CA Access Control Premium Edition

エンタープライズ管理ガイド

r12.5

第 2 版

サードパーティに関する通知

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

CA 製品リファレンス

このマニュアルが参照している CA の製品は以下のとおりです。

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

ドキュメントの表記規則

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

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

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

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ（[]）で囲まれた文字列	オプションのオペランド

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

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

CA への連絡先

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

マニュアルの変更点

第 2 版

第 2 版は r12.5 の GA 版の発表と同時にリリースされました。

この版では、以下のトピックが追加または更新されました。

- CA Access Control エンタープライズ管理 の管理ロール (20 ページ) - この更新トピックでは、新しい管理ロールである UNAB 管理者、およびいくつかの新しいレポート管理ロールが追加されました。
- 特権アクセス ロール (23 ページ) - この更新トピックでは、特権アクセス ロールをユーザに割り当てるときの考慮事項が追加されました。.
- 管理ロールへのユーザの割り当て方法 (26 ページ) - この新規トピックでは、管理ロールをユーザに割り当てるプロセスについて説明します。
- Active Directory の制限 (32 ページ) - この新規トピックでは、ユーザ ストアとして Active Directory を使用する場合に実行できない CA Access Control エンタープライズ管理 タスクについて説明します。
- ポリシーのデプロイのトラブルシューティング (83 ページ) - この更新トピックでは、[復元]オプションの変更に関する記述が追加されました。
- 特権アカウントの管理 (91 ページ) - この章の多くのトピックを更新して、ユーザが実行する PUPM 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より明確にしました。 さらに、この章では以下の変更が加えられました。
  - Windows エージェントレス接続情報 (107 ページ) - この更新トピックでは、WMI DYN Namespace エンドポイント タイプの名前が変更されました。
  - SSH Device 接続情報 (108 ページ) - この更新トピックでは、SSH DYN Namespace エンドポイント タイプの名前が変更されました。
  - SSH Device XML ファイルのカスタマイズ (109 ページ) - この新規トピックでは、SSH Device XML ファイルをカスタマイズする方法について説明します。
- 特権アカウント リクエストへの応答 (127 ページ) - この更新トピックでは、特権アカウント リクエストに応答するための要件について説明します。
- UNAB の設定方法 (136 ページ) - 「UNAB の動作の仕組み」に代わるトピックです。
- UNAB のユーザ認証の仕組み (136 ページ) - この更新トピックでは、UNAB がユーザを認証する方法についての情報が追加されました。
- 移行競合の解決 (140 ページ) - この更新トピックでは、UNAB 競合ファイル出力の例が追加されました。

第 1 版

このマニュアルの第 1 版は r12.5 と一緒にリリースされました。 この版では、リリース r12.0 SP1 に対して以下の更新が行われました。

- 概要 (15 ページ) - この章を更新して、基本的なエンタープライズ管理機能に関する情報を追加しました。
- CA Access Control エンタープライズ管理 の管理 (19 ページ) - この章の多数のトピックを更新して、インターフェースの変更を反映しました。

  また、この章に以下の新規コンテンツを追加しました。

  - 特権アクセス ロール (23 ページ) - この新規トピックでは、特権アクセス ロールについて説明します。
  - 管理タスクの作成 (28 ページ) - この新規トピックでは、管理タスクの追加方法について説明します。
  - グループのタイプ (35 ページ) - この新規セクションでは、インターフェースがサポートするグループのタイプについて説明します。
  - 監査データ (39 ページ) - この新規セクションでは、CA Access Control エンタープライズ管理 が提供する監査機能について説明します。
- エンタープライズ実装の表示 (45 ページ) - この更新された章では、インターフェースの変更および新たに利用可能になった新機能について説明します。
- ポリシーの一元管理 (49 ページ) - この章の多数のトピックを更新して、インターフェースの変更を反映し、概念の説明をより明確にしました。

  また、この章に以下の新規コンテンツを追加しました。

  - ポリシー タイプ (49 ページ) - この新規トピックでは、CA Access Control r12.5 で利用可能ではあるが、拡張ポリシー管理を使用して管理されない、2 つの追加ポリシー タイプについて説明します。
  - デプロイメント メソッドがデプロイメント タスクに影響を及ぼす仕組み (52 ページ) - この新規トピックでは、デプロイメント タスクが生成される仕組みについて説明します。
  - ポリシーのインポート (71 ページ) - この新規トピックでは、既存の PMDB または CA Access Control データベースからポリシーを作成する仕組みについて説明します。
  - 変数 (78 ページ) - この新規セクションでは、CA Access Control の新規変数、およびポリシー内でのこれらの変数の使用方法について説明します。
- 特権アカウントの管理 (91 ページ) - この新しい章では、PUPM 管理者の観点から見た、新規特権ユーザ パスワード管理 (PUPM) 機能について説明します。
- 特権アカウントの使用 (121 ページ) - この新しい章では、PUPM エンドユーザの観点から見た、PUPM の新規機能について説明します。

- エンドポイントの特権アカウントの使用（131 ページ） - この新しい章では、エンドポイントで使用可能な PUPM の新規機能について説明します。
- UNAB の使用（135 ページ） - この新しい章では、UNIX の認証ブローカ（UNAB）機能、および CA Access Control エンタープライズ管理 からこの機能を管理する方法について説明します。
- レポートの作成（145 ページ） - この更新された章では、CA Access Control エンタープライズ管理 のレポート機能に関連する現行のアーキテクチャおよびプロセス、および新規標準レポートについて説明します。
- サンプル ポリシーのデプロイ（185 ページ） - この更新された章では、サンプル ポリシーについて説明します。 この章は、以前は「エンドポイント管理ガイド」にありました。 サンプル ポリシーは、CA Access Control の変数を使用するため、もはや selang を使用した直接デプロイに適さなくなりました。

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

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

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

本書の対象読者

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

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

エンタープライズ管理

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

エンタープライズ管理インターフェース

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

中央ポリシー管理

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

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

エンタープライズ ビュー

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

特権ユーザ パスワード管理

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

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

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

UNAB 管理

UNIX 認証ブローカ(UNAB)では、Active Directory データ ストアを使用して、UNIX コンピュータにログインできます。 これは、すべてのユーザが単一のリポジトリを使用して、すべてのプラットフォームに、同じユーザ名とパスワードでログインできることを意味します。

Active Directory に UNIX アカウントを統合することにより、認証およびパスワード ポリシーをより強化し、UNIX ユーザおよびグループの基本的なプロパティを Active Directory へ転送します。 これによって、Windows でのユーザおよびグループの管理と同様に、UNIX ユーザおよびグループの一元管理が可能になります。

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

エンタープライズ レポート

CA Access Control エンタープライズ管理 のレポート オプションを使用すると、各エンドポイント(ユーザ、グループ、およびリソース)のセキュリティ ステータスを 1 か所で確認できます。 各エンドポイントからのデータの収集は、スケジュールで設定することも、オンデマンドで行うこともできます。 各エンドポイントに接続しなくても、誰がどのリソースへのアクセスを許可されているかを確認することができます。

CA Access Control は、一度の設定だけで各エンドポイントからデータの収集および中央のサーバへのデータのレポートを独立して実行します。また、手動による操作を必要とせず、エンドポイントのステータスを継続的にレポートします。 つまり、たとえ収集サーバがダウンした状態であっても、各エンドポイントは自身のステータスについてレポートします。

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

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

このセクションには、以下のトピックが含まれています。

管理スコープ

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

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

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

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

CA Access Control エンタープライズ管理 の管理ロール

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

管理ロールの作成

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

管理ロールの作成方法

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[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(26 ページ)。

8. [サブミット]をクリックします。

ロールが作成されます。

特権アクセス ロール

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

- Break Glass - このロールが割り当てられたユーザは、Break Glass 特権アカウント パスワードのチェックアウトを実行できます。 Break Glass チェックアウトを実行すると、特権アクセスが割り当てられていないエンドポイントに即座にアクセスできます。このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- エンドポイント特権アクセス ロール - このロールが割り当てられたユーザは、指定されたエンドポイント タイプ上で特権アカウント タスクを実行できます。 新しいエンドポイント タイプを初めて定義すると、CA Access Control は対応するエンドポイント特権アクセス ロールを作成します。 たとえば、CA Access Control エンタープライズ管理 で Windows エンドポイントを初めて作成すると、CA Access Control は Windows エージェントレス接続エンドポイント特権アクセス ロールを作成します。
- 特権アカウント リクエスト - このロールが割り当てられたユーザは、特権アカウント パスワードのリクエストをサブミットまたは削除できます。 このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- PUPM 承認者 - このロールが割り当てられたユーザは、CA Access Control エンタープライズ管理 ユーザがサブミットした特権アカウント リクエストに応答できます。このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。
- PUPM 監査マネージャ - この特権アカウント ロールが割り当てられたユーザは、特権アカウント アクティビティの監査および CA Enterprise Log Manager 監査収集パラメータの管理を行うことができます。
- PUPM ポリシー マネージャ - このロールが割り当てられたユーザは、ロール メンバとメンバ ポリシーの管理、ロール所有者の割り当て、およびロールの作成と削除を行うことができます。
- PUPM ターゲット システム マネージャ - このロールが割り当てられたユーザは、パスワード ポリシーと特権アカウントを管理でき、さらに特権アカウント検出ウィザードを使用してエンドポイント上の特権アカウントを検出できます。
- PUPM ユーザ - このロールが割り当てられたユーザは、使用が許可されている特権アカウント パスワードをチェックインおよびチェックアウトできます。 このロールは、デフォルトで、CA Access Control エンタープライズ管理 内のすべてのユーザに割り当てられます。

- PUPM ユーザ マネージャ - このロールが割り当てられたユーザは、CA Access Control エンタープライズ管理 ユーザ、グループ、およびパスワード ポリシーを管理し、ユーザの作業アイテムを管理できます。

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

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

特権アクセス ロールの作成

特権アクセス ロールは、ロール メンバ、管理者、および所有者が、PUPM 使用時に実行可能なタスク、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などを定義できます。

特権アクセス ロールの作成方法

注: 特権アカウントを管理するには、管理権限が必要です。

1. [ユーザおよびグループ]-[ロール]-[特権アクセス ロール]-[ロールの作成]を選択します。

   [ロールの作成]画面が表示されます。

2. [新規ロールの作成]を選択し、[OK]をクリックします。

   [ロール プロファイル]タブが表示されます。

3. [ロール名]および[説明]を入力します。 [有効化]を選択して、ロールを有効にします。

   [タスク]タブへの移動

4. プルダウン フィルタ タスクを展開し、対応するタスクを選択して、タスクを追加します。

   [メンバ]タブへ移動します。

5. [追加]をクリックしてメンバを追加します。

   [メンバ ポリシー]画面が表示されます。

6. メンバ ルールおよびスコープ ルールを選択し、[OK]をクリックします。

7. (オプション)[管理者はこのロールにメンバを追加および削除可能]チェック ボックスを選択します。

   [アクションの追加]および[アクションの削除]フィールドが表示されます。

8. 両方のフィールドから適用するオプションを選択します。

   [管理者]タブへ移動します。

   注: ロール管理者を追加するには、[メンバ]タブで[管理者はこのロールに対してメンバの追加削除が可能]を選択します。

9. [追加]をクリックして、ロールに管理者を追加します。

   ポリシー検索画面が表示されます。

10. 管理者ルール、スコープ ルール、および管理者権限を選択し、[OK]をクリックします。

    [所有者]タブへ移動します。

11. [追加]をクリックして、ロール所有者を追加します。

    [所有者の選択]画面が表示されます。

12. ロール所有者を選択し[OK]をクリックします。

13. [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 は特権アクセス ロールを作成します。

ユーザへの管理ロールの割り当て方法

以下の方法で、管理ロールをユーザに割り当てることができます。

- 複数のユーザを管理ロールに追加、または管理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。
- 単一ユーザを管理ロールに追加、または管理ロールから削除するには、[ユーザの変更]タスクの[管理ロール]タブを使用します。
- [管理ロールの変更]タスク中の[メンバ]タブを使用して、ロールのメンバ ポリシーを変更します。

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 (27 ページ) 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] (28 ページ) 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（28 ページ）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］（28 ページ）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（28 ページ）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(30 ページ)
タブの追加(30 ページ)

フィールド、イベントおよびロール使用の設定 (31 ページ)

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使用するか、新規検索画面を作成するか選択できます。新規検索画面は、このタスク専用の情報を表示し、検索オプションを提供します。

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、[OK]を選択します。

   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は、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 ロールに関するタブ表示情報を使用します。 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 (32 ページ)
グループのタイプ (35 ページ)

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
- グループの作成
- グループの削除

この制限が発生するのは、CA Access Control エンタープライズ管理 をインストールし、ユーザ ストアとして Active Directory を指定した場合、CA Access Control は Active Directory にプロキシ ユーザを作成するためです。 このプロキシ ユーザには、Active Directory でユーザとグループを作成および削除する権限がありません。

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

ユーザ パスワードをリセットするには、以下の手順に従います。 このオプションを使用するのは、何回かのログイン試行が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したか忘れた場合です。

ユーザ パスワードのリセット方法

1. ユーザ管理権限を持ったユーザとして CA Access Control エンタープライズ管理にログインします。
2. [ユーザ]-[ユーザの管理]-[ユーザ パスワードのリセット]を選択します。
   ユーザ パスワード リセットの検索ウィンドウが開きます。
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て、ユーザがそのアカウントを CA Access Control エンタープライズ管理 内で使用できるようにします。 ユーザ アカウントを無効にして、そのユーザが CA Access Control エンタープライズ管理 にアクセスできないようにし、ユーザ プロファイルをシステム内に保持します。

ユーザ アカウントを有効または無効にする方法

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. [ユーザ]-[ユーザの管理]-[ユーザの有効化/無効化]を選択します

   ユーザの有効化/無効化の検索ウィンドウが開きます。
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. 有効または無効にするユーザ アカウントを選択し、[選択]をクリックします。
5. [はい]を選択して、タスクを確認します。

   CA Access Control エンタープライズ管理 はアカウントを有効または無効にします。

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。

動的グループ クエリのパラメータ

検索時には、以下の動的なクエリ パラメータを使用できます。

LDAP:///<検索ベース DN>??<検索範囲>?<検索フィルタ>

このコマンドの形式は以下のようになります。

search_base_DN

LDAP ディレクトリ内での、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レベルにあるエントリを返します。

one -- URL で指定したベース DN よりも 1 レベル下にあるエントリを返します。

base -- 検索オプションとして指定したベースを無視して、代わりに one 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いるユーザ全員が取得されます

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。

(<論理演算子><比較><比較...>)

<論理演算子> には、以下のいずれかを使用します。

論理 OR: |

論理 AND: &

論理 NOT: !

<比較> には、<属性><演算子><値> を指定します。

例:

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

デフォルトの検索フィルタは (objectclass=*) です。

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 PUPM LDAP ディレクトリ内で行われます。

例: サンプル LDAP クエリ

以下の例は、グループ作成時に使用できる LDAP クエリのサンプルが含まれています。

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)
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。

CA Access Control エンタープライズ管理 の監査

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。

詳細情報:

サブミット済みタスクの検索 (40 ページ)
タスクの詳細の表示 (43 ページ)
イベントの詳細の表示 (44 ページ)

サブミット済みタスクの検索

サブミット済みタスクを検索するには、以下の手順に従います。

サブミット済みタスクの検索方法

1. [ホーム]-[マイ サブミット済みタスクの表示]を選択します。

   [サブミット済みタスクの表示]ページが表示されます。

2. 検索条件 (40 ページ) 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。

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: タスクのフィルタに[承認者]条件を選択した場合は、デフォルトで[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「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 ステータス

検索条件としてタスク ステータスを識別します。 タスク ステータスを選択するには、[タスク ステータスの条件 =]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

注: 詳細については、「タスク ステータスの定義」を参照してください。

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 ステータスを選択するには、[タスク ステータスの条件 =]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。

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、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[設定実行対象]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。 詳細については、この画面に関するオンライン ヘルプを参照してください。

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。

承認済みタスクの表示

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 (42 ページ)

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

PUPM 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する時に表示されます。 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、PUPM 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。

監査済み

現在のタスクが監査済みの場合に表示されます。

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には、以下の手順に従います。

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(タスクの詳細)]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. [閉じる]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には、以下の手順に従います。

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. [閉じる]をクリックします。

   [イベントの詳細]ページが閉じます。

第 3 章: エンタープライズ実装の表示

このセクションには、以下のトピックが含まれています。

ワールド ビュー

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

CA Access Control エンドポイントは、拡張ポリシー管理を使用することにより、単一のデプロイ マップ サーバ (DMS) からポリシーの更新内容を受け取ることができます。 1 回設定するだけで、CA Access Control ユーティリティおよび selang コマンド、または CA Access Control エンタープライズ管理 インターフェースを使用して、エンドポイント上のポリシー (ルール グループ) を管理することができます。

CA Access Control のエンタープライズ実装は、以下の方法で表示できます。

- ホスト名別

  DMS に定義しているホスト (エンドポイント) です。
- ホスト グループ別

  定義している論理ホスト グループです。
- ポリシー別
- 管理対象デバイス別

これらの結果を使用して、以下のことができます。

- 接続した DMS に報告されるエンドポイントを識別できます
- 各エンドポイントが DMS にハートビートを最後に送信した日時を確認できます
- 各エンドポイント上にデプロイされているポリシーを確認できます
- リンクをクリックし、CA Access Control エンドポイント管理 を使用してエンドポイントを管理できます

CA Access Control のエンタープライズ実装の表示

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

CA Access Control のエンタープライズ実装の表示方法

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

   [ワールド ビュー]ページが開き、[検索]セクションが表示されます。

2. (オプション)検索条件を定義します。

   2 種類の検索を使用できます。

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

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

3. [実行]をクリックします。

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

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

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

CA Access Control エンタープライズ管理 では、CA Access Control エンドポイント管理 に簡単にログインして、CA Access Control エンタープライズ管理 が管理する任意のエンドポイントを管理することができます。

CA Access Control でエンドポイントへ自動ログインできるようにしたい場合は、CA Access Control エンタープライズ管理 と CA Access Control エンドポイント管理 で同じユーザ名とパスワードを使用していること、および CA Access Control エンドポイント管理 を使用してエンドポイントを管理する端末アクセス権限があることを確認してください。

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

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

   CA Access Control エンドポイント管理 が開き、エンドポイントのホスト名およびユーザのクレデンシャルが自動的に入力されます。

詳細情報:

CA Access Control のエンタープライズ実装の表示 (46 ページ)

PUPM エンドポイントの変更

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

PUPM エンドポイントの変更

1. [ワールドビュー]-[ワールドビュー]タスクを選択します。
   [ワールドビュー]検索画面が表示されます。
2. クエリを入力し、[実行]をクリックします。
   クエリの検索結果が表示されます。
3. [表示]オプションを選択して、変更する PUPM エンドポイントを選択します。
   プルダウン メニューに、エンドポイント上の管理対象デバイスが表示されます。
4. [変更]を選択して、エンドポイント設定を変更します。
   [エンドポイントの変更]ウィンドウが表示され、エンドポイント設定が表示されます。
5. エンドポイント設定を変更し、[サブミット]をクリックします。
   タスクが完了したことを通知するメッセージが表示されます。

第 4 章: ポリシーの一元管理

このセクションには、以下のトピックが含まれています。

ポリシータイプ

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

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

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

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

本章では、CA Access Control ポリシーの使用方法について説明します。

詳細情報:

ホストへのログイン権限の定義 (137 ページ)
ホスト環境設定トークンの定義 (138 ページ)

ポリシーの一元管理の方法

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

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

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

- 拡張ポリシー管理 - デプロイしたポリシー(ルールの集まり)は、ホストまたはホストグループの割り当てに基づいてすべてのデータベースに伝達されます。 また、ポリシーのデプロイ解除(削除)、デプロイのステータスやデプロイの偏差の表示を行うこともできます。 この機能を使用するには、追加のコンポーネントをインストールおよび設定する必要があります。

  注: 拡張ポリシー管理の詳細については、「エンタープライズ管理ガイド 」を参照してください。

拡張ポリシー管理

作成した複数ルールのポリシー(selang コマンド)を格納し、指定した方法でエンタープライズ環境にデプロイできます。 このポリシー ベースの方法を使用すれば、ポリシーを格納したうえで、それらをホストまたはグループ ホストに割り当てることができます。 ポリシーは割り当てられると、デプロイのためにキューに登録されます。 あるいは、ホストまたはホスト グループに対するポリシー バージョンのデプロイおよびデプロイ解除を直接行うこともできます。

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

注: デュアル コントロールはこの方法では使用できません。UNIX でのみ使用可能です。 詳細については、「UNIX エンドポイント管理ガイド」を参照してください。

拡張ポリシー ベース管理のしくみ

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

以下の方法で、高度なポリシー ベースの管理作業を行います。

1. ポリシーを作成します。

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

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

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

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

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

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

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

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

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

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

6. DMS はデプロイ タスクを配布ホスト(DH)に送信します。

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

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

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

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

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

詳細情報:

