CA Access Control for Virtual Environments

製品ガイド

r2.0

サードパーティに関する通知

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

サンプル スクリプトおよびサンプル SDK コード

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

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

CA Technologies 製品リファレンス

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

- CA Access Control Enterprise Edition
- CA Access Control
- CA User Activity Reporting Module
- Identity Manager

ドキュメントの表記規則

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

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

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

形式	意味
斜体	ユーザが入力する必要のある情報
角かっこ ([]) で囲まれた文字列	オプションのオペランド
中かっこ ({}) で囲まれた文字列	必須のオペランド セット
パイプ (|) で区切られた選択項目	代替オペランド (1 つ選択) を区切ります。 たとえば、以下の例は「*ユーザ名*または*グループ名*のいずれか」を意味します。 {*username*|*groupname*}

形式	意味
...	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号(¥)	本書では、コマンドの記述が 1 行に収まらない場合があります。このような場合、行末の空白とそれに続く円記号(¥)は、そのコマンドが次の行に続くことを示します。 **注**: このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。これらの文字は、実際のコマンド構文の一部ではありません。

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

ファイル ロケーションに関する規則

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

- *ACVEInstallDir* -- CA Access Control for Virtual Environments のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer/VirtualAppliance

- *ACInstallDir* -- CA Access Control のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControl
- *ACSharedDir* -- CA Access Control for UNIX で使用されるデフォルトのディレクトリ。
  - /opt/CA/SharedComponents
- *ACServerInstallDir* -- CA Access Control エンタープライズ管理 のデフォルトのインストール ディレクトリ。
  - /opt/CA/AccessControlServer
- *JBoss_HOME* -- デフォルトの JBoss インストール ディレクトリ。
  - /opt/jboss-4.2.3.GA

CA への連絡先

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

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

このガイドでは、VMware vCenter 環境で CA Access Control for Virtual Environments を計画、デプロイ、設定、および管理する方法について説明します。

このガイドは、組織の VMware ベースの仮想環境を管理および保護するシステム管理者、セキュリティ管理者、および VMware 管理者を対象としています。

ご使用の環境で CA Access Control for Virtual Environments をデプロイおよび設定する前に、このガイドに目を通してください。

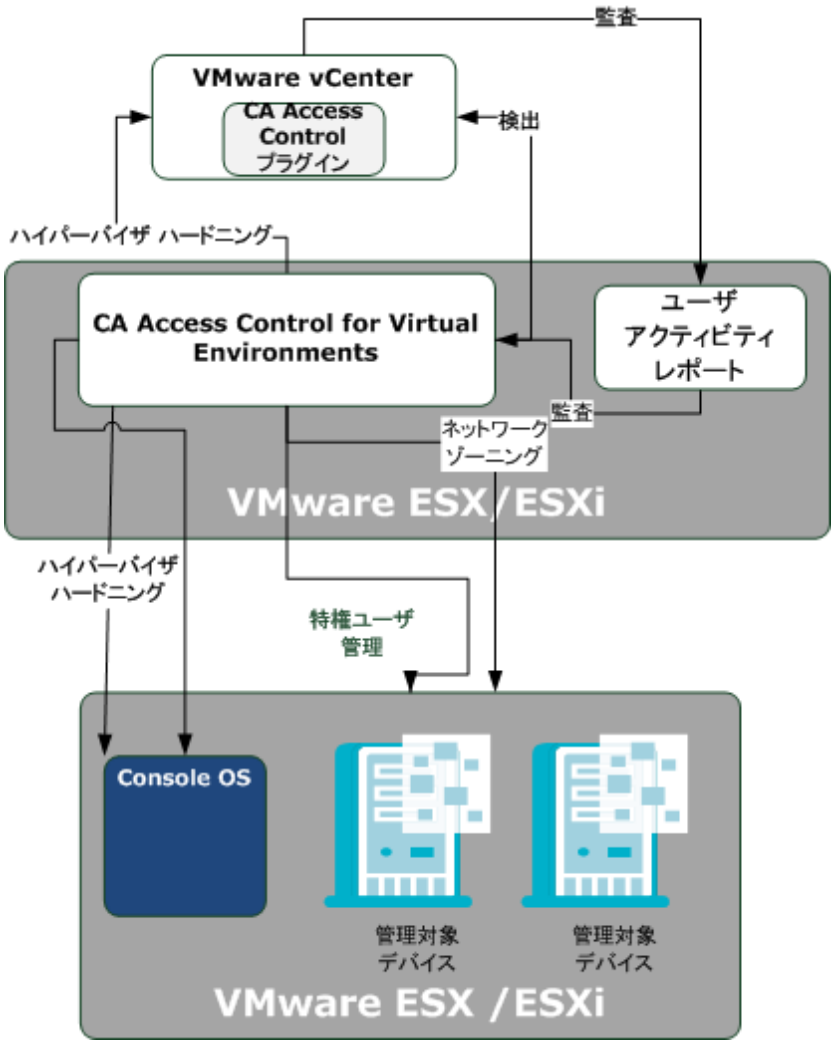
便宜上、このガイドの全体を通してこの製品を CA Access Control と表記します。

CA Access Control for Virtual Environments について

CA Access Control for Virtual Environments (CA VE)は、仮想環境への特権ユーザ アクセスを保護し、仮想環境の拡張に合わせて拡張可能なスタンド アロン ソリューションです。CA Access Control for Virtual Environments は VMware vCenter と統合され、管理対象デバイス、セキュリティ グループ、ネットワーク ゾーン、およびポリシーを制御できる管理インターフェースを提供します。CA Access Control for Virtual Environments では、タグ、タグ ルール、およびポリシーを使用することにより管理タスクの多くを自動化できるため、仮想環境の管理が容易になります。

CA Access Control for Virtual Environments 環境のアーキテクチャ

以下の図に、CA Access Control for Virtual Environments 環境のアーキテクチャを示します。

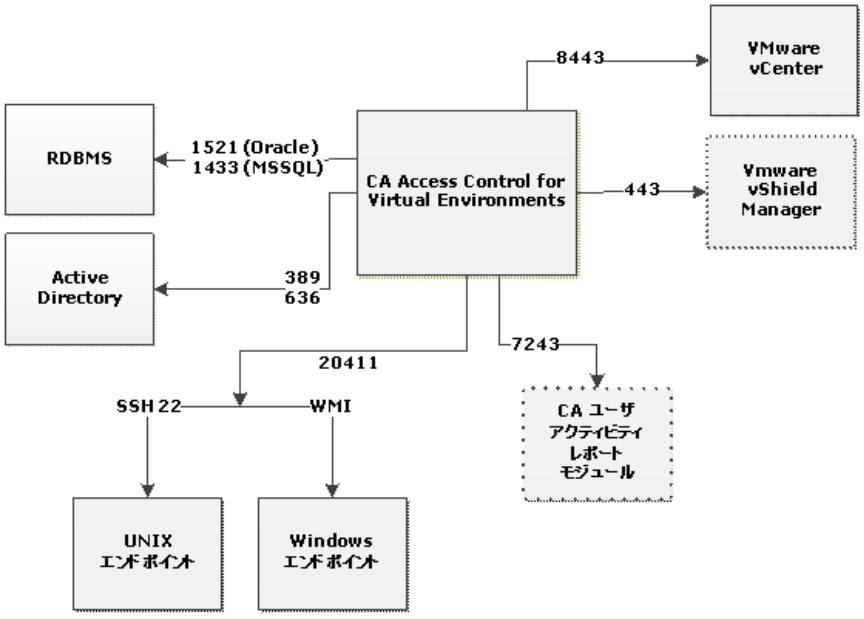


前の図に示したように、CA Access Control for Virtual Environments は以下の操作を実行します。

- 仮想環境内の管理対象デバイス上での特権ユーザ パスワード管理
- VMware ESX/ESXi サーバ上でのハイパーバイザーのハードニング
- ネットワーク ゾーニング
- 管理対象デバイスからの監査イベント コレクション（CA User Activity Reporting Module レポート生成用）

CA Access Control for Virtual Environments ネットワーク プロトコルおよびポート

以下の図に、CA Access Control for Virtual Environments によって使用されるネットワーク プロトコルおよびポートを示します。



注: 点線はオプション コンポーネントを表しています。

保護の対象

CA Access Control for Virtual Environments は、以下のエンティティを保護および拡張します。

- **ハイパーバイザー** - CA Access Control for Virtual Environments は複数のハードニング レベルをサポートしています。ハードニング ポリシーは、VMware vCenter サーバへのユーザ ログインを制限し、リモート監査コレクション、リモート管理、および SNMP トラップ コレクションを管理します。
- **管理対象デバイス** - CA Access Control for Virtual Environments では、パスワード ロックダウン ポリシーをデプロイして管理対象アカウント パスワードを管理することによって、管理対象デバイスを保護できます。また、管理対象デバイスをネットワーク ゾーンに割り当て、監査コレクション ポリシーを通して監査レコードを収集できます。

特権アカウント パスワードの管理

CA Access Control for Virtual Environments は、対象環境内の管理対象デバイスで特権アカウント パスワードを検出し、そのデータベースに格納します。CA Access Control for Virtual Environments は、特権アカウントおよびアプリケーション ID パスワードの保護されたストレージを提供し、ユーザが定義したポリシーに基づいて特権アカウントおよびパスワードへのアクセスを制御します。

ネットワーク トラフィックの分離

CA Access Control for Virtual Environments は、管理対象デバイスをセキュリティ グループに割り当てることによってネットワーク トラフィックを制御します。セキュリティ グループは管理対象デバイスの論理的なグループであり、そのメンバに対してセキュリティ制御が適用されます。セキュリティ グループの各メンバは、ネットワーク ゾーン内の他のメンバと通信できます。

