CA Access Control for Virtual Environments

統合ガイド

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
- [assign the value for UARM in your book]
- Identity Manager

ドキュメントの表記規則

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

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

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

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

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

例: コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

ファイル ロケーションに関する規則

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

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

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

CA への連絡先

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

目次

第 1 章: 概要

このセクションには、以下のトピックが含まれています。

本書の内容

本書では、CA Access Control for Virtual Environments の実装を計画および設定する方法と、CA やサードパーティの製品との統合方法について説明します。さらに、高可用性とディザスタリカバリのために CA Access Control for Virtual Environments を計画および設定する方法についても説明します。

第 2 章: ObserveIT Enterprise との統合

このセクションには、以下のトピックが含まれています。

ObserveIT の統合について

CA Access Control for Virtual Environments を ObserveIT Enterprise と統合すると、特権アカウントによる組織内のサーバへのアクセスの試行に対する制御が拡張されます。ObserveIT Enterprise セッション ログ記録ソフトウェアにより、ターゲット システムでのユーザ アクティビティが記録されます。ユーザが特権アカウント パスワードをチェックアウトし、エンドポイントにログインするとすぐに記録が開始されます。セッションが終了したとき、たとえばユーザが特権アカウント パスワードをチェックインすると、記録は終了します。

記録されたセッションは、準備した専用のデータベースに格納されます。記録されたセッションは、ObserveIT ビューアを使用して CA Access Control エンタープライズ管理 から直接再生できます。

以下のリンクを使用して、ObserveIT 社から ObserveIT Enterprise セッション ログ記録プログラムを取得できます。

http://www.observeit-sys.com/download.asp

以下のリンクで ObserveIT Enterprise のドキュメントを検索することができます。

https://support.ca.com/cadocs/

注: ObserveIT の詳細については、ObserveIT Enterprise のインストール メディアにある ObserveIT のマニュアルを参照してください。

統合をセットアップする方法

CA Access Control for Virtual Environments を ObserveIT Enterprise セッション記録ソフトウェアと統合するには、いくつかの手順を実行する必要があります。統合が完了すると、ObserveIT はすべての PUPM セッションを記録します。

注: 手順 1 ～ 5 を実行する方法の詳細については、ObserveIT のインストールメディアにある ObserveIT Enterprise のマニュアルを参照してください。

以下の手順に従います。

1. ObserveIT Enterprise のシステム要件およびインストール要件を確認します。

   使用するサーバが、ObserveIT Enterprise をインストールするための最小システム要件を満たしていることを確認します。

2. 中央データベースを準備します。

   記録されたセッションは、専用の Microsoft SQL Server に格納されます。

3. IIS（Internet Information Server）を設定します。

   ObserveIT Enterprise アプリケーション サーバは、IIS を使用して、エージェントから送信されたメタデータを処理します。

4. ObserveIT Enterprise サーバ コンポーネントをインストールします。

   ObserveIT アプリケーション サーバ、エージェント、および管理コンソールもインストールされます。

5. ObserveIT Enterprise アプリケーション サーバを設定します。

   記録設定を設定します。

6. セッション記録スクリプトをエンタープライズ管理サーバにデプロイします。

   このスクリプトによって、セッション記録のトリガとなる PUPM 自動ログインが有効になります。

7. サービス アカウントを作成します。

   エンタープライズ管理サーバで使用するサービス アカウントを作成します。

8. CA Access Control エンタープライズ管理 で ObserveIT Enterprise アプリケーション サーバへの接続を定義します。

   接続設定を設定して、セッション ログ記録を有効にします。

統合を準備する方法

ObserveIT Enterprise アプリケーション サーバのインストールが完了したら、CA Access Control for Virtual Environments との統合のためにサーバを準備します。ObserveIT Enterprise アプリケーション サーバの準備が完了すると、サーバは PUPM セッションの記録および保存を開始するように設定されます。

以下の手順に従います。

1. 管理コンソールを開きます。
2. サービス アカウントを作成します。

   CA Access Control for Virtual Environments では、ObserveIT Enterprise アプリケーション サーバへの接続に、このサービス アカウントが使用されます。

管理コンソールを開きます。

ObserveIT Enterprise をインストールして起動すると、Web ベースの管理コンソールを起動できます。

管理コンソールを開く方法

1. ブラウザを使用して、ObserveIT Enterprise 管理コンソールを開きます。以下の URL を入力します。

   http://observeit_server_name:port/ObserveIT

   例:

   `http://observeit_server:4884/ObserveIT`

2. インストール時に指定した管理者クレデンシャルを使用してログインします。

   ObserveIT Enterprise 管理コンソールが開きます。

注: [スタート]-[プログラム]-[ObserveIT]-[ObserveIT WebConsole]に順にクリックして、ObserveIT Enterprise 管理コンソールを開くこともできます。

サービス アカウントの作成

CA Access Control エンタープライズ管理 では、ObserveIT Enterprise アプリケーション サーバでの認証にサービス アカウントが使用されて、ユーザ アクティビティが記録されます。CA Access Control エンタープライズ管理 で ObserveIT Enterprise アプリケーション サーバの接続設定を設定する際に、サービス アカウントのクレデンシャルを指定します。

サービス アカウントを作成する方法

1. ObserveIT Enterprise 管理コンソールから、[Configuration]-[Console Users]の順に選択します。

   コンソールユーザ画面が開きます。

2. [Create User]を選択します。

   コンソールユーザの追加ウィンドウが開きます。

3. ユーザ名とパスワードを入力し、パスワードを確認します。

4. 認証方法を[ObserveIT.Authentication]に、ユーザ ロールを[Admin]に設定します。

5. [Add]をクリックします。

   サービス アカウントが作成されます。

注: ユーザ管理の詳細については、ObserveIT Enterprise のインストール メディアにある *ObserveIT のマニュアル*を参照してください。

セッション記録スクリプトのデプロイ

ユーザ セッション記録は、PUPM の自動ログインと連携して動作します。ユーザが特権アカウント パスワードをチェックアウトし、エンドポイントへのログインを選択すると、リモート管理ソフトウェアが起動して、ユーザは自動的にログインされます。CA Access Control エンタープライズ管理 では、エンドポイント タイプに基づいて、セッション記録スクリプトを使用してリモート管理プログラムが制御されます。

たとえば、ユーザが Windows エンドポイントへのログインを選択すると、CA Access Control エンタープライズ管理 では、リモート デスクトップ ソフトウェアを開いてエンドポイントに接続するスクリプトが使用されます。

ObserveIT Enterprise アプリケーション サーバでセッションを記録するには、セッション記録スクリプトをエンタープライズ管理サーバにデプロイします。

セッション記録スクリプトをデプロイする方法

1. CA サポート Web サイトから、セッション記録スクリプトをダウンロードし、一時ディレクトリに保存します。
2. エンタープライズ管理サーバで、以下のディレクトリ(ここで *JBoss_HOME* は、JBoss がインストールされているディレクトリを示します)へ移動します。

   `JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts`
3. セッション記録スクリプトを sso_scripts ディレクトリにコピーします。

   上書きする前に、このディレクトリ内のファイルをバックアップすることをお勧めします。
4. 既存のファイルを新規ファイルで上書きすることを選択します。

ObserveIT Enterprise アプリケーション サーバへの接続設定を設定できるようになりました。

ObserveIT への接続の定義

ObserveIT Enterprise との統合を完了するには、CA Access Control エンタープライズ管理 で ObserveIT Enterprise アプリケーション サーバへの接続設定を設定します。

ObserveIT への接続を定義する方法

1. CA Access Control エンタープライズ管理 で、[システム]-[接続管理]-[セッション記録]-[接続の作成]の順に選択します。

   [Create Connection(接続の作成)]画面が表示されます。

2. 以下の詳細を入力します。

   接続の説明

   接続の説明をフリー テキストで記述します

   再生 URL

   ObserveIT Enterprise アプリケーション サーバの URL を定義します

   例: http://observeit_host:4884/observeit/

   ユーザ ID

   サービス アカウントのユーザ名を定義します

   パスワード

   サービス アカウントのパスワードを定義します

   詳細

   以下の詳細な接続設定を指定します。

   [ビューア ページ]

   セッションが記録されることを示すメッセージを、画面の上部に表示するかどうかを指定します

   [ビューア パラメータ]

   ObserveIt ビューア ウィンドウの幅と高さを指定します

ActiveX URL

ObserveIT Enterprise の ActiveX ファイルがある場所のフル パス名を指定します。デフォルトでは、ObserveIT アプリケーション サーバの URL を指定します。

例:
http://observeit_host:4884/ObserveIT/AgentInstall/Agent.cab#version=1,0,0,0

サーバURL

ObserveIT Enterprise アプリケーション サーバが記録されたセッションを格納する場所のフルパス名を指定します。デフォルトでは、ObserveIT アプリケーション サーバの URL を指定します。

例: http//observeit_host:4884/ObserveITApplicationServer

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 により接続が作成されます。

第 3 章: PUPM セッションのログ記録

このセクションには、以下のトピックが含まれています。

セッションをログ記録する方法

各 PUPM セッションは記録されて、ObserveIT Enterprise データベースに格納されます。各セッションは、記録されたセッション全体から独立して再生できる個別のスライドに分割されます。

以下の手順では、PUPM セッションがログ記録される方法が説明されています。

1. ユーザが CA Access Control エンタープライズ管理 から特権アカウント パスワードをチェックアウトし、エンドポイントに自動的にログインすることを選択します。

   このオプションを初めて使用する場合は、ActiveX をインストールするように求められます。

2. リモート管理セッションが開き、ユーザはパスワードの入力なしでログインされます。
3. エンドポイントにインストールされている ObserveIT エージェントにより、ユーザ アクティビティの記録、および ObserveIT Enterprise アプリケーション サーバへのスライドの送信が開始されます。ObserveIT Enterprise アプリケーション サーバでは、そのデータがデータベースに保存されます。
4. ユーザがリモート管理セッションを閉じ、ObserveIT エージェントでは記録が停止されます。
5. 記録されたセッションが CA Access Control エンタープライズ管理 で表示されます。

