CA Access Control for Virtual Environments

エンタープライズ管理ガイド

r2.0

ca technologies

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。

- [set the eACee variable for your book]
- CA Access Control
- CA User Activity Reporting Module
- 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*}

形式	意味
…	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。

- *ACVEInstallDir* -- CA Access Control for Virtual Environments のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer/VirtualAppliance
- *ACInstallDir* -- CA Access Control のデフォルトのインストール ディレクトリ。
  - [set the alternate Installation Path variable]
- *ACSharedDir* -- CA Access Control for UNIX で使用されるデフォルトのディレクトリ。
  - /opt/CA/SharedComponents
- *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
- *JBoss_HOME* -- デフォルトの JBoss インストール ディレクトリ。
  - /opt/jboss-4.2.3.GA

CA への連絡先

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

目次

第 1 章: 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

このガイドでは、エンタープライズ管理、レポート、および CA Access Control エンタープライズ管理 の Web ベース インターフェースについて説明します。CA Access Control エンタープライズ管理 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、特権アカウント パスワード管理、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。

便宜上、このガイドの全体を通してこの製品を CA Access Control と表記します。

本書の対象読者

このガイドは、CA Access Control for Virtual Environments のエンタープライズ管理、サードパーティ プログラム統合機能、およびレポート機能を使用するセキュリティ管理者、システム管理者、および仮想化管理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)
- サード パーティ プログラムとの統合

エンタープライズ管理

CA Access Control エンタープライズ管理 は、組織全体でアクセス関連管理タスクを実行するための 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、多くの管理タスクを実行できます。たとえば、ある 1 つの場所から組織全体にアクセス ポリシーをデプロイしたり、個別のホストの管理、特権アカウントの管理、エンタープライズ ロボットの生成、などを行うことができます。

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。

エンタープライズ ビュー

CA Access Control エンタープライズ管理 を使用すると、仮想マシン、物理マシン、および PUPM エンドポイントに関する情報を中央の場所から取得し、これらを管理できます。CA Access Control エンタープライズ管理 ワールド ビューには、各管理対象デバイスの最終更新時の詳細情報が表示されます。また、管理対象デバイスとセキュリティ グループの設定を変更できます。

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。

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、PUPM の各エンドポイントおよび管理対象デバイスのセキュリティ ステータスを 1 か所で確認できます。エンドポイントと管理対象デバイスからのデータ収集は、スケジュール ベースまたはオンデマンドで実行できます。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 for Virtual Environments 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** - 管理対象デバイスおよび論理セキュリティ グループを定義します。

  CA Access Control ホスト マネージャは、管理対象デバイスとセキュリティ グループの作成、デバイスのセキュリティ グループへの割り当て、およびセキュリティ グループの変更ができます。CA Access Control ホスト マネージャは、ポリシーの定義とデプロイはできませんが、ワールド ビューを使用してポリシーを参照できます。

- **CA Access Control ポリシー デプロイヤ** - ポリシーを環境にデプロイします。

  CA Access Control ポリシー デプロイヤは、ホストとホスト グループへのポリシーの割り当て、ポリシーのアップグレードとダウングレード、およびホスト設定のリセットができます。また、デプロイメント監査にアクセスできます。ポリシー デプロイヤは、ポリシーとホストを表示できますが、定義はできません。また、ワールド ビューにアクセスできます。

- **CA Access Control ポリシー マネージャ** - ポリシーを作成します。

  CA Access Control ポリシー マネージャは、ポリシーの作成、変更、表示、および削除ができます。ポリシー マネージャは、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、それらを表示することはできます。また、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 のユーザとグループを管理します。また、CA Access Control エンタープライズ管理 ロールをユーザに割り当てることができます。

  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 を管理します。

  システム マネージャは、CA Access Control エンタープライズ管理 ですべてのタスクを実行、作成、および管理できます。

  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 ユーザのみにし、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** - 英語のレポートを管理します。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。

- **CA Enterprise Log Manager ユーザ** - CA Enterprise Log Manager レポートを確認します。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 レポートを管理します。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** - 作業項目を委任します。このロールが割り当てられたユーザは、作業項目をユーザに委任できます。

- **自己マネージャ** - 自分のユーザ アカウントを管理します。このロールが割り当てられたユーザは、自分のアカウントに対して管理アクションを実行できます。自己マネージャは、アカウント パスワードの変更、自分のユーザ プロファイルの変更、割り当てられたロールの表示、サブミットしたタスクの表示、および承認待ちの項目の表示ができます。

  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. 23)。
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。

以下の点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. 23)。
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. 25)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. 26)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. 26)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. 26)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. 26)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. 28)
タブの追加 (P. 29)
フィールド、イベントおよびロール使用の設定 (P. 29)

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. 32)
グループのタイプ (P. 36)

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. 42)
タスクの詳細の表示 (P. 46)
イベントの詳細の表示 (P. 47)
サブミット済みタスクのクリーンアップ (P. 47)
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. 50)
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. 52)
監査コレクタの設定 (P. 198)

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. 43)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. 45)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. 45)

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、「*Identity Manager 管理ガイド*」を参照してください。

第 3 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。

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. 25)

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。

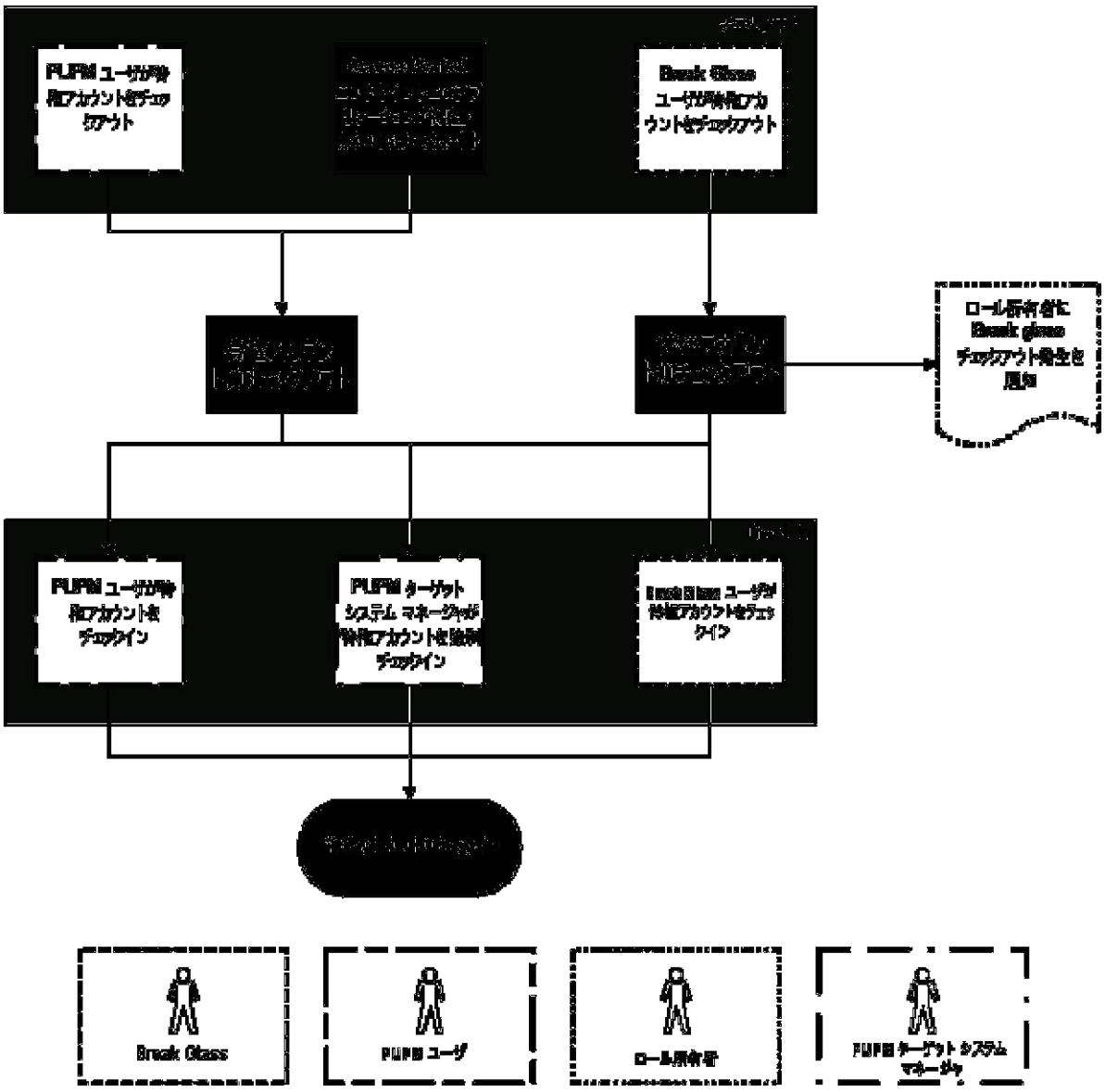
1. 特権アカウントのチェックアウトは、以下のいずれかの方法で行います。
   - PUPM ユーザ ロールが割り当てられたユーザは、特権アカウントをチェックアウトします。
   - Break Glass ロールが割り当てられたユーザは、Break Glass チェックアウトを実行します。
   - アプリケーション(たとえば CLI のパスワード コンシューマ)により、CA Access Control のエンドポイント上で特権アカウントがチェックアウトされます。