CA Access Control for Virtual Environments は VMware vShield Manager と統合して、ネイティブ ファイアウォール機能を使用してネットワーク アクセス ルールを適用します。

仮想環境ツールおよびインターフェース拡張

CA Access Control for Virtual Environments は、ネイティブ VMware 仮想管理ツールを拡張します。CA Access Control for Virtual Environments は VMware vSphere クライアントと統合することによって特権パスワード管理機能を追加し、ネイティブ環境を拡張します。

また、CA Access Control for Virtual Environments は VMware vShield App と統合してネットワーク アクセス ルールを適用します。VMware vShield Manager は、アクセス制御ポリシーを実施する vNIC レベルのファイアウォールです。

アセット タグ付け

アセット タグ付けを使用すると、管理対象デバイスとセキュリティ グループに論理的なタグを割り当てることができます。タグが割り当てられると、管理対象デバイスはそのタグが適用されるセキュリティ グループのメンバになります。

管理対象デバイスに手動でタグを割り当てて、セキュリティ グループに追加できます。タグ ルールを定義し、ルール基準を設定すると、管理対象デバイスに割り当てたタグに基づいて管理対象デバイスをセキュリティ グループに関連付けることができます。

第 2 章: 実装の準備

このセクションには、以下のトピックが含まれています。

実装サイズの設定

CA Access Control for Virtual Environments を実装する前に、実装のサイズを決定して、それに応じてリソースを割り当てます。実装の見積もり評価のために、以下の情報を使用します。

以下の表に、CA Access Control for Virtual Environments 用にサポートされている設定を示します。

コンポーネント	制限
ホストあたりの仮想マシン	320
vCenter サーバあたりのホスト	3200
vCenter サーバあたりの登録仮想マシン	15000
データセンターあたりの仮想マシン	5000
vCenter サーバあたりの電源オン仮想マシン	10000

CA Access Control for Virtual Environments のコンポーネント

CA Access Control for Virtual Environments は、以下のソフトウェア コンポーネントから構成されます。

CA Access Control Server

CA Access Control Server は、CA Access Control for Virtual Environments デプロイメントの一部としてインストールされ、VMware ESX/ESXi Server に常駐します。CA Access Control Server は、以下を管理します。

- ネットワークトラフィック管理
- ネットワーク ゾーン管理
- 特権パスワード管理
- ハイパーバイザー ハードニング

CA Access Control エンタープライズ管理

CA Access Control エンタープライズ管理 はエンタープライズを管理するユーザ インターフェースです。製品の初期インストールを完了したら、まずユーザ インターフェースの操作に習熟しておいてください。

エンタープライズ管理でぇあ、以下の操作を実行できます。

- エンタープライズの全体にわたる CA Access Control for Virtual Environments 実装の表示
- ホストとホスト グループの設定、およびセキュリティ グループと PUPM エンドポイントへのポリシーの割り当て
- 特権アカウント パスワードのチェックアウトおよびチェックイン
- 特権アカウント、エンドポイント、パスワード ポリシーおよびパスワード コンシューマの設定
- レポートの表示、スナップショット定義の管理およびスナップショット データのキャプチャ
- ユーザ、グループ、ロールおよびタスクの管理
- システム全体の接続設定の管理
- タグおよびタグ ルールの管理
- 監査レコードの表示

注: CA Access Control エンタープライズ管理 でのタスクの完了の詳細については、*オンライン ヘルプ*を参照してください

CA Access Control プラグイン

CA Access Control プラグインは、仮想環境の管理を支援します。このプラグインは、VMware vCenter サーバに組み込まれます。このプラグインを使用すると、VMware vSphere クライアントから以下の操作を実行できます。

- PUPM エンドポイントおよび特権パスワードの検出
- 特権アカウント パスワードの管理
- 管理対象デバイスへのタグの割り当て
- CA User Activity Reporting Module レポートの表示

セントラル RDBMS

セントラル RDBMS には以下が格納されています。

- レポートで使用されるエンドポイント データ
- 特権アカウントのパスワード
- Web ベース アプリケーションのセッション データ
- Web ベース アプリケーションのユーザ データ(ユーザ ストアとして Active Directory を使用しない場合)

ユーザ ストア

Active Directory またはデータベース内に定義されているグループおよびユーザを使用するよう CA Access Control for Virtual Environments を設定できます。これにより、単一のデータ ストアをすべてのユーザに対して使用できます。

第 3 章: CA Access Control for Virtual Environments の実装

このセクションには、以下のトピックが含まれています。

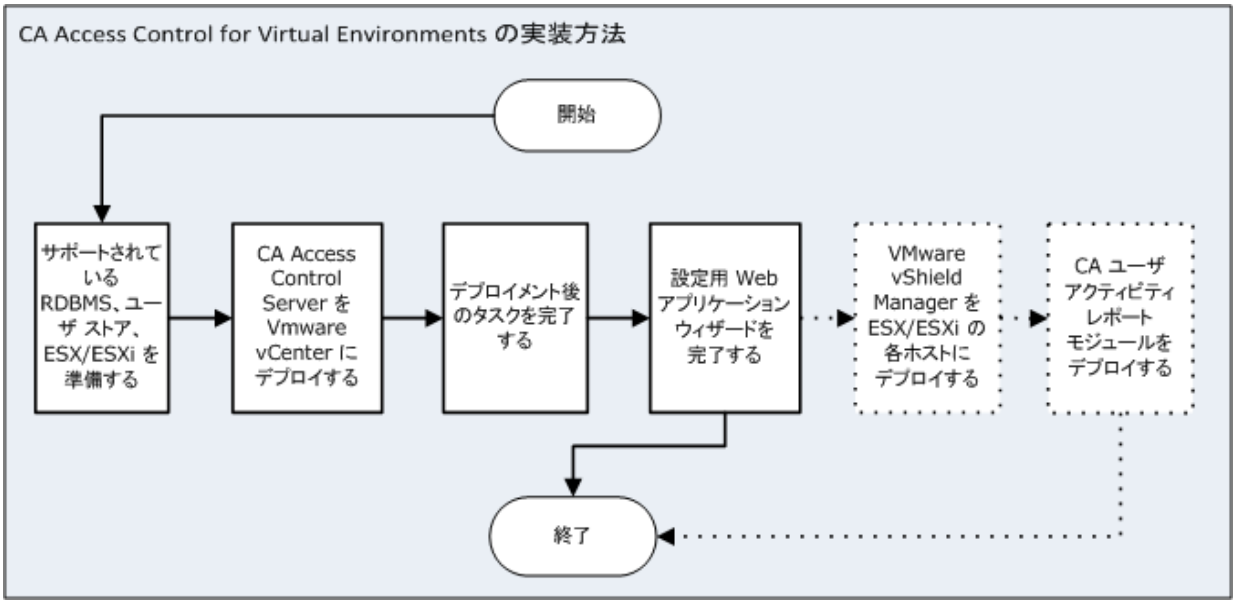
CA Access Control for Virtual Environments 仮想アプライアンスについて

CA Access Control for Virtual Environments は、仮想アプライアンスとして配布されます。*仮想アプライアンス*は、オペレーティング システムとアプリケーション パッケージがあらかじめインストールおよび設定されている仮想マシンです。

CA Access Control for Virtual Environments の実装方法

CA Access Control for Virtual Environments を使用すると、特権アカウントの管理、ネットワーク ゾーニングの設定、ハイパーバイザおよび監査コレクション ポリシーの作成、およびアセットへのタグ割り当てを実行できます。

以下の図に、CA Access Control for Virtual Environments を実装する方法を示します。



以下の点に注意してください。

- サポートされている RDBMS およびユーザ ストアの詳細については、「リリース ノート」を参照してください。
- 点線は、オプションの手順を示しています。

CA Access Control Server のデプロイ

CA Access Control for Virtual Environments 仮想アプライアンスをデプロイするには、オペレーティング システムおよび CA Access Control Server をインストールし、ESX/ESXi Server に仮想マシンを作成します。

以下の手順に従います。

1. VMware vSphere クライアントを開き、[ファイル]-[OVF テンプレートのデプロイ]に移動します。

   [OVF テンプレートのデプロイ]ウィザードが開きます。

2. [ファイルからデプロイ]ボタンをクリックし、次に[参照]をクリックして CA Access Control for Virtual Environments OVF テンプレートを検索します。

3. [次へ]]をクリックします。

   OVF テンプレートの詳細画面が表示されます。以下の手順を実行します。

   a. 詳細を参照し、[次へ]をクリックします。

      [エンド ユーザー使用許諾契約書]画面が表示されます。

   b. 使用許諾契約を確認し、[承諾]を選択して[次へ]をクリックします。

      [名前と場所]画面が表示されます。

   c. 仮想マシン名を指定し、仮想アプライアンスをデプロイするフォルダを選択します。[次へ]]をクリックします。

      [ホスト/クラスタ]画面が表示されます。

      注: この画面は、OVF テンプレートをデプロイする前にリソース プールを選択しなかった場合にのみ表示されます。

   d. 仮想アプライアンスをホストするためのデータ センターを選択します。[次へ]]をクリックします。

      [リソース プール]画面が表示されます。

   e. テンプレートのデプロイ先となるリソース プールを選択します。[次へ]]をクリックします。

      [データストア]画面が表示されます。

   f. 仮想アプライアンスを格納するデータ ストアを選択します。[次へ]をクリックします。

      ネットワーク マッピング画面が表示されます。

g. 使用するネットワークを選択します。[次へ]をクリックします。

注: OVF テンプレートが使用するネットワークを、ご使用の環境で定義されているネットワークにマップできます。

ネットワークのプロパティ画面が表示されます。

h. 以下のフィールドに値を入力します。

ドメイン名

ホスト名検索用の検索パスを指定します。複数の検索パスを指定できます。

ホスト名

仮想マシンの完全修飾名を指定します。

タイム ゾーン

CA Access Control サーバが属するタイム ゾーンを指定します。

デフォルト ゲートウェイ

デフォルト ゲートウェイ IP アドレスを指定します。DHCP を使用する場合は、このフィールドを空のままにします。

DNS

この仮想マシン用の DNS サーバを指定します。DHCP を使用する場合は、このフィールドを空のままにします。

ネットワーク IP アドレス

仮想マシン IP アドレスを指定します。DHCP を使用する場合は、このフィールドを空のままにします。

ネットワーク ネットマスク

選択したネットワーク カード用のネットマスクまたはプレフィックスを指定します。DHCP を使用する場合は、このフィールドを空のままにします。

i. [次へ]をクリックします。

j. デプロイ設定を確認し、[完了]をクリックします。

VMware vSphere クライアントはテンプレートをデプロイし、指定した場所に仮想マシンを追加します。このプロセスは、完了まで数分かかる場合があります。テンプレートが正常にデプロイされたことを示すメッセージが表示されます。