ポリシーの依存関係(64 ページ)
ポリシー検証(64 ページ)
割り当てパス(61 ページ)
ホスト アクセス制御および UNAB 設定の仕組み(137 ページ)

デプロイメント メソッドがデプロイメント タスクに影響を及ぼす仕組み

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

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

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

- 1 つ以上のホストにポリシー(GPOLICY オブジェクト)を割り当てます。

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

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

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

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

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

- 1 つ以上のホストへのポリシーの再デプロイ

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

- HNODE でポリシーをリストアします(ホストでデプロイが必要なポリシーを再デプロイします)。

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

- 1 つ以上のホストでのデプロイ済みポリシーのアップグレード

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

例: ポリシーのホストへの割り当て

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

例: ポリシーのホスト グループへの割り当て

ホスト グループ「Servers」には、「hostA.comp.com」と「hostB.comp.com」の 2 つのメンバがあります。 ポリシー IIS がホスト グループ Servers に割り当てられると、CA Access Control は 2 つのデプロイメント タスクを作成します。1 つは最新の IIS ポリシー バージョンを hostA.comp.com にデプロイするタスクで、もう 1 つは最新の IIS ポリシー バージョンを hostB.comp.com にデプロイするタスクです。

例: ホストの割り当て済みポリシーを持つホスト グループへの追加

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

例: ホストのリストア

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

例: デプロイ済みポリシーのアップグレード

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

詳細情報:

ホスト アクセス制御および UNAB 設定の仕組み(137 ページ)

DMS が保持するエンドポイント データ

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

- ポリシーのデプロイおよびデプロイ解除

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

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

- ホスト ハートビート

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

- 偏差ステータス

  各ハートビート送信後、エンドポイントはポリシー偏差を計算し、結果(偏差の検出または未検出)を送信します。 policyfetcher によってエンドポイントと DH 間のデプロイメントおよび偏差ステータスにコンフリクトが検出された場合、エンドポイントの情報に基づいてコンフリクトを解決します。

エンドポイントが DMS を更新する仕組み

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

1. DH が通知メッセージを更新ファイルに格納します。

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

2. DH がそのサブスクライバである DMS にアクセスします。

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

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

   レポートを作成するたびに、CA Access Control は DMS にある情報を取得します。

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

詳細情報:

ホスト アクセス制御および UNAB 設定の仕組み(137 ページ)

拡張ポリシー管理クラス

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

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

注: 上記のクラスで受け入れられるプロパティの詳細については、「selang リファレンス ガイド」を参照してください。

DEPLOYMENT クラス

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

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

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

GDEPLOYMENT クラス

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

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

HNODE クラス

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

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

GHNODE クラス

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

POLICY クラス

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

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

GPOLICY クラス

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

オブジェクトの名前は、論理ポリシーの名前です。

RULESET クラス

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

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

ホストおよびホスト グループ

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

エンドポイントを企業内のホストとして定義

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

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

エンドポイントを企業内のホストとして定義する方法

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

   [ホストの作成]、[ホストの削除]、[ホストの変更]、[ホストの表示]の 4 つのタスクが表示されます。

2. [ホストの作成]をクリックします。

   [ホストの作成: 標準検索画面(汎用)の設定]が表示されます。

3. [OK]をクリックします。

   [ホストの作成]タスク ページが表示されます。

4. ダイアログ ボックスで以下のフィールドを完了します。

   名前

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

   説明

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

   IP アドレス

   (オプション)ホストの IP アドレスを定義します。

   [サブミット]をクリックします。

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

論理ホスト グループの定義

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

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

論理ホスト グループの定義方法

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

   [ホスト グループの作成]が使用可能なタスク リストに表示されます。

2. [ホスト グループの作成]をクリックします。

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

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

   [ホスト グループの作成]タスク ページが表示されます。

4. ダイアログ ボックスで以下のフィールドを完了します。

   名前

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

   説明

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

5. [ホスト選択]をクリックし、次に[追加]をクリックします。

   [メンバの追加]ダイアログ ボックスが表示されます。

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

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

7. [サブミット]をクリックします。

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

ホスト グループのインポート

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

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

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

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

ホスト グループのインポート方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
   a. [ポリシー管理]をクリックします。
   b. [ホスト]サブタブをクリックします。
   c. 左側のタスク メニューで[ホスト グループ]ツリーを展開します。
      [ホスト グループ インポート]タスクが使用可能なタスク リストに表示されます。
2. [ホスト グループ インポート]をクリックします。
   [PMDB ホスト ログイン]ページが表示されます。
3. ユーザ名、パスワード、および PMDB 名を入力し、[ログイン]をクリックします。
   注: PMDB 名は「PMDB 名@ホスト」形式で、たとえば「master_pmdb@example」のように指定します。
   [全般]タスク ステージに、ホスト グループ インポート ウィザードが表示されます。
4. ウィザードを終了し、サマリを読んでから[完了]をクリックします。
   CA Access Control はホストをホスト グループに追加します。 ホストが DMS に存在しなければ、CA Access Control はホストの HNODE オブジェクトを作成してから、ホストをホスト グループ(GHNODE)に追加します。
   注: 既存のホスト グループにホストを追加する場合、CA Access Control はホスト グループに割り当てられた任意のポリシーを、自動的にホストにデプロイします。

割り当てパス

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

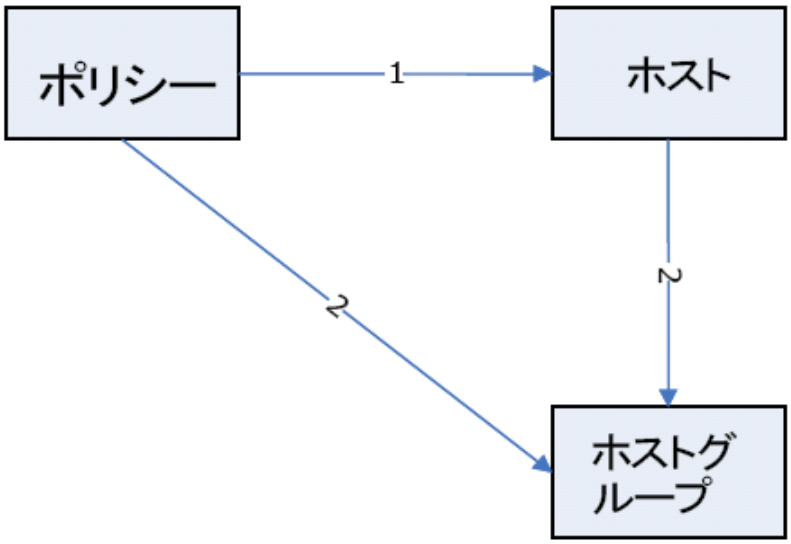
- ポリシーはホストに直接割り当てられます。
- ポリシーはホストが属するホスト グループに割り当てられます。
- ホストは、1 つ以上のポリシーが割り当てられているホスト グループに追加されます。

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

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

例: ポリシー IIS の複数の割り当てパス

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



例: 割り当てパスの削除

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

ポリシーを作成しデプロイする方法

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

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

1. ポリシー バージョンを DMS に保存します。

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

2. ポリシーを確認します。

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

3. ポリシーをファイナライズします。

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

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

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

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

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

詳細情報:

ホストへのログイン権限の定義(137 ページ)
ホスト環境設定トークンの定義(138 ページ)
割り当てパス(61 ページ)

管理要件

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

DMS にポリシーを格納する場合

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

ポリシーをホストまたはホスト グループに割り当てる方法

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

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

ポリシーの依存関係

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

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

ポリシーの依存関係は、ポリシーを作成または変更するときに定義します。

ポリシー検証

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

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

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

ポリシー検証では、デプロイ解除スクリプトを確認できません。

ポリシー検証の仕組み

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

.**注**: ポリシー検証はデフォルトでは有効になっていません。

以下のプロセスでは、ポリシー検証の仕組みについて説明します。

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

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

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

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

ポリシー検証の有効化

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

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

ポリシー検証が有効になります。

ポリシー バージョンの作成および格納

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

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

ポリシー バージョンの作成および格納

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

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

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

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

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

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

   [ポリシー]タスクが表示されます。

4. [ポリシーの作成]をクリックします。

   [ポリシーの作成: 標準検索画面 (汎用) の設定]が表示されます。

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

5. [OK]をクリックします。

   [ポリシーの作成]タスク ページが表示されます。

6. ダイアログ ボックスで以下のフィールドを完了します。

   名前

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

   説明

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

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

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

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

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

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

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

8. （オプション）このポリシー バージョンに関する説明を入力します。

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

9. （オプション）［サブミット時にファイナライズ］を選択します。

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

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

10. ［ポリシーの依存関係］タブをクリックし、［追加］をクリックします。

    ［メンバの追加］ダイアログ ボックスが表示されます。

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

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

12. [サブミット]をクリックします。

    タスクがサブミットされ、成功すると、新規ポリシー バージョンが作成されたことを示すメッセージがすぐに表示されます。

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

詳細情報:

ホストへのログイン権限の定義(137 ページ)
ホスト環境設定トークンの定義(138 ページ)

変数を定義するポリシーの作成

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

変数を定義するポリシーの作成方法

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

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

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

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

3. ポリシーを DMS に保存します。

例: 変数を定義するポリシーの作成

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

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

エンドポイントがポリシーをコンパイルすると、以下のルールを作成します。

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

例: 複数の変数値を定義するポリシーの作成

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

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

エンドポイントがポリシーをコンパイルすると、以下のルールを作成します。

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

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

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

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

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

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

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

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

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

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

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

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

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

ポリシーに関連付けられたルールの表示

DMS にポリシーを格納したら、GPOLICY、POLICY、および RULESET オブジェクトに対する読み取り権限を持つすべてのユーザが、ポリシーおよびそれに関連付けられたバージョンを参照できます。

ポリシーに関連付けられたルールを表示するには、以下の手順に従います。

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

   [ポリシー]タスクが表示されます。

2. [ポリシーの表示]をクリックして、新しいポリシーを表示します。

   [ポリシーの表示: 標準検索画面(汎用)の設定]が表示されます。

3. 検索範囲を定義して、[検索]をクリックします。

   定義した検索範囲と一致したポリシーのリストが表示されます。

4. 表示するポリシーを選択し、[選択]をクリックします。

   [ポリシーの表示: policyName]ページが表示されます。 ページ上のさまざまなタブで、ポリシーのプロパティを参照できます。プロパティには、ポリシーの名前および説明、最新のバージョンのためのデプロイおよびデプロイ解除のスクリプト、このポリシーに対して存在するすべてのポリシー バージョンのリスト、ポリシーの作成および更新に関する一般的な情報などがあります。

5. [バージョン履歴]タブをクリックします。

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

6. 以下のいずれかの操作を行います。

   - [デプロイ スクリプト]リンクをクリックします。

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

   - [デプロイ解除スクリプト]リンクをクリックします。

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

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

ポリシーのインポート

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

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

ポリシーのインポート方法

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

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

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

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

   [全般]タスク ステージに、ポリシー インポート プロセス ウィザードが表示されます。
4. 以下のフィールドに入力し、[次へ]をクリックします。

   名前

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

   説明

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

ポリシー クラス

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

依存クラスのエクスポート

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

［ポリシー スクリプト］ステージが表示されます。

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

   ［サマリ］ステージが表示されます。

6. ［終了］をクリックします。

   ポリシーが作成されます。

格納されたポリシー バージョンの割り当て

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

注: この手順は、ログイン ポリシーと設定ポリシーには適用されません。

格納されたポリシー バージョンをデプロイする方法

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

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

2. ウィザードを終了し、サマリを読んでから［完了］をクリックします。

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

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。 policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

ポリシーのメンテナンス

デプロイ済みのポリシーに対して、以下のアクションを実行できます。

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

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

割り当てられたポリシーの割り当て解除

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

割り当てられたポリシーを割り当て解除するには、以下の手順に従います。

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

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

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

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

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。 policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

割り当てられたホストを最新のポリシー バージョンにアップグレード

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

割り当てられたホストを最新のポリシー バージョンにアップグレードする方法

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

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

2. ウィザードを終了し、サマリを読んでから[完了]をクリックします。

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

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

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。 policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

割り当てられたホストを特定のポリシー バージョンにダウングレード

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

割り当てられたホストを特定のポリシー バージョンにダウングレードす方法

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

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

2. ウィザードを完了します。

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

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。 policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

削除ポリシー

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

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

削除できないポリシー

以下の場合、ポリシーを削除できません。

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

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

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

削除できないポリシー バージョン

以下の場合、ポリシーを削除できません。

- ポリシー バージョンがホスト上に割り当てられているかデプロイされている場合。

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

- ポリシー バージョンに DMS 上のステータスが含まれている場合。

  ポリシー バージョンを割り当て解除またはデプロイ解除するか、ホストからポリシー バージョンを削除してからポリシー バージョンを削除する必要があります。

- 失敗したデプロイ解除ステータスがポリシーに含まれている場合。

  このステータスを削除することはできません。 そのため、ポリシー バージョンは削除できません。

ポリシーの削除

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

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

ポリシーの削除方法

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

   [ポリシー]タスクが表示されます。

2. [ポリシーの削除]をクリックします。

   [ポリシーの表示: 標準検索画面(汎用)の設定]画面が表示されます。

3. 検索範囲を定義して、[検索]をクリックします。

   定義した検索範囲と一致したポリシーのリストが表示されます。

4. 削除するポリシーを選択し、[選択]をクリックします。

   ポリシー削除の確認メッセージが表示されます。

5. [はい]をクリックします。

   ポリシーは削除されます。

注: policydeploy ユーティリティを使用して、このタスクを実行することもできます。 policydeploy ユーティリティの詳細については、「リファレンス ガイド」を参照してください

詳細情報:

削除できないポリシー(75 ページ)

ポリシー バージョンの削除

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

ポリシー バージョンを削除するために、以下のコマンドを実行します。

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

-delete name#xx

指定されたポリシー バージョンを削除します。

-dms list

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

例: IIS 5 保護ポリシー バージョンの削除

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

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

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

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

変数

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

変数の作成方法

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

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

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

変数タイプ

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

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

ユーザ定義変数

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

静的変数

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

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

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

レジストリ値変数

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

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

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

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

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

オペレーティング システム変数

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

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

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

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

組み込み変数

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

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

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

<!HOSTNAME>

ローカル コンピュータの完全修飾ホスト名を識別します。

<!HOSTIP>

ホストの IP アドレスまたはアドレスを識別します。

<!AC_ROOT_PATH>

CA Access Control のインストール パスを識別します。

<!AC_REGISTRY_KEY>

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

<!USER_OS_ADMIN>

ローカル コンピュータ上のオペレーティング システムの管理者を識別します。

<!DOMAINNAME>

ローカル コンピュータの名前を識別します。

<!DNSDOMAINNAME>

ローカル コンピュータの DNS ドメイン名を識別します。

例: ポリシーでの組み込み変数の使用

この例では、ネットワーク リソース ルールを作成します。

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

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

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

変数使用のガイドライン

変数を使用する場合は、以下のガイドラインに準拠する必要があります。

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

エンドポイントで変数を解決する仕組み

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

1. policyfetcher がポリシーを取得すると、CA Access Control はポリシー内の変数がポリシーまたは CA Access Control データベースで定義されるかどうか確認します。以下のいずれかのイベントが発生します。

   - 変数がポリシーまたはデータベースで定義されていない場合、CA Access Control はポリシーのステータスを[デプロイの一時停止中]に変更します。

     注: .ポリシーをデプロイするには、未定義の変数を定義し、ポリシーを再デプロイする必要があります。

   - 変数がポリシーまたはデータベースで定義されている場合、CA Access Control はポリシーをコンパイルし、そのポリシーが含まれているルールを実行します。

2. すべてのハートビートで、policyfetcher は、CA Access Control データベース内で変数値が変更されているかどうか確認します。 以下のいずれかのイベントが発生します。

   - 変数値が変わっていない場合、policyfetcher は手順 2 を繰り返します。
   - 変数値が変わっている場合、CA Access Control は、変更された変数を使用している、エンドポイント上の任意のポリシーのポリシー ステータスを[非同期]に変更します。

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

ポリシーのデプロイのトラブルシューティング

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

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

以下のようなトラブルシューティング アクションがあります。

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

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

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

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

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

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

  このオプションを使用すると、すべてのポリシー デプロイ プロパティおよび拡張ポリシー管理プロパティから、エンドポイントおよび DMS でのエンドポイント ステータスが削除されます。

- Restore - 指定されたホストのポリシーをデプロイ解除した後、すべてのデプロイ タスクをそのホストに再送して実行することで、デプロイ(割り当てまたは直接デプロイ)する必要のあるすべてのポリシーをホストにリストア(直接再デプロイ)します。

  このオプションを使用するのは、エンドポイントを手動でリセット(CA Access Control またはオペレーティング システムを再インストール)して、DMS が示す、そのエンドポイントで有効なすべてのポリシーを再デプロイする場合です。

  注: 復元の実行前にホストのステータスはリセットされません。したがって、すでにいくつかのポリシーがホストに適用されている場合、復元はエラーになります。

使用されなくなったエンドポイントの削除方法

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

古くなったノードを削除するには、以下のいずれかの操作を行います。

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

  ```
  dmsmgr -cleanup number_of_days -dms name
  ```

  number_of_days

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

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

  ```
  rr HNODE HNODE_name
  ```

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

デプロイメント監査情報の表示

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

デプロイメント監査情報の表示方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]、[デプロイ]サブタブを順にクリックし、[デプロイ監査]をクリックします。

   [デプロイ監査]ページが表示されます。

2. デプロイ監査の範囲を定義して、[移動]をクリックします。

   CA Access Control エンタープライズ管理 は、定義された範囲内でデプロイに関する情報を取得し、しばらくしてから結果を表示します。

3. (オプション)デプロイのトリガをクリックして、関連付けされたデプロイ スクについて詳細情報を表示します。

ポリシー偏差計算のしくみ

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

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

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

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

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

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

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

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

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

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

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

4. 以下の 2 ファイルが出力されます。

- ACInstallDir/data/devcalc/deviation.log

  最後の偏差計算で収集されたログとエラー メッセージ。

- ACInstallDir/data/devcalc/deviation.dat

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

注: CA Access Control は監査イベントも送信します。監査イベントは seaudit -a を使用して表示できます。 seaudit ユーティリティの詳細については、「リファレンスガイド」を参照してください。

5. 検出された偏差を DMS に通知します。

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

偏差計算機能のトリガ

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

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

ポリシーの偏差ログおよびエラー ファイル

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

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

例: 偏差ログおよびエラー ファイル

偏差ログおよびエラー ファイルの例を以下に示します。

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

ポリシー偏差データ ファイル

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

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

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

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

ポリシー偏差データ ファイルに以下の行が表示されることがあります。

日付

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

形式: DATE, DDD MMM DD hh:mm:ss YYYY

Strict

偏差計算が -strict オプションを指定して実行されたことを示します。

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

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

ポリシーの開始

このポリシー バージョンの偏差を定義するポリシー ブロックを開始します。

形式: POLICYSTART, policy_name#xx

違い

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

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

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

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

ポリシーの終了

このポリシーの偏差を定義するポリシー ブロックの終了です。

形式: POLICYEND, policy_name#xx, [1|0]

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

警告

警告を示します。

形式: WARNING, "warning_text"

例: 偏差データ ファイル

以下の例は、偏差データ ファイルからの抜粋です。

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

不在要素を示す偏差

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

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

```
eu mytestuser2 operator
```

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

- USER クラスが存在する必要がある

  このルールでは、USER クラスに属するユーザが指定されています。

- USER オブジェクト mytestuser2 が存在する必要がある

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

- プロパティ OBJ_TYPE が存在する必要がある

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

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

  このルールでは、この値を明示的に設定します。

追加要素を示す偏差

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

ローカル例外で以下のような追加が行われた場合、追加の偏差が取り込まれます。

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

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

変更された要素を示す偏差

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

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

第 5 章: 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 は、特権のある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。

詳細情報:

ユーザ アカウントについて(91 ページ)

ユーザ 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にアクセス可能なアカウントです。 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 エンドポイント上にある、またはサービス 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る管理タスクを実行して、無人処理を容易に行えるようにします。

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、アクセス制御情報へのほとんどの内部制御を省略でき、アプリケーションを削除またはアクセス不能にして、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。

詳細情報:

特権ユーザ パスワード管理(91 ページ)

特権アクセス ロールおよび特権アカウント

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

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

詳細情報:

特権アクセス ロール(23 ページ)

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。 ユーザのマネージャは、CA Access Control エンタープライズ管理 でユーザを変更するときに指定できます。
- 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 (27 ページ)

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。
   - 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アウトします。

