)
□□□□/dev/mem□□□□□□(FILE□□)
□□□□/dev/port□□□□□(FILE□□)
Audit mode□□□□□□□□: Failure
Owner□□□□□□□□□□□□□: +nobody□□□□□□□(USER□□)
Create time□□□□□□□:□10-Dec-2008 10:32
Update time□□□□□□□:□10-Dec-2008□10:35
Updated by□□□□□□□□: root□□□□□□□□□□(USER□□)
Comment□□□□□□□□□□□: AC Sample - Protect OS system files
```

例: サンプル ポリシーの変数

以下の Red Hat Enterprise Linux 5 サンプル ポリシーのコードの抜粋では、サンプル ポリシーでどのように変数が使用されているかを示しています。この例では、サンプル ポリシーはローカル ホストおよび管理者ユーザ root のホーム ディレクトリの名前の候補を定義しています。

```
#
# * AC Variables Definitions *
#****************************
#
# The rules in this section define variables that policies use.
# Variables:
#     LOCALHOST             : list of possible names for local host
#     POLICY_AUDIT_MODE     : set policies audit mode
#     POLICY_DEFACCESS      : set defaccess of policies` resources
#
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("POLICY_AUDIT_MODE")   value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS")    value("ALL")     type(static)
```

詳細情報:

ユーザ定義変数 (P. 116)
組み込み変数 (P. 117)
変数使用のガイドライン (P. 118)
エンドポイントで変数を解決する仕組み (P. 121)

準拠ポリシーとベスト プラクティス ポリシー

準拠ポリシーとベスト プラクティス ポリシーにより、エンドポイント上に迅速に準拠ポリシーとベスト プラクティス ポリシーをデプロイできます。各ポリシーは 1 つの selang スクリプトであり、ポリシーの目的を説明するコメント、含まれるルール、および使用される変数が含まれています。

ポリシーは、Payment Card Industry Data Security Requirements and Security Assessment Procedures（PCI DSS）standard、および VMWare VSphere Hardening Requirements に準拠しています。

準拠ポリシーとベスト プラクティス ポリシーは、以下のオペレーティング システムおよび仮想化プラットフォームで使用できます。

- オペレーティング システム
  - Red Hat Advanced Server Linux
  - SuSE Linux
  - SLES
  - AIX
  - HP-UX
  - Solaris
  - Windows 2003 R2
  - Windows 2008 R2
- 仮想化プラットフォーム
  - VMWare サーバ ESX
  - Solaris 10 の Solaris ゾーン
  - Hyper-V

準拠ポリシーとベスト プラクティス ポリシーの格納場所

エンタープライズ管理サーバでは、インストール中に準拠ポリシーとベスト プラクティス ポリシーが DMS に格納されます。これは、エンタープライズ管理サーバの更新インストールをデプロイする際に自動的に行われます。

準拠ポリシーとベスト プラクティス ポリシーの管理は、「ポリシー管理」セクションで CA Access Control エンタープライズ管理 から行います。

個々の新しい CA Access Control インストールでは、準拠ポリシーとベスト プラクティス ポリシーは以下の場所に格納されます。

ACInstallDir/samples/Policies/OutOfTheBox

ACInstallDir

CA Access Control のインストール先ディレクトリを定義します。

CA Access Control は、ポリシーをテキスト ファイルとして提供します。このファイルには、ポリシーを実行する selang スクリプトが含まれています。また、各ポリシーには保護ポリシーのデプロイ解除に使用できる一致ポリシーが含まれています。CA Access Control エンタープライズ管理 に対するポリシーのデプロイとデプロイ解除を行います。

サンプル ポリシーの命名規則は *REGULATION_ACTION* です。

REGULATION

ポリシーの設計対象となる規則の名前を定義します。

ACTION

スクリプトが実行するポリシー アクションを定義しています。

値: deploy または undeploy

たとえば pci_dss_7.1.1_deploy.txt には、PCI DSS セクション 7.1.1 のサンプル デプロイメント ポリシーが含まれています。

注: 準拠ポリシーとベスト プラクティス ポリシーは OS に依存せず、Windows および UNIX のシステムで使用できます。

準拠ポリシーとベスト プラクティス ポリシーのスクリプト

各ポリシーは 1 つの selang スクリプトであり、ポリシーの目的を説明するコメント、および含まれるルールが含まれています。

- コメント

  サンプル ポリシーには注釈が追加されているため、サンプル ポリシーの各セクションで何が実行されるのかを理解するのに役立ちます。

- 変数