   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。

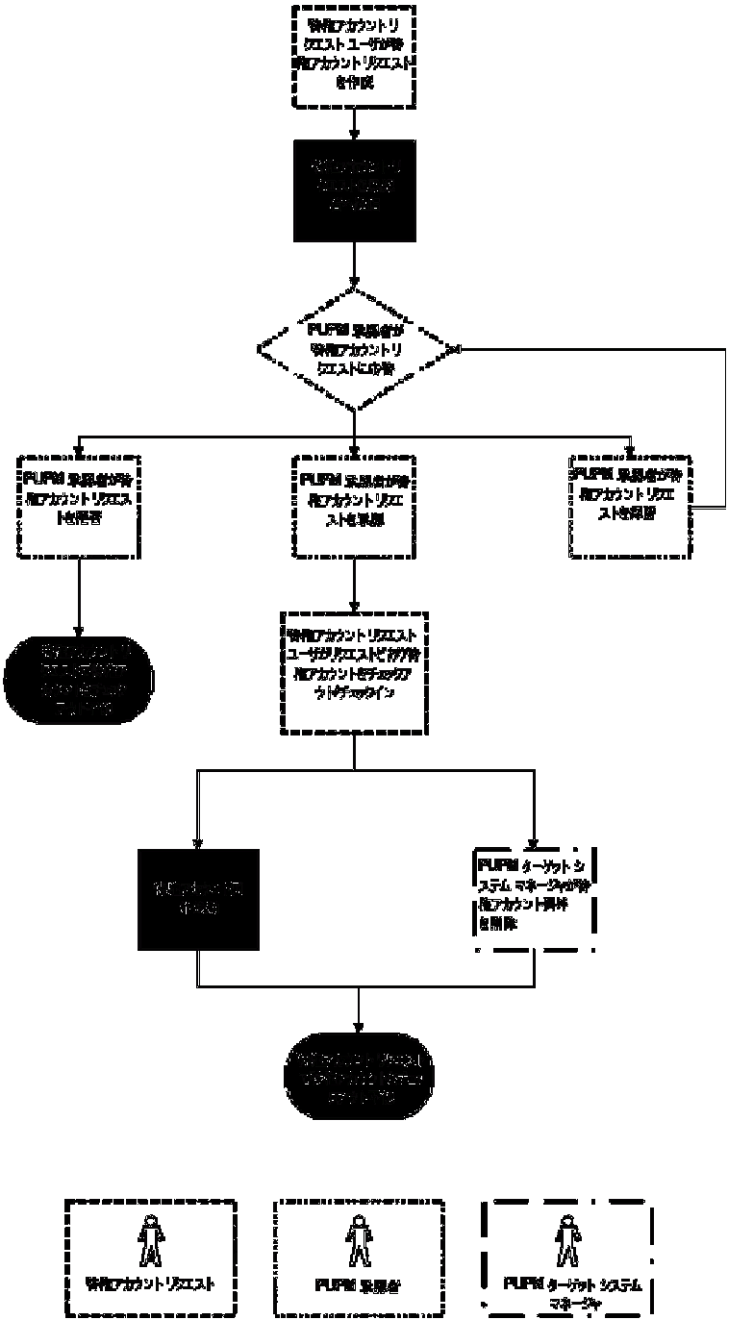
     特権アカウントリクエスト ロールを持つユーザに特権アカウント例外が付与され、そのユーザは特権アカウントをチェックアウトおよびチェックインできます。

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。



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。

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. 41)
特権アカウントの監査 (P. 164)

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. 168)

PUPM エンドポイントと CA User Activity Reporting Module を統合する方法

PUPM エンドポイントと CA User Activity Reporting Module を統合すると、特権アカウント セッションごとにエンドポイントに関する監査イベントを記録できます。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。

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:
   a. CA User Activity Reporting Module への接続を設定します。
   b. PUPM エンドポイントごとに、CA User Activity Reporting Module 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 User Activity Reporting Module]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 User Activity Reporting Module を設定します。

注: CA User Activity Reporting Module の設定方法の詳細については、CA User Activity Reporting Module のドキュメントを参照してください。

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. 168)

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。

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 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 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 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: 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。

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。

.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。

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。

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。

第 4 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、Unicenter Service Desk への接続を設定します。

   Unicenter Service Desk 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。

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。

6. ［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。

ユーザ アカウントの作成

管理対象システムおよび接続解除されたシステム上でアカウント パスワードを管理するために、特権アカウントを作成します。特権アカウントを使用して、ユーザは特権アカウント パスワードをチェックアウト/チェックインしたり、特権アカウントを作成したりできます。

複数のアカウントを作成するには、特権アカウントの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索します。単一のアカウントを作成する場合は、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

新しい特権アカウントで使用するパスワードを定義および検証します。

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。

[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. 97)

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は、説明が必要です。

   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 タイプを選択すると、PUPM がそのエンドポイントの特権アカウントを管理するために必要なクレデンシャルの指定が求められます。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。

   管理対象デバイス

   (オプション) CA Access Control for Virtual Environments 管理対象デバイスと PUPM エンドポイントを関連付けるかどうかを指定します。

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)[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、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. 102)
VMware ESX/ESXi 接続情報 (P. 103)
Windows エージェントレス接続情報 (P. 109)
Identity Manager プロビジョニング接続情報 (P. 126)
接続解除されたエンドポイント接続情報 (P. 129)

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。

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、CA Access Control for Virtual Environments 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。

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。

ポート

(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 タイプを使用して、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: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。

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. 73)

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. 111)

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. 111)

Windows Server 2008 R2 x64 エンドポイントの PUPM 用の設定

Windows Server 2008 で有効

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]をクリックします。

   アクセス許可ダイアログ ボックスが閉じます。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。

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。

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 デバイス接続情報

SSH デバイス タイプを使用して、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 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。

設定ファイル

SSH デバイスの 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. 99) 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で特権アカウント検出ウィザード (P. 90)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。

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: 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。