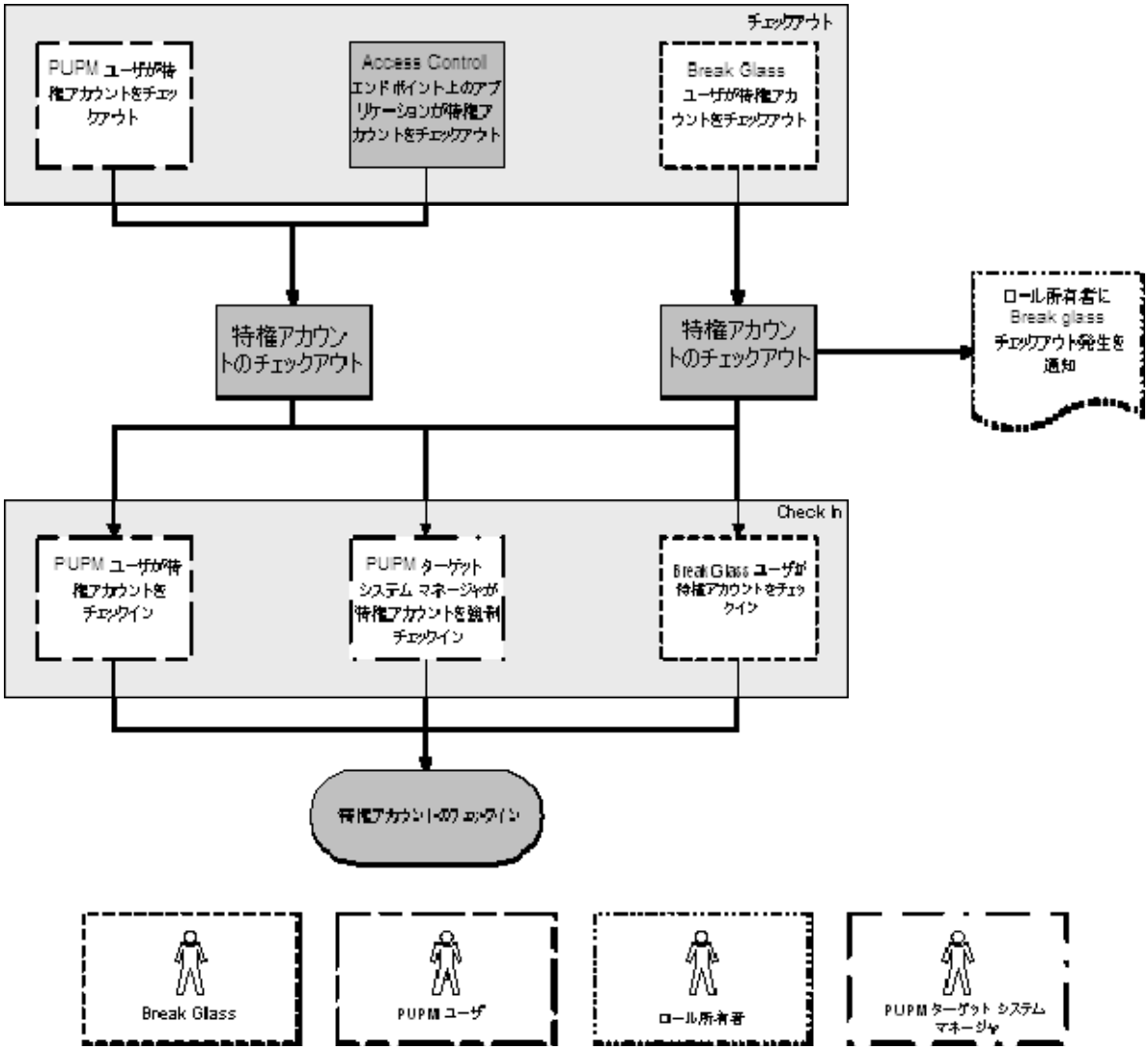
   特権アカウントがチェックアウトされます。

   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、このメッセージに監査用の情報を追加できます。

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。

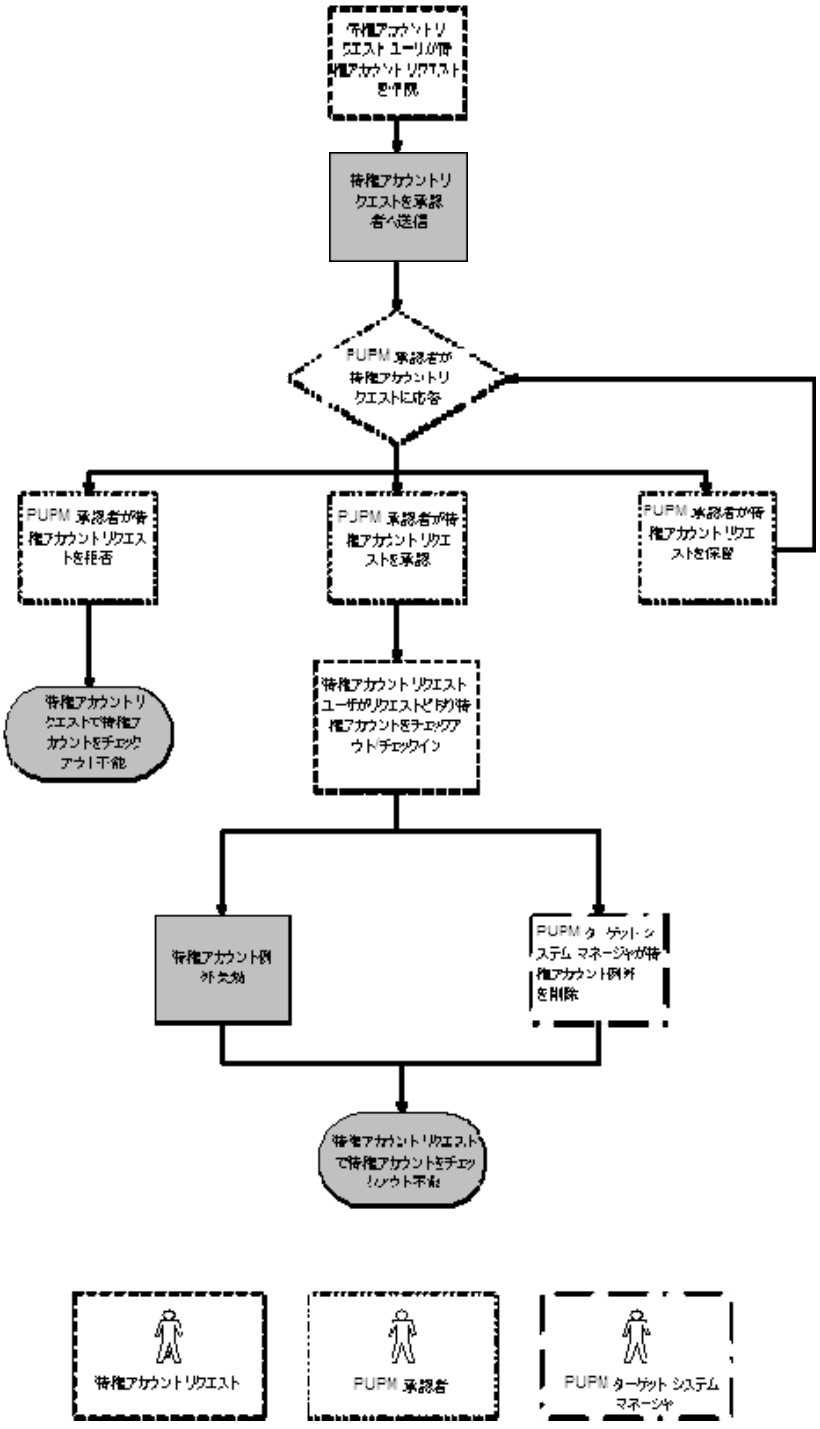
     特権アカウント リクエスト ロールを持つユーザに特権アカウント例外が付与され、そのユーザは特権アカウントをチェックアウトおよびチェックインできます。

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。

次の図に、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。

特権アカウントのセットアップ方法

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 用に設定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。

注：CA Access Control エンタープライズ管理 のインストール プロセスでは、デフォルトの Java 接続サーバ（JCS）が配布サーバの一部としてインストールおよび設定されます。 CA Access Control エンドポイント タイプ用の PUPM を使用する前に、インストールされ設定された Java 接続サーバ（JCS）が存在している必要があります。 CA Identity Manager コネクタを使用するには、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。

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。

注：システム マネージャ管理ロールが割り当てられたユーザは、このプロセスのすべてのタスクを実行できます。

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. 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。

2. 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、特権アカウントのパスワード ルールおよび制限事項を設定します。

3. PUPM ターゲット システム マネージャは、各エンドポイント上の特権アカウントを検出し、必要であれば特権アカウントを作成します。

   特権アカウントが検出されると、それらのアカウントは CA Access Control エンタープライズ管理 で管理可能になります。

4. （オプション） PUPM ターゲット システム マネージャは、追加の特権アカウントを作成します。

   たとえば、接続解除されたシステム上に特権アカウントを作成します。

5. （オプション） システム マネージャは、CA Access Control エンドポイント用のアプリケーションを作成します。

   アプリケーションを使用すると、スクリプト中のハードコーディングされたパスワードを必要な場合に限り PUPM エージェントが取得した特権アカウント パスワードで置き換えることができます。

6. PUPM ポリシー マネージャは、特権アクセス ロールのメンバ プロファイルを変更します。

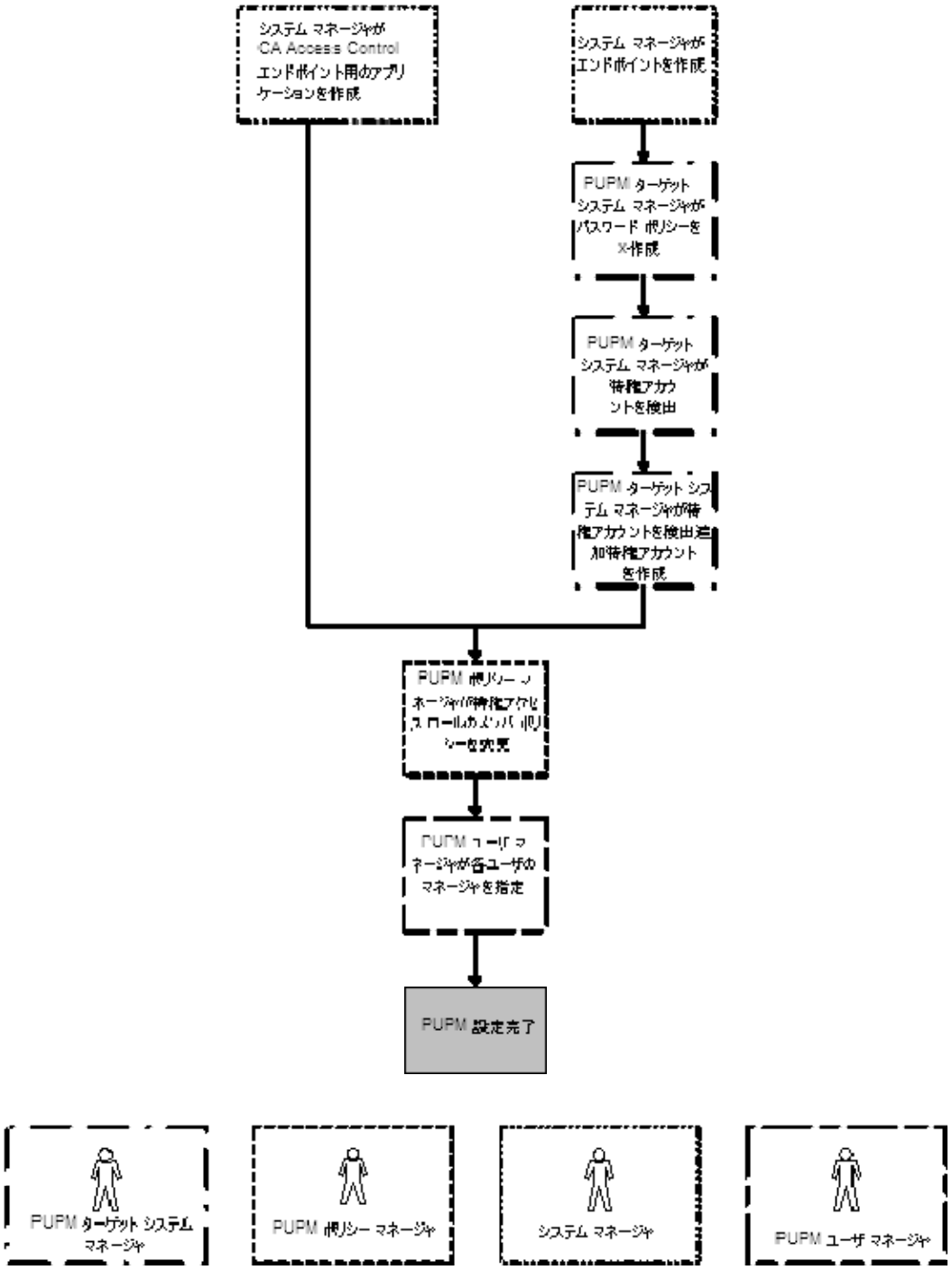
   メンバ ポリシーは、ロール内のタスクを実行できるユーザを定義します。

   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。

7. （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。

   ユーザが行う特権アカウント リクエストは、そのユーザのマネージャだけが承認できます。

次の図に、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。



エンドポイント タイプの表示

エンドポイント タイプは、サポートされている管理対象システム用の CA Access Control エンタープライズ管理 内の既存の定義です。 各エンドポイント タイプで、特権アカウントが存在するシステムのタイプを指定します。

エンドポイント タイプの表示方法

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]-[エンドポイントの表示]をクリックします。

   [エンドポイント タイプの表示:エンドポイント タイプの選択]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エンドポイント タイプのリストが表示されます。 これらは CA Access Control エンタープライズ管理 がサポートするエンドポイント タイプです。

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、エンドポイントを管理し、そのエンドポイント上の特権アカウントを検出できます。

エンドポイントを作成する方法

注: 特権アカウントを管理するには、管理権限が必要です。

1. [特権アカウント]、[エンドポイント]、[エンドポイントの作成]の順にクリックします。

   [エンドポイントの作成]検索画面が表示されます。

2. エンドポイントの作成を選択して[OK]をクリックします。

   [エンドポイントの作成]画面が表示されます。

3. 以下のパラメータを入力します。

   名前

   エンドポイント名を定義します。

   説明

   エンドポイントの説明を自由な形式で定義します。

   エンドポイント タイプ

   特権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。

   オプション: MS SQL Server(Microsoft SQL Server)、PeopleSoft、OS400(IBM i、旧 i5/OS および OS/400)、Kerberos Server、Oracle Server、Windows Agentless、SSH Device

ユーザ ログイン

ユーザのログイン名を定義します。

例: 管理者

パスワード

ユーザ アカウントのパスワーを定義します。

URL

エンドポイント タイプ別に、エンドポイントの URL を定義します。

例: ssh://computer_name.com

ホスト

ホストの完全修飾名を定義します。

4. [サブミット]をクリックします。

エンドポイントが作成されます。

MS SQL Server 接続情報

MS SQL Server エンドポイント タイプによって、Microsoft SQL Server 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、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。

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:microsoft:sqlserver://servername:port

例: jdbc:microsoft: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。

詳細

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

PeopleSoft 接続情報

PeopleSoft エンドポイント タイプによって、PeopleSoft Enterprise 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、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。

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

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

OS400 接続情報

OS400 エンドポイント タイプによって、IBM i（旧 i5/OS および OS/400）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、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。

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:as400://host;proxy server=ServerName:proxyServerPort

例: jdbc:as400://myiSeries;proxy server=myHODServer:3470

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。

詳細

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

Kerberos Server 接続情報

Kerberos Server エンドポイント タイプによって、Kerberos 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、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。

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

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

Oracle Server 接続情報

Oracle Server エンドポイント タイプを使用すると、Oracle データベース 特権アカウントを管理できます。

このタイプのエンドポイントを作成する場合、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

ユーザ ログイン

エンドポイントの管理ユーザの名前を定義します。

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。

詳細

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

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。

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。

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 だけを入力します。

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。

制限: true、false

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。

詳細

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

SSH Device 接続情報

SSH Device タイプを使用すると、UNIX 特権アカウントを管理できます。

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。

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。

環境設定ファイル

定義する SSH Device XML 環境設定ファイルの名前を指定します。

詳細

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

SSH Device XML ファイルのカスタマイズ

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を対象の SSH デバイスに適用しない場合、企業の要件に応じて SSH Device XML ファイルをカスタマイズできます。

SSH Device XML ファイルをカスタマイズする方法

1. CA Access Control エンタープライズ管理 で、ssh_connector_conf.xml ファイルを見つけます。 デフォルトでは、このファイルは以下の場所にあります。

   ```
   ¥Program Files¥CA¥AccessControlServer¥Connector Server¥conf¥override¥sshdyn¥
   ```

2. ファイルをコピーし、新しい名前で保存します。

   注: 新しいファイルを元のファイルと同じディレクトリに保存したことを確認します。

3. 作成したファイルを編集可能な形式で開きます。
4. 企業の要件に応じてパラメータを変更し、ファイルを保存します。
5. 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。(102 ページ)
6. [環境設定]フィールドに、作成した XML ファイルの名前を入力します。

   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。

7. 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(114 ページ)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。

8. 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。 デフォルトでは、ファイルは以下の場所にあります。

   ```
   ¥Program Files¥CA¥AccessControlServer¥Connector Server¥logs¥
   ```

9. 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。

例: SSH Device XML File のカスタマイズ

この例では、SSH Device XML ファイルを要件に応じてカスタマイズする方法を示します。 この例では、管理者が、エンドポイント上のユーザ アカウントを検出し、パスワードを変更するために PUPM が実行するコマンドのパラメータを修正します。

管理者は、ユーザ アカウントを検出するために PUPM が実行するコマンド(oGetUsers)のタイムアウト期間を 1000 ミリ秒に変更しました。 次に、管理者は、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(oChangePassword)のタイムアウト期間を 1500 ミリ秒に変更しました。 最後に、管理者は、アカウント パスワードをユーザに表示するときのタイムアウト期間(sWaitForText)を 1000 ミリ秒に変更しました。

```
<array name="oGetUsers">

        <item>

          <param name="sCommand" value="echo" />

          <param name="iWait" value="1000" />

        </item>

        <item>

        <param name="sCommand" value="cat /etc/passwd | cut -d: -f1 | grep -w
[%%filter%%]" />

            <param name="iWait" value="1000" />

        </item>

        </array>

                <array name="oChangePassword">

        <item>

           <param name="sCommand" value="echo" />

           <param name="iWait" value="1500" />

        </item>

        <item>

        <param name="sCommand" value="passwd [%%user%%]" />

           <param name="iWait" value="1000" />

           <param name="sWaitForText" value="word:" />

        </item>
```

CA Identity Manager プロビジョニング接続情報

CA Identity Manager プロビジョニング コネクタを使用すると、プロビジョニング サーバで定義した CA Identity Manager エンドポイントを管理できます。

注: CA Access Control エンタープライズ管理 のインストール プロセスでは、デフォルトの Java 接続サーバ(JCS)が配布サーバの一部としてインストールおよび設定されます。 CA Access Control エンドポイント タイプ用の PUPM を使用する前に、インストールされ設定された Java 接続サーバ(JCS)が存在している必要があります。 CA Identity Manager コネクタを使用するには、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。 CA Identity Manager エンドポイント タイプはすべて同じ接続情報を使用します。

このタイプのエンドポイントを作成する場合、以下の情報を提供して、CA Access Control エンタープライズ管理 がエンドポイントに接続できるようにします。

エンドポイント

CA Identity Manager プロビジョニング サーバで定義したとおりに、エンドポイント名前を定義します。

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

エンドポイントの管理対象アカウントとして、別の管理アカウントを使用するかどうかを指定します。

このオプションを指定する場合、エンドポイントに接続するために提供したアカウント情報ではなく、CA Access Control エンタープライズ管理 が使用するアカウントを定義します。

パスワード ポリシーの作成

パスワード ポリシーとは、パスワードの作成方法と、いつ期限が切れるかを決定する一連のルールおよび制限です。 パスワード ポリシーを作成するには、以下の手順に従います。

パスワード ポリシーの作成方法

注: 特権アカウントを管理するには、管理権限が必要です。

1. [特権アカウント]-[パスワード ポリシーの管理]-[パスワード ポリシーの作成]を選択します。

   [パスワード ポリシーの作成]画面が表示されます。

2. パスワード ポリシーを作成するには、[OK]をクリックします。

   [パスワード ポリシー]画面の[全般]タブが開きます。

3. パスワード ポリシーの名前および説明を入力します。

4. [有効化]を選択します。

   これによって、パスワード ポリシーの作成終了時に、そのポリシーを使用できます。

5. ユーザが自分のパスワードをリセットした場合のリダイレクト先のタスクを選択します

   デフォルトでは、[マイ パスワードの変更]タスクにリダイレクトされます。

6. 以下のパスワード ポリシー設定を行います。

   - パスワードの構成(112 ページ)
   - 正規表現
   - パスワードの詳細オプション

7. [サブミット]をクリックします。

   CA Access Control エンタープライズ管理 によってパスワード 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(112 ページ)

パスワード構成ルール

新しいパスワードの作成方法を決定するルールを指定できます。

重要: パスワード構成の設定時に、各文字要件の値を決定する際に最大パスワード長を考慮します。 パスワード ポリシーで必要な文字および数字の合計数が最大パスワード長を超えた場合、すべてのパスワードが拒否されます。