  準拠ポリシーとベスト プラクティス ポリシーはオペレーティング システムには依存しません。ただし、リソース グループはシステムによって異なります。この問題を解決するため、リソースリストは変数が使用され、ACL ではポリシーの変数が使用されます。エンタープライズ管理サーバにエンドポイントが接続されると、そのエンドポイントはオペレーティング システムに応じて一致するホスト グループへ自動的に追加され、ポリシーがエンドポイントへデプロイされます。

- ロール

  ユーザの管理を簡略化するために、サンプル ポリシーではロールに ACL を適用します。各ロールでは CA Access Control のユーザ グループが使用され、このグループに、実際のユーザを追加できます。

  ポリシー ロールでは、命名規則 ROL_*role_name* を使用します。たとえば、サンプル ポリシーは、adm および lp のような組み込みのシステム ユーザに対して ROL_SYSTEM グループを使用します。多くのポリシーでは、ユーザに(適切なシステム操作に必要な)幅広い権限を割り当てていますが、ユーザがログインに使用できないように権限を無効にすることができます。

例: 準拠ポリシーとベスト プラクティス ポリシーのコメント

PCI_DSS_7.1.1 準拠ポリシーからの以下の断片には、準拠ポリシーとベスト プラクティス ポリシーにどのような注釈が付けられているのかが説明されています。selang 構文ルールを使用しているため、ハッシュ記号 (#) から始まる行がコメントです。

```
#
# * 2. Protect <!USER_OS_ADMIN> Logon and Access Control Administration *
# ************************************************************************
#
# This section uses the TERMINAL class to restrict administrator users from
# logging in directly (read access). Access Control administration is blocked as
# well (write access).
#
# To separate security administration from system administration, the policy
# sets READ access only to these special terminals.
#
editres   TERMINAL ("<!HOSTNAME>") audit(ALL) warning
authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(READ)
# The following line is commented because the warning mode in UNIX is not
# applicable for write access to class TERMINAL.
#authorize TERMINAL ("<!HOSTNAME>") uid("<!USER_OS_ADMIN>") deniedaccess(WRITE)
```

例: 準拠ポリシーとベスト プラクティス ポリシーのロール

PCI_DSS_7.1.1 準拠ポリシーからの以下の断片には、ポリシーによりロールに対してどのように ACL が適用されているのかが説明されています。

```
#
# * 1. Role Definitions *
# ***********************
#
# The rules in this section define the roles that the policy uses.
#
#  * Define built-in OS users with the logical property. This prevents users
#    from logging in to the system.
#  * Create the user +nobody in CA Access Control only. CA Access Control
#    sets this user as the owner of many resources (to disable ownership
#    bypass). You cannot create this user in the native OS.
#  * Create at least one user in ROL_AC_ADMIN. Without this user you cannot
#    login into CA Access Control.
#    Note: By default, the rules add the superuser account to ROL_AC_ADMIN.
#          We recommend that you remove this user and add security
#          administrators to this group.
# Roles:
#     ROL_SYSTEM        : built-in OS users
#     ROL_SYSADMIN      : system administrators
#     ROL_RESTRICTED    : restricted users with permissions for specific tasks
#     ROL_AC_ADMIN      : CA Access Control administrators
#     ROL_AC_AUDITOR    : CA Access Control auditors
#     ROL_AC_OPERATOR   : CA Access Control operators
#     ROL_AC_SERVICE    : CA Access Control service managers
#     ROL_AC_PWMANAGER  : CA Access Control password managers
#

editgrp (ROL_SYSTEM ROL_SYSADMIN ROL_RESTRICTED ROL_AC_ADMIN ROL_AC_AUDITOR