4. VMware vSphere クライアントから CA Access Control for Virtual Environments マシンの電源を入れます。

CA Access Control for Virtual Environments のインストール プロセスが開始されます。このプロセスは、完了するまで数分かかる場合があります。

5. [コンソール]タブに移動します

6. root および superadminuser ユーザ アカウントのパスワードを定義します。

以下の点に注意してください。

- リモート ルート ログインはデフォルトではブロックされます。root アカウントは、CA Access Control for Virtual Environments マシン コンソールへのログインのみに使用できます。
- superadminuser アカウントを使用すると、仮想マシンをリモートに管理できます。たとえば、SSH を使用できます。
- デフォルトでは、superadminuser には root アカウントと同じパスワードが割り当てられます。CA Access Control for Virtual Environments コンソールから passwd superadminuser コマンドを実行してデフォルトのパスワードを変更します。

7. (オプション) ネットワーク設定およびホスト名を定義します(自動検出されていない場合)。「N」と入力して設定を変更するか、「Y」と入力して設定を受け入れます。

8. 「Y」と入力してインストールを完了します。

CA Access Control for Virtual Environments のインストールが終了します。このプロセスは、完了まで数分かかる場合があります。

9. CA Access Control for Virtual Environments にログインするための root ユーザ アカウント パスワードを入力します。

CA Access Control for Virtual Environments が正常にデプロイされました。次に、デプロイメント後のタスクを完了する必要があります。

デプロイメント後のタスク

CA Access Control for Virtual Environments 仮想アプライアンスをデプロイしたら、以下の手順を実行してユーザ ストアおよびデータベース接続情報を設定します。

中央データベースを準備する方法

CA Access Control for Virtual Environments には、リレーショナル データベース システム(RDBMS)が必要です。CA Access Control for Virtual Environments を設定する前に、データベースを準備する必要があります。

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

   RDBMS をインストールする前に、以下のことに注意してください。

   - サポート対象の RDBMS ソフトウェアのリストについては、「リリース ノート」を参照してください。
   - CA Access Control for Virtual Environments 仮想マシンに中央データベースをインストールする必要はありません。RDBMS のシステム要件については、お使いの製品のマニュアルを参照してください。

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

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

   - SQL Server の場合は、以下の手順に従います。
     - 大文字小文字を区別しない、新しいデータベースを作成します。
     - 並び替えの順序を SQL_Latin1_General_CP1_CI_AS に設定します。
     - 新しいユーザを作成し、新しいデータベースをそのユーザのデフォルト データベースにして、そのユーザに DBCREATOR および SYSADMIN 権限を割り当てます。

- Oracle の場合は、以下の手順に従います。
  - 中央データベース用の新規ユーザを作成し、以下の権限を割り当てます。

    CONNECT（次のシステム権限を付与：ALTER SESSION、CREATE CLUSTER、CREATE DATABASE LINK、CREATE SEQUENCE、CREATE SESSION、CREATE SYNONYM、CREATE TABLE、CREATE VIEW）

    RESOURCE（次のシステム権限を付与：CREATE CLUSTER、CREATE INDEXTYPE、CREATE OPERATOR、CREATE PROCEDURE、CREATE SEQUENCE、CREATE TABLE、CREATE TRIGGER、CREATE TYPE）
  - 以下のクエリを使用して、CA Access Control for Virtual Environments データベースに対する追加のユーザ権限を付与します。

    管理者データベーストリガを *<DB_USER>* に付与します。
  - CA Access Control for Virtual Environments をホストするテーブルスペースに対して無制限の割り当てを設定します。

データベース接続情報の設定

CA Access Control for Virtual Environments には、リレーショナル データベース システム(RDBMS)が必要です。

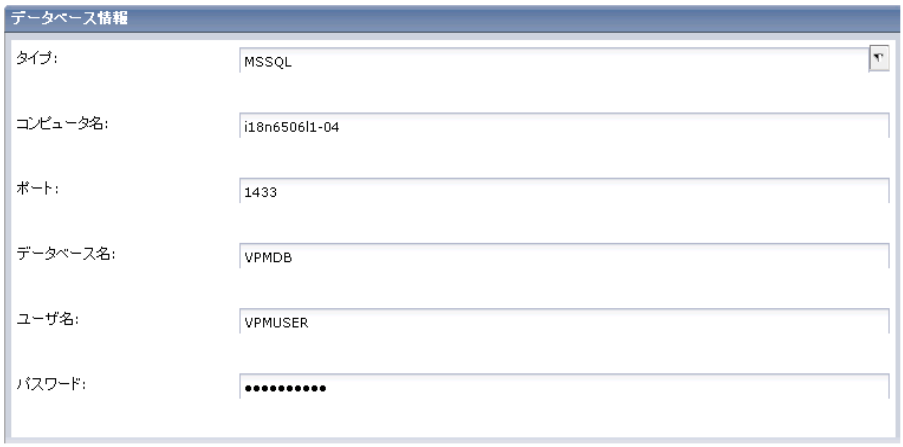
以下の手順に従います。

1. Web ブラウザを開き、お使いのホストに応じて以下の URL を入力します。

   `https://enterprise_host:18443/iam/ac`

   例: https://192.168.1.1:18443/iam/ac

   CA 仮想アプライアンス設定ウィザードが開き、データベース情報テーブルが表示されます。



2. 以下のフィールドに値を入力します。

   データベース タイプ -- サポートされている RDBMS を指定します。

   コンピュータ名 -- RDBMS がインストールされているホストの名前を指定します。

   ポート番号 -- 指定した RDBMS によって使用されるポートを定義します。

   - **Oracle** -- 1521
   - **SQL** -- 1433

   データベース名 -- 作成したデータベースの名前を定義します。

   ユーザ名 -- データベースに接続するために CA Access Control for Virtual Environments が使用するユーザ名を定義します。データベースを準備したとき作成したユーザ名を指定してください。

3. ［次へ］をクリックします。

   サーバ名の設定画面が表示されます。

4. エンタープライズ管理サーバの完全修飾ドメイン名を入力します。

5. ［次へ］をクリックします。

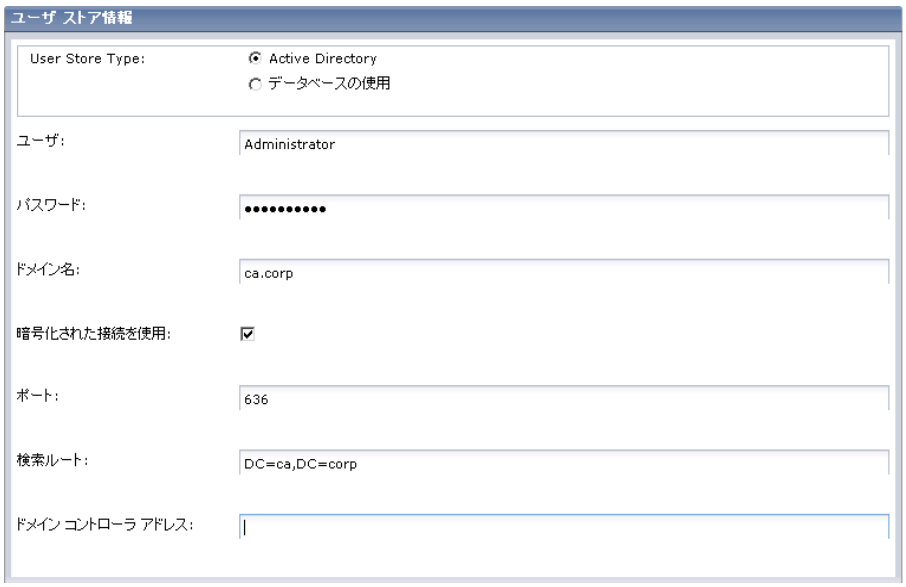
   インストール プログラムは、続行する前にデータベースへの接続を確認します。次にユーザ ストア接続情報を設定します。

ユーザ ストア接続情報の設定

CA Access Control for Virtual Environments は、ユーザ ストアとして Active Directory および指定済みのデータベースをサポートしています。

以下の手順に従います。

1. ［CA 仮想アプライアンス設定］画面から、ユーザ ストア タイプを選択します。



以下の*いずれか*を選択します。

Active Directory - 接続情報の詳細を指定します。

データベース - ユーザ情報を RDBMS に格納します。

2. (Active Directory) 以下のフィールドに入力します。

ユーザ

CA Access Control for Virtual Environments を管理するために使用する Active Directory ユーザ アカウント名を定義します。

注: このパラメータには、読み取り専用権限を持ったユーザを定義できます。

パスワード

CA Access Control for Virtual Environments を管理するために使用する Active Directory ユーザ アカウントのパスワードを定義します。