パスワード構成の設定には以下のものがあります。

パスワードの最小文字数

ユーザ パスワードの最小長を指定します。

最大繰り返し文字数

パスワード内で連続して使用可能な反復文字の最大数を決定します。

たとえば、この値を「3」に設定すると、パスワードに「aaaa」のように指定することはできません。 ただし、「aaa」は指定できます。 この値を設定して、ユーザが入力するパスワードが 1 種類の文字のみで構成されないようにします。

大文字

大文字の使用を許可するかどうかを指定し、許可する場合は、パスワードに含める必要がある最小文字数を指定します。

小文字

小文字の使用を許可するかどうかを指定し、許可する場合は、パスワードに含める必要がある最小文字数を指定します。

文字

文字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小文字数を指定します。

注: 大文字と小文字の使用を許可すると、[文字]チェック ボックスは自動的にオンになります。

数字

数字の使用を許可するかどうかを指定し、許可する場合、はパスワードに含める必要がある最小数字数を指定します。

文字と数字

文字と数字の使用を許可するかどうかを指定し、許可する場合はパスワードに含める必要がある最小数を指定します。 [数字]でこの設定を行うと、文字は両方の要件を満たすことができます。 たとえば、この設定を行い、[数字]が 4 の場合、パスワード「1234」は有効です。

注: 大文字、小文字、文字、または数字の使用を許可すると、[文字と数字]チェック ボックスは自動的にオンになります。

句読点

句読点の使用を許可するかどうかを指定し、許可する場合は、パスワードに含める必要がある最小句読点数を指定します。 句読点とは、ピリオド、カンマ、感嘆符、スラッシュ、ダッシュおよびハイフンです。

印刷不能

印刷不可能文字の使用を許可するかどうかを指定し、許可する場合は、パスワードに含める必要がある最小印刷不能文字数を指定します。 印刷不可能文字は、コンピュータ画面には表示されません。

注: 一部のブラウザでは、印刷不可能文字をサポートしていません。

英数字以外

キーボードに表記されている句読点およびその他の記号(「@」、「$」、「*」など)のように、英数字でない文字の使用を許可するかどうかを指定し、許可する場合は、パスワードに含める必要がある最小文字数を指定します。 非印刷可能文字もこの合計に含まれます。 また、英数字でない文字は [句読点] および [印刷不可能文字] の文字要件も満たします。

禁止文字

特権アカウント パスワードを作成または変更する場合、使用が禁止される文字を定義します。 禁止される文字には、文字(大文字小文字の両方)、数字、記号およびそれらの文字の任意の組み合わせが含まれます。

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。

注: 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の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 エンドポイントで初めて特権アカウントを検出した場合、 CA Access Control エンタープライズ管理 は Windows エージェントレス接続エンドポイント特権アクセス ロールを自動的に作成します。

特権アカウントの検出方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[アカウント]-[特権アカウント検出ウィザード]をクリックします。

   [特権アカウント検出ウィザード: 特権アカウントの選択]ページが表示されます。

2. リストから[エンドポイント タイプ]を選択します。

3. 検索属性を選択し、フィルタ値を入力し、[検索]をクリックします。

   フィルタ条件に一致するエンドポイントのリストが表示されます。

4. 管理する特権アカウントを選択します。

   以下のテーブル列見出しには説明が必要です。

   検出されたアカウント

   アカウントが CA Access Control エンタープライズ管理 にすでに認識されているかどうかを示します。 既知のアカウントには、CA Access Control エンタープライズ管理 がすでに管理しているアカウント、および、CA Access Control エンタープライズ管理 がエンドポイントを管理するために使用する管理者アカウントなどがあります。

   エンドポイント管理者

   CA Access Control エンタープライズ管理 がエンドポイントを管理するために、このアカウントを使用するかどうかを指定します。

   重要: エンドポイント管理者アカウントを選択しないでください。 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。 たとえば、UNIX 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として root アカウントを指定した場合、root を管理対象特権アカウントにしないでください。

   [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。

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。

[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

CA Access Control エンタープライズ管理 の特権アカウントによって、ユーザに基幹のデータおよびプロセスにアクセス可能な特権システム アカウントへのアクセスが提供されます。 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タスクを実行できます。

特権アカウントの作成手順

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. ダイアログ ボックスで以下のフィールドを完了します。

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。

エンドポイント タイプ

特権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。

オプション: MS SQL Server（Microsoft SQL Server）、PeopleSoft、OS400（IBM i、旧 i5/OS および OS/400）、Kerberos Server、Oracle Server、Windows Agentless、SSH Device

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。

コンテナ

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。

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。

パスワード

ユーザが新しい特権アカウントで使用するパスワードを定義および検証します。

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。

パスワード ポリシー

特権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。

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。

[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。

Break Glass プロセス中に発生するイベント

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 アカウントは、[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。

アプリケーションの作成

アプリケーションを作成すると、PUPM エージェントを呼び出すスクリプトを実行して CA Access Control エンドポイントから特権アカウントを取得できます。 必要な場合のみ、スクリプト中のハードコーディングされたパスワードを、PUPM エージェントが取得した特権アカウント パスワードで置き換えることができます。

アプリケーションは、CA Access Control エンドポイントで実行するスクリプトを表します。

使用するスクリプトごとにアプリケーションを作成し、特定の特権アカウントをそのスクリプトに割り当てます。

アプリケーションを作成する方法

注: 特権アカウントを管理するには、管理権限が必要です。

1. [特権アカウント]、[アプリケーション]、[アプリケーションの作成]の順にクリックします。

   [アプリケーションの作成: アプリケーションの検索]画面が表示されます。

2. アプリケーション タイプの新しいオブジェクトの作成を選択して、[OK]をクリックします。

   [アプリケーションの作成]ウィンドウが表示されます。

3. フォームに以下の値を入力します。

   名前

   アプリケーション(スクリプト)の名前を定義します。

   説明

   アプリケーション(スクリプト)の説明を定義します。

   アプリケーション パス

   アプリケーション(スクリプト)のフル パスを定義します。

   例: /opt/scripts/myscript/sh

   ホスト

   実行するスクリプトが存在するホストの名前を定義します。

   例: myhost.com

   クライアント タイプ

   PUPM エージェントのタイプを指定します。

   オプション: CLI

   識別子ホスト

   実行するスクリプトが存在するホストの名前を定義します。

例: myhost.com

識別子ユーザ

スクリプトの実行を許可するユーザのカンマ区切りリストを定義します。

例:mydomain/user1, mydomain/user2

アカウント

このアプリケーションに関連付ける特権アカウントを定義します。

有効

このアプリケーションを有効化するかどうかを指定します。

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 はアプリケーション設定を作成します。

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

アカウントの所属先のエンドポイントを管理するために、特権アカウント パスワードをチェックアウトします。

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 は管理対象エンドポイントにアクセスするために使用するパスワードを表示します。

特権アカウント パスワードのチェックアウト方法

1. CA Access Control エンタープライズ管理 にログインします。
2. [ホーム]-[マイ アカウント]-[マイ チェックアウト特権アカウント]タブを選択します。

   [マイ アカウント]ウィンドウが表示され、チェックアウト可能なアカウントが示されます。
3. 検索クエリを入力し、[検索]をクリックします。

   クエリによって検索結果が返されます。
4. チェックアウトするアカウントを選択し、[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 はアカウント パスワードを表示します。
5. [OK]をクリックします。

特権アカウント パスワードのチェックイン

管理対象システムからログアウトした後に、特権アカウント パスワードをチェックインします。 システム ユーザまたはプログラムによってアカウントがチェックインされる場合、またはチェックアウト期間が失効した場合、CA Access Control エンタープライズ管理 は自動的にアカウント パスワードを変更して、前のパスワードを無効にします。

アカウントが専用アカウントでない場合、およびそのように設定されている場合、すべてのユーザがアカウントをチェックインした場合に限り、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。

特権アカウントのチェックイン方法

1. CA Access Control エンタープライズ管理 にログインします。
2. [ホーム]-[マイ アカウント]-[マイ チェックアウト特権アカウント]タブを選択します。

   現在、ユーザがチェックアウト済みのすべてのアカウントのリストが表示されます。
3. 検索クエリを入力し、[検索]をクリックします。

   クエリによって検索結果が返されます。
4. チェックインするアカウントを選択し、[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:

特権アカウントの検出(114 ページ)
特権アカウント パスワードのチェックアウト(121 ページ)
特権アカウントのパスワードの要求(122 ページ)

特権アカウントのパスワードの要求

[特権アカウント要求]オプションを使用して、ユーザ アカウントに割り当てられた特権アクセス ロールに従って、アクセス権限のない特権アカウントのパスワードをチェックアウトします。

特権アカウントのパスワードの要求方法

1. CA Access Control エンタープライズ管理 にログインします。
2. [ホーム]-[マイ アカウント]-[特権アカウント要求]を選択します。

   [特権アカウント要求]検索ウィンドウが表示されます。
3. 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. チェックアウトするアカウントを選択し、[選択]をクリックします。
5. リクエストの理由および説明を記入し、[サブミット]をクリックします。

   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。
6. [OK]をクリックします。

例: 特権アカウント パスワード リクエスト プロセスの動作の仕組み

この例では、リクエスト フォームを使用して、特権アカウントへのアクセスをリクエストする仕組みを示します。

通常アクセス権限がないエンドポイントを管理するアカウントの特権アカウント パスワードをチェックアウトするとします。 アカウントへのアクセス リクエストの理由、およびアカウントを使用する時間枠を指定します。

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へリクエストを転送します。 リクエストは承認または拒否されるまで保留中されます。

承認されると、リクエスト承認者が指定した条件に従って、アカウント パスワードが提供され、特権アカウントが[マイ アカウント]タスクに表示されます。

Break Glass 特権アカウントのチェックアウト

ユーザのアカウントに対して定義された特権アクセス ロールに従って、Break Glass チェックアウト 手順を使用して、アクセス権限のないエンドポイントへアクセスします。

Break Glass 特権アカウント パスワードのチェックアウト方法

1. CA Access Control エンタープライズ管理 にログインします。
2. [ホーム]-[マイ アカウント]-[Break Glass]を選択します。

   [Break Glass 特権アカウント チェックアウト検索]ウィンドウが表示されます。
3. 検索クエリを入力し、[検索]をクリックします。

   クエリは、入力したクエリに従って結果を返します。
4. チェックアウトする Break Glass アカウントを選択し、理由を記入して、[チェックアウト]をクリックします。

   アカウント パスワードが表示されます。

Break Glass 特権アカウントのチェックイン

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 特権アカウントのチェックイン方法

1. CA Access Control エンタープライズ管理 にログインします。
2. [ホーム]-[マイ アカウント]-[Break Glass]を選択します。

   [Break Glass 特権アカウント検索]ウィンドウが開きます。
3. [マイ チェックアウト特権アカウント]タブを選択します。

   現在チェックアウトされている特権アカウントのリストが表示されます。
4. 検索クエリを入力し、[検索]をクリックします。

   クエリは検索結果を表示します。
5. チェックインするアカウントを選択し、[チェックイン]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。

特権アカウント パスワードの強制チェックイン

以下の手順に従って、特権アカウント パスワードを強制的にチェックインします。 このオプションを使用して、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します。

このオプションでは、専用および標準の特権アカウント パスワードを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

注: 特権アカウントを管理するには、管理権限が必要です。

1. [特権アカウント]-[特権アカウントの管理]-[強制チェックイン]を選択します。

   [強制チェックイン]検索画面が表示されます。

2. 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。

3. チェックインする特権アカウントを選択し、[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]をクリックしてタスクを完了します。

   パスワードが正常にチェックインされたことを伝える確認メッセージが表示されます。

特権アカウントの自動パスワード 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。

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。 旧パスワードを非常に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。

自動パスワード リセットの実行方法

注: 特権アカウントを管理するには、管理権限が必要です。

1. [特権アカウント]-[特権アカウントの管理]-[自動パスワード リセット]を選択します。

   [自動パスワード リセット]検索画面が表示されます。

2. 検索クエリを入力し、[検索]を選択します。

   クエリの検索結果が表示されます。 CA Access Control エンタープライズ管理 は利用可能なアカウント、およびアカウントをチェックアウトしたユーザを表示します。

3. 少なくとも 1 つの特権アカウントを選択し、[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]をクリックします。

   CA Access Control エンタープライズ管理 は選択されたアカウント パスワードをリセットし、新しいパスワードを生成します。

5. [OK]をクリックします。

   パスワードが自動的にリセットされます。

特権アカウントの手動パスワード 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。

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。 旧パスワードを非常に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、接続解除システムの特権アカウント管理を行う場合のみにすることを強くお勧めします。CA Access Control エンタープライズ管理 は、接続解除システムの特権アカウントのパスワード ボールとして機能します。 接続解除システム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 を使用して、パスワードを変更する必要があります。

手動パスワード リセットの実行方法

1. 特権アカウント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. [特権アカウント]-[特権アカウントの管理]-[手動パスワード リセット]を選択します。

   [手動パスワード リセット]検索画面が表示されます。

3. 検索クエリを入力し、[検索]をクリックします。

   クエリによって、アカウントをチェックアウトしたユーザの名前などの検索結果が表示されます。

4. 少なくとも 1 つの特権アカウントを選択し、[選択]をクリックします。

   特権アカウントの手動パスワード リセット画面が表示されます。

5. 両方のフィールドに新しいパスワードを入力し、[サブミット]をクリックします。

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. 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。

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方法

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。

第 7 章: エンドポイントの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。

エンドポイントの特権アカウントの使用法

特権アカウントのパスワードは、CA Access Control の CA Access Control エンタープライズ管理 から取得できます。

エンドポイントから特権アカウント パスワードを取得するには、コマンド プロンプト画面から PUPM エージェント (acpwd) を実行し、一連のパラメータを入力して CA Access Control エンタープライズ管理 のアカウントをチェックアウトするか、または CA Access Control エンタープライズ管理 に戻します。

また、スクリプトの中で <pum> エージェントを使用して、必要に応じて特権アカウント パスワードをチェック アウトできます。 このオプションは、スクリプト中のハードコーディングされたパスワードを置き換えるために使用します。 スクリプトの実行中、PUPM エージェントは特権アカウント クレデンシャルを CA Access Control エンタープライズ管理 に送信します。 CA Access Control エンタープライズ管理 はアカウント設定を検証し、承認した場合はそのアカウント パスワードを返します。

スクリプトの実行が許可され、特権アカウント パスワードを取得するユーザのリストを定義できます。

この処理は以下の手順で行われます。

1. 以下のいずれかの操作を行います。
    a. エンドポイントでコマンド プロンプト ウィンドウを開きます。
    b. エンドポイントで PUPM エージェントを呼び出すスクリプトを作成します。CA Access Control エンタープライズ管理 でアプリケーションを定義します。 アプリケーションにはスクリプトおよび特権アカウント設定が含まれています。

2. PUPM エージェントを使用して、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します。
3. PUPM エージェントは認証のために要求を CA Access Control エンタープライズ管理 に転送します。
4. CA Access Control エンタープライズ管理 は特権アカウント パスワードをエンドポイントに送信し、PUPM はそのパスワードを表示して確認メッセージをログに記録します。
5. CA Access Control エンタープライズ管理 は、アカウント パスワードをパスワード保管領域に戻し、PUPM エージェントは確認メッセージのログを記録します。
6. PUPM エージェントは、チェックインに成功したことを示す確認メッセージをログに記録します。

コマンド プロンプトを使用したエンドポイントからの特権アカウント パスワードのチェックアウト

PUPM エージェントを使用して、特権アカウント パスワードを CA Access Control から直接チェックアウトし、エンドポイント上の管理対象デバイスにログインします。

コマンド プロンプトを使用したエンドポイントからの特権アカウント パスワードのチェックアウト方法

1. コマンド プロンプト ウィンドウを開きます。
2. 以下のコマンドを実行します。

   `acpwd -checkout -account<アカウント名> -ep<エンドポイント名> -eptype<エンドポイント タイプ> [-container<コンテナ名] [-nologo]`

   確認メッセージが表示され、アカウント パスワードのチェックアウトが正常に実行されたことが通知されます。

   注: 数字がゼロ(0)の確認メッセージは、パスワードのチェックアウトが正常に実行されたことを示します。

詳細については、「リファレンス ガイド」を参照してください。

コマンド プロンプトを使用したエンドポイントからの特権アカウント パスワードのチェックイン

エンドポイント上の管理対象デバイスへのログインにもうパスワードが必要なくなった場合に、PUPM エージェントを使用して、CA Access Control 円 d ポイントから直接特権アカウント パスワードをチェックインできます。

コマンド プロンプトを使用したエンドポイントからの特権アカウント パスワードのチェックイン方法

1. コマンド プロンプト ウィンドウを開きます。
2. 以下のコマンドを実行します。

   acpwd -checkin -account<アカウント名> -ep<エンドポイント名> -eptype<エンドポイント タイプ> [-container<コンテナ名] [-nologo]

   確認メッセージが表示され、アカウント パスワードのチェックインが正常に実行されたことが通知されます。

   注: 数字がゼロ(0)の確認メッセージは、パスワードのチェックインが正常に実行されたことを示します。

詳細については、「リファレンス ガイド」を参照してください。

ハードコーディング スクリプト パスワードのチェックアウト特権アカウント パスワードへの置き換え

スクリプトの中で PUPM エージェントを使用して、ハードコーディングされたパスワードを CA Access Control エンタープライズ管理 からチェックアウトするパスワードに置き換えることができます。 このようにすると、スクリプトの中にハードコーディングされたパスワードを組み込む必要がなくなります。

注: スクリプトで PUPM を使用するには、CA Access Control エンタープライズ管理でそのスクリプトをアプリケーションとして定義しておく必要があります。

ハードコーディングされたスクリプト パスワードをチェックアウトされる特権アカウント パスワードに置き換えるには、スクリプトに以下のコマンドを追加します。

```
acpwd -checkout -account name -ep name -eptype type [-container name] -nologo
```

また、このスクリプトを修正して、コマンドの出力(チェックアウト特権アカウント パスワード)を使用することもできます

注: PUPM エージェントの構文については、「リファレンス ガイド」を参照してください。

例: Windows で PUPM エージェント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するスクリプト

以下は、Windows 上の特権アカウント パスワードのチェックアウトを PUPM エージェントに要求するためのサンプル スクリプトの一部です。 この例では、PUPM エージェントが CA Access Control エンドポイントにインストールされ、CA Access Control エンタープライズ管理 でアプリケーションが定義されていることを前提としています。

このサンプル スクリプトは、CA Access Control エンタープライズ管理 から取得した特権アカウント パスワードを使用して、Windows レジストリのエントリの追加および削除を試行します。

```
set AdminUser=PowerUser
FOR /F "tokens=*" %%i IN ('"C:\Program Files\AccessControl\bin\acpwd.exe" -checkout
-account PowerUser -ep comp1_123 -eptype "Windows Agentless" -container "Windows
Accounts" -nologo') DO SET AdminPassword=%%i
set runasadmin="C:\utils\psexec.exe" -u %AdminUser% -p
%runasadmin% %AdminPassword% REG ADD "HKLM\SOFTWARE\PUPM Registry"
%runasadmin% %AdminPassword% REG DELETE "HKLM\SOFTWARE\PUPM Registry" /F
```

上の例では、スクリプトは PUPM エージェントを実行して特権アカウント パスワード をチェックアウトします。このスクリプトには、アカウント名 (PowerUser)、エンドポイント名 (comp1_123)、エンドポイント タイプ (Windows Agentless)、ユーザのコンテナ名 (Windows Accounts) が含まれています。 このスクリプトは、パスワードだけを表示するように PUPM エージェントに指示し、そのパスワードを使用して、レジストリ エントリを追加および削除する管理者ユーザとして PsExec プログラムを実行します。

詳細情報:

アプリケーションの作成 (119 ページ)

第 8 章: UNAB の使用

このセクションには、以下のトピックが含まれています。

UNAB コンポーネント

UNIX 認証ブローカ(UNAB)は、Active Directory ユーザによる UNIX ホストへのアクセスを管理および制御する、いくつかのコンポーネントで構成されています。

- UNAB 認証エージェント - UNAB 認証エージェント(uxagent)デーモンは、Active Directory との接続を提供し、ユーザの認証および権限付与、Active Directory へのホスト登録、ユーザおよびグループの移行、ローカル アクセス ファイルの管理などに関して、Active Directory との安全な接続を保持します。
- uxconsole - xconsole は、Active Directory に UNIX ホストを登録し、ユーザとグループを移行し、UNAB をアクティブにするために使用する UNAB 管理コンソールです。 uxconsole によって、UNAB がインストールされているすべての UNIX ホストからユーザのログインを管理できます。
- CA Access Control エンタープライズ管理 UNAB - CA Access Control エンタープライズ管理 によって、中央の場所から UNAB ホストを管理できます。 CA Access Control エンタープライズ管理 を使用して、企業内の UNAB ホストへの Active Directory ユーザおよびグループのアクセスを制御します。

UNAB の設定方法

UNAB（UNIX Authentication Broker）が UNIX ホストへのアクセスを制御する仕組みを理解しておくと、実装および設定プロセス中に役立つ情報を活用することができます。