Identity Manager プロビジョニング接続情報

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 Identity Manager エンドポイントを管理できます。PUPM 内で 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: 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
```

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。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、「*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

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 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 Identity Manager プロビジョニング マネージャの設定 (P. 127)

PUPM 用の 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 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 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 Identity Manager プロビジョニング マネージャの設定方法

1. 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. Identity Manager - プロビジョニング サーバおよび Identity Manager - コネクタ サーバ(Java)サービスを再開します。

   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。

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、Identity Manager プロビジョニング コネクタは 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。

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。以下の手順を実行します。
   a. 以下のディレクトリに移動します。*ACServerInstallDir* は、エンタープライズ管理サーバがインストールされているディレクトリを示します。

      ```
      ACServerInstallDir/Connector_Server/bin
      ```
   b. 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。例:

   ```
   <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 以上がコンピュータにインストールされている必要があります。

- 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。

以下の点に注意してください。

- 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。

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]-[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。

注: 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:

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. 115)

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。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、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 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

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 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。

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/waiting
   ToBeProcessed
   ```

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. 121)

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。

特権アカウント CSV ファイルを作成する方法

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。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。

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/waitingToBeProcessed

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。

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。

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. 152)

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。

第 5 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. 164)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. 45)

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. 164)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. 71)

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 6 章: 特権アカウントの使用

このセクションには、以下のトピックが含まれています。

特権アカウント パスワードのチェックアウト

アカウントが所属するエンドポイントにログインするために、特権アカウント パスワードをチェックアウトします。特権アカウントのチェックアウト時に、パスワードの表示、パスワードのクリップボードへのコピー、またはエンドポイントへのログインを選択できます。

ユーザが SSH を使用して SSH Device エンドポイントに接続し、PUPM が異なるアカウントを使用してエンドポイントに接続、管理する場合、両方のアカウントをチェックアウトできます。接続アカウントのクレデンシャルを使用して SSH Device エンドポイントに接続し、次に、管理アカウントのクレデンシャルを使用して、そのアカウントを代理実行(su)します。

特権アカウント パスワードのチェックアウト方法

1. [ホーム]-[マイ アカウント]-[マイ特権アカウント]をクリックします。

   [マイ アカウント]ページが表示され、チェックアウト可能なアカウントが表示されます。

2. (オプション)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、特権アカウントの絞り込みリストが表示されます。

3. チェックアウトするアカウントおよびエンドポイントを選択し、次に、[アクション]メニューから以下のオプションのいずれかを選択します。
   - [チェックアウト]を選択してパスワードをチェックアウト
   - エンドポイントへログインするために設定したログイン アプリケーションの選択
   - [パスワードの表示]を選択してパスワードを表示
   - [クリップボードにコピー]を選択してパスワードをクリップボードにコピー
   - [拡張ログイン]を選択してログイン アプリケーションおよびログイン先のエンドポイントのホスト名を設定

   CA Access Control エンタープライズ管理 はタスクをサブミットし、選択したオプションに従って処理します。

   エンドポイントへのログインを選択している場合、CA Access Control エンタープライズ管理 は確認メッセージを表示し、エンドポイント上にウィンドウが表示されます。このウィンドウを使用して、ログインできます。

   注: これがエンドポイントへの最初のログイン試行である場合、アクションの確認を求めるダイアログ ボックスが表示されます。確認を行わないと、エンドポイントに接続できません。

   重要: Microsoft Windows 2008 Server で、Microsoft Internet Explorer ブラウザのセキュリティ設定で「ActiveX コントロールに対して自動的にダイアログを表示」を有効にします。無効な場合、ブラウザはリモート デスクトップ アプリケーションの実行に必要な ActiveX ファイルをブロックします。

詳細情報:

PUPM で UNIX エンドポイントに接続する方法 (P. 119)

特権アカウント パスワードのチェックイン

管理対象エンドポイントからログアウトしてから、特権アカウント パスワードをチェックインします。一旦特権アカウント パスワードをチェックインすれば、CA Access Control エンタープライズ管理で、そのように設定されていれば、パスワードを変更する場合があります。

特権アカウント パスワードのチェックイン方法

1. [ホーム]-[マイ アカウント]-[マイ特権アカウント]をクリックします。

   [マイ 特権アカウント]ページが表示され、チェックイン可能なアカウントが表示されます。

2. (オプション) 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、特権アカウントの絞り込みリストが表示されます。

3. チェックインするアカウント パスワードを選択し、[アクション]メニューから[チェックイン]を選択します。

   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。

詳細情報:

特権アカウント パスワードのチェックアウト (P. 173)
特権アカウントへのアクセス リクエスト (P. 175)

特権アカウントへのアクセス リクエスト

特権アカウント パスワードが必要だが、ユーザ アカウントにアカウントのチェックアウトに必要な特権アクセスがない場合は、そのアカウントのチェックアウト リクエストをサブミットできます。CA Access Control エンタープライズ管理 は、リクエストを承認または拒否できる承認者にリクエストを転送します。承認されると、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。

特権アカウントのパスワードの要求方法

1. [ホーム]-[マイ アカウント]-[特権アカウント要求]をクリックします。

   [特権アカウント要求: 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. チェックアウトする特権アカウントを選択し、[選択]をクリックします。
4. リクエストを完了して、[サブミット]をクリックします。また、Unicenter Service Desk チケット番号が必要になる場合があります。

   リクエストがサブミットされたことを伝えるウィンドウが表示されます。

   リクエストは承認者に転送され、承認または拒否されるまで、保留のままになります。リクエストが承認されると、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。