ドメイン名

Active Directory DNS ドメイン名を定義します。

暗号化された接続を使用

Active Directory との暗号化された接続を使用することを指定します。

ポート

Active Directory に対する LDAP クエリにデフォルトで使用されるポートを定義します (例: 636)。

検索ルート

検索ルート定義します (例: ou=DomainName, DC=com)。

注: 検索ルートは、ディレクトリ ツリー内でユーザが定義されているコンテナより少なくとも 1 ノード上位に設定します。そのようにしない場合、CA Access Control for Virtual Environments は起動時にタブを表示しない場合があります。

ドメイン コントローラ アドレス

ドメイン コントローラの IP アドレスを定義します。

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

3. (データベース) データベースを準備したときに作成した RDBMS パスワードを定義します。
4. [次へ]をクリックします。

   システム ユーザ画面が表示されます。
5. 以下のフィールドに値を入力します。

   システム ユーザ

   (Active Directory のみ) CA Access Control for Virtual Environments で System Manager 管理ロールが割り当てられている Active Directory ユーザの DN を定義します。

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

   パスワード

   (データベースのみ) CA Access Control for Virtual Environments の管理者である *superadmin* のパスワードを定義します。インストール完了時に CA Access Control for Virtual Environments にログインできるように、パスワードをメモしておきます。

   注: この手順では、データベースに superadmin ユーザを作成します。superadmin ユーザには、CA Access Control エンタープライズ管理 のシステム マネージャ管理ロールが割り当てられます。CA Access Control for Virtual Environments への初回ログイン時には、superadmin としてログインします。システム マネージャ管理ロールの詳細については、「*エンタープライズ管理ガイド*」をご覧ください。
6. [次へ]をクリックします。

   データベースおよびユーザ ストア接続情報の定義が完了しました。次に、VMware vCenter への接続を設定します。

VMware vCenter サーバへの接続の設定

VMware vCenter への接続を設定して、CA Access Control のセキュリティ機能を VMware vCenter サーバの管理対象デバイスに統合します。

以下の手順に従います。

1. [CA 仮想アプライアンス設定]ウィザードから、[vCenter 接続設定]に進みます。

   以下の画面が表示されます。

   ダイアログ ボックスで以下のフィールドに値を入力します。

   名前

   VMware vCenter 接続に使用する名前を定義します。

   説明

   (オプション)この VMware vCenter 接続に関する説明を定義します。

   サーバ名

   管理する VMware vCenter サーバの DNS 名を定義します。

   例: vcenter.company.com

   ユーザ名

   VMware vCenter サーバの管理者権限を持つユーザ アカウントの名前を定義します。

   パスワード

   VMware vCenter サーバの管理者権限を持つユーザ アカウントのパスワードを定義します。

2. ［次へ］をクリックします。

   CA Access Control for Virtual Environments は設定を検証し、共有秘密画面に進みます。

3. 以下のフィールドに値を入力します。

   通信パスワード

   CA Access Control エンタープライズ管理サーバ コンポーネント間通信に使用されるパスワードを定義します。［次へ］をクリックします。

   サーバ名設定画面が表示されます。

4. エンタープライズ管理サーバの完全修飾ドメイン名を定義します。［次へ］をクリックします。

   サマリ画面が開きます。

5. 情報を確認し、［完了］をクリックしてウィザードを終了します。

   CA Access Control for Virtual Environments はデータベースおよびユーザ ストアを設定して使用可能な状態にします。

   CA Access Control for Virtual Environments は、VMware vCenter サーバへの接続試行時に指定した情報を使用します。情報が正しい場合は、接続が設定されます。これで、VMware vSphere クライアントを使用して CA Access Control for Virtual Environments のエンタープライズ デプロイメントを管理できるようになりました。情報が正しくない場合、CA Access Control for Virtual Environments は VMware vCenter に接続できず、エラー メッセージが表示されます。このメッセージでは、接続が確立できなかった理由が示されます。

SSL 通信用に CA Access Control for Virtual Environments を設定する方法

デフォルトでは、インストールされた CA Access Control for Virtual Environments は自己署名証明書を使用する SSL をサポートします。別の証明書を使用する SSL サポートを設定するには、Active Directory を使用するときに CA Access Control for Virtual Environments が SSL を使用するように設定します。

以下の手順に従います。

1. DER、CRT または CERT 形式のユーザ ディレクトリ証明書を取得します。
2. 証明書をキーストアに追加します。

詳細情報:

キーストアへのユーザ ディレクトリ証明書の追加 (P. 32)

キーストアへのユーザ ディレクトリ証明書の追加

SSL 通信を使用するよう CA Access Control for Virtual Environments を設定する前に、ユーザ ディレクトリ証明書をキーストアに追加する必要があります。

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

例: キーストアへの Active Directory 証明書の追加

重要: この例では、Active Directory と安全な通信を行うために SSL を使用するよう CA Access Control for Virtual Environments を設定する方法を示します。この手順を開始する前に、DER、CER または CERT にエンコードされたバイナリ形式の Active Directory 証明書を取得する必要があります。

1. CA Access Control Server で、JBoss を停止します(実行されている場合)。以下の手順を実行します。
   - JBoss ジョブ ウィンドウから、プロセスを中断します(Ctrl+C)。

2. 以下のディレクトリに移動します。ここで *JBOSS_HOME* は、JBoss をインストールしたディレクトリです。

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

3. 以下のコマンドを入力します。

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

   パスワードの入力を促すメッセージが表示されます。

   -import

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

   -alias

   キーストアへのエントリの追加で使用するエイリアスを指定します。

   -file

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

4. 「*secret*」というパスワードを入力します。

5. JBoss bin ディレクトリへ移動します。デフォルトでは、このディレクトリは以下にあります。

   JbossInstallDir/bin

6. run.bat ファイルを開いて、trusted ユーザ ストア データで java_ops パラメータを設定します。例:

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

7. ファイルを保存して、JBoss を起動します。

   ユーザ ストア証明書がキーストアに追加されました。

第 4 章: CA Access Control for Virtual Environments 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。

CA Access Control for Virtual Environments を開く

CA Access Control Server をインストールして起動したら、CA Access Control for Virtual Environments 用の URL を使用して Web ベース インターフェースをリモート コンピュータから起動できます。

次の手順に従ってください:

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

   `https://enterprise_host:18443/iam/ac`

2. ログインする CA Access Control Server をインストールしたときに指定したクレデンシャルを使用します。

   CA Access Control for Virtual Environments のホームページが表示されます。

例: CA Access Control for Virtual Environments を開く

ネットワーク上の任意のコンピュータから CA Access Control for Virtual Environments を開くには、Web ブラウザに次の URL を入力します。

```
https://appserver123:18443/iam/ac
```

この URL から、CA Access Control for Virtual Environments が appserver123 という名前のホストにインストールされ、デフォルトの CA Access Control for Virtual Environments ポート 18443 を使用しているのがわかります。

ワールド ビュー

CA Access Control for Virtual Environments のワールド ビューでは、管理している CA Access Control for Virtual Environments のエンタープライズ実装を表示することができます。

ワールド ビューを使用して、以下を実行できます。

- CA Access Control for Virtual Environments が管理する、管理対象デバイスおよびセキュリティ グループを識別します。
- VMware vCenter 階層をナビゲートします。
- 管理対象デバイスおよびセキュリティ グループの詳細を表示します。詳細情報には、デプロイされているポリシー、グループと管理対象デバイスの合計、および各デバイスのコンプライアンス ステータスが含まれます。
- 管理対象デバイスおよびセキュリティ グループを管理します。
- セキュリティ グループの管理として、ポリシー、メンバ、タグ、タグ ルールの割り当ておよび削除を行います。

エンタープライズ実装の管理

CA Access Control エンタープライズ管理 を使用して、CA Access Control for Virtual Environments のエンタープライズ実装を表示および管理することができます。エンタープライズの「ワールド ビュー」は、ユーザの PUPM エンドポイントおよび管理対象デバイスと、関連する論理セキュリティ グループ、デプロイされたポリシー、およびポリシー タブのスナップ ショットです。

エンタープライズのデプロイメント スナップショットは、VMware vCenter サーバで設定した管理対象デバイスおよびグループの階層に基づきます。VMware vCenter で階層に加えた変更は、すべてワールド ビューでも表示されます。

以下の手順に従います。

1. [ワールド ビュー]タブ - [セキュリティ グループ] - [セキュリティ グループ管理]に移動します。

   [セキュリティ グループ管理]ページが表示され、CA Access Control サーバによって定義された、VMware vCenter サーバ上のセキュリティ グループおよび論理グループが表示されます。

   注: 設定、修正、または変更できるのは CA Access Control for Virtual Environments の管理対象デバイスの階層のみです。

2. (オプション) CA Access Control サーバ内に追加の管理対象デバイス、セキュリティ グループ、タグおよびタグ ルールを定義できます。[アクション]メニューから以下を選択します。

   - セキュリティ グループの作成 (P. 38)
   - タグの作成 (P. 51)
   - タグ ルールの作成 (P. 52)
   - ポリシー ステータスの表示

3. [セキュリティ グループ]セクションで、セキュリティ グループを選択します。

   CA Access Control エンタープライズ管理 に、セキュリティ グループの詳細、割り当てられたポリシー、グループ メンバ、および各メンバのコンプライアンス ステータスが表示されます。

4. セキュリティ グループ ポリシーを管理するために[ポリシーの追加]を選択します。

   利用可能なポリシーを以下に示します。

   - ネットワーク ゾーン (P. 46) -- ネットワークの分離ポリシーを設定します。
   - 監査コレクション (P. 59) --CA User Activity Reporting Module の監査コレクションポリシーを設定します。
   - ハイパーバイザー ハードニング (P. 56) -- ハイパーバイザー ハードニング ポリシーを設定します。
   - パスワード ロックダウン (P. 43) -- 特権アカウントのパスワード ロックダウン ポリシーを設定します。