UNAB を UNIX ホストにインストールしたら、UNAB を Active Directory に登録し、UNAB がエンタープライズ ユーザのログインを認証できるようにします。 次に、移行プロセスを開始して、ローカル ユーザおよびグループを Active Directory に移行します。

1. UNAB がインストールされたら、UNIX ホストを Active Directory に 登録します。

   この段階では、UNAB はログイン要求をインターセプトしません。

2. UNIX ホストへのアクセスを許可および拒否するエンタープライズ ユーザを定義します。 そのためには、CA Access Control エンタープライズ管理 からログイン認証ポリシーを作成します。

3. UNAB を有効にして、UNIX ホストへのユーザ アクセスを認証できるようにします。

4. UNAB ログイン認証ポリシーにエンタープライズ ユーザおよびグループを追加して、新しいユーザがログインできるようにします。

   この段階では、ローカル ユーザ ストア（etc.passed）または UNAB ログイン認証ポリシーで定義されたユーザのログインが許可されます。

5. UNAB をアクティブにした後、Active Directory へのユーザおよびグループの移行を開始できます。

UNAB のユーザ認証の仕組み

UNAB を UNIX ホスト上にインストールし設定した後、ユーザは使用を選択した統合モードに従って、Active Directory ユーザ アカウントまたはローカル ユーザ アカウントを使用して、ログインできます。

ユーザが UNAB が実行中の UNIX ホストへのログインを試みる場合、以下のイベントが発生します。

1. 有効な Active Directory またはローカル アカウントのユーザ名およびパスワードの入力を促すダイアログ ボックスが表示されます。

2. UNAB は、Active Directory、ログイン認証ポリシー、およびローカル ホストのアクセス ファイルでユーザのクレデンシャルを認証し、ユーザのアカウントから取得された追加情報を確認します。

3. ユーザが認証されると、UNAB はユーザに UNIX ホストへのアクセス権限を付与します。 認証されない場合、UNAB は、ホストへのユーザ アクセスをブロックします。

ホスト アクセス制御および UNAB 設定の仕組み

CA Access Control エンタープライズ管理 から、UNIX ホストへのユーザおよびグループのアクセスを制御し、UNAB を設定できます。 UNIX ホストへのユーザおよびグループのアクセスの制御は、ホストへのログインが許可されたユーザおよびグループにのみアクセス権を付与することで行います。

UNAB ホストの設定は、ホストへのアクセス制御と同様の方法で行います。 CA Access Control エンタープライズ管理 を使用して、企業内の UNAB ホストの機能を制御し、それをすべてのホストに適用します。

ユーザおよびグループの割り当て、またはトークン値の定義を行った後に、CA Access Control エンタープライズ管理 は情報をポリシーに変換し、以下の操作を行います。

1. CA Access Control エンタープライズ管理 は、ユーザおよびグループのリスト、または設定パラメータが含まれたデプロイメント パッケージを作成し、そのパッケージを、ポリシーが適用されるホストまたはホスト グループへ割り当てます。
2. CA Access Control エンタープライズ管理 はパッケージを配布サーバに転送し、ホスト上で配布します。
3. UNAB は配布サーバからパッケージを取得し、ポリシーをインストールし、CA Access Control エンタープライズ管理 に確認メッセージを送信します。

注: ユーザがエンタープライズ ポリシーおよび UNAB ログイン ポリシーの両方をホストにデプロイした場合、エンタープライズ ポリシーは UNAB ログイン ポリシーに優先します。

ホストへのログイン権限の定義

UNAB ホストまたはホスト グループへのユーザのログインを制御するには、アクセス権限を付与するユーザまたはグループのリストを作成します。 次に、このリストを、CA Access Control エンタープライズ管理 が選択されたホストに割り当て、デプロイするポリシーに変換します。 ポリシー コマンドが表示されます。 デプロイメントのステータスは、[デプロイメント監査]ウィンドウに表示されます。

重要: ログイン権限は、現在変更中のホストにのみ適用されます。 このホストがグループのメンバである場合、そのホスト グループに適用されるログイン権限を編集する必要があります。

ホストへのログイン権限の定義方法

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

   [ホストの作成]、[ホストの削除]、[ホストの変更]、[ホストの表示]の 4 つのタスクが表示されます。

2. [ホストの変更]をクリックします。

   [ホストの変更: 標準検索画面(汎用)の設定]が表示されます。

3. 変更するホストの名前を入力し、[検索]をクリックします。

   クエリの検索結果が表示されます。

4. 編集するホストを選択し、[選択]をクリックします。

   [全般]タブが表示されます。

5. [ログイン許可]タブに移動します。

   [ログイン許可]タブが開きます。

6. 許可済ログイン リストにユーザまたはグループを追加するには、[ユーザの追加]または[グループの追加]をクリックします。

   [ユーザの選択]または[グループの選択]検索ウィンドウが開きます。

7. 検索パラメータを入力し、[検索]をクリックします。

   クエリの検索結果が表示されます。

8. リストに追加するユーザまたはグループを選択し、[選択]をクリックします。

   選択したユーザおよびグループがリストに表示されます。

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 は、ユーザおよびグループのリストを選択したホストまたはホスト グループに割り当てます。

ホスト環境設定トークンの定義

すべての UNAB ホストの環境設定トークンを定義できます。 CA Access Control エンタープライズ管理 は、UNAB の環境設定ファイル(uxauth.ini)または CA Access Control の環境設定ファイル(accommon.ini)で、トークンの値を設定するのに役立ちます。

トークンへの値の割り当てを完了すると、CA Access Control エンタープライズ管理 は「環境設定ポリシー」と呼ばれるポートを作成し、ホストに割り当てます。

重要: 変更する環境設定トークンは、現在変更中のホストにのみ適用されます。 このホストがグループのメンバである場合、そのホスト グループに適用される環境設定トークンを編集する必要があります。

ホスト環境設定トークンの定義方法

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

   [ホストの作成]、[ホストの削除]、[ホストの変更]、[ホストの表示]の 4 つのタスクが表示されます。

2. [ホストの変更]をクリックします。

   [ホストの変更: 標準検索画面(汎用)の設定]が表示されます。

3. 変更するホストの名前を入力し、[検索]をクリックします。

   クエリの検索結果が表示されます。

4. 変更するホストを選択し、[選択]をクリックします。

   [全般]タブが表示されます。

5. [UNAB の環境設定]タブへ移動します。

   [UNAB 環境設定トークン]ウィンドウが表示されます。

6. メニューから編集する環境設定ファイルを選択します。

   選択された環境設定ファイル トークンが表示されます。

7. 環境設定トークン値を変更し、[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、選択された UNAB ホストまたはホスト グループ上の値を設定します。

CA Access Control エンタープライズ管理のホストへのポリシーのコミットの確認

権限リストと設定リストの作成後、[デプロイメント監査] オプションで、CA Access Control エンタープライズ管理 が変更を UNAB ホストにコミットしたことを確認できます。

CA Access Control エンタープライズ管理のホストへのポリシーのコミットの確認方法

1. CA Access Control エンタープライズ管理 で、[ポリシー管理]タブ、[ポリシー]タスクを順に選択して、[デプロイメント]オプションを展開します。

   [デプロイメント]オプション メニューが開きます。

2. [デプロイメント監査]オプションを選択します。

   [デプロイメント監査]検索画面が開きます。

3. ホストおよび表示するポリシーを選択して、[実行]をクリックします。

   クエリの検索結果が表示されます。

   注: ログイン ポリシーには、プレフィックス「login@」が含まれています。

4. 結果行をクリックして、デプロイメント ステータスを表示します。

   CA Access Control エンタープライズ管理 はデプロイメント タスクのステータスおよび出力を表示します。

移行競合の解決

UNAB は、移行処理中に検出された競合を競合ファイルに記録します。 このファイルには、ローカル ホストから Active Directory へのユーザとグループの移行を妨害した競合の原因の詳細が記録されます。

競合ファイルを CSV ファイルへエクスポートし、スプレッドシートをコンピュータにダウンロードし、競合を調査して解決します。 変更したスプレッドシートは、後で再び CA Access Control エンタープライズ管理 にアップロードできます。CA Access Control エンタープライズ管理 はアップロードされたスプレッドシートをメッセージ キュー サーバに送信します。 UNAB はこのファイルを取得し、移行プロセスを再実行して移行されなかったユーザおよびグループを移行します。

注: ホスト グループを移行すると、競合ファイルをダウンロードできません。 しかし、修正された競合ファイルをアップロードして、移行プロセスにおける競合を解決することができます。

移行競合の解決方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
   a. [ポリシー管理]をクリックします。
   b. [UNIX 認証]サブタブをクリックします。

      使用可能なタスクのリストが表示されます。

2. 以下のいずれかの操作を実行します。
   - [ホスト移行競合の解決]をクリックします。

     [ホスト移行競合の解決: ホスト検索]画面が表示されます。
   - [ホスト グループ移行競合の解決]をクリックします。

     [ホスト グループ移行競合の解決: ホスト グループ検索]画面が表示されます。

3. 競合を解決するホストまたはホスト グループの名前を入力し、[検索]をクリックします。

   フィルタ条件に一致するホストまたはホスト グループのリストが表示されます。

4. 競合を解決するホストまたはホスト グループを選択し、[選択]をクリックします。

   [UNAB 移行: ホスト名]または[UNAB 移行: ホスト グループ名] ページが」表示されます。

5. (オプション) ホスト移行用の競合ファイルをダウンロードし、以下の手順で、競合を解決します。

   a. [UNAB 移行競合詳細のダウンロード]セクションで、[エクスポートとダウンロード]リンクを選択します。

      ダイアログ ウィンドウが開きます。

   b. ファイルの保存場所に移動し、[保存]を選択します。

      CSV ファイルが指定された場所へダウンロードされます。

   c. CSV ファイルを開き、ファイル内で報告されている競合を解決し、ファイルを保存して閉じます。

6. (オプション) ホスト グループ移行に関して、競合を解決する CSV ファイルを作成し、保存します。

7. CSV ファイルをアップロードすると、以下のようにして、ホストまたはホスト グループの競合が解決されます。

   a. [UNAB 移行ソリューションのアップロード]セクションで、[参照]ボタンを選択します。

      ダイアログ ウィンドウが開きます。

   b. ファイルを参照して[開く]をクリックします。

   c. [アップロード]をクリックします。

      ファイルがアップロードされます。

8. [サブミット]をクリックします。

   CA Access Control エンタープライズ管理 はファイルをメッセージ キュー サーバに送信します。 UNAB はキューからファイルを取得し、移行プロセスを再開して、解決されたアカウントおよびグループの移行を試行します。

9. 移行終了後に移行ファイルを再度確認して、ファイルで前回報告されていたアカウントおよびグループが正常に移行されたことを確認します。

例: UNAB 競合ファイルの出力

以下の例は、移行処理中に作成された UNAB 競合ファイル出力の一部です。

```
USER,john,MIGRATE,,NO AD,1354,/tmp,201,,,user for doall proc
```

上の例では、ユーザ john が Active Directory に移行され(MIGRATE)、競合が検出されなかった(NO)ことが示されています。 さらに、このファイルにはユーザ ID (1354)、ホーム ディレクトリ(/tmp)、グループ ID (201)、および GECOS 情報(user for doall proc)が記述されています。

注: UNAB 競合の詳細については、「リファレンス ガイド」を参照してください。

UNAB の停止

Active Directory ユーザが UNIX コンピュータへのアクセスするのを拒否する場合、または UNAB の新バージョンをインストールする場合は、UNAB を停止する必要があります。

uxauthd デーモンを停止して、UNAB を停止します。

UNAB の停止方法

1. UNIX コンピュータにスーパユーザとしてログインします。
2. 以下のコマンドを入力します。

   ```
   ./uxauthd -stop
   ```

   UNAB デーモンが停止します。

   デーモンが停止したことを通知するメッセージが表示されます。

UNAB ステータスの表示

UNAB の現在のステータスを表示するためにこのオプションを使用します。

UNAB ステータスの表示方法

1. そのコンピュータの管理権限を持っているユーザとして UNIX コンピュータにログインします。
2. 以下の引数を指定して uxauthd プログラムを実行します。

   ```
   ./uxauthd -status
   ```

   UNAB の現在のステータスを通知するメッセージが表示されます。

UNAB デバッグ ファイル

UNAB 環境設定ファイル（uxauth.ini ファイル内の）のエージェント セクションは、実行時にエージェントによって収集されるデバッグ情報を定義します。 デフォルトでは、UNAB は、以下のファイル内のデバッグ情報を収集します。

<インストール ディレクトリ>/log/debug/

/gent_debug

UNAB デバッグ ファイル内でデバッグ メカニズムが有効である限り、エージェントの起動時に（開始オプションで）、エージェントはデバッグ メッセージをデバッグ ファイルに記録します。

-debug オプションを使用して UNAB を起動すると、デバッグ メッセージはユーザ コンソールに表示されます。

第 9 章: レポートの作成

このセクションには、以下のトピックが含まれています。

セキュリティ基準

企業の業務環境が紙ベースから電子媒体中心に移行した現在では、電子データは社内と社外の双方から攻撃を受けるという、深刻な状況に直面しています。 このような問題に対処するために、いくつものセキュリティ対策が幅広い分野において導入されています。たとえば、一般的なグローバル セキュリティ、財務の正確性と財務報告、個人の資金に関する情報や個人の識別情報の保護、福祉に関する情報の保護、および米国政府機関のセキュリティのベスト プラクティスの標準化などの分野です。

CA Access Control レポート サービスによって実行されているベスト プラクティス レポートの基盤であるセキュリティ基準、法律、および要求事項の概要を以下に説明します。

Payment Card Industry Data Security Standards(PCI DSS、ペイメント カード業界データ セキュリティ標準)

PCI DSS は、詐欺やハッキングなどのセキュリティに関する問題の発生を防止する目的で、大手クレジット カード会社によって策定された業界標準です。 クレジット カードやデビット カードのデータの受け付け、記録、保存、送信、または処理を行う企業は、PCI DSS に準拠する必要があります。

Health Insurance Portability and Accountability Act(HIPAA、医療保険の相互運用性と説明責任に関する法律)

HIPAA は、労働者が転職または失業した際にも健康保険を利用できるように保護する米国連邦法です。 HIPAA はまた、保健医療関連のデータのセキュリティおよびプライバシーにも対処しています。

Sarbanes-Oxley Act(SOX、サーベンス オクスリー法)

SOX は、財務報告の基準を規定した米国連邦法です。 この法律は、すべての米国公開企業の役員会に適用されます。

レポート タイプ

CA Access Control のデータおよびイベントに関する情報は、2 種類の異なるレポートで表示できます。

- CA Access Control レポート - ユーザおよびユーザが実行できるアクションについて記述します。

  CA Access Control レポートは、各エンドポイント上の CA Access Control データベース内のデータ、すなわち、エンドポイント上にデプロイするルールおよびポリシー、およびポリシー偏差に関する情報を提供します。 CA Access Control レポートは、CA Business Intelligence に表示されます。

- 監査レポート - ユーザおよびユーザが実行したアクションについて記述します。

  監査レポートは、各エンドポイント上の監査ログ ファイル（seos.audit）のデータ、すなわち、エンドポイント上でどのユーザがどんなアクションを実行したかに関する情報を提供します。 監査レポートは、CA Enterprise Log Manager および CA Access Control エンタープライズ管理 に表示されます。

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

注: CA Access Control レポートおよび CA Access Control 監査レポートを表示するには、追加コンポーネントをインストールし、設定する必要があります。 詳細については、「実装ガイド」を参照してください。

レポート サービス

CA Access Control レポート サービスを使用すると、各エンドポイント（ユーザ、グループ、およびリソース）のセキュリティ ステータスを一括して確認できます。 各エンドポイントからのデータの収集は、スケジュールで設定することも、オンデマンドで行うこともできます。 各エンドポイントに接続しなくても、誰がどのリソースへのアクセスを許可されているかを確認することができます。 CA Access Control は、一度の設定だけで各エンドポイントからデータの収集および中央のサーバへのデータのレポートを独立して実行します。また、手動による操作を必要とせず、エンドポイントのステータスを継続的にレポートします。 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 レポート サービスは、BS 7799/ISO 17799、Sarbanes-Oxley（SOX）、Payment Card Industry（PCI）、Health Insurance Portability and Accountability Act（HIPAA）、Federal Information Security Management Act（FISMA）などの環境で役立ちます。 レポート サービスは、何千ものエンドポイントにわたるユーザ、グループ、およびリソースのアクセスにおけるエンドポイント ステータスの正確な確認を可能にするソリューションです。

レポート サービスの構造では、各エンドポイントから収集されたデータを問い合わせて取得することが可能です。 さまざまな目的に応じてカスタム レポートを作成することも、CA Access Control が独自に提供する既存のレポートを使用することもできます。 レポート サービスはサーバに基づくサービスであるため、 レポート ストレージを集中させて一元的に管理し、レポートへの安全なアクセス(SSL)を確保することができます。 レポート サービスは可用性が高くなるように構成することができます。 レポート サービス コンポーネントは単一サーバ上へのインストール、または分散構成のインストールが可能です。

注: レポート サービス コンポーネントは CA Access Control コア機能の外部にあるので、既存の実装を再構成しなくても機能を強化することができます。

レポート サービス コンポーネント

レポート サービスは、以下のコア コンポーネントで構成されています。

- Report Agent は、各 CA Access Control または UNAB エンドポイント上で実行される Windows サービスまたは UNIX デーモンで、配布サーバ上の指定された Message Queue のキューに情報を送信します。
- メッセージ キューは、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る配布サーバのコンポーネントです。 レポートについては、メッセージ キューは、CA Access Control Web サービスを使用して、エンドポイント データベースのスナップショットを中央データベースに転送します。 冗長性およびフェールオーバを実現するために、情報を収集し転送する複数の配布サーバを使用できます。
- 中央データベースは、レポートなどの CA Access Control エンタープライズ管理機能の情報を保持するリレーショナル データベース管理システム(RDBMS)です。 さまざまなツールを使用することで、データベースに格納された CA Access Control 実装に関するデータを問い合わせて取得できます。
- レポート ポータルは、CA Access Control レポートを提供するアプリケーション サーバです。 このサーバでは、BusinessObjects InfoView ポータルを使用することで、中央データベースに格納されたレポート情報を対話式で操作できるようにしています。
- 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。
- レポートを表示および管理することができる Web ベースのインターフェースを実行しているコンピュータ。

注: CA Access Control レポート サービスの実装およびアーキテクチャの詳細については、「実装ガイド」を参照してください。

レポート サービスの機能

レポート サービスを使用すると、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。

- 各エンドポイントからデータを収集します。
- 収集したデータを中央サーバに格納します。
- 格納されたデータからレポートを生成します。

  中央データベースでデータが利用可能になると、レポート ポータルを使用して、レポートを生成し、格納されたデータを問い合わせて取得できます。なお、レポート ポータルは、BusinessObjects InfoView ポータルの CA バージョンです。これは中央データベースに接続するように構成され、既製の CA Access Control レポートにバンドルされています。

各エンドポイントからレポート用のデータを収集する方法

レポートを生成するには、各エンドポイントからデータを収集する必要があります。 レポート サービスは、各エンドポイントにインストールされたレポート エージェントを使用し、スケジュールされた時刻に、またはオンデマンドでそのエンドポイントからデータを収集します。

注: レポート エージェントは、CA Enterprise Log Manager と統合するために、監査データを収集してルーティングする必要もあります。 このプロセスでは、レポート エージェントが CA Access Control エンドポイントに関してレポートするために実行するアクションについてのみ説明します。

レポート エージェントは、各エンドポイントで以下のアクションを実行します。

1. 偏差計算を実行し、結果をレポート サーバに送信します。

   重要: レポート エージェントが定期的に実行するように設定され、 DMS の更新が必要ない場合は、ポリシー偏差計算を別途スケジュールする必要はありません。

2. CA Access Control データベース(seosdb)と各 Policy Model データベース(PMDB)のコピーをエンドポイントに作成します。

   これはレポート エージェントが使用する一時コピーです。このコピーを使用することで CA Access Control のパフォーマンスに影響を及ぼすことなくデータを処理できます。

3. 各データベースからのデータを XML 構造体にダンプします。

   データベース内のすべてのオブジェクトをダンプします。つまり、データベース インターフェース ユーティリティ(selang など)を介して確認できるデータだけでなくすべてのデータがキャプチャされます。

4. データベースの XML バージョンをレポート サーバに送信します。

   レポート エージェントはレポート サーバのレポート キューにデータを送信します。

各エンドポイントからのデータを処理および格納する方法

データが各エンド ポイント上で収集されると、そのデータは処理するために配布サーバに送信されます。 処理されたデータは、レポートの生成のために中央データベースのストレージに送信されます。

配布サーバは、以下のアクションを実行します。

1. エンドポイントのレポート エージェントから XML ダンプ(データベース全体のスナップショット)を受信します。

   各 XML ダンプは、データベース全体のスナップショットです。

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 メッセージ ファイルは、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 オブジェクトが中央データベースに挿入されます。