特権アカウント リクエストへの応答

デフォルトの PUPM 承認者ロールまたは、同等のロールが割り当てられている場合、ユーザがサブミットし、保留中の特権アカウント アクセス リクエストに応答できます。以下のアクションの*いずれか*で応答できます。

- **承認** - リクエストを承認し、特権アカウントのチェックアウトをユーザに許可します。
- **拒否** - 特権アカウント リクエストを拒否します。
- **項目の保留** - リクエストを保留し、後で検討します。リクエストを保留すると、CA Access Control エンタープライズ管理 はその作業項目を他の承認者の作業リストから削除します。後でこの項目に戻り、承認または拒否できます。
- **項目のリリース** - 他の承認者が応答できるように、リクエストをリリースします。以前、自分で保留した項目のみリリースできます。

また、承認者を追加して、作業項目を再度割り当て、承認保留中の項目を受け取れるようにできます。

注: Break Glass チェックアウト リクエストはリクエストの [マイ承認の待機]リストに表示されます。ただし、これらのリクエストを承認または拒否する必要はありません。これらのリクエストは、ユーザが Break Glass アカウントをチェックアウトしたという通知としてのみ表示されます。

注: 特権アカウント リクエストに応答するには、PUPM 承認者の特権アクセス 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。

特権アカウント リクエストへの応答方法

1. [ホーム]-[マイ アカウント]-[マイ承認の待機]をクリックします。

   保留中の特権アカウント リクエストのリストが表示されます。

2. 検討する保留中のリクエストをクリックします。

   [特権アカウント要求を承認]ページが表示されます。

3. (オプション)このリクエストの承認者を追加するには、以下の手順に従います:

   a. [担当者の追加]をクリックします。

      [ユーザの選択]検索ウィンドウが開きます。

   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. 追加するユーザを選択し、[選択]をクリックします。

      選択されたユーザが承認者リストに追加されます。

4. (オプション)リクエストの詳細を見直し、以下のように、必須パラメータを変更します。

   a. [特権アカウント]タブをクリックします。

      アカウントおよびリクエストの詳細が表示された、[特権アカウント]タブが表示されます。

   b. チェックアウト失効タイムアウトを無効にするために、[有効期限] フィールドを使用します。

   c. [チケット番号]フィールドを使用し、Unicenter Service Desk のチケットを確認します。

   d. リクエストへの対応について説明するコメントを入力します。

5. 以下の*いずれか*の操作を行います。

   - [承認]をクリックします。

     リクエストが承認され、保留リクエストのリストから削除されます。これで、要求者が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。

   - [拒否]をクリックします。

     リクエストは拒否され、保留リクエストのリストから削除されます。

- [項目の保留]をクリックします。

  リクエストは自分用に保留され、他の承認者の保留リクエストのリストから削除されます。

- [項目のリリース]をクリックします。

  リクエストは他のすべての承認者にリリースされます。リリースできるのは保留した項目のみです。

Break Glass

Break Glass タスクは、特権アクセス権限がないエンドポイントへの*即時*アクセスが必要な場合に使用します。

注: エンドポイントへの即時アクセスの必要がない場合は、特権アカウントへのアクセスをリクエストして、リクエストが承認されるのを待機することができます。

Break Glass の実行方法

1. [ホーム]-[マイ アカウント]-[マイ特権アカウント]をクリックします。

   [マイ アカウント]ページが表示され、チェックアウト可能なアカウントが表示されます。

2. アカウントを選択するフィールドで[詳細]を選択します。

   詳細検索オプションが表示されます。

3. [Break Glass アカウントを含む]-[検索]を選択します。

   フィルタ条件に一致する、特権アカウントの絞り込みリストが表示されます。

4. [アクション]メニューから、チェックアウトする特権アカウントを選択します。

5. [理由]に値を入力し、[チェックアウト]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、成功した場合、確認メッセージにアカウント パスワードが表示されます。

注: パスワードをチェックアウトした後、[アクション]メニューには[チェックアウト]、[ログイン アプリケーション]、[パスワードの表示]の各オプションが表示されます。

Break Glass 特権アカウント パスワードのチェックイン

管理対象エンドポイントからログアウトしたら、Break Glass 特権アカウント パスワードをチェックインします。

Break Glass 特権アカウント パスワードのチェックイン方法

1. [ホーム]-[マイ アカウント]-[マイ特権アカウント]をクリックします。

   [マイ アカウント]ページが表示され、チェックイン可能なアカウントが表示されます。

2. アカウントを選択するフィールドで[詳細]を選択します。

   詳細検索オプションが表示されます。

3. [Break Glass アカウントを含む]-[検索]を選択します。

   フィルタ条件に一致する、特権アカウントの絞り込みリストが表示されます。

4. チェックインするアカウントを選択し、[アクション]メニューから[チェックイン]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、アカウントをチェックインします。

第 7 章: CA User Activity Reporting Module との統合

このセクションには、以下のトピックが含まれています。

CA User Activity Reporting Module について

CA User Activity Reporting Module は、IT のコンプライアンスおよび保証に重点的に取り組んでいます。 これを使用することによって、IT アクティビティを収集し、標準化し、集約して報告し、コンプライアンス違反が発生した場合にアクションを必要とするアラートを生成することができます。異なるセキュリティ デバイスおよびセキュリティ以外のデバイスからデータを収集できます。

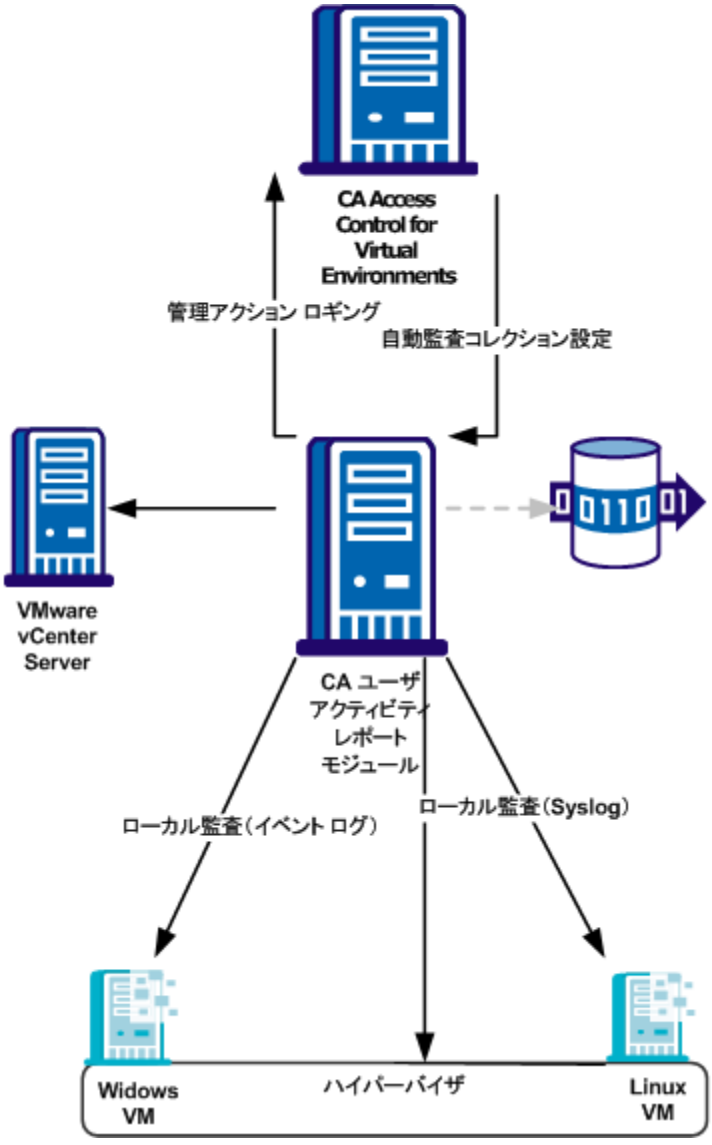
UARM 統合アーキテクチャ

CA User Activity Reporting Module との統合により、各管理対象デバイスから監査イベントを収集して CA User Activity Reporting Module でレポートを生成できます。

各管理対象デバイスを設定して、ローカル マシンの監査ファイルに監査イベントを収集できます。その後、CA User Activity Reporting Module を設定してイベント(メッセージ)をプルできます。CA User Activity Reporting Module はこれらのイベントを処理して、CA User Activity Reporting Module サーバに送信します。

CA Access Control for Virtual Environments インストールは CA User Activity Reporting Module 統合をサポートします。

以下の図に、CA User Activity Reporting Module 統合コンポーネントのアーキテクチャを示します。



上の図は、以下のことを示します。

- 各管理対象デバイスは、ローカル ファイルに監査データを収集します。
- CA User Activity Reporting Module は、監査コレクション ポリシーが適用されると管理対象デバイスから監査レコードをプルします。
- CA User Activity Reporting Module は、CA Access Control for Virtual Environments で実行する管理アクション時に監査レコードを収集します。
- CA User Activity Reporting Module は、VMware vCenter サーバとハイパーバイザから監査レコードを収集します。

注: CA User Activity Reporting Module 統合はレポートするサービス コンポーネントに依存します。そのため、CA User Activity Reporting Module 統合では使用されないその他のレポート サービスのコンポーネントや機能もアーキテクチャに含まれます。そのようなコンポーネントや機能は、図中で淡色表示されています。

CA User Activity Reporting Module 統合コンポーネント

CA User Activity Reporting Module 統合では、以下の CA Access Control for Virtual Environments コンポーネントを使用します。これらのコンポーネントは、CA Access Control エンタープライズ レポーティング サービスの一部です。

- レポート エージェントは、各管理対象デバイス上で実行され、VPM サーバ上に存在する設定されたメッセージ キュー内のキューに情報を送信します。CA User Activity Reporting Module 統合の場合、レポート エージェントが監査ログ ファイルから監査メッセージを定期的に収集し、収集したイベントを設定済みの配布サーバ上にある監査キューに送信します。
- *メッセージ キュー*は、配布サーバのコンポーネントの 1 つで、レポート エージェントが送信するエンドポイント情報を受信するように設定されています。レポートの場合、メッセージ キューは CA Access Control for Virtual Environments データベース スナップショットを中央データベースに転送します。

注: デフォルトでは、CA Access Control for Virtual Environments は CA Access Control Server に配布サーバをインストールします。

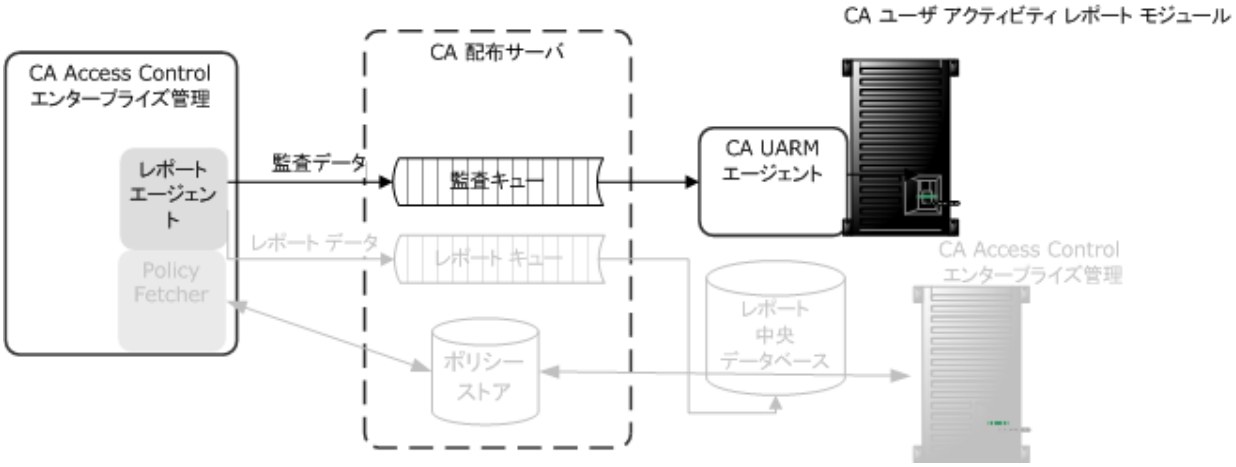
CA User Activity Reporting Module 統合では次の CA User Activity Reporting Module コンポーネントも使用します。

- CA Access Control for Virtual Environments コネクタは、CA Access Control 監査イベント ソース用の使いやすい CA User Activity Reporting Module 統合です。コネクタを使用すると、配布サーバからの生のイベント収集が可能になり、変換されたイベントをイベント ログ ストアにルール ベースで送信できるようになります。イベント ログ ストアでイベントはホット データベースに挿入されます。
- 収集サーバは、受信イベント ログの調整、ホット データベースへの受信イベント ログの挿入、設定サイズに達したホット データベースのウォーム データベースへの圧縮、関連管理サーバへのウォーム データベースの定期的な自動アーカイブを行う CA User Activity Reporting Module サーバです。

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

CA Access Control for Virtual Environments と CA User Activity Reporting Module 間の監査データ フローの概要