重要: Internet Explorer による ActiveX のダウンロードを有効にするには、[ローカル イントラネット ゾーン]または[信頼済みゾーン]で ObserveIT エンタープライズ ホスト名を指定し、[署名 済み ActiveX コントロールのダウンロード]セキュリティ オプションを有効にします。

注: セッション記録の詳細については、ObserveIT Enterprise のインストール メディアにある *ObserveIT のマニュアル*を参照してください。

セッションがログ記録される場所

ObserveIT Enterprise アプリケーション サーバでは、専用の Microsoft SQL Server に PUPM のセッションがログ記録されます。ObserveIT データベース サーバでは、専用データベースが 2 つ使用されます。最初のデータベースは ObserveIT という名前で、設定とメタデータが保持されます。2 番目のデータベースは ObserveIT_Data という名前で、記録されたセッションの実行中に ObserveIT エージェントで収集されたスクリーンショットが格納されます。

注: セッション ログ記録の詳細については、ObserveIT Enterprise のインストール メディアにある *ObserveIT のマニュアル*を参照してください。

セッションの再生

記録された PUPM のセッションを CA Access Control エンタープライズ管理 から再生します。セッションの再生を選択すると、CA Access Control エンタープライズ管理 により、記録されたセッションが新しいウィンドウで再生されます。プレーヤ ウィンドウには、セッション内を移動するために使用するコントロール ボタンがあります。記録されたセッション内でフリー テキスト検索を実行することもできます。

注: フリー テキスト検索の詳細については、ObserveIT Enterprise のインストール メディアにある *ObserveIT のマニュアル*を参照してください。

セッションを再生する方法

1. CA Access Control エンタープライズ管理 で、[特権アカウント]-[Audit subtask]の順に選択します。

   [特権アカウントの監査]タスクが、使用可能なタスク リストに表示されます。

2. [特権アカウントの監査]を選択します。

   [特権アカウントの監査]検索ウィンドウが開きます。

   注: PUPM の Audit Manager ロールがこの手順の実行者に割り当てられていることを確認します。

3. 検索条件を指定し、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。

4. セッションの詳細列の再生アイコンをクリックして、セッションを再生します。

   プレーヤ ウィンドウが開き、セッションが始めから再生されます。

   注: セッション内を移動するには、ウィンドウ下部のコントロールを使用します。

第 4 章: エンタープライズ レポート機能の実装

このセクションには、以下のトピックが含まれています。

エンタープライズ レポート機能

CA Access Control エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ (CA Access Control レポート ポータル) を使用して、レポート機能を提供します。エンタープライズ レポート機能を使用すると、各エンドポイント (ユーザ、グループ、リソース) のセキュリティ ステータスを 1 つの場所で確認できます。CA Access Control レポートは、各エンドポイントについて、誰が何を実行できるかを定義するルールおよびポリシーを記述し、ポリシーの例外があれば示します。

設定が終了すると、CA Access Control エンタープライズ レポート機能は単独で機能して、手動操作の必要なく継続的に各エンドポイントからデータを収集し、情報を中央サーバに格納します。各エンドポイントからのデータの収集は、スケジュールで設定することも、オンデマンドで行うこともできます。各エンドポイントに接続しなくても、誰がどのリソースへのアクセスを許可されているかを確認することができます。収集サーバが稼働しているかダウンしているかに関係なく、各エンドポイントは自身のステータスについてレポートします。

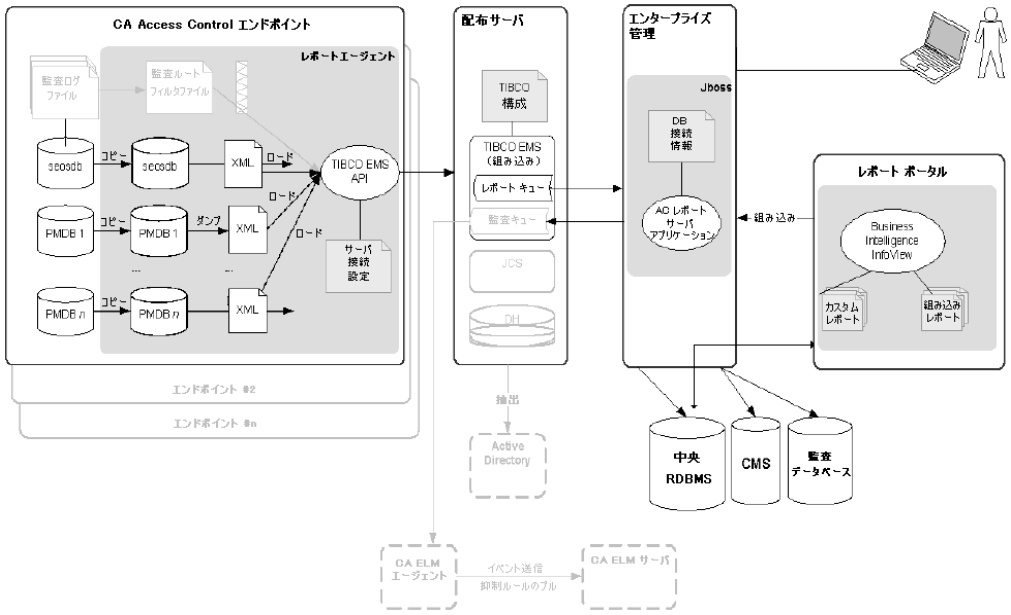
レポート サービスのアーキテクチャ

CA Access Control レポート サービスは、CA Access Control エンタープライズ レポートの作成に対応するサーバ ベースのプラットフォームを提供します。このプラットフォームを使用して、すべての CA Access Control エンドポイントから取得したデータを含むレポートを作成できます。作成したレポートは、Web 対応のアプリケーション上で表示および管理できます。

レポート サービスでは、既存の CA Access Control インフラストラクチャ上にレポート環境を構築できます。

注: エンタープライズ レポートの詳細については、「エンタープライズ管理ガイド」を参照してください。

以下の図に、レポート サービス コンポーネントのアーキテクチャを示します。この図では、コンポーネント間でのデータの流れについても示します。



上の図は、以下のことを示します。

- CA Access Control データベース（seosdb）および任意の数の Policy Model（PMDB）が含まれる各エンドポイントには、レポート エージェント コンポーネントがインストールされています。
- レポート エージェントはエンドポイントからデータを収集し、配布サーバに処理のため送信します。
- シンプルなエンタープライズ モデルでは、1 つの配布サーバがすべてのエンドポイント データを処理し、処理したデータを中央データベースに格納のため送信します。配布サーバ コンポーネントを複製することで、大規模な企業環境においてフォルト トレランスおよび高速処理を実現する設計が可能です。
- 中央データベース（RDBMS）はエンドポイント データを格納します。
- レポート ポータルを利用すると、中央データベース内のデータにアクセスして組み込み型のレポートを作成すること、またはデータについて問い合わせを行いカスタム レポートを作成することができます。

レポート サービス サーバ コンポーネントの設定方法

エンタープライズ レポートを使用するには、CA Access Control レポーティング サービスのサーバ コンポーネントをインストールして設定します。サーバ コンポーネントをインストールして設定してから、各エンドポイントでレポート エージェントを設定します。

注: レポート エージェントのインストールと設定は、CA Access Control および [assign the value for unab in your book] エンドポイントのインストールの一環として行われるものであり、この手順では取り扱いません。

レポート サービス サーバ コンポーネントをセットアップするには、以下の手順に従います。

1. まだ行っていない場合は、エンタープライズ管理サーバをインストールして設定します。
2. レポート ポータル コンピュータ（CA Business Intelligence）をセットアップします。

   CA Business Intelligence インストール ファイルは、CA サポートの Web サイトにあります。
3. レポート ポータルで CA Access Control レポート パッケージをデプロイします。
4. CA Business Intelligence への接続を設定します。
5. スナップショット定義を作成します。

   ここで、CA Business Intelligence と CA Access Control エンタープライズ管理でレポートを作成して表示できます。

注: レポートの作成と表示の詳細については、「*エンタープライズ管理ガイド*」を参照してください。

レポート ポータル コンピュータのセットアップ方法

レポート ポータルを使用すると、CA Access Control エンタープライズ管理 が中央データベースに格納するエンドポイント データにアクセスして、組み込みレポートの作成、またはデータを問い合わせて、カスタム レポートの作成を行うことができます。レポート ポータルは、CA Business Intelligence を使用します。

注: レポート ポータルの旧バージョン、または CA Business Intelligence または [assign the value for boe in your book]XI がスタンドアロンでインストールされている場合、アップグレードの必要はなく、既存のインストールを代わりに使用できます。

レポート ポータルをセットアップするには、以下の手順に従います。

1. Oracle データベースを使用する場合は、レポート ポータル コンピュータに完全な Oracle クライアントをインストールします。
2. Microsoft SQL Server を使用する場合は、レポート ポータル コンピュータに Microsoft SQL Server Native Client をインストールします。
3. まだ実行していない場合は、中央データベースおよび配布サーバをセットアップします。

   注: エンタープライズ管理サーバのインストール時に、中央データベースおよび配布サーバをセットアップします。
4. (UNIX) レポート ポータル コンピュータが Solaris または Linux のコンピュータである場合は、CA Business Intelligence インストール用に UNIX コンピュータを準備 (P. 30)します。
5. レポート ポータル コンピュータおよびエンタープライズ管理サーバのシステム時刻を同期します。