   これで、エンドポイントからのデータは、中央データベースから取得できるようになりました。

標準レポート

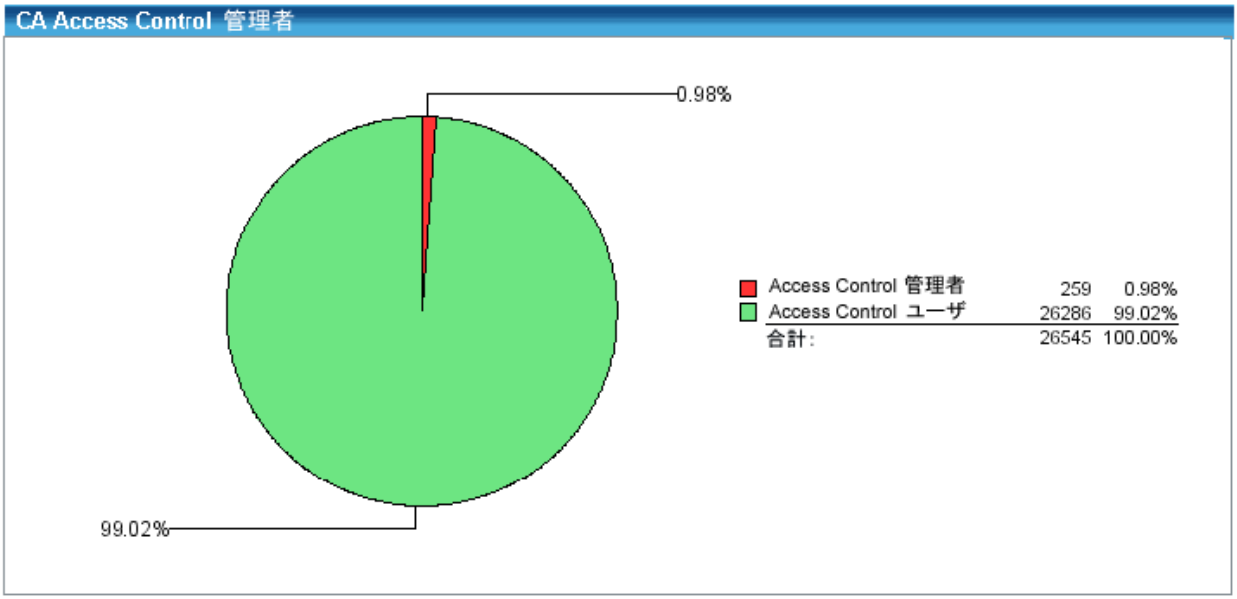
CA Access Control レポート サービスは、標準レポートと同じくデフォルトの製品インストールの一部として提供されており、すぐに使用が可能です。 レポートは、以下のカテゴリに分類されます。

- アカウント管理レポート(152 ページ)
- 権限レポート(156 ページ)
- その他のレポート(157 ページ)
- ポリシー管理レポート(160 ページ)
- パスワード ポリシー レポート(163 ページ)
- 特権アカウント管理レポート(164 ページ)
- UNIX 認証ブローカ レポート(168 ページ)

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、特定のエンドポイント位置での脆弱性をひとめで判定できるように視覚的に参照しやすい方法で表現するには、円グラフが利用されます。 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、グラフ内の赤色の広い扇形の部分は、現在の企業ユーザ数のほぼ 1% が CA Access Control 管理を実行できることを示しています。これはセキュリティ面で好ましくありません。



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 管理者レポートによるこの表のサンプルを以下に示します。

CA Access Control 管理者

ユーザ名	フル ネーム	ホスト ID	管理者モードあり	パスワード管理者モードあり	オペレータモードあり
_seagent					
		SYSTEMA	はい		
		SYSTEMB	はい		
		SYSTEMC	はい		

アカウント管理レポート

標準的なアカウント管理レポートには、ユーザ アカウントの概要が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なアカウント管理レポートのリストを以下に示します。

CA Access Control 管理者

CA Access Control 管理者レポートには、CA Access Control 管理者権限を持つすべてのユーザのリストが表示されます。 これには、ADMIN、PWMANAGER、または OPERATOR 属性を持つユーザが含まれます。 レポートには、サマリ データが円グラフで表示され、ユーザ名別の詳細なリストが表形式で表示されます。

CA Access Control を管理できるユーザが多くなると、企業はセキュリティ面でリスクにさらされる恐れがあります。 もちろん、評価対象のエンドポイントが開発環境またはテスト環境にある場合、システムのユーザの大部分が CA Access Control 管理者であることはまったく正常であると考えられます。

CA Access Control グループ ユーザ メンバシップ

CA Access Control グループ ユーザ メンバシップ レポートには、ユーザ グループとそのメンバが表示されます。 レポートには、詳細が表形式で表示されます。

管理を簡略化するために、CA Access Control 環境内の各ユーザを、現在定義されている 1 つまたは複数の CA Access Control グループのメンバとして取り込むことができます。 また、ユーザ定義に加え、グループ定義に基づいてリソース アクセスを許可することができます。 したがって、目的としていないリソースへのアクセス権をグループ メンバシップが決して許可しないようにするには、グループとそのメンバを注意深く確認することが重要です。

CA Access Control グループ

CA Access Control グループ レポートには、グループが存在する定義済みホスト、グループの説明、およびネストされたグループと呼ばれる子グループがグループの中に存在するかどうかが表示されます。

企業内でどのホストがどのグループに属するかを把握しておくと、管理作業が簡単になります。 さらに、どのグループがほかのグループを含んでいるかを把握しておけば、特定のユーザまたはグループが特定のリソースになぜアクセスできるかを特定する際に役立ちます。

CA Access Control 非アクティブ日

CA Access Control 非アクティブ日レポートには、指定された期間中（たとえば、90 日の間）にログオンしなかったユーザが表示されます。 このレポートには、そのようなユーザが一時停止されたかどうか、まだシステムにアクセスできる状態にあるかどうかについても表示されます。 レポートには、アカウントが非アクティブで一時停止されているユーザ、およびアカウントが非アクティブで一時停止されていないユーザを強調表示するサマリ円グラフが含まれています。

どのような企業環境であっても、監査において重要なポイントは、環境に対するアクセス権を持っているのはどのユーザか、また最後にアクセスを行ったのはいつかを把握しておくことです。 ユーザが最後にリソースにアクセスした日時（たとえばエンドポイントにログインした日時など）に加え、アカウントが非アクティブになっている期間を表示することも必要です。 このレポートは、サービス アカウントのアクセス周期を判別する場合や、まだ開いているアカウントのうち、特定の期間アクセスがないものを識別する場合に役立ちます。

CA Access Control パスワード変更

CA Access Control パスワード変更レポートには、指定された期間内にパスワードを変更する必要があるユーザ アカウントのリストが表示されます。 レポートにはサマリ円グラフが表示され、パスワードを変更する必要のないユーザ アカウント、パスワードを更新する必要があるユーザ アカウント、パスワードが期限切れになっているユーザ アカウントが示されます。 レポートにはまた、ホスト ID およびユーザ アカウントのパスワードの有効期限切れまでの残日など、詳細なデータが表示されます。

しばらく変更されていないパスワードの状態を把握することと同様に、監査では、パスワードの変更が保留になっているユーザのリストを把握する必要もあります。 この情報を使用すると、まもなく古くなると考えられるアカウントから、懸案のセキュリティ脅威を特定できます。

CA Access Control パスワード失効

CA Access Control パスワード失効レポートには、指定された日数以内にパスワードを更新していないユーザ アカウントが表示されます。 レポートにはサマリ円グラフが表示され、パスワードを更新したユーザ アカウント、パスワードの有効期限切れが原因でシステム アクセスが一時停止されているユーザ アカウント、およびパスワードの有効期限が切れているのに、まだシステムにアクセスしているユーザが示されます。 レポートには、過去 X 日にわたりパスワードを変更していないユーザ アカウントに関する詳細が表示されます。たとえば、ホスト ID、最後のパスワード変更日、ユーザ アカウントがまだシステムにアクセスしている理由などが表示されます。

CA Access Control は、パスワードの追加の品質チェック、そして以前のパスワード履歴の保持による、頻繁なパスワードの再使用禁止によって、エンドポイントのパスワード セキュリティの強化が可能です。 このコンポーネントの一部として、最後のパスワード変更日が保持されます。 このようなパスワード品質モデルのコンポーネントを使用することにより、CA Access Control は企業内のどのユーザが指定の期間内にパスワードを変更していないかを識別できます。 このレポートの重要な点は、このレポートを使用することで、しばらく変更されていないパスワードが原因で企業のログイン環境に生じる可能性のある弱点を明らかにできることです。

CA Access Control パスワード ポリシー準拠（アカウント）

CA Access Control パスワード ポリシー準拠（アカウント）レポートには、パスワード長や数字および英字の最低文字数などを規定したパスワード ポリシーに準拠していないパスワードを持つユーザ アカウントが表示されます。 レポートにはサマリ円グラフが表示され、ポリシーに準拠しているユーザ アカウント数とポリシーに準拠していないユーザ アカウント数が示されます。 レポートにはまた、ポリシーに準拠していないユーザ アカウントの詳細が表形式で表示されます。

CA Access Control パスワード ポリシー準拠（ホスト）

CA Access Control パスワード ポリシー準拠（ホスト） レポートには、パスワード長や数字および英字の最低文字数などを規定したパスワード ポリシーに準拠していないパスワードを持つユーザ アカウントが存在するホストが表示されます。 レポートにはサマリ円グラフが表示され、ポリシーに準拠しているホスト数とポリシーに準拠していないホスト数が示されます。 レポートにはまた、ポリシーに準拠していないホストおよびそのようなホスト上のユーザ アカウントに関する詳細が表形式で表示されます。

CA Access Control 職務分掌

CA Access Control 職務分掌レポートには、職務分掌のポリシー(たとえば、「ユーザは管理者ユーザ グループと監査担当者ユーザ グループの両方に属することはできない」など)に違反しているユーザ アカウントが表示されます。 レポートには、ポリシーに準拠するユーザ メンバとポリシーに準拠しないユーザ メンバとを比較するサマリ円グラフが表示されます。 レポートにはまた、ポリシーに準拠しないユーザ アカウントに関する詳細、ホスト ID などが含まれます。

あらゆる企業環境のエンドポイントはすべて、ユーザによる保守を必要とします。この保守作業では、OS およびアプリケーション コンポーネントに対するアクセス権が必要となります。 一般的に、システム管理者は OS の観点からコンピュータの保守を行い、アプリケーション管理者はアプリケーションの観点からコンピュータの保守を行います。 たとえば、Solaris システム管理者は UNIX ホスト ファイル内のエントリを更新し、Oracle DBA は Oracle データベース内のテーブルの保守を行うなどのケースです。

このモデルの利点は、システム管理者の側からアプリケーションを攻撃することが困難になり、アプリケーション管理者の側からの OS への攻撃も困難となることにあります。 システム管理者にアプリケーション管理者も兼任させるというやり方は、一般的に適切ではありません。

このレポートを利用すれば、複数のグループに属するユーザを見分けることにより、ロールの範囲が正しく設定されていないユーザを識別できます。 このグループ論理積検出は、ISO7799、SOX、PCI、HIPAA、および DoD 用の主要な監査ポイントの 1 つを満たすのに非常に有利です。

CA Access Control ユーザ グループ メンバシップ

CA Access Control ユーザ グループ メンバシップ レポートには、デプロイメント内のホストごとに、ユーザおよびユーザが属するグループが表示されます。 レポートには、ユーザおよびユーザが属するグループのホスト ID 別に詳細が表示されます。

CA Access Control ユーザ作成日

CA Access Control ユーザ作成日レポートには、デプロイメント内の指定されたホストまたはすべてのホスト上で特定の期間内に作成されたユーザ アカウントが表示されます。 レポートには、ユーザ アカウントが作成された日付の詳細が、ホスト ID 別、およびユーザ アカウント別に表示されます。

CA Access Control ユーザー時停止日

CA Access Control ユーザー時停止日レポートには、デプロイメント内の指定されたホストまたはすべてのホスト上で特定の期間内に一時停止されたユーザ アカウントが表示されます。 レポートには、ユーザ アカウントが一時停止された日付の詳細が、ホスト ID 別、およびユーザ アカウント別に表示されます。

CA Access Control ユーザ更新日

CA Access Control ユーザ更新日レポートには、デプロイメント内の指定されたホストまたはすべてのホスト上で特定の期間内に更新されたユーザ アカウントが表示されます。レポートには、ユーザ アカウントが更新された日付の詳細が、ホスト ID 別、およびユーザ アカウント別に表示されます。

権限レポート

標準的な権限レポートには、ユーザ権限およびリソース権限の概要が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的な権限レポートのリストを以下に示します。

CA Access Control ベースライン リソース コンプライアンス(ホスト) (156 ページ)
CA Access Control グループ権限 (156 ページ)
CA Access Control グループ別リソース アクセス (157 ページ)
CA Access Control ユーザ別リソース アクセス (157 ページ)
CA Access Control ユーザ権限 (157 ページ)

CA Access Control ベースライン リソース コンプライアンス(ホスト)

CA Access Control ベースライン リソース コンプライアンス(ホスト)レポートには、指定されたリソースに対してデフォルト以外のアクセスを行うユーザ アカウントが表示されます。 レポートには、サマリ円グラフが表示され、デフォルト以外のアクセスが許可されたホストの個数およびデフォルト以外のアクセスを行うユーザ アカウントの総数を示します。レポートにはまた、デフォルト以外のアクセスを行う各ユーザ アカウントについて、アクセス許可の詳細がホスト別に表示されます。

CA Access Control グループ権限

CA Access Control グループ権限レポートには、ユーザ グループがアクセスできるすべてのリソースのリストが表示されます。 レポートでは、リソース名別に以下の情報が表形式で詳細に表示されます。

- ホスト ID
- アクセス権限
- アクセスがデフォルトで許可されているか、プログラムを使用することでアクセスが許可されるか

- あらゆる制限。たとえば、カレンダやほかの時間に関する適用可能な制限
- ユーザ グループがリソースを所有しているのでアクセスが許可されるかどうか

このレポートを使用すると、企業全体にわたる定義リソースまたは特定のホストに対する定義リソースにアクセスするユーザ グループを特定することができます。 確認後、セキュリティ ポリシーに準拠するようにアクセス権限に変更を加えることができます。

CA Access Control グループ別リソース アクセス

CA Access Control グループ別リソース アクセス レポートには、指定されたリソースについて、ユーザ グループに付与されたアクセス権限が表示されます。 レポートには、指定のリソースにアクセスするすべてのユーザ グループに関する詳細なリストが表示されます。たとえば、ホスト ID、アクセス権限、デフォルト アクセスが許可されているかどうか、そのほかの任意の制限(日時指定など)が表示されます。

CA Access Control ユーザ別リソース アクセス

CA Access Control ユーザ別リソース アクセス レポートには、指定されたリソースについて、ユーザ アカウントに付与されたアクセス権限が表示されます。 レポートには、指定のリソースにアクセスするすべてのユーザ アカウントに関する詳細なリストが表示されます。たとえば、ホスト ID、アクセス権限、デフォルト アクセスが許可されているかどうか、そのほかの任意の制限(日時指定など)が表示されます。

CA Access Control ユーザ権限

CA Access Control ユーザ権限レポートは、ユーザのアクセス権限をリソース別に表示します。 このレポートでは、ユーザがアクセスできる各リソースに対して、ユーザのアクセス タイプ、デフォルト アクセス、リソースにアクセスするためにユーザが使用可能なプログラム、およびユーザのリソースへのアクセスに対する時間帯制限の情報が提供されます。 また、ユーザがリソース所有者かどうかも表示されます。

その他のレポート

標準的なその他のレポートには、監視対象ファイル、監視対象プログラム、およびシステムを再起動せずに CA Access Control カーネルをアンロードする UNIX ホストの対応状況に関する情報が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なその他のレポートのリストを以下に示します。

CA Access Control 監視対象ファイル(158 ページ)
CA Access Control 監視対象プログラム(158 ページ)
アンロードに関する考慮事項がある CA Access Control UNIX ホスト(158 ページ)

CA Access ControlUNIX アンロード対応（159 ページ）

CA Access Control 監視対象ファイル

CA Access Control 監視対象ファイル レポートには、企業内のホストにある重要なシステム ファイルの状態が表示されます。 レポートには、ファイルが監視されていないホスト、監視状態にあるファイルが変更されているホスト、ファイルが監視状態にあり、かつ信頼状態にあるホストがサマリ円グラフに表示されます。 また、ホスト ID など、ファイルに関する詳細も表示されます。これにより、該当するホスト上のファイルに対するポリシーを確認したり、ファイルに対する修正が権限のあるユーザによって行われたかどうかを確認したりできます。

重要なシステム ファイルが確実に監視されるようにすることは、データの整合性を保護するための必須条件です。 ファイルに対する変更が行われた日時を把握することで監査証跡が可能になります。結果として、権限のあるユーザが所定のセキュリティ ポリシーに従って変更を行ったことを検証できます。

CA Access Control 監視対象プログラム

CA Access Control 監視対象プログラム レポートには、企業内のホストにある重要なプログラムの状態が表示されます。 このレポートには、プログラムが監視されていないホスト、監視状態にあるプログラムが変更されているホスト、およびプログラムが監視され信頼状態にあるホストがサマリ円グラフに表示されます。 また、ホスト ID など、プログラムに関する詳細も表示されます。これにより、該当するホスト上のプログラムに対するポリシーを確認したり、プログラムに対する修正が権限のあるユーザによって行われたかどうかを確認したりできます。

重要なプログラムが確実に監視されるようにすることは、データの整合性を保護するための必須条件です。 プログラムに対する変更が行われた日時を把握することで監査証跡が可能になります。結果として、権限のあるユーザが所定のセキュリティ ポリシーに従って変更を行ったことを検証できます。

アンロードに関する考慮事項がある CA Access Control UNIX ホスト

アンロードに関する考慮事項がある CA Access Control UNIX ホスト レポートは、CA Access Control カーネルのアンロードを妨げる可能性のある、インターセプトされたシステム コールを持つ UNIX ホストを表示します。 これらのホストでは、カーネルのアンロードや CA Access Control のアップグレードを実行する前に、コンピュータを再起動する必要があります。

このレポートでは、アンロードに関する考慮事項がある各ホストに対して、プロセスおよび親プロセス ID、プログラム名、ブロック時間およびしきい値時間がリストされます。 また、各システム コールがブロック中かどうかを表示します。

このレポートでは、ホストを以下のカテゴリにまとめます。

- Not ready（overflow）- システム コール テーブルはそのサイズを超えます。また、カーネルをアンロードする場合、再起動する必要があります。
- Not ready（blocking system calls）- ブロック中のインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動する必要があります。
- Probable（non-blocking system calls）- ブロック中ではないインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動は必要ありません。

CA Access ControlUNIX アンロード対応

CA Access ControlUNIX アンロード対応レポートは、システムを再起動せずに CA Access Control カーネルのアンロードおよび CA Access Control のアップグレードを実行する UNIX ホストの対応状況を表示します。

このレポートでは、カーネルをアンロードする準備が完了したホスト、カーネルをアンロードする準備ができた可能性のあるホスト、カーネルをアンロードする準備ができていないホストの割合を示すサマリ円グラフが提供されます。 また、各ホストに対してインターセプトされ、かつブロックされていないシステム コールの数を提供します。

このレポートでは、ホストを以下のカテゴリにまとめます。

- Not ready（overflow）- システム コール テーブルはそのサイズを超えます。また、カーネルをアンロードする場合、再起動する必要があります。
- Not ready（blocking system calls）- ブロック中のインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動する必要があります。
- Probable（non-blocking system calls）- ブロック中ではないインターセプトされたシステム コールが存在します。また、カーネルをアンロードする場合、再起動は必要ありません。
- Ready - インターセプトされたシステム コールは存在しません。また、カーネルをアンロードする場合、再起動する必要はありません。
- Not applicable - 対象のホストは、UNIX ホストではありません。
- Unknown status - ホスト情報が取得できません。

ポリシー管理レポート

標準的なポリシー管理レポートには、ユーザの CA Access Control エンタープライズ管理 ポリシーに関する情報が提供されます。

注: レポートのタイトルは、BusinessObjects InfoView に表示されるような名前となります。

標準的なポリシー管理レポートのリストを以下に示します。

CA Access Control ポリシー割り当て

CA Access Control ポリシー割り当てレポートでは、ホストおよびホスト グループ上にデプロイされたポリシー割り当てに関する詳細情報を表示します。このホストおよびホストグループは指定された DMS 上に定義されています。 レポートには、以下の情報が提供されます。

- ポリシー名
- 割り当てタイプ(ホストまたはホスト グループ)
- ポリシーをデプロイするホストおよびホスト グループの名前

CA Access Control ポリシー デプロイメント スコアカード

CA Access Control ポリシー デプロイメント スコアカード レポートは、特定のポリシーのデプロイメント情報を表示します。 このレポートでは、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートではポリシー デプロイメントに関する問題の詳細をホスト別に提供します。