5. (オプション)既存のポリシーを変更する場合は[設定]を、ポリシーを削除する場合は[削除]を選択します。

セキュリティ グループの作成

ユーザ環境内のセキュリティ グループを管理して、メンバの追加や削除、タグの割り当てや削除を行います。

以下の手順に従います。

1. [ワールド ビュー]タブ - [セキュリティ グループ] - [セキュリティ グループ管理]に移動します。

   [セキュリティ グループ管理]ページが表示され、VMware vCenter サーバ上のセキュリティ グループと CA Access Control サーバの詳細が表示されます。

2. [作成]または[変更]を選択してセキュリティ グループ設定にアクセスします。

   [全般]タブが開きます。

3. 以下のフィールドに値を入力します。

   名前

   セキュリティ グループ名を示します。

   説明

   セキュリティ グループの説明を指定します。

   所有者

   セキュリティ グループの所有者の名前を指定します。

   組織単位

   セキュリティ グループの組織単位を指定します。

4. 管理対象デバイス選択タブを選択します。

   [ホスト選択]タブが開きます。

5. [追加]をクリックして、管理対象デバイスをグループに追加します。

6. [セキュリティ グループ メンバ]タブを選択します。

   [グループ]タブが開き、グループのメンバであるセキュリティ グループが表示されます。

7. [追加]をクリックして、セキュリティ グループをグループのメンバとして追加します。

8. [タグ]タブを選択します。

   [タグ]タブが開き、割り当てられているタグが表示されます。

9. [追加]をクリックして、コンピュータのグループにタグを割り当てます。

10. [タグ別メンバシップ]タブを選択します。

    [タグ別メンバシップ]タブが開きます。

11. [追加]をクリックして、タグをメンバシップ条件に追加します。[追加]をクリックして、タグを条件リストに追加します。

    メンバシップ条件がリストに追加されます。

    注: 1 つのメンバシップ条件にはタグを 3 つまで追加できます。

12. [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、セキュリティ グループに対して変更をコミットします。

タグ メンバシップ条件について

管理対象デバイスの管理を自動化し、容易にするためにタグ メンバシップ条件を使用できます。タグ メンバシップ条件を使用して、セキュリティ グループを定義し、そのメンバが準拠する条件ルールを定義できます。CA Access Control for Virtual Environments は、条件ルールが適用される各管理対象デバイスをセキュリティ グループに自動的に追加します。

タグ メンバシップ条件には、以下の構文を使用します。

```
[タグ 1] AND | OR [タグ 2] AND | OR [タグ 3]
```

例:タグ メンバシップ条件の作成

以下の例では、Development 、Accounting、Marketing のいずれかのタグを割り当てられている管理対象デバイスを割り当てるためのタグ メンバシップ条件を設定します: 。

```
Development OR Accounting OR Marketing
```

以下の例では、Accounts および Marketing タグのみを割り当てられている管理対象デバイスを自動的に割り当てるためのタグ メンバシップ条件を設定します。

```
Accounts AND Marketing
```

管理対象デバイスのステータスの表示

ステータス ビューでは、管理対象デバイスに関するエラー メッセージや警告メッセージを確認できます。アラートには、セキュリティ グループに割り当てた、デプロイされたポリシーに関する情報が表示されます。

以下の手順に従います。

1. ワールド ビュー、ビュー、ステータスを選択します。

   ステータス ウィンドウが開き、最新のアラートが表示されます。

2. すべてのメッセージ、またはエラーと警告メッセージのみのいずれかを選択して表示します。
3. [更新]をクリックすると、アラートのリストが更新されます。

特権アカウント パスワードの管理

特権アカウント パスワードのロックダウン ポリシーにより、統一されたポリシーを設定し、セキュリティ グループ内のすべての特権アカウントに割り当てることができます。

CA Access Control for Virtual Environments によるエンドポイントおよびアカウント作成の仕組み

CA Access Control for Virtual Environments は PUPM エンドポイントを自動的に作成し、特権アカウントを検出し、アカウント パスワードにパスワード ポリシーを割り当てます。

以下のプロセスでは、CA Access Control for Virtual Environments が PUPM エンドポイントおよびアカウントを設定する仕組みについて説明します。

1. 仮想化管理者は、セキュリティ グループへ PUPM エンドポイントを追加します。
2. 管理者は CA Access Control エンタープライズ管理 で、セキュリティ グループ内の各エンドポイント タイプに対して、管理者特権のある、接続解除された特権アカウントを作成します。

   CA Access Control for Virtual Environments は、接続解除されたアカウントを使用して各エンドポイントに接続し、特権アカウント パスワードを検出します。

3. CA Access Control エンタープライズ管理 で、管理者はパスワード ロックダウン ポリシーを設定し、セキュリティ グループに割り当てます。
4. CA Access Control for Virtual Environments はエンドポイントを検出し、エンドポイントの接続設定を自動的に設定し、そのエンドポイント上に特権アカウントを設定するよう試行します。
5. 成功した場合、CA Access Control for Virtual Environments は、そのエンドポイント タイプの特権アカウントを使用するためにエンドポイント特権アクセス ロールを作成します。

   たとえば、Windows エージェントレス エンドポイント上で初めて特権アカウントを検出した場合、CA Access Control for Virtual Environments 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。
6. CA Access Control for Virtual Environments は、セキュリティ グループに属する各メンバの特権アカウントに、特権アカウント パスワード ポリシーを自動的に割り当てます。

アカウント パスワード ロックダウン ポリシーの設定

アカウント パスワード ロックダウン ポリシーは、CA Access Control for Virtual Environments が管理する各セキュリティ グループに対して設定します。グループに追加する各管理対象デバイスには、CA Access Control for Virtual Environments により、特権パスワード ロックダウン ポリシーが適用されます。

重要: この手順を完了する前に、CA Access Control for Virtual Environments で作成し、管理する各エンドポイント タイプに対して管理特権を持つ、特権アカウントを作成します。

以下の手順に従います。

1. [ワールド ビュー] - [セキュリティ グループ] - [セキュリティ グループ管理] に移動します。

   [セキュリティ グループ管理]ページが表示され、VMware vCenter サーバ上のセキュリティ グループと CA Access Control サーバの詳細が表示されます。

2. セキュリティ グループを選択します。

   CA Access Control エンタープライズ管理 にセキュリティ グループ詳細とメンバが表示されます。

3. [アクション]メニューから[アカウント パスワード ロックダウン ポリシーの追加]を選択します。

   <ホスト名> のパスワード管理ロックダウン ウィンドウが表示されます。

4. ドロップダウン メニューからオペレーティング システム プロファイルを選択します。オプション

   - Windows マシン プロファイル
   - Linux マシン プロファイル
   - Solaris マシン プロファイル

   各オペレーティング システム プロファイルに対して固有のパスワード ロックダウン ポリシーを設定できます。

5. 以下のフィールドに値を入力します。

説明

パスワード ロックダウン ポリシーの説明を指定します。

オペレーティング システム プロファイル

事前に選択したオペレーティング システム プロファイルが表示されます。

接続アカウント

各管理対象デバイスに接続するために CA Access Control for Virtual Environments が使用する管理者ユーザ アカウントを定義します。[アカウントの作成]を選択して、管理者アカウントを作成します。

接続アカウント

アカウントが接続済みアカウントであることを指定します。

管理対象アカウント

各管理対象デバイス上に CA Access Control for Virtual Environments が作成する特権アカウントを定義します。

パスワード ポリシー

特権またはサービス アカウントに適用するパスワード ポリシーを指定します。[パスワード ポリシーの作成]を選択して、パスワード ポリシーを作成します。

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。

注: このオプションはサービス アカウントに適用されません。

ログイン アプリケーション

このエンドポイントに割り当てるログイン アプリケーションを指定します。

注: ログイン アプリケーションをエンドポイントに割り当てる前に、まず、ログイン アプリケーションを作成します。複数のログイン アプリケーションを同じエンドポイントに割り当てることができます。

6. [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、特権アカウント パスワード ロックダウン ポリシーをグループに対してサブミットします。

ネットワーク分離

ネットワーク分離は、セキュリティまたは仮想化管理者がホストやタグの物理的な場所などの共通の条件に基づいて、ネットワーク ゾーン内で管理対象デバイスのグループを定義するプロセスです。

ネットワーク ゾーン内のメンバは同じゾーン内の他のメンバとのみ通信でき、ネットワーク上の他のネットワーク ゾーンやホストにアクセスすることはできません。ネットワーク サービスをセキュリティ グループに割り当てると、メンバはネットワークにアクセスできるようになります。

CA Access Control エンタープライズ管理 でのネットワーク ゾーン ポリシーの設定

ユーザが定義するネットワーク分離ルールにより、ネットワーク ゾーンが指定され、セキュリティ グループに適用されます。適用されると、メンバはゾーン内での通信のみ可能になります。セキュリティ グループを定義してメンバを割り当てるか、または、自動的に作成されたセキュリティ グループを使用できます。

注: ネットワーク ゾーン ポリシーを設定する前に、使用するネットワーク サービスを定義します。

以下の手順に従います。

1. [ワールド ビュー] - [セキュリティ グループ] - [セキュリティ グループ管理]に移動します。

   [セキュリティ グループ管理]ページが表示され、VMware vCenter サーバ上のセキュリティ グループと CA Access Control サーバの詳細が表示されます。