   システム時刻を同期しない場合、CA Access Control エンタープライズ管理が生成するレポートのステータスが保留または循環のままになります。

6. ご使用のオペレーティング システムに対応する CA Business Intelligence をインストールします。

   CA Business Intelligence インストール ファイルは、CA サポートの Web サイトにあります。

   注: Windows 用のレポート ポータルでは、デフォルトで Microsoft SQL Server 認証を使用して、接続が認証されます。認証にドメイン ユーザ アカウント設定を使用する場合、Windows 認証で動作 (P. 38)するようにレポート ポータルを設定できます。

   レポート ポータルがセット アップされ、これで CA Access Control レポート パッケージをデプロイできるようになりました。

注: CA Business Intelligence の詳細については、CA Technologies サポートから入手可能な「*CA Business Intelligence インストール ガイド*」を参照してください。

例: Windows への CA Business Intelligence のインストール

以下の手順は、Windows への CA Business Intelligence のインストール手順を示しています。

注: インストールは、完了まで約 1 時間かかる場合があります。

1. CA Business Intelligence for Windows DVD をご使用の光ディスクドライブに挿入します。
2. ¥Disk1¥InstData¥VM フォルダに移動し、install.exe をダブルクリックします。

   CA Business Intelligence のインストール ウィザードが起動します。
3. 以下の表を使用して、インストール ウィザードを完了します。

情報	アクション
インストール言語	使用するサポート対象インストール言語を選択し、[OK]をクリックします。 **注**: 英語以外のサポート対象言語のいずれかにインストールする場合、ローカライズされたオペレーティング システムが必要です。
使用許諾契約書	[使用許諾契約書の条項に同意します]を選択し、[次へ]をクリックします。
インストール タイプ	[標準]を選択して、[次へ]をクリックします。
root 以外のクレデンシャル	root 以外のユーザ名とパスワードを入力します。

情報	アクション
BusinessObjects XI 管理者パスワード	「P@ssw0rd」と 2 回入力して、パスワードを設定、確認し、[次へ]をクリックします。 **注**: パスワード ルールについては、「*CA Business Intelligence* インストール ガイド」をご覧ください。これは、CA Access Control Enterprise Edition のマニュアル選択メニューからご利用いただけます。
Web サーバ設定	[次へ]をクリックして、デフォルト設定をそのまま使用します。
CMS データベース設定	以下の情報を入力して、[次へ]をクリックします。 ■ **MySQL root パスワード:** P@ssw0rd ■ **ユーザ名:** cadbusr ■ **パスワード:** C0nf1dent1al ■ **データベース名:** MySQL1 **注**: CA Business Intelligence Central Management Server (CMS) は内部管理目的のみに使用されます。
監査の有効化	[次へ]をクリックして、デフォルト設定をそのまま使用します。
監査データベース設定	以下の情報を入力して、[次へ]をクリックします。 ■ **ユーザ名:** cadbusr ■ **パスワード:** C0nf1dent1al ■ **データベース名:** MySQL1
設定の確認	設定を確認し、[インストール]をクリックして、インストールを完了します。

インストールが開始されます。完了まで約 1 時間かかる場合もあります。

重要: CA Business Intelligence Central Management Server (CMS) は内部管理目的のみに使用され、レポートの生成と表示に使用されるレポート データは含まれていません。CA Access Control エンタープライズ管理 をインストールした際に定義したレポート データベースには、レポート エージェントが配布サーバにアップロードするデータが含まれています。CMS の詳細については、「CA Business Intelligence インストール ガイド」を参照してください。

CA Business Intelligence インストールのための Solaris/Linux の準備

CA Business Intelligence を Solaris または Linux にインストールするには、コンピュータを事前に準備しておく必要があります。コンピュータを準備する際は、CA Business Intelligence インストール用に root 以外のユーザを作成し、Oracle RDBMS が CA Business Intelligence のインストールで認識されることを確認し、環境変数を設定します。

以下の手順に従います。

1. root ユーザとしてログインします。
2. root 以外のユーザを作成します。CA Business Intelligence インストールでは root 以外のユーザが必要になります。

   たとえば、以下のコマンドを入力し、グループ「other」に属する bouser という名前のユーザを作成します。

   ```
   groupadd other
   useradd -d /home/bouser -g other -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

   プロンプトが表示されたら、定義済みのユーザのパスワードを入力して確認します。
3. （Linux）LANG 環境変数が以下のように設定されていることを確認します。

   ```
   LANG=en US.utf8
   ```
4. 作成した root 以外のユーザとしてログインします。
5. 以下のコマンドを入力して、ORACLE_HOME および TNS_ADMIN 環境変数が正しく設定されていることを確認します。

   ```
   echo $ORACLE_HOME
   echo $TNS_ADMIN
   ```

   出力が空でなければ、これらの環境変数が有効であることがわかります。例:

   ```
   /opt/oracle/app/oracle/product/10.2.0/client_1
   /opt/oracle/app/oracle/product/10.2.0/client_1/admin/network
   ```

   コマンドで空の出力を受信した場合は、root でないユーザとして作成したユーザ用に変数が設定されていることを確認します。たとえば、/home/bouser/.profile を次のように編集します。

   ```
   ORACLE_HOME=/opt/oracle/app/oracle/product/10.2.0/client_1
   export ORACLE_HOME
   TNS_ADMIN=$ORACLE_HOME/network/admin
   export TNS_ADMIN
   ```

6. root でないユーザに対する LD_LIBRARY_PATH に以下のパスが含まれていることを確認します。

   ```
   $ORACLE_HOME/lib:$ORACLE_HOME/lib32
   ```

   たとえば、次のコマンドを入力し、出力を検索してこれらのパスを探します。

   ```
   echo $LD_LIBRARY_PATH
   ```

   これらのパスが見つからない場合は、LD_LIBRARY_PATH に追加します。たとえば、/home/bouser/.profile を次のように編集します。

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$ORACLE_HOME/lib:$ORACLE_HOME/lib32
   export LD_LIBRARY_PATH
   ```

7. LD_LIBRARY_PATH および TNS_ADMIN 内のフォルダがアクセス可能であることを次のように確認します。

   ```
   ls -l $ORACLE_HOME
   ls -l $TNS_ADMIN/tnsnames.ora
   ```

   これらのコマンドから「**アクセス許可が拒否されました**」というエラーが返されなければ問題ありません。もし返された場合は、適切なアクセス許可を付与する必要があります。たとえば、root/oracle ユーザは、次のコマンドを実行する必要があります。

   ```
   chmod -R +xr $ORACLE_HOME
   ```

8. TNS Ping ユーティリティを以下のように使用して、Oracle 接続が有効であることを確認します。

   ```
   $ORACLE_HOME/bin/tnsping service_name
   ```

   TNS Ping からの出力は、以下の例のようになります。

   ```
   TNS Ping Utility for Solaris: Version 10.2.0.1.0 - Production on 07-MAY-2008
   09:17:02
   Copyright(c)1997, 2005, Oracle.  All rights reserved.
   使用されるパラメータ ファイル
   /opt/oracle/app/oracle/oracle/product/10.2.0/client_1/network/admin/sqlnet.or
   a
   別名を解決するために使用される TNSNAMES アダプタ
   問合わせ中(DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST =
   172.16.234.75)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = service_name)))
   OK(30 msec)
   ```

   CA Business Intelligence を Solaris または Linux にインストールできるようになりました。

CA Business Intelligence のインストール用の Linux の準備

Linux で CA Business Intelligence をインストールする前に、コンピュータを準備する必要があります。 コンピュータを準備する際に、CA Business Intelligence インストールのための root 以外のユーザを作成し、環境変数を設定します。

注: 使用する Linux のバージョンが CA Business Intelligence でサポートされていることを確認します。

CA Business Intelligence のインストール用に Linux を準備する方法

1. root 以外のユーザを作成します。CA Business Intelligence インストールでは root 以外のユーザが必要になります。

   たとえば、以下のコマンドを入力し、bouser という名前のユーザを作成して、パスワードを設定します。

   ```
   useradd -d /home/bouser -m -s /bin/bash -c bouser bouser
   passwd bouser
   ```

2. LANG 環境変数が以下のように設定されることを確認します。

   ```
   LANG=en US.utf8
   ```

レポート パッケージのデプロイ

レポート パッケージは.BIAR ファイルで、これによって CA Access Control の 標準レポートがデプロイされます。レポート パッケージには、レポート ポータル 上でのデプロイに使用するアーティファクトおよびディスクリプタの集合体が含まれています。これらの標準レポートを使用するには、レポート パッケージ ファイルを BusinessObjects InfoView にインポートする必要があります。

注: このパッケージは、レポート ポータルの旧バージョンと下位互換性があります。最新のレポート パッケージを利用するためにレポート ポータルをアップグレードする必要はありません。また、ローカライズされたレポート パッケージをデプロイできます。これは、横に並んだ、別々の .biar ファイルとして提供されます。

レポート ポータルでのレポート パッケージのデプロイ

標準の CA Access Control レポートを使用するには、レポート パッケージ ファイルを BusinessObjects InfoView にインポートします。

注: この手順では、レポート ポータル上に、同じパッケージの旧バージョンがすでにデプロイされていない場合に、レポート パッケージをデプロイする方法について説明します。

以下の手順に従います。

1. 中央データベース、配布サーバ、レポート ポータルが設定されていることを確認します。

   注: JAVA_HOME 変数がレポート ポータル コンピュータ上でセットアップされていることを確認します。

2. CA Business Intelligence for Windows DVD を光ディスクドライブに挿入し、¥Disk1¥cabi¥biconfig フォルダに移動します。
3. biconfig ディレクトリの中身を一時ディレクトリにコピーします。
4. お使いのオペレーティング システム用の適切な CA Access Control Enterprise Edition サーバ コンポーネント DVD を光ディスクドライブに挿入し、¥ReportPackages フォルダにアクセスします。
5. 以下のファイルを、光ディスクドライブから同じ一時ディレクトリにコピーします。

   - ¥ReportPackages¥*RDBMS*¥*import_biar_config*.xml
   - ¥ReportPackages¥*RDBMS*¥*AC_BIAR_File*.biar