CA Access Control for Virtual Environments が CA User Activity Reporting Module とどのように統合されるか、また、この統合の設定に関して何を検討すべきか理解するには、最初に CA Access Control for Virtual Environments と CA User Activity Reporting Module の間の監査データのフローを検討する必要があります。以下の図は、CA Access Control for Virtual Environments が監査イベントを配布サーバ上のメッセージ キューにルーティングする方法を示しています。配布サーバ上で、CA User Activity Reporting Module の CA Access Control コネクタによってイベントのプル、マップ、および変換が行われ、CA User Activity Reporting Module サーバに送信されます。



1. レポート エージェントはローカル エンドポイントの監査ファイルから監査イベントを収集し、フィルタリング ポリシーを適用し、配布サーバ上にある監査キューにイベントを格納します。
2. CA User Activity Reporting Module コネクタは監査キューに接続し、そこからイベント(メッセージ)をプルします。
3. CA User Activity Reporting Module はデータ マッピングおよび解析ファイルを使用して Common Event Grammar(CEG)にイベントをマップし、CA User Activity Reporting Module サーバにイベントをルーティングする前に、抑制および要約ルールを適用します。
4. CA User Activity Reporting Module サーバはイベントを受け取り、場合により、イベントを格納する前に追加の抑制および要約ルールを適用します。

注: CA User Activity Reporting Module の動作の詳細については、CA User Activity Reporting Module のマニュアルを参照してください。

CA Access Control for Virtual Environments に対する CA User Activity Reporting Module のセット アップ方法

CA User Activity Reporting Module を使用して、すべての仮想マシンからの監査データを含むレポートを作成するには、最初にエンタープライズ レポートを実装します。CA User Activity Reporting Module との統合の前に、エンタープライズ レポートを実装する必要があります。これは、エンタープライズ レポートによって CA Access Control Server でレポート エージェントが有効になったためです。エンタープライズ レポートを実装したら、CA User Activity Reporting Module を CA Access Control for Virtual Environments 用に設定します。

CA Access Control for Virtual Environments に対して CA User Activity Reporting Module をセット アップするには、以下の手順に従います。

1. CA User Activity Reporting Module サーバをインストールする

   注: 詳細については、「*CA User Activity Reporting Module Implementation Guide*」を参照してください。

2. CA User Activity Reporting Module の CA User Activity Reporting Module API 証明書を設定する

   CA Access Control エンタープライズ管理 から CA User Activity Reporting Module への接続を作成するときには、証明書の詳細を指定します。

3. CA User Activity Reporting Module コネクタを設定する (P. 187)

4. CA User Activity Reporting Module で監査コレクション プロファイルを設定する

   カスタム監査コレクション プロファイルを設定するか、またはデフォルト コレクション プロファイルを使用できます。

5. CA Access Control エンタープライズ管理 から CA User Activity Reporting Module への接続を作成する

   CA User Activity Reporting Module が管理対象デバイスから監査レコードを収集できるようにするためには、接続を設定します。

6. CA Access Control エンタープライズ管理 で監査コレクション ポリシーを設定する

コネクタの詳細

コンピュータに CA User Activity Reporting Module エージェントをインストールすると、そのコンピュータは CA User Activity Reporting Module サーバ管理インターフェースに表示されます(たとえば、「デフォルト エージェント グループ」のコンピュータを表示するには、[管理]-[ログ収集]-[エージェント エクスプローラ]-[デフォルト エージェント グループ]をクリックし、*computer_name* をクリックします)。このとき、コネクタを作成する必要があります。このトピックでは、コネクタ作成ウィザードの[コネクタの詳細]ページで行う必要がある設定について説明します。

統合

テンプレートとして使用する統合を指定します。

適切な CA Access Control 統合を選択します。

例: AccessControl_R12SP5_TIBCO。

任意でコネクタ名を変更して、説明を追加することもできます。さらに、コネクタによって処理されるイベントに抑制ルールを適用できます。

注: イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「*オンライン ヘルプ*」を参照してください。

抑制ルールおよび要約ルール

コネクタを作成してコネクタの詳細を指定したら、任意でコネクタ作成ウィザードの[抑制ルールの適用]ページで抑制ルールを適用できます。

CA Access Control の抑制および要約ルールに関する理想モデルの名前は、ホスト IDS/IPS です。ルールを作成する場合、イベントを特定するために必要に応じてイベント カテゴリ、イベント クラス、およびイベント アクションの値を選択してください。

注: イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「*オンライン ヘルプ*」を参照してください。フィールドの意味や個々の値の詳細については、CA User Activity Reporting Module オンライン ヘルプの「Common Event Grammar Reference」を参照してください。

コネクタ設定の要件

コネクタを作成してコネクタの詳細を指定したら、コネクタを設定できます。このトピックでは、イベント収集を開始するために、コネクタ作成ウィザードの[コネクタ設定]ページで行う*必要*がある設定について説明します。

注: イベント収集をカスタマイズできるその他のオプション設定については、「*CA User Activity Reporting Module Administration Guide*」および「*オンライン ヘルプ*」を*参照してください*。

TIBCO サーバ

メッセージ キュー(TIBCO サーバ)のホスト名または IP アドレスを次の形式で指定します。

Protocol://server IP or name:Port number

メッセージ キューは CA Access Control エンタープライズ管理 にインストールされます。

- 以下の値を定義します。

  ssl://ACentmserver:7243

ポート値および通信方法は CA Access Control エンタープライズ管理 が使用するデフォルト ポートです。CA Access Control エンタープライズ管理 をインストールした後に別の値を設定した場合、そのポートと通信方法の値を使用します。

TIBCO ユーザ

メッセージ キューの認証用のユーザ名を指定します。CA Access Control では、「reportserver」という名前のデフォルト ユーザを定義します。

TIBCO パスワード

メッセージ キューの認証用のパスワードを指定します。CA Access Control エンタープライズ管理 のインストール時に、[通信パスワード]ダイアログ ボックスで定義したパスワードを入力します。

イベント ログ名

イベント ソースのログ名を指定します。

デフォルトの「CA Access Control」を使用します。

ポーリング間隔

メッセージ キューが使用不可になったり切断された場合に、イベントをポーリングするまでエージェントが待機する秒数を指定します。

SourceName

メッセージ キューの識別子を指定します。

デフォルトの「queue_audit」を使用します。

TIBCO キュー

ログ センサによるメッセージ(イベント)の読み取り元であるメッセージ キューの名前を指定します。

デフォルトの「queue/audit」を使用します。

コレクション スレッドの数

メッセージ キューのメッセージを読み取るためにログ センサが生成するスレッドの数を指定します。

この値を調整する場合、メッセージ キュー内のイベントの数および CA User Activity Reporting Module エージェント システムの CPU を考慮する必要があります。

制限: 最小値は 1 です。ログ センサが生成できるスレッドの最大数は 20 です。

設定によるレポート エージェントへの影響

CA User Activity Reporting Module 統合の場合、レポート エージェントが監査ログ ファイルからエンドポイント監査メッセージを定期的に収集し、そのイベントを設定済み配布サーバ上の監査キューにルーティングします。レポート エージェントの設定をチューニングすると、パフォーマンスを向上させることができます。

注: レポート エージェントは CA Access Control エンタープライズ レポート サービスの一部であり、エンドポイント レポートの目的でデータベース スナップショットの送信も担当します。このプロセスは、CA User Activity Reporting Module への監査イベント ルーティングのためにレポート エージェントが行うアクションのみを示します。

監査収集を有効にした場合（audit_enabled 設定を 1 に設定）、レポート エージェントでは以下を実行します。

- エンドポイント監査ファイルを読み取ってメモリにコミットすることによって、新しい監査レコードを収集します。

  レポート エージェントは、audit_read_chunk 設定に定義された監査レコードの数を読み取り、audit_sleep 設定に定義された間だけ待機してから、監査ファイルを再度読み取ります。レポート エージェントは、アクティブな監査ログおよびすべてのバックアップ監査ファイル内の読み取られていないレコードを読み取ります。そして、監査フィルタ ファイルに定義した監査フィルタ（audit_filter 構成設定）を通過するレコードをメモリにコミットします。

- メモリにある監査レコードのグループを audit_queue 設定に定義された配布サーバ メッセージ キューに送信します。

  次のいずれかの場合に該当すると、レポート エージェントは監査レコードを送信します。

  - メモリのレコードの数が audit_send_chunk 構成設定で定義された数に達する。
  - 最後の監査レコードが送信されてから経過した時間が、audit_timeout 設定で定義された間隔に等しい。

例：監査収集とルーティングに関するレポート エージェントのデフォルト設定

この例は、レポート エージェントのデフォルト構成設定がどのように設定されているか、その設定がどのような環境に適するか、およびその設定がパフォーマンスにどのように影響するかを示します。

平均的な環境で、秒あたりのイベント数（EPS）30 を想定しています。したがって、レポート エージェントは毎秒通過する 30 のイベントを読み取ります。その他の実行中のアプリケーションに対する影響（CPU 使用およびコンテキスト スイッチ）を減らすために、以下のようにレポート エージェントのイベント読み取りを 10 秒ごとに 300 としています。