CA Access Control ホスト別ポリシー デプロイメント スコアカード

CA Access Control ホスト別ポリシー デプロイメント スコアカード レポートは、ポリシーのデプロイメント情報をホスト別に表示します。 このレポートには、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストまたはホスト グループに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートではポリシー デプロイメントに関する問題の詳細をホスト別に提供します。

CA Access Control ホスト グループ別ポリシー デプロイメント スコアカード

CA Access Control ホスト グループ別ポリシー デプロイメント スコアカード レポートでは、ポリシーのデプロイメント情報をホスト グループ別に表示します。 このレポートには、以下の情報がサマリ円グラフで提供されます。

- ポリシーが正常にデプロイされたホストの数。
- ポリシーがデプロイされたがエラーまたは偏差が発生したホストの数。
- 危険な状態にあるホストの数。(ポリシーがホストまたはホスト グループに割り当てられましたが、ホストにデプロイされていません。)

また、このレポートでは、ポリシー デプロイメントに関する問題の詳細をホスト グループ別に提供します。

CA Access Control ホスト別ポリシー デプロイメント ステータス

CA Access Control ホスト別ポリシー デプロイメント ステータス レポートでは、ポリシーのステータス情報をホスト別に表示します。 このレポートには、以下のような各ポリシーのバージョン情報が提供されます。

- 偏差ステータス
- デプロイメント日時
- ポリシーをデプロイしたユーザ名

CA Access Control ホスト グループ別ポリシー デプロイメント ステータス

CA Access Control ホスト グループ別ポリシー デプロイメント ステータス レポートは、ポリシーのステータス情報をホスト グループ別に表示します。 このレポートには、以下のような各ポリシーのバージョン情報が提供されます。

- 偏差ステータス
- デプロイメント日時
- ポリシーをデプロイしたユーザ名

また、このレポートではポリシーがデプロイされたホスト グループに存在するホストを一覧表示します。

CA Access Control ポリシー インベントリ

CA Access Control ポリシー インベントリ レポートは、以下のような DMS に格納されたポリシーのスナップショットを表示します。

- 各ポリシーが最後に更新された時間
- ポリシーを最後に更新したユーザ名
- ポリシーがデプロイされたバージョンの数
- 最後にポリシーが確定されたバージョン
- 依存先のポリシー名

注: ポリシーが他のポリシーに依存している場合、依存先のポリシーがデプロイされるまでそのポリシーはデプロイできません。

CA Access Control ポリシー ルール

CA Access Control ポリシー ルール レポートは、ポリシーにある各ルールのデプロイ スクリプトおよびデプロイ解除スクリプトをポリシー名別に表示します。 このレポートには、ルールの最終更新日およびルールの最終更新ユーザ名が提供されます。 さらに、ポリシーが確定されデプロイメントの準備ができているか、またポリシーのバージョン番号を表示します。

CA Access Control ポリシー バージョン

CA Access Control ポリシー バージョン レポートは、各ポリシーのバージョン情報をポリシー名別に表示します。 レポートには、各ポリシーに対して以下の情報が提供されます。

- 現在のバージョン番号
- 現在のバージョンのデプロイ日
- 現在のバージョンをデプロイしたユーザ名

また、このレポートでは現在のバージョンが最終バージョンかどうかを表示します。

CA Access Control ホスト別ルール偏差

CA Access Control ホスト別ルール偏差レポートは、ポリシー ステータスおよびルール偏差をホスト別に表示します。 このレポートには、各ホストに存在するポリシーの一覧、および各ポリシーのステータス、バージョン、偏差ステータスが提供されます。 このポリシーにルール偏差が存在する場合、レポートには偏差の詳細、つまり偏差の適用先となるリソースおよびプロパティの詳細が提供されます。

CA Access Control ホスト グループ別ルール偏差

CA Access Control ホスト グループ別ルール偏差レポートは、ポリシー ステータスおよびルール偏差をホスト グループ別に表示します。 このレポートには、各ホストに存在するポリシーの一覧、および各ポリシーのステータス、バージョンおよび偏差ステータスが提供されます。 このポリシーにルール偏差が存在する場合、レポートにはホスト グループの各ホスト メンバに対する偏差の詳細、つまり偏差の適用先となるリソースおよびプロパティの詳細が提供されます。

パスワード ポリシー レポート

パスワード ポリシー レポートは、CA Access Control で定義されたパスワード ポリシーに関する情報を提供します。

パスワード ポリシーによる CA Access Control 特権アカウント

このレポートは、システム内のすべての特権アカウントのリスト、およびそれに対応するパスワード ポリシーを表示します。 このレポートを使用すると、どの特権アカウントがどのパスワード ポリシーに関連付けられているかが分かります。 レポートの確認後、現在のスタータスがユーザのニーズに適合しているかどうか、または特権アカウントを再割り当てする必要があるかどうか、判断できます。

レポートには、以下の情報が提供されます。

- スナップショット作成日時
- パスワード ポリシー名
- エンドポイント タイプおよび名前
- アカウント名
- 前回のチェックアウト日
- 前回のパスワード変更

CA Access Control PUPM パスワード ポリシー

このレポートは、その複雑性に従って、現在のパスワード ポリシーを表示します。 このレポートを使用すると、既存パスワード ポリシーの最小長および最大長、その他のポリシー パラメータがユーザのセキュリティ基準に適合しているかどうか判断できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日
- パスワード ポリシーの名前および説明
- 最大長
- 最小長
- パスワード ポリシー パラメータ

特権アカウント管理レポート

特権アカウント管理レポートは、特権アカウント管理の詳細を表示します。

以下に、標準的な特権アカウント管理レポートのリストを示します。

エンドポイント別 CA Access Control 特権アカウント(165 ページ)
ユーザ別 CA Access Control PUPM ロールおよび特権アカウント(165 ページ)
エンドポイント別 CA Access Control 特権アカウント リクエスト(166 ページ)
承認者別 CA Access Control 特権アカウント リクエスト(166 ページ)
要求者別 CA Access Control 特権アカウント リクエスト(167 ページ)

特権アカウント別 CA Access Control PUPM ユーザ(167 ページ)
ロール別 CA Access Control PUPM ユーザ(168 ページ)

エンドポイント別 CA Access Control 特権アカウント

このレポートは、エンドポイント タイプおよびエンドポイント名別に、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。 レポートの確認後、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。 このレポートの確認後、どのロールが特権アカウントおよび CA Access Control エンタープライズ管理 ユーザ アカウントの両方に関連付けられているか特定できます。

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
- 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

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、承認者に従って、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、リクエストを承認したユーザに従って、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
- リクエストの説明
- 有効期限
- 承認者コメント

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従って、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

特権アカウント別 CA Access Control PUPM ユーザ

このレポートは、エンドポイント タイプ、エンドポイント名および名前に従って、特権アカウントにアクセスするユーザ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にアクセスする方法、および各特権アカウントが所属するエンドポイントのタイプと名前を特定できます。

このレポートには、以下の情報が表示されます。

- スナップショット タイプ :
- エンドポイントのタイプおよび名前
- 特権アカウント名
- ユーザ名
- ユーザ ID
- リクエスト

ロール別 CA Access Control PUPM ユーザ

このレポートは、ユーザおよびそれらに関連付けられた特権アカウント ロールのリストを表示します。 このレポートを使用すると、ユーザが特権アカウント ロールにどのように関連付けられるか特定し、現在のステータスがユーザのセキュリティ条件に適合しているかどうか判断できます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- ロール名
- メンバ数
- ユーザ名
- ユーザ ID
- 電子メール アドレス

UNIX 認証ブローカ レポート

UNAB レポートは、UNAB 管理タスクの詳細を表示します。

以下は、標準的な UNIX 認証ブローカ レポートのリストです。

CA Access Control UNAB ホスト別エンタープライズ ユーザ アクセス

このレポートでは、UNAB ホストにアクセスしたエンタープライズ ユーザのリストをホスト別に表示します。 レポートには、各ホストにアクセスしたエンタープライズ ユーザ、前回のログイン試行、および誰がホストへのアクセスを許可されたか(ユーザまたはグループ)についての情報が提供されます。 このレポートを確認した後、エンタープライズ ユーザがホストに対して持っているアクセス権限を変更できます。

CA Access Control UNAB エンタープライズ ユーザ別ホストへのアクセス

このレポートでは、UNAB ホストにアクセスしたエンタープライズ ユーザのリストをユーザ別に表示します。 レポートには、各ホストにアクセスしたエンタープライズ ユーザ、前回のログイン試行、および誰がホストへのアクセスを許可されたか(ユーザまたはグループ)についての情報が提供されます。 このレポートを確認した後、エンタープライズ ユーザがホストに対して持っているアクセス権限を変更できます。

CA Access Control UNAB Active Directory ユーザ

このレポートには、ローカル ホストへのアクセスが許可されているエンタープライズ ユーザのリストが表示されます。 このレポートを使用すると、現在のエンタープライズ ユーザ アカウント、ID、ホーム ディレクトリ、およびシェル タイプを参照できます。 このレポートの参照後、ユーザのパラメータの変更およびエンタープライズ ユーザの追加または削除を行うことができます。

このレポートには以下の情報が表示されます。

- スナップショット時間
- エンタープライズ ユーザ
- ユーザ ID
- プライマリ グループ
- ホーム ディレクトリ
- ログイン シェル
- ユーザ数

CA Access Control UNAB Active Directory ユーザ アクティビティ

このレポートには、移行および一部移行されたエンタープライズ ユーザ アカウントのアクティビティ リストが表示されます。 このレポートを使用すると、UNIX ホスト上でのエンタープライズ ユーザのアクティビティを参照できます。 このレポートを参照すると、前回の成功および失敗ログイン、ユーザによる前回の成功パスワード変更などの情報を確認できます。

このレポートには以下の情報が含まれています。

- ユーザ名
- フルネーム
- 成功したログイン
- 失敗したログイン
- パスワードの変更
- 前回の失敗ログイン

CA Access Control UNAB エンタープライズ グループ

このレポートには、エンタープライズ グループの属性が表示されます。 このレポートを使用して、エンタープライズ グループのプロパティを参照します。このレポートを参照すると、エンタープライズ グループに関する詳細(グループ ID など)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。

- グループ名
- GID
- グループの説明

ホスト別 CA Access Control UNAB グループ移行ステータス

このレポートには、グループ移行プロセスのステータスがホスト別に表示されます。 このレポートを使用して、ローカル ホストの各グループの状態を確認します。 このレポートには、グループの移行ステータス(Migrated、Local Account、Partial Migration、および Not Migrated)および移行中に検出された競合(競合する名前、ID など)に関する情報が表示されます。

このレポートには以下の情報が表示されます。

- ホスト名
- ローカル グループ名
- グループ移行ステータス
- 競合する名前
- 競合する GID
- 競合するメンバー
- エンタープライズ グループなし
- UNIX 属性なし

グループ別 CA Access Control UNAB グループ移行ステータス

このレポートには、グループ移行プロセスのステータスがグループ別に表示されます。 このレポートを使用して、Active Directory への移行を選択したグループの移行ステータスを参照します。 このレポートには、グループが存在したホストのリスト、移行ステータス(Migrated、Local Group、Partial Migration、および Not Migrated)、および移行プロセス中に検出された競合が表示されます。

このレポートには以下の情報が表示されます。

- グループ名
- ホスト名
- 移行ステータス
- 競合する名前
- 競合する GID
- 競合するメンバー
- エンタープライズ グループなし
- UNIX 属性なし

ホスト グループ別 CA Access Control UNAB ホスト

このレポートには、UNAB ホスト グループがホスト グループ別に表示されます。 このレポートを使用すると、UNAB ホストの現在のグルーピングおよび各 UNAB ホストの ACL リストの場所に関する概要を確認できます。 このソースは、ローカル ACL ファイル（allow および .deny アクセス ファイル）または DMS です。 また、このレポートには各ホストのデフォルト アクセス設定も表示されます。

このレポートには以下の情報が含まれています。

- ホスト グループ
- ホスト名
- ソース
- デフォルト アクセス

CA Access Control UNAB ローカル グループ

このレポートには、各グループの移行プロセスのステータスが表示されます。 このレポートを使用すると、各ホストでの移行プロセスの現在のステータスを参照できます。

このレポートには以下の情報が表示されます。

- スナップショット時間
- ホスト名
- 移行ステータス
- グループ名
- グループ ID
- 名前の競合
- GID の競合
- メンバーの競合
- Active Directory グループ競合なし
- エントリ数

CA Access Control UNAB ローカル グループ サマリ

このレポートには、ローカル グループ パラメータの要約が表示されます。 このレポートを使用すると、同じグループのインスタンスが各ホストにどのくらい存在するかについての概要を確認できます。 このレポートの参照後、グループ パラメータを変更するかどうかを選択できます。

このレポートには以下の情報が表示されます。

- スナップショット時間
- ホスト数
- グループ名
- グループ ID
- インスタンス数

CA Access Control UNAB ローカル ユーザ

このレポートは、ユーザ 移行プロセスのステータスを表示します。 このレポートを使用すると、Active Directory へのユーザ移行プロセスの現在のステータスを確認できます。このレポートは、すべてのユーザの移行ステータス、ローカルおよび Active Directory (グローバル)の属性などを表示します。 このレポートを確認することによって、各ホストの移行プロセスのステータスを推察し、移行プロセスで識別された競合を解決できます。

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
- ホスト名
- 移行ステータス
- ローカル ユーザ名
- ローカル ユーザ ID
- Active Directory ユーザ ID
- プライマリ ローカル グループ ID
- プライマリ Active Directory グループ ID
- ローカル ホーム ディレクトリ
- Active Directory ホーム ディレクトリ
- ローカル ログイン シェル
- Active Directory ログイン シェル
- ローカル GECOS

- グループの競合
- エントリ数

CA Access Control UNAB ローカル ユーザ サマリ

このレポートは、ローカル ユーザ パラメータの概要を表示します。 このレポートの情報では、単一ユーザアカウントが UNIX ホストに表示されるインスタンスの数が表示されます。

このレポートには、以下の情報が表示されます。

- スナップショット作成日時
- ホスト数:
- ユーザ名
- ユーザ ID
- グループ ID
- ホーム ディレクトリ
- ログイン シェル
- エントリ数

CA Access Control UNAB 非標準ローカル ユーザ

このレポートは、その属性が Active Directory のユーザ属性と一致しないローカル ユーザのリストを、ユーザ別に表示します。 このレポートを使用すると、移行プロセス中に検出された、ローカル ユーザのプロパティと Active Directory アカウントのプロパティの間の相違を検証し、修正できます。 このレポートには、アカウントの所属先の各ホストで表示されるのと同様の、ユーザ アカウント情報が表示されます。

このレポートには、以下の情報が表示されます。

- ユーザ名
- ホスト名
- ユーザ ID
- グループ ID
- ホーム ディレクトリ
- ログイン シェル

CA Access Control UNAB 非標準ローカル グループ

このレポートは、Active Directory のグループ属性と一致しないローカル グループ属性を、グループ別に表示します。 このレポートを使用すると、移行プロセス中に検出された、ローカル グループのプロパティと Active Directory グループのプロパティの間の相違を検証し、修正できます。 このレポートには、このグループがある各ホストに表示されるのと同様の、ローカル グループ情報が表示され、検出された相違が強調されます。

このレポートには、以下の情報が表示されます。

- グループ名
- ホスト名
- グループ ID

ホスト別 CA Access Control UNAB ユーザ アクセス

このレポートは、ホストによって示された UNIX ホストにアクセス可能な Active Directory ユーザのリストを表示します。 このレポートを使用すると、ホストへのアクセスを許可または拒否されたユーザ別に、各ホストを確認し、最近の成功ログインおよび失敗ログインなどの概要を表示できます。 このレポートで情報を確認した後に、ホストへのユーザ アクセスを変更する場合があります。

注:: このレポートは、ホストへのデフォルト アクセス権限を持つユーザをリスト表示しません。

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
- ホスト名
- ホスト グループ
- ユーザ名
- ユーザ グループ
- アクセス
- 成功したログインはありません。
- 前回の失敗ログイン
- 前回の失敗したログイン試行
- ルール ソース
- アカウントの数

ホスト別 CA Access Control UNAB ユーザ移行テータス

このレポートは、ローカル ユーザの移行ステータスを、ホスト別に表示します。 このレポートを使用すると、ローカル ホストから Active Directory へ移行するために選択した各ユーザのステータスを表示できます。 このレポートは、移行ステータス(グローバルまたはマップされた)、および移行プロセス中に検出された競合を表示します。

このレポートには、以下の情報が表示されます。

- ホスト名
- ローカル ユーザ名
- アカウント名へのマップ
- 移行ステータス
- 競合

ユーザ別 CA Access Control UNAB ユーザ移行テータス

このレポートは、ローカル ユーザの移行ステータスを、ユーザ別に表示します。 このレポートを使用すると、ローカル ホストから Active Directory へ移行するために選択した各ユーザのステータスを表示できます。 このレポートは、このアカウントがあるホストのリスト、移行ステータス(グローバル、ローカル、マップ済み、および未移行)、および移行プロセス中に検出された競合が表示されます。

このレポートには、以下の情報が表示されます。

- ローカル ユーザ名
- ホスト名
- マップ先
- 移行ステータス
- 競合

CA Enterprise Log Manager レポート

CA Enterprise Log Manager レポートは、CA Access Control および UNAB のアカウント アクティビティ、リソース管理などに関する詳細情報を表示します。

CA Enterprise Log Manager レポートの詳細については、CA Enterprise Log Manager のマニュアルを参照してください。

BusinessObjects InfoView レポート ポータル

レポート ポータルは、CA Access Control レポートを提供するアプリケーション サーバです。 このサーバでは、BusinessObjects InfoView ポータルを使用することで、中央データベースに格納されたレポート情報を対話式で操作できるようにしています。

レポートを使用するための InfoView の起動

BusinessObjects InfoView を使用して CA Access Control レポートにアクセスします。以下の手順は、レポート インターフェース(BusinessObjects InfoView)にアクセスする方法について説明します。

レポートを使用できるように InfoView を起動するには、以下の手順に従います。

1. 以下のいずれかの方法で、InfoView を起動します。
   - BusinessObjects InfoView がインストールされているコンピュータで、[スタート]-[プログラム]-[BusinessObjects XI Release 2]-[BusinessObjects Enterprise]-[BusinessObjects Enterprise Java InfoView]を選択します。
   - 任意のコンピュータのブラウザから、次の URL にアクセスします。

     `http://ACRPTGUI_host:ACRPTGUI_port/businessobjects/enterprise115`

     ACRPTGUI_host は、InfoView がインストールされているコンピュータの名前または IP アドレスです(レポート ポータル)。

     ACRPTGUI_port は、InfoView へのアクセスに使用するポート番号(デフォルトは 9085)です。

   [InfoView Log On]ページが表示されます。
2. InfoView のインストール時に設定した認証情報を入力し、[Log On]をクリックします。

   [InfoView Home]ページが表示されます。

注: BusinessObjects InfoView の使用方法の詳細については、「BusinessObjects Enterprise XI Release 2 InfoView User's Guide」を参照してください。

レポートの実行

レポート インターフェース(BusinessObjects InfoView)を開いたら、レポートを選択し、それを実行できるようになります。

レポートを実行するには、以下の手順に従います。

1. InfoView を開きます。

   [InfoView Home]ページが表示されます。

2. [Home]-[Public Folders]-[CA Reports]を展開し、左側のフレームにある[CA Access Control]をクリックします。

   CA Access Control ページが表示されます。

3. 表示するレポートのリンク付けされたタイトルをクリックします。

   レポートのページが表示され、表示するレポートの範囲を定義する値を入力できるようになります。

4. フォーム フィールドに値を入力して取得するレポートの範囲を定義し、[OK]をクリックします。

   レポートの出力ページが表示されます。

   追加のクエリを実行して、レポート生成に反映させることができます。 たとえば、すべてを含めるように指定したり、特定のホストを選択したりして、既知のすべてのホストまたは単一のホストに基づくレポートを作成できます。 さらに、日付範囲を指定して、すべての履歴データを表示したり、特定の日付のデータのみを表示したりできます。

   注: %(パーセント)記号を使用して、ワイルドカード値を指定できます。 % の用法は SQL の標準的な選択表記記号で、通常、ワイルドカードを指定する場合のように単一の文字を表すものではありません。

注: BusinessObjects InfoView の使用方法の詳細については、「BusinessObjects Enterprise XI Release 2 InfoView User's Guide」を参照してください。

レポートのスケジュール

レポートを実行するには、さまざまな方法があります。 レポート タイトルをクリックし値を指定してレポートを実行することも、さまざまなオプションから選択してレポートをスケジュールすることも可能です。

レポートをスケジュールするには、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. 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。

生成されたレポートの表示

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。

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 によって提供されています。 CA 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. 認証情報を入力し、[OK]をクリックします。

   Quick Design ウィザードの開始画面が表示されます。

3. [Run this Wizard at Startup]チェック ボックスをオフにし、[Cancel]をクリックします。

   空の Designer セッションが開きます。 タイトル バー内にユーザ名およびリポジトリ名が表示されます。

4. [File]-[Open]をクリックし、CA Access Control Universe を含んでいるディレクトリを参照して CA Access Control.unv ファイルを選択し、[Open]をクリックします。