   RDBMS

   CA Access Control レポートで使用される RDBMS のタイプを定義します。

   値: Oracle、MSSQL2005

import_biar_config.xml

使用する RDBMS のインポート構成ファイル（.xml）の名前を定義します。

値: import_biar_config_oracle10g.xml、
import_biar_config_oracle11g.xml、
import_biar_config_mssql_2005.xml

注: 中央データベースとして MS SQL Server 2008 を使用する場合は、import_biar_config_mssql_2005.xml ファイルを設定します。

AC_BIAR_File.biar

使用する言語と RDBMS の CA Access Control レポート ファイル（.biar）の名前を定義します。

注: 使用する RDBMS 用のインポート設定ファイルの <biar-file name> プロパティは、このファイルを指します。デフォルトでは、RDBMS の英語バージョンの名前に設定されます。

6. *import_biar_config*.xml ファイルのコピーを編集します。以下の XML プロパティを定義します。

<biar-file name>

CA Access Control レポート ファイル（.biar）への完全なパス名を定義します。ファイルは前の手順でコピーしました。

<networklayer>

使用する RDBMS でサポートされているネットワーク層を定義します。

値（Windows）:

- OLE DB -- MS SQL Server 認証モードの場合
- Oracle OCI
- ODBC -- Windows 認証モードの場合

値（UNIX）: UNIX、Oracle CLI

<rdms>

CA Access Control レポートで使用される RDBMS のタイプを定義します。

値（Oracle OCI）： Oracle 10 または Oracle 11

値（ODBC）： 一般的な ODBC データソース

値（OLE DB）： MS SQL Server 2005 あるいは Oracle 10 または Oracle 11 *以外*の任意の値

注：MS SQL Server 2008 を使用する場合は、このプロパティに MS SQL Server 2005 を指定します。このプロパティに指定できる値の詳細については、CA Business Intelligence のドキュメントを参照してください。

<username>

エンタープライズ管理用に中央データベースを準備した際に作成した RDBMS 管理者ユーザのユーザ名を定義します。

<password>

エンタープライズ管理用に中央データベースを準備した際に作成した RDBMS 管理者ユーザのパスワードを定義します。

<datasource>

以下の*いずれか*を定義します。

- （Oracle）データベースの名前
- （SQL Server 2005 または 2008）作成したデータベース
- （ODBC）作成した DSN

重要：CA Business Intelligence CMS ではなく、CA Access Control によってレポート用に使用されるデータベースの名前を指定します。

<server>

SQL Server 2005 または 2008 コンピュータの名前を定義します。Oracle Database 10g、11g、および ODBC では、この値を空のままにします。

7. 以下のいずれかの操作を行います。

   - （Windows）コマンド プロンプトを開き、以下のコマンドを入力します。

     System_Drive:¥BO¥biconfig.bat -h *host_name* -u *user_name* -p *password* -f *ac_biar_config*.xml

     host_name

     レポート ポータルのホスト名を定義します。

user_name

レポート ポータルをインストールした時に設定したレポート ポータル管理者を定義します。

password

レポート ポータル管理者のパスワードを定義します。

例:

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
C:¥BO¥import_biar_config_oracle11g.xml
```

- (UNIX) 以下のとおり、スクリプト ファイル biconfig.sh に実行許可を設定し、実行します。

```
temp_dir/biconfig.sh -h host_name -u user_name -p password -f
ac_biar_config.xml
```

例:

```
biconfig.sh -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
/tmp/rp/import_biar_config_orcl.xml
```

バッチ ファイルによって CA Access Control レポートが InfoView にインポートされます。インポートは、完了するまで数分かかる場合があります。バッチ ファイルと同じフォルダにログ ファイル (biconfig.log) が作成され、インポートが成功したかどうかを示します。

例: Oracle Database 11g インポート設定ファイルのサンプル

以下のコードは、Oracle Database 11g 用に編集されたインポート設定ファイル (import_biar_config_oracle11g.xml) の例です。

```
<?xml version="1.0"?>
<biconfig version="1.0">
□□<step priority="1">
□□□□<add>
□□□□□□<biar-file name="c:¥temp¥AccessControl_R12.5_EN_ORCL_22_JUN_2009.biar">
□□□□□□□□<networklayer>Oracle OCI</networklayer>
□□□□□□□□<rdms>Oracle 11</rdms>
□□□□□□□□<username>root</username>
□□□□□□□□<password>P@ssw0rd</password>
□□□□□□□□<datasource>orcl</datasource>
□□□□□□□□<server></server>
□□□□□□</biar-file>
□□□□</add>
□□</step>
</biconfig>
```

例: Microsoft SQL Server 2005 インポート設定ファイルのサンプル

以下のコードは、MS SQL Server 2005 用に編集されたインポート設定ファイル（import_biar_config_mssql2005.xml）の例です。

```
<?xml version="1.0"?>
<biconfig version="1.0">
□□<step priority="1">
□□□□<add>
□□□□□□<biar-file name="c:¥temp¥AccessControl_R12.5_EN_SQL_11_JUN_2009.biar">
□□□□□□□□<networklayer>OLE DB</networklayer>
□□□□□□□□<rdms>MS SQL Server 2005</rdms>
□□□□□□□□<username>dbAdmin</username>
□□□□□□□□<password>P@ssw0rd</password>
□□□□□□□□<datasource>r125db</datasource>
□□□□□□□□<server>rdbms.org</server>
□□□□□□</biar-file>
□□□□</add>
□□</step>
</biconfig>
```

レポート ポータル用の Windows 認証設定

Windows で有効

レポート ポータル（CA Business Intelligence）をインストールし、CMS データベースとして Microsoft SQL Server を使用することを選択すると、認証モードは SQL Server 認証に設定されます。Microsoft SQL Server 認証では、データベース接続を認証するために SQL ユーザ アカウントが使用されます。

ユーザの組織で Active Directory が使用される場合には、認証方式を Windows 認証に変更できます。Windows 認証では、CMS データベースへの接続はローカル ユーザ アカウントではなく Domain ユーザ アカウントを使用して認証されます。

Windows 認証による接続の認証では、すべてのレポート ポータル コンポーネント間にセキュリティで保護された伝達方法が提供されます。ユーザ クレデンシャルが格納されたデータベースへの ODBC 接続を設定することにより、レポート ポータル上でデプロイするレポート パッケージからクリア テキストのパスワードを排除できます。

重要: Windows 認証では、Internet Information Server（IIS）と Microsoft SQL Server の両方を使用する必要があります。

Windows 認証で動作するようにレポート ポータルを設定する方法

レポート ポータルのデータベース接続認証モードを変更するために実行する手順を理解すると、Windows 認証でレポート ポータルを実装する際に役に立ちます。

レポート ポータルを Windows 認証用に設定するには、以下の手順を実行します。

1. Microsoft SQL Server 2005 のデータベースを準備して、CMS データベースとして使用します。
2. デフォルトのユーザと照合を使用して、CA Business IntelligenceCMS データベースを準備します。
3. System DSN を作成して、SQL Server 認証を使用するように指定します。

   System DSN はレポート ポータルの CMS データベースに接続するために使用されます。
4. Active Directory ユーザをローカル Administrators グループに追加します。

   このユーザを指定して、レポート ポータルを設定する際に Windows 認証で動作するように認証します。
5. ASP.NET Web Service Extension to Allowed を設定します。
6. レポート ポータル CA Business Intelligence をインストールします (P. 27)。インストール中に以下の手順を実行します。
   a. CA Business Intelligence のカスタム モードでのインストールを選択します。
   b. データベースとして Microsoft SQL Server 2005 を指定します。
   c. Web サーバとして IIS を指定します。
7. レポート ポータルを Windows 認証用に設定します。

   Active Directory ユーザ アカウントを使用して Windows 認証で認証するように CA Business Intelligence サービスを設定します。
8. Windows 認証を使用して、CA Access Control のレポート データベース用の System DSN を作成します。

   System DSN は CA Access Control のレポート ポータルへ接続するために使用されます。
9. レポート ポータルでレポート パッケージをデプロイします。

Windows 認証用のレポート ポータルの設定

レポート ポータルをインストールしたら、Windows 認証で動作するようにレポート ポータルを設定できます。Active Directory のユーザ アカウントを使用するようにレポート ポータルを設定し、さらに System DSN 接続パラメータを変更します。

Windows 認証用にレポート ポータルを設定する方法

1. オペレーティング システムの管理者としてレポート ポータルのホストにログインします。
2. Windows NT 認証に対するレポート ポータル CMS 用に System DSN を変更します。
3. [スタート]-[プログラム]-[BusinessObjects XI Release 2]-[BusinessObjects Enterprise]-[Central Configuration Manager]の順に選択します。

   Central Configuration Manager が開かれて、CA Business Intelligence サービスが表示されます。
4. すべての CA Business Intelligence サービスを停止します。
5. サービスの Log On As 設定を Active Directory のユーザ クレデンシャルに変更します。すべての CA Business Intelligence サービスに対して、これを実行します。

   重要: WinHTTP Web Proxy Auto-Discovery と World Wide Web Publishing サービスの設定は変更しないでください。
6. すべての CA Business Intelligence サービスを開始します。

   これで、レポート ポータルは Windows 認証で認証を行うように設定されています。

   注: Microsoft SQL Server Activity Monitor から、レポート対象のデータベースへの接続で Active Directory のユーザ アカウントが使用されることが確認できます。

例: CA Business Intelligence サービスの Log On As 接続設定の変更

以下の例では、CA Business IntelligenceConnection Server サービスの Log On As クレデンシャルをシステム アカウントから Active Directory アカウントに変更する方法が示されています。

1. リストで Connection Server サービスを右クリックし、[プロパティ]を選択します

   Connection Server サービス プロパティ ウィンドウが表示されます。

2. Log On As セクションで、System Account オプションからマークを削除します。

   接続設定フィールドは有効です。

3. Active Directory ユーザ名とパスワードを入力し、パスワードを確認します。

   例: Domain/username

   [OK]をクリックします。サービス接続設定が変更されます。

4. Central Configuration Manager を終了します。

System DSN 接続設定の例

System DSN 接続設定では、データベースに接続するために必要とされるパラメータが定義されます。以下の例では、インストールされている場合、レポート ポータルでは SQL 認証のサポートだけが行われるので、SQL Server 認証でのユーザ接続を認証する System DSN を作成します。CA Business Intelligence をインストールする前に、CMS データベースの System DSN を設定します。

以下の例では、レポート ポータルの CMS データベース用の System DSN を作成します。

1. [スタート]-[設定]-[コントロール パネル]-[管理ツール]-[データ ソース (ODBC)]の順に選択します。

   ODBC データ ソース アドミニストレータが表示されます。

2. [システム DSN] タブで、[作成]を選択します。

   [Select a New Data Source]ウィンドウが開きます。

3. 下へスクロールして、[SQL Server]を選択してから、[完了]をクリックします。

   [Create a New Data Source to SQL Server]ウィザードが表示されます。

4. 接続名、説明および SQL サーバ名を入力します。[次へ]をクリックします。
5. SQL Server 認証を使用するように選択します。
6. 管理者ユーザのクレデンシャルを入力して、SQL サーバに接続します。[次へ]をクリックします。
7. [Change the default database to option]を選択して、リストからレポート ポータルの CMS データベースを選択します。[次へ]をクリックします。
8. [完了]をクリックします。接続のテストを選択してから、[OK]をクリックします。

   System DSN が作成されます。

Windows 認証で動作するレポート ポータル上でのレポート パッケージのデプロイ

Windows で有効

標準の CA Access Control レポートを使用するには、BusinessObjects InfoView にレポート パッケージ ファイルをインポートする必要があります。

注: この手順では、レポート ポータル上に、同じパッケージの旧バージョンがすでにデプロイされていない場合に、レポート パッケージをデプロイする方法について説明します。

レポート ポータルでレポート パッケージをデプロイする方法

1. 中央データベース、配布サーバ、レポート ポータルが設定されていることを確認します。

   注: JAVA_HOME 変数がレポート ポータル コンピュータ上でセットアップされていることを確認します。

2. CA Access Control のレポート対象データベース用の System DSN を作成して、Windows NT 認証を使用するように指定します。

   作成する System DSN は CA Access Control のレポート対象データベースに接続するために使用されます。System DSN はレポート パッケージを設定する際に指定します。

3. CA Business Intelligence for Windows DVD を光ディスクドライブに挿入し、¥Disk1¥cabi¥biconfig フォルダに移動します。

4. biconfig ディレクトリの中身を一時ディレクトリにコピーします。
5. お使いのオペレーティング システム用の適切な CA Access Control Enterprise Edition サーバ コンポーネント DVD を光ディスクドライブに挿入し、¥ReportPackages フォルダにアクセスします。
6. 以下のファイルを、光ディスクから同じ一時ディレクトリにコピーします。
   - ¥ReportPackages¥*RDBMS*¥*import_biar_config*.xml
   - ¥ReportPackages¥*RDBMS*¥*AC_BIAR_File*.biar

   RDBMS

   CA Access Control レポートで使用される RDBMS のタイプを定義します。

   値: MSSQL2005

   import_biar_config.xml

   使用する RDBMS のインポート構成ファイル(.xml)の名前を定義します。

   値: import_biar_config_mssql_2005.xml

   注: 中央データベースとして MS SQL Server 2008 を使用する場合は、import_biar_config_mssql_2005.xml ファイルを設定します。

   AC_BIAR_File.biar

   使用する言語と RDBMS の CA Access Control レポート ファイル(.biar)の名前を定義します。

   注: 使用する RDBMS 用のインポート設定ファイルの <biar-file name> プロパティは、このファイルを指します。デフォルトでは、RDBMS の英語バージョンの名前に設定されます。
7. *import_biar_config*.xml ファイルのコピーを編集します。以下の XML プロパティを定義します。

   重要: ファイルからユーザ名、パスワードおよびサーバのフィールドを削除します。

   <biar-file name>

   CA Access Control レポート ファイル(.biar)への完全なパス名を定義します。これは前の手順でコピーしたファイルです。

   <networklayer>

   使用する RDBMS でサポートされているネットワーク層を定義します。

   値: ODBC

<rdms>

CA Access Control レポートで使用される RDBMS のタイプを定義します。

値: 汎用 ODBC データ ソース

<datasource>

作成した DSN を定義します。

重要: CA Business Intelligence CMS ではなく、CA Access Control によってレポート用に使用されるデータベースの名前を指定します。

8. コマンド プロンプト ウィンドウを開いて、以下のコマンドを入力します。