2. セキュリティ グループを選択します。

   CA Access Control エンタープライズ管理 にセキュリティ グループ詳細とメンバが表示されます。

3. [アクション]メニューから、[ネットワーク ゾーン ポリシーの追加]を選択します。

   [ネットワーク ルールの管理]ウィンドウが開きます。

4. 以下を入力します。

   説明

   ネットワーク ゾーン ポリシーの説明を指定します。

   サービス

   ネットワーク ゾーン ポリシーに割り当てるネットワーク サービスを定義します。割り当てるネットワーク サービスを検索するには、[追加]をクリックします。

   方向

   ネットワーク サービスで使用を許可するネットワークトラフィックの方向を定義します。

   オプション: インバウンド、アウトバウンド、双方向

5. [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、ネットワーク分離ルールをサブミットします。タスクが正常に完了したことを通知する確認メッセージが表示されます。

ネットワーク ゾーン ポリシーがセキュリティ グループに正常に適用されました。

ネットワーク サービスの設定

ネットワーク ゾーンのメンバがネットワーク ゾーン外のサービスおよびリソースにアクセスできるように、セキュリティ グループのネットワーク サービスを設定します。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
   a. [システム]をクリックします。
   b. [ネットワーク サービス]をクリックします。
   c. ネットワーク サービスの設定を選択します。

   [ネットワーク サービスの設定:ネットワーク検索の設定]画面が表示されます。
2. (オプション)既存のネットワーク サービスを選択してコピーを作成します。以下の手順に従います。
   a. ネットワーク サービス オブジェクト タイプ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ネットワーク サービスのリストが表示されます。
   c. 新規ネットワーク サービス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。

   ［ネットワーク サービスの作成］タスク ページが表示されます。既存のオブジェクトからネットワーク サービスを作成した場合、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。

4. 以下のフィールドに値を入力します。以下のフィールドには、説明が必要です。

   ネットワーク アドレス

   ネットワーク サービスを提供するサーバのホスト名または IP アドレスを定義します。

   サービス

   以下のネットワーク サービス プロパティを定義します。

   - プロトコル — UDP、TCP
   - ポート番号
   - サービス

5. ［追加］をクリックします。

   CA Access Control エンタープライズ管理 によってネットワーク サービスが追加されます。

   注: 各セキュリティ グループに複数のネットワーク サービスを定義できます。

6. ［サブミット］をクリックします。

   CA Access Control エンタープライズ管理 はタスクをサブミットし、ネットワーク サービスをセキュリティ グループに割り当てます。

アセット タグ付け

アセット タグ付けは、システム、セキュリティまたは仮想化環境管理者が管理対象デバイスおよびセキュリティ グループにタグを関連付けるプロセスです。タグの割り当てることにより、管理者は個々のアセットをグループとして管理し、ポリシー配布の自動化や管理スコープの定義を行うことができます。

管理を自動化するには、セキュリティ グループに追加したタグを、各管理対象デバイスが継承する必要があります。IP アドレスの範囲などのアセット属性に基づいて、タグ付けルールを定義できます。タグ付けポリシーも定義できます。タグ付けポリシーは、グループ内のすべてのメンバに CA Access Control for Virtual Environments が自動的に配布します。

セキュリティ グループを管理するためのタグの使用方法

タグおよびタグ ルールを使用することにより、セキュリティ グループ管理を簡単に行うことができるようになります。定義したタグとタグ ルールに基づいて、CA Access Control エンタープライズ管理 は、管理対象デバイスをセキュリティ グループに自動的に追加し、管理対象デバイスにポリシーを適用できます。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 にタグを作成します。
2. 以下のいずれかを実行します。
   - 管理対象デバイスにタグを手動で割り当てます。

     管理対象デバイスがセキュリティ グループに追加されます。セキュリティ グループに割り当てられたポリシーが、管理対象デバイスに適用されます。
   - タグ ルールの作成
3. タグ ルールを定義し、作成したルールにタグを関連付けて、ルール条件を定義します。
4. CA Access Control エンタープライズ管理 は以下を実行します。
   a. タグが関連付けられているセキュリティ グループにルールを適用する
   b. タグ ルールに従う各管理対象デバイスにタグを割り当てる
   c. タグ ルールに従う管理対象デバイスをセキュリティ グループに追加する
   d. 管理対象デバイスに対して設定したポリシーを管理対象デバイスに適用する

   管理対象デバイスをセキュリティ グループから管理できるようになりました。

   注: タグ ルールを削除すると、CA Access Control エンタープライズ管理 は管理対象デバイスをセキュリティ グループから削除します。

CA Access Control エンタープライズ管理 でのタグの設定

CA Access Control エンタープライズ管理 は、フォルダ、データセンター、リソース プールなどの管理対象デバイスをホスト グループにマッピングします。セキュリティ グループへのタグの割り当てにより、仮想化された環境でのアセットの管理が単純化されます。割り当てたタグに基づいて、管理スコープの定義を容易に行うことができます。

以下の手順に従います。

1. [ワールド ビュー] - [タグ] - [タグの作成]に移動します。

   [タグの作成:タグ検索]ウィンドウが表示されます。

2. (オプション)既存のタグを選択して、タグをそのコピーとして、以下のように作成します。

   a. タグ タイプの新規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タグのリストが表示されます。

   c. 新規タグ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。

   [タグの作成]ウィンドウが表示されます。

4. タグの名前を入力します。

5. [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 によりタグが作成されます。管理対象デバイスへのタグの割り当てや、タグ ルールを作成できるようになりました。

CA Access Control エンタープライズ管理 でのタグ ルールの作成

ユーザ定義のプロパティに基づいて管理対象デバイスをセキュリティ グループへ割り当てるタグ ルールを作成します。CA Access Control for Virtual Environments では、IP アドレスがタグ ルールと一致する管理対象デバイスが検出されると、そのデバイスにはタグが付けられ、セキュリティ グループと関連付けられます。

以下の手順に従います。

1. [ワールド ビュー] - [タグ] - [タグ ルールの作成]に移動します。

   [タグ ルールの作成:タグ ルール検索]ウィンドウが表示されます。

2. (オプション)既存のタグ ルールを選択して、タグをそのコピーとして、以下のように作成します。

   a. タグ ルール タイプの新規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タグ ルールのリストが表示されます。

   c. 新規タグ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。

   [タグ ルールの作成]ウィンドウが表示されます。

4. 以下のフィールドに値を入力します。

   名前

   タグ ルールの名前を指定します。

   説明

   タグ ルールの説明を指定します。

   適用されるタグ

   タグ付けルールに関連付けるタグを選択します。

   マッチするオブジェクト タイプ

   タグ ルールが適用されるオブジェクト タイプを表示します。

   条件

   以下に従って、タグ ルール条件を指定します。

   名前|*IP アドレス*|*ホスト* [equal|not equal] *管理対象デバイス*

   名前

   管理対象デバイスの DNS 名を指定します。

   IP

   管理対象デバイスの IP アドレスを指定します。

   OS 情報

   VMware vCenter に定義されている、管理対象デバイスのオペレーティング システムを指定します。

   VMネットワーク

   管理対象デバイスが使用する仮想ネットワークの名前を指定します。

   注釈

   VMware vCenter に定義されている、注釈キーを指定します。

   例:「所有者=John」

   注: 複数の管理対象デバイスにタグ ルールを適用する場合は、ワイルドカード(*)を使用します。

5. [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 によってタグ ルールが作成され、管理対象デバイスに適用されます。

VMware vSphere クライアントでの管理対象デバイスへのタグの割り当て

CA Access Control for Virtual Environments が管理する各管理対象デバイスに対して VMware vSphere クライアント からタグを割り当てることができます。

以下の手順に従います。

1. 左ペインから管理対象デバイスを選択し、次に[CA Security]タブを選択します。

   [CA Security]タブが開き、サマリ タブのコンテンツが表示されます。

2. [タグの追加]ボタンをクリックします。
3. ドロップダウン メニューからタグを選択し、[OK]をクリックします。

   タグが管理対象デバイスに割り当てられます。

ハイパーバイザー ハードニング

VMware ハイパーバイザ、vSphere Client コンソール、および管理対象デバイスは、悪意のある攻撃や、ユーザによる意図しないダメージによって影響を受ける可能性があります。ハイパーバイザや vSphere Client コンソールを強化すると、ユーザの VMware 環境は保護され、攻撃を受けにくくなります。

CA Access Control for Virtual Environments は、システム、セキュリティ、または VMware 管理者によるポリシーの設定に役立ちます。ポリシーを使用すると、ハイパーバイザおよび VMware vSphere クライアント コンソールは CA Access Control エンタープライズ管理 によって強化され、ポリシーはホスト グループにデプロイされます。

注: VMware ハイパーバイザおよび vSphere Client コンソールの強化の詳細については、VMware の Web サイト上にある「*VMware vSphere Hardening Guide*」を参照してください。