   現在の Designer ウィンドウで CA Access Control Universe が開きます。

   注: CA Access Control Universe は、デフォルトの universe ファイル ストアとして指定されたディレクトリ内で CA Universe¥CA Access Control の下に格納されています。

標準レポートのカスタマイズ

標準レポートはいずれもカスタマイズすることができます。 たとえば、タイトル、色、ロゴ、およびフォントを必要に応じて変更できます。 変更を行うには、レポートを Crystal Reports Designer XI で開く必要があります。 どのレポートもそれぞれ対応する .rpt ファイルを使用しています。 このファイルを開いて、レポートをカスタマイズします。

標準レポートをカスタマイズするには、以下の手順に従います。

1. カスタマイズする .rpt ファイルを Designer で開きます。

   レポートのデザイン ビューが表示されます。

2. 以下のいずれかの操作を行います。

   - レポートのタイトルを変更するには、[File]-[Summary Info]をクリックし、[Title]フィールドにタイトルを入力します。
   - テキストをカスタマイズするには、デザイン ビュー内の希望のテキストを強調表示し、それをダブルクリックして編集を行います。
   - テキストの表示方法を変更するには、開いているレポート内のテキストを右クリックして[Format text]を選択し、必要に応じてプロパティを変更します。

3. custom .rpt ファイルを保存します。

   新しいカスタム レポートが保存され、いつでも公開できるようになります。

カスタム レポートの公開

カスタム レポートは、BusinessObjects InfoView を使用して公開する必要があります。

カスタム レポートを公開するには、以下の手順に従います。

1. BusinessObjects InfoView を開き、管理者権限でログインします。

   [InfoView Home]ページが表示されます。

2. [New]-[Folder]をクリックし、[Public Folders]の下に新しいフォルダを作成します。

   [Create A New Folder]タスク ページが表示されます。

3. カスタム レポート フォルダの名前および説明を入力し、[OK]をクリックします。

   新しいフォルダが作成されます。

4. 作成したフォルダで、[New]-[Document from local computer]-[Crystal Report]をクリックします。

   [Add a document from your local computer]タスク ページが表示されます。

5. レポートのタイトルとカスタマイズされた rpt ファイルへのパス名を入力し、[OK]をクリックします。

   カスタム レポートが公開され、BusinessObjects InfoView から表示できるようになりました。 カスタム レポートは、ほかの任意のレポートと同様にスケジュールすることもできます。

第 10 章: サンプル ポリシーのデプロイ

このセクションには、以下のトピックが含まれています。

既定のサンプル ポリシー

CA Access Control とともに提供されるサンプル ポリシーでは、オペレーティング システムおよびアプリケーション ソース保護のために推奨される、職務分掌およびベスト プラクティスをご紹介しています。 各ポリシーは selang スクリプトになっており、その中のコメントによって、ポリシーの目的と含まれているルールが説明されています。

これらのポリシーは、CA Access Control によるシステム保全のための基準を提供するものです。 これらサンプルのポリシーは、個別のセキュリティ ポリシーおよび環境に合わせてカスタマイズする必要があります (オペレーティング システム ポリシーは、実際にインストールされている OS パッケージに依存します)。 独自のポリシーの基盤としてこれらのサンプル ポリシーを使用することで、所属組織のためのポリシー作成プロセスを簡便化できます。

サンプル ポリシーは以下の共通アプリケーションならびにオペレーティング システムで使用可能です。

- アプリケーション:
  - Apache
  - JBoss アプリケーション サーバ
  - CA Access Control Web サービス
  - Microsoft SQL Server
  - Oracle Database 10g
- オペレーティング システム:
  - AIX
  - HP-UX
  - Red Hat Enterprise Linux
  - SuSE Linux Enterprise Server

  - Sun Solaris
  - Windows 2003
- 仮想化システム:
  - VMware ESX Server
  - Hyper-V
  - Solaris 10 ゾーン

サンプル ポリシーの保存場所

CA Access Control は、サンプル ポリシーを以下のディレクトリにインストールします。

```
ACInstallDir/samples/Policies/
```

ACInstallDir

CA Access Control のインストール先ディレクトリを定義します。

この場所には 3 つのサブディレクトリがあります。

- Applications - アプリケーション サーバのポリシーが含まれています。
- OS - オペレーティング システムのポリシーが含まれています。
- Virtualization - 仮想システムのポリシーが含まれています。

CA Access Control は、ポリシーをテキスト ファイルとして提供します。このファイルには、ポリシーを実行する selang スクリプトが含まれています。 また、各ポリシーには保護ポリシーのデプロイ解除に使用できる一致ポリシーが含まれています。

ポリシー ロールの命名規則は OS_ACTION です。

OS

ポリシーの設計対象となるオペレーティング システムを定義しています。

ACTION

スクリプトが実行するポリシー アクションを定義しています。

値: deploy または undeploy

たとえば、ファイル「_LINUX40_deploy.txt」の場合、Red Hat Enterprise Linux 4.0 用のサンプル デプロイメント ポリシーが含まれています。

注: アプリケーション ポリシーにデプロイ解除スクリプトはありません。

サンプル ポリシー スクリプト

各ポリシーは selang スクリプトになっており、その中のコメントによって、ポリシーの目的と含まれているルールが説明されています。 サンプル ポリシー スクリプトはベスト プラクティスの実例を示すために提供されます。

- コメント

  サンプル ポリシーには注釈が追加されているため、サンプル ポリシーの各セクションで何が実行されるのかを理解するのに役立ちます。

- コンテナ

  サンプル ポリシーでは、関連するリソースを 1 つのコンテナ リソースにまとめています。 この方法により、共通のポリシーが関連するすべてのリソースに一度で適用されます。 ポリシー ルール(ACL)を個々のリソースに適用する必要はありません。 たとえば、ポリシーで 1 つのコンテナを使用して、すべてのシステム環境設定ファイルをまとめることができます。

  ポリシー コンテナでは、命名規則 POL_container_name を使用します。 これらのコンテナをサブポリシーと見なすことができます。 たとえば、OS サンプル ポリシーでは、POL_SYS_CONF コンテナを使用して OS 環境設定ファイルを保護します。

- ロール

  ユーザの管理を簡略化するために、サンプル ポリシーではロールに ACL を適用します。 各ロールは、CA Access Control のユーザ グループを使用します。このグループには、実際のユーザを追加することができます。

  ポリシー ロールでは、命名規則 ROL_role_name を使用します。 たとえば、サンプル ポリシーは、adm および lp のような組み込みのシステム ユーザに対して ROL_SYSTEM グループを使用します。 多くのポリシーでは、ユーザに(適切なシステム操作に必要な)幅広い権限を割り当てていますが、ユーザがログインに使用できないように権限を無効にすることができます。

- 変数

  デプロイ時に適用する変更を最小限に抑える必要があるため、サンプル ポリシーでは CA Access Control 変数を使用します。 サンプル ポリシーは、組み込み変数を使用してローカルのシステム リソース(例えば、ローカル ホストの端末ルール)を保護します。 また、ポリシーの変更を簡略化するためにユーザ定義の変数も使用します。 たとえば、ユーザ定義の変数に管理者ユーザのホーム ディレクトリを含めることができます。 管理者ユーザが別のホーム ディレクトリを使用する場合、ユーザ定義の変数を一度書き換えるだけで、影響を受けるすべてのルールが自動的に変更されます。

例: ポリシー スクリプト コメント

以下の Solaris SPARC 9 サンプル ポリシーのコードの抜粋では、サンプル ポリシーにどのようにコメントが追加されているかを示しています。 selang 構文ルールを使用しているため、ハッシュ記号 (#) から始まる行がコメントです。

```
#
# * Home Directories Protection Policy *
#**************************************
#
# This policy uses the FILE class to protect the home
# directories of sensitive users so that only the owner
# of each directory can access it.
#
# Prerequisites:
#     None
#
# Roles:
#     None
#
# Containers:
#     POL_HOME_DIR      - home directories of sensitive users
#
# define container POL_HOME_DIR
# Protect home directories
editres  CONTAINER POL_HOME_DIR audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
comment("AC Sample - Protect home directories")
authorize CONTAINER POL_HOME_DIR uid(* _undefined)  access(NONE)
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editusr  < ! (USER_OS_ADMIN> )
# define specific FILE resources and connect them with POL_HOME_DIR
editres FILE ("<!HOME_OS_ADMIN>/*") audit(<!POLICY_AUDIT_MODE>) owner(+nobody)
defaccess(NONE) <!POLICY_WARNING_MODE>  comment("AC Sample")
authorize FILE ("<!HOME_OS_ADMIN>/*") uid(<!USER_OS_ADMIN>) access(ALL)
chres CONTAINER POL_HOME_DIR mem+("<!HOME_OS_ADMIN>/*") of_class(FILE)
```

例: サンプル ポリシーのコンテナ

以下の selang 出力は、POL_SYS_FILES のプロパティを示しています。 AIX サンプル ポリシーには、システム ファイルを保護するこのサブポリシーが含まれています。

```
AC> sr container POL_SYS_FILES
Data for CONTAINER 'POL_SYS_FILES'
------------------------------------------------------------------------
ACLs              :
    Accessor                Access
    ROL_SYSADMIN  (GROUP  ) All
    ROL_SYSTEM    (GROUP  ) All
    *             (USER   ) R, Chdir
    _undefined    (USER   ) R, Chdir
Members           :
    /boot/*       (FILE   )
    /dev/kmem     (FILE   )
    /dev/mem      (FILE   )
    /dev/port     (FILE   )
Audit mode        : Failure
Owner             : +nobody       (USER   )
Create time       : 10-Dec-2008 10:32
Update time       : 10-Dec-2008 10:35
Updated by        : root          (USER   )
Comment           : AC Sample - Protect OS system files
```

例: サンプル ポリシーの変数

以下の Red Hat Enterprise Linux 5 サンプル ポリシーのコードの抜粋では、サンプル ポリシーでどのように変数が使用されているかを示しています。 この例では、サンプル ポリシーはローカル ホストおよび管理者ユーザ root のホーム ディレクトリの名前の候補を定義しています。

```
#
# * AC Variables Definitions *
#****************************
#
# The rules in this section define variables that policies use.
# Variables:
#    LOCALHOST          : list of possible names for local host
#    HOME_OS_ADMIN      : root's home directory
#    POLICY_WARNING_MODE  : set policies warning mode (set to WARNING or WARNING-)
#    POLICY_AUDIT_MODE    : set policies audit mode
#    POLICY_DEFACCESS     : set defaccess of policies` resources
#
```

```
editres ACVAR ("LOCALHOST") value("localhost") type(static)
editres ACVAR ("LOCALHOST") value+("127.0.0.1")
editres ACVAR ("LOCALHOST") value+("0.0.0.0")
editres ACVAR ("HOME_OS_ADMIN") value("/root") type(static)
editres ACVAR ("POLICY_WARNING_MODE") value("WARNING") type(static)
editres ACVAR ("POLICY_AUDIT_MODE")  value("FAILURE") type(static)
editres ACVAR ("POLICY_DEFACCESS")   value("ALL")    type(static)
```

詳細情報:

ユーザ定義変数(79 ページ)
組み込み変数(80 ページ)
変数使用のガイドライン(81 ページ)
エンドポイントで変数を解決する仕組み(82 ページ)

ポリシー デプロイメント

CA Access Control ポリシーをデプロイする場合、エラーを発生させずに正常にポリシーのデプロイおよび実行を行うために、いくつかの共通手順に従う必要があります。以下のセクションでは、サンプル ポリシーのデプロイ前またはデプロイ後に実行する必要があるアクションについて説明します。

ポリシー デプロイメントのためにエンドポイントを準備する方法

ポリシーを実装する前に、ポリシーのエンドポイントを準備する必要があります。 実行すると、このポリシーに関連する問題を後で分離することができます。

ポリシー デプロイメントのためにエンドポイントを準備する方法

- オペレーティング システムまたはアプリケーションの新規インストールを使用する

  OS ポリシー用に、製造者から提供された OS の最新バージョンおよびパッチを使用します。 これにより、変更によってシステムの安全性が潜在的に損なわれる前に、システムを保護することができます。 ポリシーを適用した後、パッチを適用したり、必要に応じてシステムを設定し、悪意のある変更や偶発的な変更からシステムを保護することができます。 アプリケーションにも同じことがあてはまります。

- 職務分掌を実装する

  ポリシー ルールを確認し、必要に応じて他のロールを追加します。 ロール、ユーザおよびそれらの関係(ロール メンバシップ)を定義する独自のポリシーを作成します。 サンプル ポリシーのデプロイ前または後にこのポリシーをデプロイできます。

  単一ユーザに必要以上の権限を割り当てていないことを確認してください。 たとえば、デフォルトではスーパーユーザが CA Access Control 管理者権限を提供する ROL_AC_ADMIN に追加されています。 最良の方法として、このユーザを削除し、代わりにセキュリティ管理者をこのグループに追加することをお勧めします。

- 新しい CA Access Control データベースの作成する、または既存のデータベースをバックアップする

  ポリシーを実装する前に、新しいデータベースを作成します。 これにより、ポリシールールの競合またはデータベースの既存ルールへの変更が発生しないようになります。 新しいデータベースを作成することができない場合、データベースをバックアップし、そのバックアップを使用してポリシー適用前の状態にリストアできるようにしてください。

- 新しい監査ログ ファイルを使用する

  既存の監査ログ ファイルをバックアップし、それを消去します。 これによって、新しいイベントをログに記録する際、CA Access Control は新しい監査ログ ファイルを作成します。 監査ログ ファイルにはデプロイするポリシーに関連したイベントのみが記録されているため、このポリシーに関連する問題の確認および分離を迅速に行うことができます。

- CA Access Control ユーザ定義変数を設定する

  設定済みの CA Access Control 変数の値(「AC Variables Definitions」セクション)を検証し、使用中の環境に一致させるか、または必要に応じて値の追加、変更を行います。

段階的なポリシーのデプロイ方法

ポリシーをデプロイする際、いくつかのアクションを実行することで、ポリシーのデプロイおよびポリシーの実行をエラーを発生させず、正常に行うことができます。 ポリシーをデプロイするためにエンドポイントを準備した後、段階的にポリシー デプロイメントを実行することをお勧めします。

段階的な方法でポリシーをデプロイする方法

1. ポリシーを警告モードでデプロイします

   現在、このポリシーはアクティブですが、そのルールは適用されません。 そのため、ポリシーを有効にする前に、対象となるポリシーの結果を監査ログでプレビューすることができます。

   注: サンプル ポリシー クリプトでは、すべてのポリシー ルールがデフォルトで警告モードに設定されています。

2. 警告メッセージがあるかどうか CA Access Control 監査ログを確認します

   ポリシーをデプロイした後、ポリシー違反があれば警告として監査ログに表示されます(ポリシー ルールが警告モードを使用している場合)。

3. 実際のシナリオでシステムを使用し、再び監査ログを分析します。

   ポリシーを効果的にテストするために、コンピュータ上で通常の操作手順を実行することができます(ログイン、サービスおよびアプリケーションの起動、停止など)。次に、監査ログを再度分析し、新しい警告が表示されているかどうかを確認することができます。

4. 必要に応じてポリシーを修正します

   監査ログから収集した情報を使用すると、使用中の環境で正しく動作するようにポリシーを修正することができます。

5. ポリシーを有効にするために、警告モードを削除します

   本稼働環境でポリシーのルールを適用する準備ができたら、ルールを有効にするために警告モードを削除できます。

   ポリシーが適用されます。

注: ポリシーを変更する場合、まずポリシーの適用を無効にします(警告モードを使用します)。ポリシーに変更を加えた後、変更が希望どおりに機能していることが確認できたら、ポリシーを再度有効にします。

詳細情報:

サンプル ポリシーの展開(192 ページ)
環境にあわせたサンプル ポリシーのカスタマイズ方法(193 ページ)
サンプル ポリシー適用の有効化(194 ページ)

サンプル ポリシーの展開

CA Access Control のサンプル ポリシーを展開する方法は 2 種類あります。

- エンドポイント上の selang でポリシー ファイルを実行する。 この方法では、ポリシー内の各ルールがローカルの CA Access Control データベース上で実行されます。 selang コマンドが実行を完了すると、ポリシーがそのエンドポイント上に展開されます。

  注: selang を使ってファイルでコマンドを実行する方法の詳細については、「selang リファレンス ガイド」を参照ください。

- 拡張ポリシー管理を使用する。 この方法では、CA Access Control エンタープライズ管理を使用してサンプル ポリシーを DMS 上に格納しておき、複数のエンドポイントに割り当てることができます。

  注: CA Access Control エンタープライズ管理および拡張ポリシー管理の詳細については、「エンタープライズ管理ガイド」を参照ください。

例: サンプルの RHEL 5 ポリシーを selang を使って展開

以下のコマンドでは、Red Hat Enterprise Linux 5 に対するサンプル ポリシーを含んだ selang スクリプトの展開方法を示しています。

```
selang -f _LINUX50_deploy.txt > _LINUX50_deploy.log
```

環境にあわせたサンプル ポリシーのカスタマイズ方法

サンプル ポリシーはセキュリティ ポリシーの基本として提供されます。 サンプル ポリシーをデプロイするには、環境に合わせてカスタマイズする必要があります。

環境にあわせてサンプル ポリシーをカスタマイズする方法

- CA Access Control およびシステム ログ ファイルを確認します。

  デプロイメント プロセス中に発生した警告およびエラーの検索、識別を行い、これらの原因となるポリシーを修正します。

- ユーザをポリシー ロールに追加します。

  サンプル ポリシーでは、権限付与にロールを使用します。 そのため、組織のユーザをロールに割り当てる必要があります。

  重要: ポリシーをデプロイ解除する場合、作成したユーザおよびグループを削除しないでください。 削除すると、同じユーザおよびグループを使用する他のポリシーで、ACL リストの正常な動作やアクセサの関連付けに影響を及ぼす場合があります。

- (Windows のみ) 共存ユーティリティ eACoexist.exe を実行します。

  このユーティリティは、CA Access Control と他のインストール済みプログラムの間で発生した競合を識別し、そのプログラムにバイパスを作成することによって競合を解決します。

サンプル ポリシー適用の有効化

デフォルトでは、サンプル ポリシー スクリプトは変数を使用するすべてのポリシー ルールを警告モードに設定しています。 このポリシーをデプロイする際、ポリシーはアクティブですが、そのルールは適用されません。 ポリシーに習熟し、必要に応じてポリシーをカスタマイズした後、ポリシーを有効にする準備が完了するとポリシー ルールが適用されます。

サンプル ポリシーの適用を有効にする方法

1. ポリシー スクリプトを編集し、POLICY_WARNING_MODE 変数の値を「WARNING-」に変更します。

   スクリプト ルールは最終的に以下になります。

   ```
   editres ACVAR ("POLICY_WARNING_MODE") value("WARNING-") type(static)
   ```

   warning- をリソースまたはアクセサに設定するルールを実行すると、CA Access Control はリソースまたはアクセサから警告モードを削除します。

2. 編集したポリシーをデプロイします。

   ポリシーの適用が有効になります。

サンプル ポリシー適用の無効化

デフォルトでは、サンプル ポリシー スクリプトは変数を使用するすべてのポリシー ルールを警告モードに設定しています。 ポリシーの適用を有効にするには、警告モードを削除します。 ポリシーの適用を無効にするには、警告モードを再度導入する必要があります。

サンプル ポリシーの適用を無効にする方法は以下のとおりです。

以下のいずれかの操作を行います。

- 以下のようにポリシーを警告モードで再デプロイします。

  a. ポリシー スクリプトを編集し、POLICY_WARNING_MODE 変数の値を「WARNING」に変更します。

     スクリプト ルールは最終的に以下のようになります。

     ```
     editres ACVAR ("POLICY_WARNING_MODE") value("WARNING") type(static)
     ```

     リソースまたはアクセサに warning を設定するルールを実行すると、CA Access Control はリソースまたはアクセサに警告モードを追加します。

  b. 編集したポリシーをデプロイします。

     ポリシーの適用が無効になります。

  リソースまたはアクセサに warning を設定するルールを実行すると、CA Access Control はリソースまたはアクセサを警告モードに設定します。

- ポリシーを確認して影響を受けるクラスを識別し、これらのクラスに対して警告モードを設定します。

ポリシーの適用が無効になります。

デプロイ済みのサンプル ポリシーがある場合のシステム メンテナンス実行方法

システムをアップグレードしたり、新しいアプリケーションをインストールするために、特定の時間にシステム メンテナンスを実行しなければならない場合があります。 システム メンテナンス中にエラーが発生するのを避けるため、ポリシーを無効にする必要があります。

デプロイ済みのサンプル ポリシーがある場合、システム メンテナンスを実行するには以下の手順に従います。

1. ポリシーの適用を無効にします。
2. メンテナンスを実行します。
3. ポリシーの適用を有効にします。
4. CA Access Control 監査ログ ファイルを確認します。

   監査ログには、メンテナンスによる影響を受けたファイルへの警告が含まれています。