```
System_Drive:¥BO¥biconfig.bat -h host_name -u user_name -p password -f
ac_biar_config.xml
```

host_name

レポート ポータルのホスト名を定義します。

user_name

レポート ポータルをインストールした時に設定したレポート ポータル管理者を定義します。

password

レポート ポータル管理者のパスワードを定義します。

例:

```
biconfig.bat -h reportportal.comp.com -u Administrator -p P@ssw0rd -f
C:¥BO¥import_biar_config_mssql_2005.xml
```

例: Windows 認証を使用するように設定された Microsoft SQL Server 2005 Import Configuration ファイル

以下のコード断片が、Windows 認証で動作するレポート ポータル上でデプロイする MS SQL Server 2005 用に編集されたインポート設定ファイル（import_biar_config_mssql2005.xml）の例です。

```
<?xml version="1.0"?>
<biconfig version="1.0">
        <step priority="1">
                <add>
                        <biar-file name="c:¥temp¥biconfig¥
                        AccessControl_R12.5_EN_JP_KR_SQL_6_DEC_2009.biar">
                                <networklayer>ODBC</networklayer>
                                <rdms>Generic ODBC datasource</rdms>
                                <datasource>acdb</datasource>
                        </biar-file>
                </add>
        </step>
</biconfig>
```

大規模デプロイに対する BusinessObjects の設定

大規模デプロイで CA Access Control レポートを実行するには、BusinessObjects のデフォルト設定を変更する必要があります。BusinessObjects ページ サーバで作成できる同時接続の最大数を変更します（デフォルトは 20,000）。また、入力パラメータ選択リストに表示される値の最大数も変更します。

大規模デプロイに対して BusinessObjects を設定する方法

1. BusinessObjects ページ サーバで作成可能な同時接続数を変更します。
   a. レポート ポータルのコンピュータ上で、[スタート]-[プログラム]-[Crystal Enterprise]-[Crystal Configuration Manager]をクリックします。

      BusinessObjects Configuration Manager が開きます。

   b. [Crystal Page Server]を右クリックし、[停止]を選択します。
   c. [Crystal Page Server]を右クリックし、[プロパティ]を選択します。
   d. 実行ファイルへのパスを示すフィールドで、*-restart* の後ろに以下のテキストが表示されていることを確認します。

      ```
      -maxDBResultRecords 0
      ```

   e. BusinessObjects ページ サーバを再起動します。

2. レポート用の入力パラメータ選択リストに表示される値の最大数を変更します。

   a. Windows レジストリ エディタを開きます。

   b. 以下のレジストリ キーに移動します。

      ```
      HKEY_CURRENT_USER/Software/Business Objects/Suite 11.5/Crystal Reports/Database
      ```

   c. [編集]-[新規]-[DWORD 値]をクリックします。

      REG_DWORD タイプの新しいレジストリ エントリが表示されます。

   d. このエントリの名前を「*QPMaxLOVSize*」に変更します。

   e. エントリをダブルクリックして、値データを「1000」に変更します。

      新しいレジストリ エントリが設定されます。

   f. BusinessObjects Central Management Console（CMC）を開きます。

   g. [Servers management area]領域に移動します。

   h. 設定を変更する Web Intelligence Report Server へのリンクをクリックします。

      [Property]タブ内で[Web Intelligence Report Server]ページが開きます。

   i. 以下の値を 1000 を超える値に、または必要数に変更します。

      - [List of Values Batch Size]
      - [Maximum Size of List of Values for Custom Sorting]

      [Apply]をクリックして変更をサブミットし、変更がただちに有効になるようにサーバを再起動します。

CA Business Intelligence への接続を設定します。

CA Access Control エンタープライズ管理 は CA Business Intelligence 共通レポート サーバ（CA Access Control レポート ポータル）を使用して、レポート機能を提供します。レポート ポータルをインストールし、レポートを展開した後に、CA Access Control エンタープライズ管理 から CA Business Intelligence への接続を設定する必要があります。この接続を設定するには Identity Manager 管理コンソールを使用します。

CA Business Intelligence への接続の設定方法

1. Identity Manager 管理コンソールを有効にします。
2. Identity Manager 管理コンソールを開きます。
3. ［環境］-［ac-env］-［詳細設定］-［レポート］をクリックします。

   ［レポート プロパティ］ウィンドウが表示されます。
4. データベースおよび Business Objects のプロパティを入力します。

   重要： CA Business Intelligence Central Management Server（CMS）は内部管理目的のみに使用され、レポートの生成と表示に使用されるレポート データは含まれていません。CMS の詳細については、「*CA Business Intelligence インストール ガイド*」を参照してください。

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

   重要： Business Objects のポート フィールドで、レポート ポータルが使用するポート番号を入力します。デフォルトのポートは 8080 です。Business Objects レポート フォルダ フィールドで、「CA Access Controlr12」と入力します。
5. ［Save］をクリックします。

   CA Business Intelligence 設定が保存されます。

注：CA Business Intelligence の詳細については、CA Technologies サポートから入手可能な「*CA Business Intelligence インストール ガイド*」を参照してください。

スナップショット定義の作成

レポートは、CA Access Control および [assign the value for unab in your book] エンドポイントから収集されて中央データベースに格納されるデータ スナップショット、CA Access Control エンタープライズ管理 からの PUPM データ、ユーザ ストアからデータに基づいて生成されます。

CA Access Control レポートを実行および表示するには、スナップショット定義を作成し、スナップショット データをキャプチャする必要があります。スナップショット定義には、CA Access Control が収集するレポート データおよびデータ収集のスケジュールを指定します。

スナップショット パラメータ XML ファイルは、CA Access Control が収集するレポート データを指定します。デフォルトでは、このファイルで、すべての CA Access Control および [assign the value for unab in your book] エンドポイント、PUPM データ、およびユーザ ストアからのデータをレポート スナップショットに含めるように指定します。スナップショット パラメータ XML ファイルをカスタマイズして、レポート スナップショットの範囲を制限できます。

レポートに常に最新のデータが含まれるようにするには、エンドポイントのスナップショットより頻繁にスナップショットが実行されることのないようにスケジュールを設定します。たとえば、エンドポイントで毎週スナップショットが送信されるように設定し、CA Access Control エンタープライズ管理 で毎日スナップショットがキャプチャされるように設定した場合、レポート データはエンドポイントから週に一度収集されますが、PUPM およびユーザ ストアからは毎日取得されるため、古いエンドポイント データがレポートに含まれることになります。

重要: 複数のスナップショット定義を有効にしないでください。複数のスナップショット定義が有効に設定されている場合、CA Access Control エンタープライズ管理 ではすべてのレポートを正常に実行できません。

注: デフォルトでは、スナップショット定義を作成するには「システム マネージャ」ロールが必要です。

スナップショット定義を作成する方法

1. CA Access Control エンタープライズ管理 で、以下の手順を実行します。
   a. [レポート]をクリックします。
   b. [タスク]サブタブをクリックします。
   c. 左側のタスク メニューで[スナップショット定義の管理]ツリーを展開します。

      [スナップショット定義の作成]タスクが使用可能なタスク リストに表示されます。
2. [スナップショット定義の作成]をクリックします。

   [スナップショット定義の作成: スナップショット定義の選択]ページが表示されます。
3. [OK]をクリックします。

   [スナップショット定義の作成]ページが表示されます。
4. [プロファイル]タブで以下のフィールドに入力します。

   スナップショット定義名

   スナップショット定義の名前を定義します。

   スナップショット定義の説明

   スナップショット定義を説明する追加情報を指定します。

   有効

   CA Access Control エンタープライズ管理 がスナップショット定義を有効にするかどうかを指定します。

   注: このチェック ボックスを選択しない場合、CA Access Control エンタープライズ管理 でスナップショットはキャプチャされず、レポートを表示できません。一度に有効にできるスナップショットは 1 つのみです。