ハイパーバイザーのハードニング ポリシー

適用するハードニングのレベルを決定する前に、サポートされている以下のハードニング ポリシーを参照してください。

- **リモート アクセス** -- (ESXi のみ)リモート アクセスを制限します。ロックダウン モードを有効化して、ESXi サーバへのすべてのリモート アクセスを無効化します。有効にすると、ロックダウン モードにより、管理者が 1 つの場所からタスクを実行することしかできなくなり、監査されていないタスクが実行されるリスクが軽減されます。
- **リモート Syslog** -- イベントを 1 つの場所に記録することにより、管理性が向上し、1 箇所からすべてのデバイスを監視できます。さらに、1 つの場所にイベントを格納すると、ログの改ざん防止に役立ちます。
- **永続ロギング** -- 永続的なログ記録をデータベースに設定すると、サーバのログが長期にわたって保持されます。永続的なログ記録により、イベントの監視やサーバの問題の診断が容易になります。
- **NTP 時間同期** -- 時間設定が不正確だと、攻撃の特定や追跡ができなくなる場合があります。NTP 時間同期を設定すると、すべてのシステムが同じ時間ソースを使用するため、攻撃の追跡や関連付けに役立ちます。
- **SNMP 設定** -- (ESXi のみ) SNMP エージェントが正しく設定されていないと、攻撃者は悪意のあるホストにトラップをリダイレクトし、不正な目的で情報を利用する場合があります。
- **ダイレクト コンソール ユーザ インターフェース**(ESXi のみ) --ダイレクト コンソール ユーザ インターフェース(DCUI)は、管理者によるホストの設定およびタスクの保守を可能にする ESXi の管理コンソールです。ローカル管理者権限を持つユーザは、DCUI で直接アクションを実行できます。このアクションは、VMware vCenter サーバによって監査されません。ESXi サーバ上で管理タスクを直接実行できないようにするには、DCUI を無効にします。
- **テクニカル サポート モード**(ESXi のみ) -- テクニカル サポート モードは、サーバ コンソールまたは SSH コンソールで利用可能な対話型コマンド ラインです。有効化されている場合、トラブルシューティングやサポート関連タスクを ESXi サーバ上で直接実行できます。サーバへの不正なアクセスを禁止する場合は、テクニカル サポート モードを無効にします。
- **VMSafe ネットワーク API** -- VMSafe ネットワーク API は、仮想環境用のセキュリティ アーキテクチャを提供します。VMSafe ネットワーク API を使用していない場合は、VMSafe ネットワーク API を無効にします。

CA Access Control エンタープライズ管理 でのハイパーバイザー ハードニング ポリシーの設定

ハイパーバイザー ハードニング ポリシーを使用すると、ハイパーバイザーへのユーザアクセスを制限し、リモート システム ロギング、時間同期、および SNMP エージェントを設定することができます。

注: 仮想マシンのアクセス権限を管理するためには、システム マネージャ ロールが割り当てられている必要があります。

重要: この手順を完了する前に、VMware vCenter サーバへの接続が設定されていることを確認してください。また、ハードニング ポリシーを適用する各ハイパーバイザーに PUPM エンドポイントを作成してください。

以下の手順に従います。

1. [ワールド ビュー] - [セキュリティ グループ] - [セキュリティ グループ管理] に移動します。

   [セキュリティ グループ管理]ページが表示され、VMware vCenter サーバ上のセキュリティ グループと CA Access Control サーバの詳細が表示されます。

2. セキュリティ グループを選択します。

   CA Access Control エンタープライズ管理 にセキュリティ グループ詳細とメンバが表示されます。

   重要: 選択したセキュリティ グループに、グループのメンバとして 1 つ以上の ESX サーバが登録されていることを確認してください。

3. [アクション]メニューから、[ハイパーバイザー ハードニング ポリシーの追加]を選択します。

   [セキュリティ グループ ハイパーバイザー ハードニングの管理:*ホスト グループ名*]ページが表示されます。

4. 以下のフィールドに値を入力します。

   コメント

   ハードニング ポリシーの説明を指定します。

   ロックダウン

   ハイパーバイザーへのリモート アクセスをブロックすることを指定します。

   ダイレクト コンソール UI

   ローカルの管理コントロールを無効化することを指定します。

テクニカル サポート モード

テクニカル サポート モードを無効化することを指定します。

テクニカル サポート モード タイムアウト

テクニカル サポート モードが無効化されるまでの時間を秒単位で指定します。

ローカル データストア パス

(ESXi のみ) syslog がメッセージを記録するデータストアのフルパス名を指定します。

例: [storage1]/var/log/messages

リモート Syslog ホスト

リモート syslog ホスト名を定義します。

リモート ポート

リモート syslog ホストのポート番号を定義します。

NTP サーバ

NTP (ネットワーク タイム プロトコル) サーバ名を指定します。

有効

SNMP 設定の有効化を指定します。

SNMP ポート

SNMP のリスニング ポート番号を定義します。

読み取り専用コミュニティ

読み取り専用アクセス権を持つコミュニティの名前を指定します。

例: SNMP - サーバ コミュニティのパブリック RO

トラップ ターゲット

SNMP トラップ ターゲットのホスト名、ポートおよびコミュニティを定義します。

形式: *target_hostname@ポート/コミュニティ*

例: SNMP_host@55222/comm

VMSafe **ネットワーク** API

VMSafe ネットワーク API の無効化を指定します。

ハイパーバイザー管理者

ハイパーバイザー管理者アカウントの名前を定義します。CA Access Control for Virtual Environments は、このアカウントを使用してハイパーバイザーに接続します。

5. [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、ハードニング ポリシーをグループにデプロイします。

監査コレクション

CA User Activity Reporting Module を使用することによって、IT アクティビティを収集し、標準化し、集約して報告し、コンプライアンス違反が発生した場合にアクションを必要とするアラートを生成することができます。

CA User Activity Reporting Module の監査コレクション ポリシーでは、グループに割り当てた監査コレクション プロファイルに従って、各仮想マシン グループにポリシーを割り当てることができます。

注: CA Access Control for Virtual Environments と CA User Activity Reporting Module の統合の詳細については、「*エンタープライズ管理ガイド*」を参照してください。

CA Access Control エンタープライズ管理 での監査コレクション ポリシーの設定

監査コレクション ポリシーは、CA Access Control for Virtual Environments が管理する各セキュリティ グループに設定します。CA Access Control for Virtual Environments は、グループに追加した各仮想マシンに監査コレクション ポリシーを適用します。

以下の手順に従います。

1. [ワールド ビュー] - [セキュリティ グループ] - [セキュリティ グループ管理] に移動します。

   [セキュリティ グループ管理]ページが表示され、VMware vCenter 上のコンピュータ グループと CA Access Control Server の詳細が表示されます。

2. [セキュリティ グループ]セクションで、グループを選択します。

   CA Access Control エンタープライズ管理 にグループ詳細とメンバが表示されます。

3. [アクション]メニューから、[監査コレクション ポリシーの追加]を選択します。

   [セキュリティ グループ監査コレクションの管理: *セキュリティ グループ名*] ウィンドウが表示されます。

4. 以下のフィールドに値を入力します。

   説明

   監査コレクション ポリシーの説明を指定します。

   有効

   管理対象デバイスのイベント収集を有効にすることを選択します。

   オペレーティング システム プロファイル

   監査コレクション ポリシーを適用するオペレーティング システム プロファイルを選択します。

   監査コレクション プロファイル

   CA User Activity Reporting Module で定義した監査コレクション プロファイルを指定します。

   プロファイルの説明

   監査コレクション プロファイルの説明を指定します。

   認証アカウント

CA User Activity Reporting Module への接続に使用するユーザ アカウントを定義します。

注: このフィールドは、選択した監査コレクション プロファイルに応じて有効化または無効化されています。

5. [サブミット]を選択します。

   CA Access Control エンタープライズ管理 は監査コレクション ポリシーを作成し、セキュリティ グループに割り当てます。CA User Activity Reporting Module では、管理対象デバイスから監査イベントを直接収集できるようになりました。

VMware vSphere クライアントでの CA User Activity Reporting Module レポートの表示

CA User Activity Reporting Module が管理対象デバイスから監査レコードを収集するよう設定されている場合、CA User Activity Reporting Module レポートを VMware vSphere クライアントから表示することができます。

以下の手順に従います。

1. 左ペインから管理対象デバイスを選択し、次に[CA Security]タブを選択します。

   [CA Security]タブが開き、サマリ タブのコンテンツが表示されます。

2. [ユーザ アクティビティ レポート モジュール]タブを選択します。
3. ドロップダウン メニューからレポートを選択します。

   レポートが表示されます。

特権アカウント パスワードの検出

特権アカウント パスワードの検出とは、CA Access Control for Virtual Environments において特権アカウントおよびアプリケーション ID のパスワードの検出、ボールト、管理を行うプロセスです。検出後は、CA Access Control for Virtual Environments を使用して、定義済みのポリシーに基づいて特権アカウントおよびパスワードへのアクセスを制御できます。

VMware vSphere クライアントでの特権アカウント パスワードの手動検出

特権アカウント パスワードへのアクセスを制御するには、管理対象デバイス上で特権アカウントを識別し、次に特権アカウント パスワードを CA Access Control for Virtual Environments に格納します。

以下の手順に従います。

1. 左ペインから管理対象デバイスを選択し、[CA Security]タブを選択します。

   [CA Security]タブが開き、サマリ タブのコンテンツが表示されます。

2. [サービス]フィールドから[設定]を選択します(PUPM が無効化されアカウント検出ウィザードが起動できない場合)。

   アカウント検出および保管ウィザードが起動します。

3. 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

   設定する管理対象デバイスの名前を識別します。

   説明

   エンドポイントの説明を指定します。

   エンドポイント タイプ

   エンドポイントのタイプを定義します。

   注: エンドポイント タイプを選択すると、別のダイアログ ボックスが開きます。このダイアログ ボックスを使用して、そのエンドポイント タイプの特権アカウントを管理するために必要なクレデンシャルを提供します。選択するエンドポイント タイプは、提供する必要がある接続情報に影響します。

4. [検証]を選択します。

   CA Access Control for Virtual Environments は、エンドポイント接続設定の検証を試行します。

5. [次へ]をクリックします。

6. 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。

7. 管理する特権アカウントを選択し、[次へ]をクリックします。

   [ロックダウン プロパティ]画面が表示されます。

8. ダイアログ ボックスの以下のフィールドに入力します。以下のフィールドには、説明が必要です。

接続解除システム

アカウントの場所を接続解除システムにするかどうかを指定します。

このオプションを選択すると、PUPM はアカウントを管理しません。代わりに、PUPM は、接続解除システムの特権アカウントのパスワード ボールトとしてのみ機能します。パスワードを変更するたびに、管理対象エンドポイント上のアカウント パスワードも手動で変更する必要があります。

