CA Access Control Premium Edition

ObserveIT Enterprise 統合ガイド

12.6

サードパーティに関する通知

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

サンプル スクリプトおよびサンプル SDK コード

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

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

CA Technologies 製品リファレンス

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

- CA Access Control Premium Edition
- CA Access Control
- CA Single Sign-On（eTrust SSO）
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM、旧 Unicenter NSM and Unicenter TNG）
- CA Software Delivery（旧 Unicenter Software Delivery）
- Unicenter Service Desk（旧 Unicenter Service Desk）
- [assign the value for UARM in your book]（旧 [set the CALM variable for 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*}
…	前の項目または項目のグループが繰り返し可能なことを示します
下線	デフォルト値
スペースに続く、行末の円記号（¥）	本書では、コマンドの記述が 1 行に収まらない場合があります。このような場合、行末の空白とそれに続く円記号（¥）は、そのコマンドが次の行に続くことを示します。 **注**：このような円記号はコピーしないでください。また、改行はコマンドに含めないようにしてください。これらの文字は、実際のコマンド構文の一部ではありません。

例：コマンドの表記規則

以下のコードは、本書でのコマンド表記規則の使用方法を示しています。

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

この例の内容

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

ファイル ロケーションに関する規則

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

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

CA への連絡先

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

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、ObserveIT Enterprise セッション記録プログラムを CA Access Control Premium Edition に統合する方法を説明しています。このガイドでは、PUPM セッションを記録するために行うプロセスと手順を説明しています。

このガイドは、CA Access Control を使用するセキュリティ管理者およびシステム管理者の方で、ObserveIT Enterprise のセッション記録プログラムの機能を活用したい方を対象にしています。

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

ObserveIT の統合について

CA Access Control 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。記録が開始されるのは、ユーザが特権アカウント パスワードをチェックアウトするとき、およびエンドポイントにログインするときで、終了するのは、セッションが終了するときです (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き)。

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。

第 2 章: 統合のセットアップ

このセクションには、以下のトピックが含まれています。

統合をセットアップする方法

CA Access Control を ObserveIT Enterprise セッション記録ソフトウェアに統合するには、いくつかの手順を実行する必要があります。統合が終了すると、PUPM セッションはすべて ObserveIT Enterprise ソフトウェアによって記録されます。

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。

統合をセットアップするには、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 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。

統合を準備するには、以下の手順を実行します。

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 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。