識別子

レポート スナップショットの範囲を定義するスナップショット パラメータ XML ファイルを指定します。

デフォルト: PPM_ALL.xml

過去の保存件数

中央データベースに格納される正常なスナップショットの数を指定します。データベース内のスナップショットの数が指定した数に達すると、CA Access Control は古いスナップショットを削除します。

注: スナップショットの数は 0 より大きい数値にする必要があります。このフィールドの値を指定しない場合、CA Access Control に格納されるスナップショットの数に制限はありません。最大 3 つの正常なスナップショットを格納するよう設定することをお勧めします。

5. [繰り返し]タブをクリックし、[スケジュール]を選択します。

   スケジュール オプションが表示されます。

6. スナップショットの実行時間および繰り返しのパターンを指定し、[サブミット]をクリックします。

   注: スナップショットの実行頻度は、CA Access Control および [assign the value for unab in your book] スナップショットの実行頻度より低くスケジュールすることをお勧めします。

   スケジュールされた時間および頻度でスナップショットがキャプチャされるよう CA Access Control が設定されます。

注: スナップショット定義を作成した後に、オンデマンドでスナップショットをキャプチャするか、スケジュールされた時間と頻度でスナップショットをキャプチャするか選択できます。スナップショット データのキャプチャの詳細については、「*エンタープライズ管理ガイド*」を参照してください。

レポート スナップショットのスコープの制限

CA Access Control エンタープライズ管理 がレポート スナップショットをキャプチャする場合、CA Access Control および [assign the value for unab in your book] エンドポイントのスナップショットからデータを収集します。また、CA Access Control エンタープライズ管理 から PUPM データ、ユーザ ストアからデータを収集します。CA Access Control エンタープライズ管理 はレポート データを収集した後で、中央データベースにデータを格納します。

スナップショット パラメータ XML ファイルは、CA Access Control エンタープライズ管理 が収集するレポート データを指定します。スナップショット パラメータ XML ファイルのカスタマイズによりレポート スナップショットのスコープを制限できます。

たとえば、ユーザ ストアとして Active Directory を使用する場合、CA Access Control エンタープライズ管理 はレポート スナップショットをキャプチャするとき、各 Active Directory ユーザのデータを収集します。この処理には時間がかかる場合があります。スナップショットのキャプチャに要する時間を削減するため、、スナップショット パラメータ XML ファイルのカスタマイズにより Active Directory スナップショットのスコープを制限できます。

レポート スナップショットのスコープを制限する方法

1. 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/config/com/netegrity/config/imrexport/sample
   ```

2. PPM_ALL.xml ファイルをコピーして名前を変更し、同じディレクトリに保存します。

   これで、新しいスナップショット パラメータ XML ファイルが作成されます。

3. 編集可能な形式で新しいスナップショット パラメータ XML ファイルを開きます。

4. <!--IM COLLECTORS--> セクションのエントリを編集し、ユーザ ストアから CA Access Control エンタープライズ管理 が収集するデータのスコープを指定します。

5. <!--PUPM COLLECTORS--> セクション内で、レポート スナップショットに含めない CA Access Control エンタープライズ管理 コンポーネントに該当するエントリを、(!--) および (--) でコメント アウトします。

6. （オプション）Active Directory スナップショットのスコープを制限します。

   a. 「LDAP クエリでレポート スナップショットを制限するしくみ (P. 57)」および「LDAP 構文の考慮事項 (P. 58)」のトピックを確認します。

      これらのトピックの情報は、LDAP クエリを以下の手順で正確に定義する際に役立ちます。

   b. <!--PUPM COLLECTORS--> セクションで、以下のエレメントを検索します。

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
      </export>
      ```

      このエレメントは、スナップショットに含める Active Directory ユーザ データを指定します。

   c. エレメントを以下のように編集します。*ldap_query* は、データを収集するユーザを定義する LDAP クエリを指定します。

      ```
      <export object="com.ca.ppm.export.ADUsersCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

   d. <!--PUPM COLLECTORS--> セクションで、以下のエレメントを検索します。

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
      </export>
      ```

   e. エレメントを以下のように編集します。*ldap_query* は、データを収集するグループを定義する LDAP クエリを指定します。

      ```
      <export object="com.ca.ppm.export.ADGroupsCollector">
              <where attr="%USER" satisfy="ANY">
                      <value op="EQUALS">(ldap_query)</value>
              </where>
      </export>
      ```

      Active Directory スナップショットのスコープが制限されました。

7. 新しいスナップショット パラメータ XML ファイルを保存し、閉じます。

8. 新しいスナップショット パラメータ XML ファイルを使用するために、CA Access Control エンタープライズ管理 のスナップショット定義を変更します。

   キャプチャ スナップショット タスクを実行すると、スナップショット パラメータ XML ファイルで指定したデータのみ収集します。

例: レポート スナップショットのスコープを CA Access Control エンドポイントに制限

PUPM および [assign the value for unab in your book] を使用しない場合、CA Access Control エンドポイントからのみデータを収集するよう、レポート スナップショットのスコープを制限できます。データ収集のスコープを CA Access Control エンドポイントに制限するには、<-- PUPM COLLECTORS --> セクション内の ReportIdMarkerCollector エントリ*以外*のすべてのエントリに (!--) および (--) をコメントします。

以下は、PPM_ALL.xml ファイルのスニペットです。ReportIdMarkerCollector エントリを除く、<-- PUPM COLLECTORS --> セクションのすべてのエントリがコメントに変更されています。

```
<!--  PUPM COLLECTORS -->
        <!-- export object="com.ca.ppm.export.AccountPasswordCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMRolesCollector">
                <exportattr attr="|rolemembers|" />
        </export -->

        <!-- export object="com.ca.ppm.export.
                PrivilegedAccountExceptionCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.PPMPasswordPolicyCollector">
        </export -->

        <!-- export object="com.ca.ppm.export.ADUsersCollector">
        </export -->

        <export object="com.ca.ppm.export.PPMAccountUserAccessCollector">
        </export --!>

        <!-- export object="com.ca.ppm.export.ADGroupsCollector">
                <exportattr attr="|groupmembers|" />
        </export -->

        <export object="com.ca.ppm.export.ReportIdMarkerCollector">
        </export>
```

スナップショット パラメータ XML ファイル構文 -- レポート スナップショットの制限

スナップショット パラメータ XML ファイルは、CA Access Control エンタープライズ管理 が収集するレポート データを指定します。スナップショット パラメータ XML ファイルを編集して、レポート スナップショットの範囲を制限できます。

CA Access Control エンタープライズ管理 が収集するレポート データは、ユーザがスナップショット パラメータ XML ファイルで定義する条件を満たしたオブジェクトのもののみです。ファイル内の各コレクタによって、CA Access Control エンタープライズ管理 が収集するオブジェクト セットを定義します。

各コレクタの構造は以下のようになっています。

```
<export object=" ">
        <where attr=" " satisfy=" ">
                <value> </value>
        </where>
        <exportattr attr=" " />
</export>
```

注: <where>、<value>、<exportattr> エレメントはオプションです。

各コレクタには、以下のエレメントが含まれています。

<export>

CA Access Control エンタープライズ管理 が収集するオブジェクト データを示します。たとえば、<export> エレメントは、CA Access Control エンタープライズ管理 がユーザ データを収集することを指定する場合があります。