```
audit_sleep=10
audit_read_chunk=300
```

レポート エージェントと配布サーバ間のメッセージ伝送のために CA Access Control が使用するメッセージ バスは、短い間隔で小さなパケットを処理するよりも長い間隔で送信される大きなパケットを処理するのに適しています。次の構成設定は、レポート エージェントが収集する監査レコードの数が定義された数に達すると、それらのレコードをレポート エージェントが配布サーバに送信するように指定しています。1 秒間 30 イベントとすると、レポート エージェントがおよそ 1 分(60 秒)間隔で監査レコードを送信するようにするには、レポート エージェントを次のように設定する必要があります。

```
audit_send_chunk=1800
```

ただし、夜間などの時間帯で 1 秒間 30 未満のイベントになると、1 分間 1800 未満のイベントになります。レポート エージェントが今後も定期的に監査レコードを配布サーバに送信するためには、監査レコード送信間隔を次のとおり最大 5 分に設定します。

```
audit_timeout=300
```

CA User Activity Reporting Module からのイベントのフィルタリング

フィルタ ファイルを使用して、CA Access Control がログ ファイル内のすべての監査レコードを CA User Activity Reporting Module に送信するのを防ぐことができます。フィルタ ファイルは、CA User Activity Reporting Module に送信されない監査レコードを指定します。

注: このフィルタ ファイルによって、指定された監査イベントを CA Access Control が配布サーバに送信しないようにしますが、CA Access Control が監査イベントをローカル ファイルに書き込むことを防ぐわけではありません。ローカルの監査ファイルから監査イベントを除外するには、logmgr セクションの AuditFiltersFile 設定に定義されているファイルでフィルタ ルールを変更します(デフォルトでは audit.cgf)。

CA User Activity Reporting Module からのイベントをフィルタするには、エンドポイント上の監査フィルタ ファイルを編集します。同じフィルタ ルールを複数のエンドポイントに適用する場合、監査フィルタリング ポリシーを作成し、そのポリシーを対象のエンドポイントへ割り当てることをお勧めします。

注: 詳細については、「リファレンス ガイド」を参照してください。

例: 監査フィルタ ポリシー

監査フィルタ ポリシーの例を以下に示します。

```
env config
er config auditrouteflt.cfg line+("FILE;*;*;R;P")
```

この例は、次の行を auditrouteflt.cfg ファイルに書き込みます。