ROL_AC_OPERATOR ROL_AC_SERVICE ROL_AC_PWMANAGER)
chgrp (ROL_SYSADMIN ROL_AC_ADMIN) audit(LOGINSUCCESS LOGINFAILURE FAILURE)
editusr (+nobody) comment("AC OOTB - Resource owner used for disabling ownership
bypass")
chusr (+nobody) owner(+nobody)
join ("<!USER_OS_ADMIN>") group(ROL_SYSTEM)
join ("<!USER_OS_ADMIN>") group(ROL_AC_ADMIN)
```

ポリシー デプロイメント

CA Access Control ポリシーをデプロイする場合、エラーを発生させずに正常にポリシーのデプロイおよび実行を行うために、いくつかの共通手順に従う必要があります。以下のセクションでは、サンプル ポリシーのデプロイ前またはデプロイ後に実行する必要があるアクションについて説明します。

ポリシー デプロイメントのためにエンドポイントを準備する方法

ポリシーを実装する前に、ポリシーのエンドポイントを準備する必要があります。実行すると、このポリシーに関連する問題を後で分離することができます。

ポリシー デプロイメントのためにエンドポイントを準備する方法

- オペレーティング システムまたはアプリケーションの新規インストールを使用する

  OS ポリシー用に、製造者から提供された OS の最新バージョンおよびパッチを使用します。これにより、変更によってシステムの安全性が潜在的に損なわれる前に、システムを保護することができます。ポリシーを適用した後、パッチを適用したり、必要に応じてシステムを設定し、悪意のある変更や偶発的な変更からシステムを保護することができます。アプリケーションにも同じことがあてはまります。

- 職務分掌を実装する

  ポリシー ルールを確認し、必要に応じて他のロールを追加します。ロール、ユーザおよびそれらの関係(ロール メンバシップ)を定義する独自のポリシーを作成します。サンプル ポリシーのデプロイ前または後にこのポリシーをデプロイできます。

  単一ユーザに必要以上の権限を割り当てていないことを確認してください。たとえば、デフォルトではスーパーユーザが CA Access Control 管理者権限を提供する ROL_AC_ADMIN に追加されています。最良の方法として、このユーザを削除し、代わりにセキュリティ管理者をこのグループに追加することをお勧めします。

- 新しい CA Access Control データベースの作成する、または既存のデータベースをバックアップする

  ポリシーを実装する前に、新しいデータベースを作成します。これにより、ポリシー ルールの競合またはデータベースの既存ルールへの変更が発生しないようになります。新しいデータベースを作成することができない場合、データベースをバック アップし、そのバックアップを使用してポリシー適用前の状態にリストアできるようにしてください。

- ユーザに適切な管理ロール(システム管理者、セキュリティ管理者、アプリケーション管理者)を割り当てる。

- 新しい監査ログ ファイルを使用する

  既存の監査ログ ファイルをバックアップし、それを消去します。これによって、新しいイベントをログに記録する際、CA Access Control は新しい監査ログ ファイルを作成します。監査ログ ファイルにはデプロイするポリシーに関連したイベントのみが記録されているため、このポリシーに関連する問題の確認および分離を迅速に行うことができます。

- CA Access Control ユーザ定義変数を設定する

  設定済みの CA Access Control 変数の値(「AC Variables Definitions」セクション)を検証し、使用中の環境に一致させるか、または必要に応じて値の追加、変更を行います。

段階的なポリシーのデプロイ方法

ポリシーをデプロイする際、いくつかのアクションを実行することで、ポリシーのデプロイおよびポリシーの実行をエラーを発生させず、正常に行うことができます。ポリシーをデプロイするためにエンドポイントを準備した後、段階的にポリシー デプロイメントを実行することをお勧めします。

ポリシーは最初にテスト環境にデプロイし、必要に応じてポリシーを調整してから実稼働環境へデプロイすることをお勧めします。

段階的な方法でポリシーをデプロイする方法

1. ポリシーを警告モードでデプロイします

   現在、このポリシーはアクティブですが、そのルールは適用されません。そのため、ポリシーを有効にする前に、対象となるポリシーの結果を監査ログでプレビューすることができます。

   注: サンプル ポリシー クリプトでは、すべてのポリシー ルールがデフォルトで警告モードに設定されています。

2. 警告メッセージがあるかどうか CA Access Control 監査ログを確認します

   ポリシーをデプロイした後、ポリシー違反があれば警告として監査ログに表示されます(ポリシー ルールが警告モードを使用している場合)。

3. 実際のシナリオでシステムを使用し、再び監査ログを分析します。

   ポリシーを効果的にテストするために、コンピュータ上で通常の操作手順を実行することができます(ログイン、サービスおよびアプリケーションの起動、停止など)。次に、監査ログを再度分析し、新しい警告が表示されているかどうかを確認することができます。

4. 必要に応じてポリシーを調整します。

   監査ログから収集した情報を使用して、実際の環境で想定される使われ方に合わせてポリシーを調整できます。

5. ポリシーを有効にするために、警告モードを削除します