<export> エレメントには 1 つ以上の <exportattr> および <where> エレメントを含めることができます。これによって、一定の条件を満たすデータのみを収集できます。<exportattr> または <where> エレメントをまったく指定しない場合、CA Access Control エンタープライズ管理 はオブジェクトのすべてのデータを収集します。

<export> エレメントには object パラメータしかありません。

<where>

<value> エレメントで定義された条件に基づいて、収集されたデータをフィルタします。<where> エレメントには 1 つ以上の <value> エレメントが必要です。また、複数の <where> エレメントを指定して、フィルタを絞り込むことができます (エレメントは OR エレメントとして機能します)。

以下の表では、<where> エレメントのパラメータについて説明します。

パラメータ	説明
attr	フィルタに使用する属性を示します。
satisfy	収集するオブジェクトまたは属性について、値の評価の一部または全部を満たす必要があるかどうかを示します。 ■ ALL - 属性またはオブジェクトは値の評価のすべてを満たす必要があります。 ■ ANY - 属性またはオブジェクトは 1 つ以上の値の評価を満たす必要があります。

<value>

<where> エレメントで、収集される属性またはオブジェクトが満たす必要がある条件を定義します。<value> エレメントには operator（op）パラメータが必要です。operator には EQUALS または CONTAINS を指定します。

注: スナップショット パラメータ XML ファイルの <!--PUPM COLLECTORS--> セクションで、<value> エレメントに LDAP 構文を使用できます。LDAP 構文によって、CA Access Control エンタープライズ管理 が Active Directory から収集する ユーザおよびグループのデータを指定できます。

<exportattr>

収集する特定の属性を示します。<exportattr> エレメントを使用して、収集するオブジェクトの属性のサブセットを収集します。たとえば、ユーザの ID のみを収集する場合、<exportattr> エレメントを使用できます。

<exportattr> エレメントには attr パラメータがあります。

以下の表は、<where> エレメントまたは <exportattr> エレメントで使用できる属性を、オブジェクトごとに示しています。

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
role	name 属性を使ってフィルタリングできます。 name - フィルタ基準を満たす名前が付けられたロール	以下の属性のいずれかを収集できます。 ■ |tasks| - ロールに関連付けられているすべてのタスク ■ |rules| - ロールに適用されるすべてのメンバ、管理、所有者、およびスコープルール ■ |users| - ロールのすべてのメンバ、管理者、および所有者 ■ |rolemembers| - すべてのロール メンバ ■ |roleadmins| - すべてのロール管理者 ■ |roleowners| - すべてのロール所有者
ユーザ	汎用属性またはフィジカル アトリビュート、および以下の属性のいずれか。 ■ |groups| - グループのメンバ ■ |roles| - ロールのメンバ ■ |orgs| - フィルタ基準を満たす組織にプロファイルが存在するユーザ	以下の属性のいずれかを収集できます。 ■ |all_attributes| - すべての使用可能なユーザ属性 ■ |groups| - ユーザがメンバまたは管理者であるすべてのグループ ■ |roles| ― ユーザがメンバ、管理者、または所有者であるすべてのロール

オブジェクト	<where> エレメントで使用できる属性	<exportattr> エレメントで使用できる属性
group	汎用属性またはフィジカル アトリビュート、あるいは以下の属性。 |groups| - フィルタ基準を満たすグループ内の、ネストされたグループのリスト	汎用属性または物理属性、あるいは以下の属性のいずれかを収集できます。 ■ |all_attributes| - ディレクトリ設定ファイル（directory.xml）で Group オブジェクトに定義されたすべての属性 ■ |groups| - グループ内のすべてのネストされたグループ ■ |users| - グループのすべてのメンバ ■ |groupadmins| - 指定したグループの管理者であるすべてのユーザ ■ |groupmembers| - 指定したグループのメンバであるすべてのユーザ ■ |users| - すべてのグループ管理者とグループ メンバ
organization	汎用属性またはフィジカル アトリビュート	汎用属性または物理属性、あるいは以下の属性のいずれかを収集できます。 ■ |all_attributes| - ディレクトリ設定ファイル（directory.xml）で Organization オブジェクトに定義されたすべての属性 ■ |orgs| - 組織内のすべてのネストされた組織 ■ |groups| - 組織内のすべてのグループ ■ |users| - 組織内のすべてのユーザ

レポート スナップショットで LDAP クエリがユーザおよびグループ データを制限する仕組み

Active Directory をユーザ ストアとして使用する場合、レポート スナップショットでキャプチャされたユーザおよびグループ データを指定できます。

ユーザ別またはグループ別に Active Directory データをフィルタリングするスナップショット パラメータ XML ファイルで LDAP クエリを使用できます。ただし、ロール メンバシップ別に Active Directory データをフィルタリングする LDAP クエリは使用できません。LDAP クエリを使用できるのは、スナップショット パラメータ XML ファイルの <!--PUPM COLLECTORS--> でのみです。

以下のプロセスでは、スナップショット パラメータ XML ファイル内の LDAP クエリが、CA Access Control エンタープライズ管理 が収集する Active Directory データをどのように制限するかについて説明します。この情報によって、レポート スナップショットを制限する、適切な LDAP クエリを記述できます。

CA Access Control エンタープライズ管理 が Active Directory レポート スナップショットをキャプチャする際に、以下を行います。

1. 以下のエレメント内の LDAP クエリで指定されている Active Directory ユーザのみのデータを収集します。

   ```
   <export object="com.ca.ppm.export.ADUsersCollector">
   ```

   エレメントに LDAP クエリが含まれていない場合、CA Access Control エンタープライズ管理 はすべての Active Directory ユーザのデータをスナップショットに含めます。

2. 以下のエレメント内の LDAP クエリで指定されている Active Directory グループのみのデータを収集します。

   ```
   <export object="com.ca.ppm.export.ADGroupsCollector">
   ```

   エレメントに LDAP クエリが含まれていない場合、CA Access Control エンタープライズ管理 はすべての Active Directory グループのデータをスナップショットに含めます。

   注: CA Access Control エンタープライズ管理 は、ステップ 1 でクエリによって返されなかったユーザのデータは収集しません。ユーザがステップ 2 でクエリによって返されるグループのメンバであるが、ユーザがステップ 1 のクエリによって返されない場合、CA Access Control エンタープライズ管理 はそのユーザのデータを Active Directory スナップショットに含めません。

LDAP 構文の考慮事項

Active Directory スナップショットのスコープを制限する LDAP クエリを記述する際に、以下を考慮します。

- LDAP クエリで以下の論理演算子を使用できます。
  - EQUAL TO (=)
  - OR (|)
  - AND (&)

    注: 一部の制限は、アンパサンド(&)文字の使用に適用されます。
  - NOT (!)
  - ワイルドカード(*)
- アンパサンド文字(&)と左山形かっこ(<)は、以下の状況でのみ使用できます。
  - マークアップ区切り文字として
  - コメント内で
  - 処理命令内で
  - CDATA セクション内で

他の状況でアンパサンド文字を表すには、文字列「**&**」または Unicode 文字参照を使用します。他の状況で左山形かっこ文字を表すには、文字列「**<**」または Unicode 文字参照を使用します。

- 右山形かっこ文字(>)は、CDATA セクションの終わりを示す文字列(]]>)でのみ使用できます。

  他の状況で右山形かっこ文字を表すには、文字列「**>**」または Unicode 文字参照を使用します。

例: アンパサンド文字

以下のスナップショット パラメータ XML ファイルの一部では、レポート スナップショットに Active Directory ユーザ データをすべて含めるように指定しています。この LDAP クエリの一部では、アンパサンドを表すために & 文字列を使用しています。

```
<export object ="com.ca.ppm.export.ADUsersCollector">
        <where attr="%USER%" satisfy="ANY">
                <value op="EQUALS">(&amp;(objectClass=user))</value>
        </where>
</export>
```

第 5 章: CA Access Control for Virtual Environments REST API

このセクションには、以下のトピックが含まれています。

REST-based API

REST (Representational State Transfer) は、URL でアクセス可能なオブジェクトの状態を作成および変更するために、ハイパーメディアの固有のプロパティに依存するソフトウェアのアーキテクチャ スタイルの特徴を表します。

RESTful シナリオでは、ドキュメント (オブジェクトの状態を表す) がクライアントとサービスの間で交換されます。これは、どちらの側も 1 つの要求または応答に含まれているエンティティ以外については一切認識していないという前提で行われます。

REST-based API のスキーマを取得するには、以下の URL にアクセスし、空のページのソースを参照します。

`https://hostname:18443/iam/api/1.0/restapi/schemas`

注: スキーマの詳細については、このセクションの例を参照してください。

REST-based 認証

CA Access Control for Virtual Environments REST 要求には、要求情報の一部として認証情報が含まれます。CA Access Control for Virtual Environments は HTTP 基本認証方式をサポートします。たとえば、以下の基本認証を使用できます。

```
Authorization: Basic c3VwZXJhZG1pbjpkZWZhdWx0c3VwZXJhZG1pbjpkZWZhdWx0
```

上記の例は、ユーザ "superadmin" およびパスワード "default" の Base 64 エンコーディングを表しています。

タグの取得

すべてのタグのリストを取得するには、GET コマンドを使用してすべてのタグを取得します。

HTTP GET 要求を以下の URL に送信します。

```
https://hostname:18443/iam/api/1.0/restapi/environment/ac/tags
```

特定のタグを取得するには、以下のように GET コマンドを使用してタグ名を指定します。

HTTP GET 要求を以下の URL に送信します。

```
https://hostname:18443/iam/api/1.0/restapi/environment/ac/tags/<tag_name>
```

タグの作成

タグを作成するには POST コマンドを使用します。

HTTP POST 要求を以下の URL に送信します。

```
https://hostname:18443/iam/api/1.0/restapi/environments/ac/tags
```