```
FILE;*;*;R;P
```

この行は、ファイル リソースへの読み取りアクセスのためにアクセサが行った許可された試行を記録した監査レコードをフィルタします。CA Access Control はこの監査レコードを配布 サーバに送信しません。

SSL を使用した安全な通信

CA Access Control エンタープライズ管理 をインストールする場合、SSL を使用して配布サーバとレポート エージェントの間の通信を保護するか、通信を保護しないか選択できます。いずれのオプションを選択した場合でも、エンドポイントにレポート エージェントをインストールするときと同じオプションを指定する必要があります。

たとえば、SSL を使用してレポート エージェントと配布サーバ間の通信を暗号化する場合 (デフォルト)、レポート エージェントが配布サーバと通信するときに必要なパスワードなどの認証情報を、CA Access Control エンタープライズ管理 のインストール時に提供する必要があります。

これは、CA User Activity Reporting Module エージェントの[Connector Configuration]ページで、エンドポイントの CA Access Control レポート エージェントを設定するときに指定するパスワードです。

レポート エージェントをインストールするときに、同じ情報を指定する必要があります。 正しい証明書とパスワード情報を提供できるレポート エージェントのみが、配布サーバ上の監査キューにイベントを書き込むことができ、書き込まれたイベントは CA User Activity Reporting Module によって取得されます。

CA User Activity Reporting Module 統合のための監査ログ ファイルのバックアップ

監査データを収集するために、レポート エージェントは構成設定に従って CA Access Control 監査ログ ファイルを読み取ります。レポート エージェントは、設定された時間間隔で設定された数の監査レコードを監査ログ ファイルから読み取ります。デフォルトのレガシー インストールの場合、またはインストール時に監査ログ ルーティングを有効にしていない場合、CA Access Control はサイズによる監査ログ バックアップ ファイルのみを保存します。監査ログが設定された最大サイズに達するたびに、既存の監査ログ バックアップ ファイルが上書きされてバックアップ ファイルが作成されます。そのため、レポート エージェントがすべてのレコードを読み取る前に、バックアップ ファイルが上書きされる可能性があります。

CA Access Control が監査ログ ファイルのタイムスタンプ付きバックアップを保存するように設定することを強くお勧めします。こうすると、保存されるべき監査ログ ファイルの設定された最大数に達するまで、CA Access Control はバックアップの監査ログ ファイルを上書きしません。これは、エンドポイント上へのインストール時に、監査ログ ルーティング サブ機能を有効にした場合のデフォルト設定です。

例: 監査ログ バックアップの設定

この例は、推奨の構成設定がどのように CA User Activity Reporting Module 統合に影響するかを示します。エンドポイント上へのインストール時に、監査ログ ルーティング サブ機能を有効にすると、CA Access Control は logmgr セクションの以下の環境設定を行います。