   本稼働環境でポリシーのルールを適用する準備ができたら、ルールを有効にするために警告モードを削除できます。

   ポリシーが適用されます。

注: ポリシーを変更する場合、まずポリシーの適用を無効にします(警告モードを使用します)。ポリシーに変更を加えた後、変更が希望どおりに機能していることが確認できたら、ポリシーを再度有効にします。

詳細情報:

ポリシー デプロイメント (P. 395)
環境に合わせてポリシーをカスタマイズする方法 (P. 396)
サンプル ポリシー適用の有効化 (P. 397)

ポリシー デプロイメント

サンプル ポリシーおよびベスト プラクティス ポリシーには CA Access Control の変数が含まれているため、これらのポリシーは拡張ポリシー管理方法を使用してデプロイする必要があります。

注: エンドポイント上で、selang でサンプル ポリシー ファイルを直接実行することはできません。

CA Access Control エンタープライズ管理 を使用して、DMS 上にサンプル ポリシーを格納し、必要に応じて複数のエンドポイントに割り当てます。

詳細情報:

拡張ポリシー管理 (P. 74)
ポリシーを作成しデプロイする方法 (P. 96)

環境に合わせてポリシーをカスタマイズする方法

サンプル ポリシーおよびベスト プラクティス ポリシーは、独自のセキュリティ ポリシーのベースとして提供されます。ポリシーをデプロイするには、環境に合わせてポリシーをカスタマイズする必要があります。

環境に合わせてポリシーをカスタマイズする方法

- CA Access Control およびシステム ログ ファイルを確認します。

  デプロイメント プロセス中に発生した警告およびエラーの検索、識別を行い、これらの原因となるポリシーを修正します。

- ユーザをポリシー ロールに追加します。

  ポリシーでは、許可のためにロールが使用されます。そのため、組織のユーザをロールに割り当てる必要があります。

  重要: ポリシーをデプロイ解除する場合、作成したユーザおよびグループを削除しないでください。削除すると、同じユーザおよびグループを使用する他のポリシーで、ACL リストの正常な動作やアクセサの関連付けに影響を及ぼす場合があります。

- (Windows のみ) 共存ユーティリティ eACoexist.exe を実行します。

  このユーティリティは、CA Access Control と他のインストール済みプログラムの間で発生した競合を識別し、そのプログラムにバイパスを作成することによって競合を解決します。

サンプル ポリシー適用の有効化

デフォルトでは、サンプル ポリシー スクリプトはすべてのポリシー ルールを警告モードに設定します。このポリシーをデプロイする際、ポリシーはアクティブですが、そのルールは適用されません。ポリシーに習熟し、必要に応じてポリシーをカスタマイズしたら、ポリシーを有効にしてポリシー ルールを適用できます。

注: この手順では、単一のポリシーの適用を有効にする方法について説明します。システム メンテナンスの実行後に複数のポリシーの適用を有効にする方法については、お使いのオペレーティング システム用の「*エンドポイント管理ガイド*」を参照してください。

サンプル ポリシーの適用を有効にする方法

1. ポリシー スクリプトを編集して、**warning** の各インスタンスを **warning-** に変更します。

   リソースまたはアクセサに warning を設定するルールを実行すると、CA Access Control はリソースまたはアクセサに警告モードを追加します。

2. 編集したポリシーをデプロイします。

   ポリシーの適用が無効になります。

例: Windows サンプル ポリシーの適用の有効化

以下の例は、Windows 用のサンプル JBoss ポリシーの一部です。「warning」が「warning-」に変更されているため、このポリシーは有効になっています。

```
# Protect JBoss files
# -------------------

# Protect JBoss files in the application directory.
# These rules apply protection to files that are not protected by other rules.
editfile    ("<!JBOSS_HOME>¥*") owner(nobody) defaccess(NONE) warning- comment ("AC
Sample - JBoss base dir")
authorize FILE ("<!JBOSS_HOME>¥*") id(ROL_JBOSS_ADMIN) access(ALL)
via(pgm("<!JBOSS_HOME>¥bin¥*"))
authorize FILE ("<!JBOSS_HOME>¥*") id(jboss_pgm)       access(READ,CHDIR)
via(pgm("<!JBOSS_HOME>¥bin¥*", "<!JBOSS_JAVA_PGM>"))
```

サンプル ポリシー適用の無効化

デフォルトでは、サンプル ポリシー スクリプトはすべてのポリシー ルールを警告モードに設定します。ポリシーの適用を有効にするには、警告モードを削除します。ポリシーの適用を無効にするには、警告モードに再設定する必要があります。

注: この手順では、単一のポリシーの適用を無効にする方法について説明します。システム メンテナンスの実行時に複数のポリシーの適用を無効にする方法については、お使いのオペレーティング システム用の「*エンドポイント管理ガイド*」を参照してください。

サンプル ポリシーの適用を無効にする方法

1. ポリシー スクリプトを編集して、**warning-** の各インスタンスを **warning** に変更します。

   リソースまたはアクセサに warning を設定するルールを実行すると、CA Access Control はリソースまたはアクセサを警告モードに設定します。

2. 編集したポリシーをデプロイします。

   ポリシーの適用が無効になります。