HTTP 本文には、タグを作成するために以下の情報が含まれている必要があります。

```
<Tag>
  <Name>Tag Name</Name>
  <Description>Tag Description</Description>
</Tag>
```

<Name>

タグ名を指定します

<Description>

タグの説明を指定します

タグの変更

タグを変更して、管理対象デバイスにタグを割り当てたり、タグを削除することができます。

次の手順に従ってください:

1. GET コマンドを使用して、タグの状態を取得します。

   `https://hostname:18443/iam/api/1.0/restapi/environments/ac/<tag_name>`

   以下のような XML 応答ドキュメントが返ります。

```
<Tag>
  <Name>testtag</Name>
  <Description />
  <Devices>
    <Device>
      <ID>vm-11</ID>
    </Device>
  </Devices>
</Tag>
```

2. 変更されたタグでデバイスを更新します。

   HTTP PUT コマンドを以下の URL に送信します。

   `https://hostname:18443/iam/api/1.0/restapi/environments/ac/<tag_name>`

タグの削除

タグを削除するには、DELETE コマンドを使用します。

HTTP DELETE 要求を以下の URL に送信します。

`https://hostname:18443/iam/api/1.0/restapi/environments/ac/tags/</tag_name>`

管理対象デバイスへのタグ付け

管理対象デバイスにタグを付けて、そのマシンをセキュリティ グループに追加してリモートで管理することができます。

次の手順に従ってください:

1. CA Access Control for Virtual Environments が管理対象デバイスに使用する ID を取得します。

   CA Access Control for Virtual Environments が管理対象デバイスに使用する ID を取得するには、REST 要求を使用し、フィルタを使用してデバイス詳細を取得します。例:

   ```
   https://hostname:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394
   ```

   注: 前述の例では、VMware MOB (Managed Object Browser) に定義されるように、フィルタリング パラメータとして vCenter UUID および VM UUID を渡しています。

   以下のような XML 応答ドキュメントが返ります。

   ```
   <Devices>
     <Device>
       <ID>vm-19</ID>
       <ParentID>esx-3</ParentID>
       <Name>ESXi in a box</Name>
       <Type>VirtualMachine</Type>
       <VirtualMachineProperties>
         <ManagedObjectID>vm-394</ManagedObjectID>

   <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObjectVCenterUUID>
         <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
         <GuestOSArchitecture>X86</GuestOSArchitecture>
         <GuestOSDescription>Red Hat Enterprise Linux 5 (64-bit)</GuestOSDescription>
       </VirtualMachineProperties>
       <SecurityGroups>
         <SecurityGroup>
           <ID>sg-13</ID>
           <Name>weiig01esxi01.ca.com</Name>
           <Description/>
           <Owner>superadmin</Owner>
         </SecurityGroup>
   ```

```
      <SecurityGroup>
        <ID>sg-15</ID>
        <Name>Discovered virtual machine</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
      <SecurityGroup>
        <ID>sg-22</ID>
        <Name>vSphere in a box</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
    </SecurityGroups>
  </Device>
</Devices>
```

デバイスの ID は XML 応答ファイルに指定されているとおり vm-19 です。

2. 割り当てられたタグでデバイスを更新します。

   HTTP PUT コマンドを以下の URL に送信します。

   ```
   https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/<managed_device_ID>
   ```

   注: HTTP コンテンツには、新しく割り当てられたタグ情報だけでなく、デバイスの既存のプロパティがすべて含まれている必要があります。既存のプロパティを取得するには、デバイスの CA Access Control for Virtual Environments ID をフィルタするときに、XML 応答ファイルから <Device> タグと </Device> タグの間にあるデータをコピーします。

   新しいタグ関係を含む HTTP コンテンツの例:

   ```
   <Device>
     <ID>vm-19</ID>
     <ParentID>esx-3</ParentID>
     <Name>ESXi in a box</Name>
     <Type>VirtualMachine</Type>
     <VirtualMachineProperties>
       <ManagedObjectID>vm-394</ManagedObjectID>

   <ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObject
   VCenterUUID>
       <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
       <GuestOSArchitecture>X86</GuestOSArchitecture>
       <GuestOSDescription>Red Hat Enterprise Linux 5
   (64-bit)</GuestOSDescription>
     </VirtualMachineProperties>
   ```

```
<Tags>
  <Tag>
    <Name>testtag</Name>
    <Description>testtag2 description</Description>
  </Tag>
</Tags>
<SecurityGroups>
  <SecurityGroup>
    <ID>sg-13</ID>
    <Name>weiig01esxi01.ca.com</Name>
    <Description/>
    <Owner>superadmin</Owner>
  </SecurityGroup>
  <SecurityGroup>
    <ID>sg-15</ID>
    <Name>Discovered virtual machine</Name>
    <Description/>
    <Owner>superadmin</Owner>
  </SecurityGroup>
  <SecurityGroup>
    <ID>sg-22</ID>
    <Name>vSphere in a box</Name>
    <Description/>
    <Owner>superadmin</Owner>
  </SecurityGroup>
</SecurityGroups>
</Device>
```

管理対象デバイスからのタグの削除

管理対象デバイス上のタグを削除して、そのデバイスをセキュリティグループから削除できます。

次の手順に従ってください:

1. CA Access Control for Virtual Environments が管理対象デバイスに使用する ID を取得します。

   CA Access Control for Virtual Environments が管理対象デバイスに使用する ID を取得するには、フィルタを使用します。例:

   ```
   https://hostname:18443/iam/api/1.0/restapi/environments/ac/devices?managed-object-vcenter-uuid=54E79C3A-49D5-4958-A983-8B919F470CEC&managed-object-id=vm-394
   ```

   注: 前述の例では、VMware MOB（Managed Object Browser）に定義されるように、vCenter UUID および VM UUID を渡しています。

以下のような XML 応答ドキュメントが返ります。

```
<Devices>
  <Device>
    <ID>vm-19</ID>
    <ParentID>esx-3</ParentID>
    <Name>ESXi in a box</Name>
    <Type>VirtualMachine</Type>
    <VirtualMachineProperties>
      <ManagedObjectID>vm-394</ManagedObjectID>

<ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-8B919F470CEC</ManagedObject
VCenterUUID>
      <GuestOSVersion>LINUX_REDHAT_5</GuestOSVersion>
      <GuestOSArchitecture>X86</GuestOSArchitecture>
      <GuestOSDescription>Red Hat Enterprise Linux 5
(64-bit)</GuestOSDescription>
    </VirtualMachineProperties>
    <SecurityGroups>
      <SecurityGroup>
        <ID>sg-13</ID>
        <Name>weiig01esxi01.ca.com</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
      <SecurityGroup>
        <ID>sg-15</ID>
        <Name>Discovered virtual machine</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
      <SecurityGroup>
        <ID>sg-22</ID>
        <Name>vSphere in a box</Name>
        <Description/>
        <Owner>superadmin</Owner>
      </SecurityGroup>
    </SecurityGroups>
  </Device>
</Devices>
```

デバイスの ID は XML 応答ファイルに指定されているとおり vm-19 です。

2. 以下のとおり、デバイスを更新してタグを削除します。

   a. 手順 1 の XML 応答ファイルを編集し、<Tags> から </Tags> タグまでにあるコンテンツをすべて削除します。

   b. HTTP PUT コマンドを使用して、更新された XML ファイルを以下の URL に送信します。

      ```
      https://<host>:18443/iam/api/1.0/restapi/environments/ac/devices/vm-19
      ```

例 : HTTP スキーマ

サポートされた REST-based API コマンドのスキーマ例を以下に示します。

- HTTP POST :

  ```
  POST /iam/api/1.0/restapi/environments/ac/tags HTTP/1.1
  Content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Cache-Control: no-cache
  Pragma: no-cache
  Host: 10.112.196.244
  Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
  Connection: keep-alive
  Content-Length: 79

  <Tag><Name>testtag</Name><Description>testtag2
  description</Description></Tag>
  ```

- HTTP GET :

  ```
  GET /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Host: 10.112.196.169:9998
  ```

- HTTP PUT :

  ```
  PUT /iam/api/1.0/restapi/environments/ac/devices/vm-19 HTTP/1.1
  Content-type: application/xml; charset=UTF-8
  Authorization: Basic YWRtaW46ZGVmYXVsdA==
  Cache-Control: no-cache
  Pragma: no-cache
  Host: 10.112.196.244
  Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
  Connection: keep-alive
  Content-Length: 959
  ```

```
<Devices><Device><ID>vm-19</ID><ParentID>esx-3</ParentID><Name>ESXi in a
box</Name><Type>VirtualMachine</Type><VirtualMachineProperties><ManagedObject
ID>vm-394</ManagedObjectID><ManagedObjectVCenterUUID>54E79C3A-49D5-4958-A983-
8B919F470CEC</ManagedObjectVCenterUUID><GuestOSVersion>LINUX_REDHAT_5</GuestO
SVersion><GuestOSArchitecture>X86</GuestOSArchitecture><GuestOSDescription>Re
d Hat Enterprise Linux 5
(64-bit)</GuestOSDescription></VirtualMachineProperties><Tags><Tag><Name>test
tag</Name><Description>testtag2
description</Description></Tag></Tags><SecurityGroups><SecurityGroup><ID>sg-1
3</ID><Name>weiig01esxi01.ca.com</Name><Description/><Owner>superadmin</Owner
></SecurityGroup><SecurityGroup><ID>sg-15</ID><Name>Discovered virtual
machine</Name><Description/><Owner>superadmin</Owner></SecurityGroup><Securit
yGroup><ID>sg-22</ID><Name>vSphere in a
box</Name><Description/><Owner>superadmin</Owner></SecurityGroup></SecurityGr
oups></Device></Devices>
```

- HTTP DELETE:

```
DELETE /iam/api/1.0/restapi/environments/ac/tags/testtag HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
```