パスワード ポリシー

特権またはサービス アカウントに適用するパスワード ポリシーを指定します。

チェックアウト期限

チェックアウト アカウントが失効するまでの期間を分単位で指定します。

専用アカウント

単一ユーザだけがいつでもアカウントを使用することができるかどうかを指定します。*専用アカウント*は、アカウントの使用を1 回に 1 ユーザに制限する、特権アカウントの制限事項です。

チェックアウト時にパスワードを変更

特権アカウントがチェックアウトされるたびに、PUPM 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、PUPM 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、PUPM は新規特権アカウント パスワードを生成します。

9. [次へ]をクリックします。

[サマリ]画面が表示されます。

10. 内容を確認して、[完了]をクリックします。

エラーがない場合、CA Access Control for Virtual Environments はタスクをサブミットし、選択された特権アカウントを作成します。

詳細情報:

Windows エージェントレス接続情報 (P. 63)
SSH デバイス接続情報 (P. 64)
VMware ESX/ESXi 接続情報 (P. 66)

Windows エージェントレス接続情報

Windows エージェントレス エンドポイント タイプを使用すると、Windows 特権アカウントを管理できます。

注: ローカル コンピュータ上でドメイン ユーザを設定した場合、CA Access Control for Virtual Environments はそのドメイン ユーザのパスワードを変更できません。この制限は、Windows の動作に起因するものです。

このタイプのエンドポイントを作成する場合は、以下の情報を提供します。

ユーザ名

エンドポイントの管理ユーザの名前を定義します。CA Access Control エンタープライズ管理 はこのアカウントを使用して、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

例: myhost-ac-1

ホストドメイン

このホストがメンバであるドメイン名を指定します。

注: ホストドメイン名には接頭辞だけを指定します。たとえば、完全なドメイン名が company.com である場合、接頭辞の company のみを入力します。

Active Directory

ユーザ アカウントが Active Directory アカウントかどうかを指定します。

ユーザ ドメイン

このユーザがメンバであるドメイン名を指定します。

注: ユーザ ドメイン名は接頭辞だけを指定します。たとえば、完全なドメイン名が company.com である場合、接頭辞の company のみを入力します。

重要: PUPM 自動ログインを使用してエンドポイントにログインする場合、ホストドメイン名が指定されていることを確認します。エンドポイントがワークグループのメンバである場合は、ワークグループ名ではなくホスト名を指定します。

注: Windows エージェントレス エンドポイントを設定するのに必要な追加手順の詳細については、「エンタープライズ管理ガイド」を参照してください。

SSH デバイス接続情報

SSH デバイス タイプを使用して、UNIX 特権アカウントを管理できます。

重要: PUPM SSH エンドポイントを設定する前に、エンドポイント上のトンネル化されたクリア テキスト パスワードを無効にしてから、エンドポイントを設定します。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control エンタープライズ管理 がデバイスに接続できるようにします。

ユーザ名

エンドポイントの管理ユーザの名前を定義します。CA Access Control エンタープライズ管理 はこのアカウントを使用して、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクを実行します。操作管理者アカウントを指定すると、PUPM は、そのアカウントを使用してエンドポイント上で管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

操作管理者ユーザ ログイン

(オプション) エンドポイントの操作管理ユーザの名前を定義します。PUPM は、このアカウントを使用してエンドポイントに対する管理タスクを実行します。たとえば、特権アカウントのパスワードを検出し、変更します。ユーザが操作管理者ユーザを指定しない場合も、PUPM はユーザ ログイン アカウントを使用して、エンドポイントに対する管理タスクを実行します。

Check Point ファイアウォールを使用する SSH エンドポイントに対して操作管理者ユーザを指定する場合、エキスパート ユーザを指定します。ただし、PUPM を使用してエンドポイント上のエキスパート アカウントのパスワードを変更することはできません。この制限は、エキスパート アカウントが PUPM 内の接続解除されたアカウントである必要があることを意味します。

操作管理者パスワード

(オプション) 操作管理者ユーザのパスワードを定義します。

設定ファイル

SSH デバイスの XML 設定ファイルの名前を指定します。ニーズに合わせて XML ファイルをカスタマイズできます。

注: このフィールドの値を指定しない場合、CA Access Control エンタープライズ管理 は ssh_connector_conf.xml ファイルを使用します。

注: SSH デバイス エンドポイントを設定するのに必要な追加手順の詳細については、「エンタープライズ管理ガイド」を参照してください。

VMware ESX/ESXi 接続情報

VMware ESX/ESXi エンドポイント タイプによって、VMware ESX/ESXi 特権アカウントを管理できます。

このタイプのエンドポイントを作成する場合、以下の情報を指定して、CA Access Control for Virtual Environments がエンドポイントに接続できるようにします。

ユーザ名

エンドポイントの管理ユーザの名前を定義します。CA Access Control エンタープライズ管理 はこのアカウントを使用して、エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクを実行します。

注: [詳細]オプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。代わりに、PUPM は特定の特権アカウントを使用して、エンドポイントに対する管理タスクを実行します。

パスワード

エンドポイントの管理ユーザのパスワードを定義します。

ホスト

エンドポイントのホスト名を定義します。

詳細

エンドポイントへの接続、アカウントの検出、パスワードの変更など、エンドポイントに対する管理タスクの実行に特権管理アカウントを使用するかどうかを指定します。たとえば、複数のエンドポイントに対して管理タスクを実行できる特権ドメイン アカウントを指定できます。

このオプションを指定すると、PUPM は管理タスクの実行に[ユーザ ログイン]アカウントを使用しません。

VMware vSphere クライア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

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

以下の手順に従います。

1. VMware vSphere クライアント ウィンドウの左ペインから管理対象デバイスを選択し、[CA Security]タブを選択します。

   [CA Security]タブが開き、サマリ タブのコンテンツが表示されます。

2. [特権アカウント管理]タブに移動します。

   [特権アカウント管理]タブが開き、チェックアウト可能なアカウントが表示されます。

3. チェックアウトするアカウントおよび管理対象デバイスを選択し、[アクション]メニューから以下のオプションのいずれかを選択します。

   - [チェックアウト]を選択してパスワードをチェックアウト
   - [自動ログイン]を選択して管理対象デバイスにログイン
   - [パスワードの表示]を選択してパスワードを表示

   VMware vSphere クライアントは選択したオプションに従ってタスクを処理します。

   管理対象デバイスへのログインを選択した場合は、管理対象デバイス上でウィンドウが開いてログインできます。

   注: 初めて管理対象デバイスにログインするときには、接続する前にアクションの確認を求めるダイアログが表示されます。

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

VMware vSphere クライアントからの特権アカウント パスワードのチェックイン

管理対象エンドポイントからログアウトしたら、特権アカウント パスワードをチェックインします。特権アカウント パスワードをチェックインしたら、CA Access Control for Virtual Environments は設定オプションの設定に基づいてパスワードを変更できます。

以下の手順に従います。

1. VMware vSphere クライアント ウィンドウの左ペインから管理対象デバイスを選択し、[CA Security]タブを選択します。

   [CA Security]タブが開き、サマリ タブのコンテンツが表示されます。

2. [特権アカウント管理]タブに移動します。

   [特権アカウント管理]タブが開き、チェックイン可能なアカウントが表示されます。

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

   CA Access Control for Virtual Environments はアカウントをチェックインします。

Break Glass プロセス中に発生するイベント

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

Break Glass アカウントは、ユーザ ロールに従ってユーザに割り当てられていない特権アカウントです。ただし、ユーザはアカウント パスワードを取得できます。

Break Glass チェックアウト プロセスでは、Break Glass チェックアウト プロセスが発生したことを管理者に伝える通知メッセージがロール管理者に送信されます。ただし、管理者はそのプロセスを承認したり停止したりすることはできません。

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]オプションで、そのユーザの[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。

CA Access Control エンタープライズ管理 からの Break Glass

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

注: エンドポイントへの即時アクセスが必要ではない場合は、特権アカウントへのアクセスを要求します。その後、管理者が要求を承認します。

以下の手順に従います。

1. CA Access Control エンタープライズ管理 で、[ホーム]-[マイ アカウント]-[マイ特権アカウント]をクリックします。

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

2. アカウントを選択するフィールドで[詳細]を選択します。

   詳細検索オプションが表示されます。

3. [Break Glass アカウントを含む]-[検索]を選択します。

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

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

5. [理由]に値を入力し、[チェックアウト]をクリックします。

   CA Access Control エンタープライズ管理 はタスクをサブミットし、成功した場合、確認メッセージにアカウント パスワードが表示されます。

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

VMware vSphere Client の Break Glass

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

以下の手順に従います。

1. [ホスト情報]画面から、[特権アカウント管理]を選択します。

   [特権アカウント管理]タブが開き、Break Glass を行うために利用できる特権アカウントが表示されます。

2. チェック アウトする特権アカウントを選択し、[Break Glass]を選択します。
3. [理由]に値を入力し、[チェックアウト]をクリックします。

   CA Access Control for Virtual Environments はタスクをサブミットし、成功した場合、確認メッセージにアカウント パスワードが表示されます。

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

CA Access Control エンタープライズ管理 での Break Glass 特権アカウント パスワードのチェックイン

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

以下の手順に従います。

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

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

2. アカウントを選択するフィールドで[詳細]を選択します。

   詳細検索オプションが表示されます。

3. [Break Glass アカウントを含む]-[検索]を選択します。

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

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

   CA Access Control エンタープライズ管理 はタスクをサブミットして、アカウントをチェックインします。