```
BackUp_Date=yes
audit_max_files=50
```

この場合、CA Access Control は監査ログ ファイルの各バックアップ コピーにタイムスタンプを付け、最大 50 のバックアップ ファイルを保存します。これによって、レポート エージェントがすべての監査レコードをファイルから読み取ったり、必要に応じてバックアップ ファイルを安全に保管するために手動でコピーしたりすることが行いやすくなります。

重要: audit_max_files を 0 に設定すると、CA Access Control はバックアップ ファイルを削除せずに蓄積し続けます。バックアップ ファイルを外部プロシージャによって管理する場合、CA Access Control がデフォルトでバックアップ ファイルを保護することに注意してください。

CA Access Control イベントのクエリおよびレポート

CA Access Control のクエリ、レポート、およびアクション警告は、CA User Activity Reporting Module インターフェースの[Server Resource Protection]タグにまとめられています。

注: 詳細については、http://ca.com/jp/support にある CA User Activity Reporting Module 製品ページを参照してください。

CA Access Control で CA User Activity Reporting Module レポートを有効にする方法

CA Access Control エンタープライズ管理 で CA User Activity Reporting Module レポートを表示できるようにするには、CA User Activity Reporting Module レポートを有効にし、CA User Activity Reporting Module 証明書をエクスポートして追加し、CA Access Control エンタープライズ管理 から CA User Activity Reporting Module への接続を設定する必要があります。

1. 高度な設定により、CA User Activity Reporting Module レポートを有効にします。
2. CA User Activity Reporting Module の trusted 証明書をエクスポートして、キーストアに追加します。
3. CA Enterprise Log Manager への接続を設定します。
4. (オプション) 監査コレクタを設定します (P. 198)。

   PUPM 監査イベントを CA User Activity Reporting Module に送信する場合は、監査コレクタを設定します。

CA User Activity Reporting Module の trusted 証明書のキーストアへの追加

CA User Activity Reporting Module レポートは、トラステッド証明書を使用して認証されます。証明書は、レポートに表示されている情報がトラステッド CA User Activity Reporting Module ソースのものであることを証明します。トラステッド CA Enterprise Log Manager ソースはデータの信頼性を証明します。

注: この手順を開始する前に、CA User Activity Reporting Module の信頼済み証明書を取得してインストールします。CA User Activity Reporting Module の信頼済み証明書のインストールの詳細については、CA User Activity Reporting Module のドキュメントを参照してください。

以下の手順に従います。

1. エンタープライズ管理サーバで、コマンド プロンプト ウィンドウを開き、以下のディレクトリに移動します。

jbossInstallDir/server/default/deploy/IdentityMinder.ear/custom/ppm/truststore

1. 以下のコマンドを入力します。

   `keytool -import -file <certificate.cert> -keystore`

   -import

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

   -file

   信頼済み証明書ファイルの完全パス名を指定します。

   パスワードの入力を促すメッセージが表示されます。

2. キーストアのパスワードを入力します。デフォルトのパスワードは、「secret」です。
3. [はい]をクリックして、証明書を信頼します。

   証明書がキーストアに追加されます。

CA User Activity Reporting Module への接続の設定

CA Access Control エンタープライズ管理 は CA Access Control の関連情報を記載したレポートを表示するために CA User Activity Reporting Module と通信します。これらのレポートを表示するには、CA User Activity Reporting Module への接続を設定する必要があります。

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、以下の手順を実行します。
   a. ［システム］をクリックします。
   b. ［接続管理］サブタブをクリックします。
   c. 左側のタスク メニューで、UARM ツリーを展開します。

   ［CA User Activity Reporting Module 接続の管理］タスクが使用可能なタスクリストに表示されます。
2. ［CA User Activity Reporting Module 接続の管理］をクリックします。

   ［CA User Activity Reporting Module 接続の管理: *PrimaryCALMServer*］タスク ページが表示されます。
3. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

   接続名

   CA User Activity Reporting Module 接続の名前を識別します。

   説明

   （オプション）この接続に関する説明を定義します。

   ホスト名

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

   例: host1.comp.com

   ポート番号

   CA User Activity Reporting Module ホストが通信に使用するポートを定義します。

   デフォルト: 5250

信頼済みルート証明書の検証

CA User Activity Reporting Module への接続で、認証局が署名した信頼済みルート証明書を使用するかどうかを指定します。

注: このオプションが適切に機能するためには、CA User Activity Reporting Module の信頼済みルート証明書がインストールされている必要があります。

証明書名

証明書の名前を定義します。

パスワード

証明書のパスワードを定義します。

4. [サブミット]をクリックします。

   CA Access Control エンタープライズ管理 が CA User Activity Reporting Module の接続設定を保存します。

例: CA User Activity Reporting Module 証明書情報の取得

以下の例では、CA Access Control エンタープライズ管理 内で CA User Activity Reporting Module 接続設定を作成および管理する際に必要な CA User Activity Reporting Module 証明書情報の取得方法を示しています。

1. 以下の形式で、Web ブラウザに CA User Activity Reporting Module の URL を入力します。

   `https://host:port/spin/calmapi/products.csp`

   例: https://localhost:5250/spin/calmapi/products.csp

2. 有効なユーザ名とパスワードを入力して、CA User Activity Reporting Module にログインします。

3. CA User Activity Reporting Module に証明書を登録するための登録オプションを選択します。

   新しい製品の登録画面が表示されます。

4. 証明書名とパスワードを入力し、登録を選択します。

   証明書の登録が正常に完了したことを通知するメッセージが表示されます。

監査コレクタの設定

CA Access Control エンタープライズ管理 は、PUPM 監査イベントなどの監査イベントを収集し、中央データベースに格納します。監査イベントを CA User Activity Reporting Module に送信するように、CA Access Control エンタープライズ管理 を設定できます。

監査コレクタの設定方法

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

      [監査コレクタの作成]タスクが使用可能なタスク リストに表示されます。
2. [監査コレクタの作成]をクリックします。

   [監査コレクタの作成: 監査コレクタ検索画面]が表示されます。
3. (オプション)既存の監査コレクタのコピーを以下のように作成します。
   a. [UARM 送信者タイプのオブジェクトのコピーの作成]を選択します。
   b. 検索属性を選択し、フィルタ値を入力し、[検索]をクリックします。

      フィルタ条件に一致する UARM 送信者のリストが表示されます。
   c. 新規監査コレクタのベースとして使用するオブジェクトを選択します。
4. [OK]をクリックします。

   [監査コレクタの作成]タスク ページが表示されます。監査コレクタを既存のオブジェクトから作成した場合、ダイアログ ボックスのフィールドには、既存オブジェクトの値がすでに入力されています。
5. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

   ジョブの有効化

   監査コレクタを有効にするかどうかを指定します。

   名前

   監査コレクタの名前を定義します。

キュー JNDI

CA Access Control エンタープライズ管理 が監査イベント メッセージを送信するメッセージ キューの名前を定義します。

例: *queue/audit*

スリープ

データベース クエリの間隔を分単位で定義します。

デフォルト: 1

タイムアウト

監査イベント メッセージのメッセージ キューへの送信に関して、コレクタのタイムアウト期間を分単位で定義します。

デフォルト: 10

注: このタイムアウト期間が経過すると、キュー内のメッセージ数が[メッセージ ブロック サイズ]フィールドで定義されたレベルに達していなくとも、コレクタはメッセージを送信します。

メッセージ ブロック サイズ

データベースに蓄積するメッセージの最大数を定義します。この数に達すると、メッセージはキューに送信されます。

デフォルト: 100

6. [サブミット]をクリックします。

CA Access Control エンタープライズ管理 は監査コレクタを作成します。

第 8 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 for Virtual Environments 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 for Virtual Environments 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 for Virtual Environments レポートは、各管理対象デバイスの CA Access Control データベース内のデータ、つまり、エンドポイントにデプロイする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 for Virtual Environments レポートは、[assign the value for cabi in your book] 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、各管理対象デバイスにあるデータ、つまり、エンドポイントで実行されたアクションと実行したユーザに関する情報を提供します。監査レポートは、VMware vSphere クライアントの CA User Activity Reporting Module および CA Access Control エンタープライズ管理 で表示できます。

  注: CA User Activity Reporting Module での監査レポートの表示の詳細については、「*CA User Activity Reporting Module Overview Guide*」を参照してください。

注: CA Access Control for Virtual Environments レポートおよび CA Access Control for Virtual Environments 監査レポートを表示するための追加コンポーネントをインストールする必要があります。詳細については、「*製品ガイド*」を参照してください。

レポート サービス

CA Access Control for Virtual Environments 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 for Virtual Environments 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 アクセスのステータスを確認するための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 for Virtual Environments がデフォルトで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 for Virtual Environments 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 Server に存在する設定済みメッセージ キュー上のキューに情報を送信する Windows サービスまたは UNIX デーモンです。
- *メッセージ キュー*は、CA Access Control Server 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。
- *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。
- 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。

レポート サービスの機能

レポート サービスを使用すると、各管理対象デバイスから収集されるデータ、ユーザ ストア、および PUPM ポリシー ストアを参照できます。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。

- 各管理対象デバイスからデータを収集します。

  各管理対象デバイスは、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 for Virtual Environments 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 for Virtual Environments 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 for Virtual Environments レポートにバンドルされています。

レポート用のデータの収集方法

レポートを生成するには、各管理対象デバイス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、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その管理対象デバイスからデータを収集します。

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 CA Access Control Server に送信します。
2. 管理対象デバイス上で CA Access Control 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。

   これは、データベース内のすべてのオブジェクトのダンプです。つまり、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 バージョンをレポート CA Access Control Server に送信します。

   レポート エージェントは CA Access Control Server のレポート キューにデータを送信します。

詳細情報:

設定によるレポート エージェントへの影響 (P. 189)

データの処理および格納方法

データが各管理対象デバイス上で収集されると、そのデータは CA Access Control Server で処理するために送信されます。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。

CA Access Control Server は、以下のアクションを実行します。

1. レポート エージェントから、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。

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、管理対象デバイスに関する情報を提供する CA Access Control for Virtual Environments レポートを作成および表示する方法を示します。また、CA Access Control for Virtual Environments レポートを [assign the value for cabi in your book] 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 for Virtual Environments 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. レポート用に管理対象デバイスが設定されていることを確認します。
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。

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。

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、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、オンライン ヘルプ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

レポートは、CA Access Control for Virtual Environments 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 for Virtual Environments 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、[assign the value for cabi in your book] では、繰り返されるレポートをスケジュールできます。[assign the value for cabi in your book] 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、[assign the value for cabi in your book] でそのレポートを表示できます。

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、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。

   - 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. 214)

レポートの表示

CA Access Control for Virtual Environments レポートは、管理対象デバイスに関する情報を提供します。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。

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、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。

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。

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。

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*。

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。

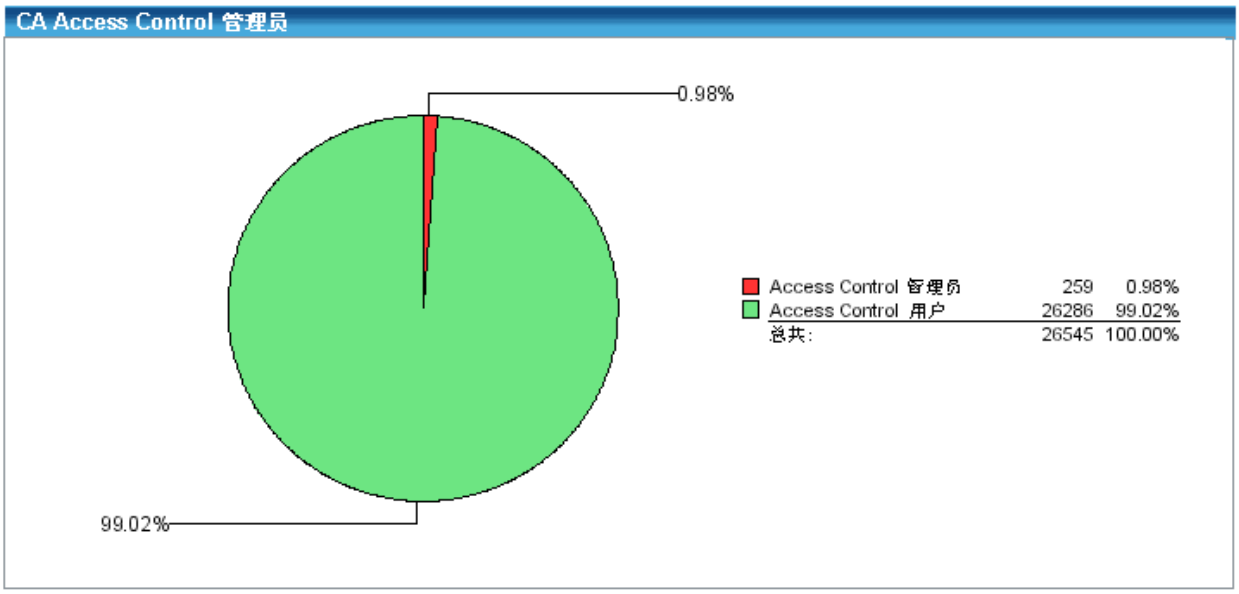
標準レポート

デフォルトによって、CA Access Control for Virtual Environments 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。

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		

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

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
- アカウント
- 要求者
- 要求の説明
- 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
- アカウント
- 要求者の名前と ID
- 要求の説明
- 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
- アカウント
- 要求の説明
- 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

CA User Activity Reporting Module レポート

CA User Activity Reporting Module レポートは、CA Access Control for Virtual Environments 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 User Activity Reporting Module レポートの詳細については、CA User Activity Reporting Module ドキュメント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。