CA Access Control 高级版

ObserveIT Enterprise 集成指南

12.6

第三方通知

示例脚本和示例 SDK 代码

CA Access Control 产品随附的示例脚本和示例 SDK 代码均“按原样”提供，仅供参考之用。 在特定环境下，可能需要对它们进行调整，而且在生产系统中部署它们之前，未经事先测试和验证不应将其用于生产。

CA Technologies 不向这些示例提供支持，而且对于这些脚本可能会引起的任何错误概不负责。

CA Technologies 产品引用

本文档引用以下 CA Technologies 产品：

- CA Access Control 高级版
- CA Access Control
- CA Single Sign-On (eTrust SSO)
- CA Top Secret®
- CA ACF2™
- CA Audit
- CA Network and Systems Management（CA NSM，以前为 Unicenter NSM 和 Unicenter TNG）
- CA Software Delivery（以前为 Unicenter Software Delivery）
- Unicenter Service Desk（以前为 Unicenter Service Desk）
- [assign the value for UARM in your book]（以前是 [set the CALM variable for your book]）
- Identity Manager

文档约定

CA Access Control 文档使用以下约定：

格式	含义
等宽字体	代码或程序输出
斜体	重点或新术语
粗体	必须完全按照显示内容键入的文本
正斜杠 (/)	用于描述 UNIX 和 Windows 路径的独立于平台的目录分隔符

文档在解释命令语法和用户输入（以等宽字体显示）时还会使用以下特殊约定：

格式	含义
斜体	您必须提供的信息

格式	含义
用方括号括起来 ([])	可选运算符
用大括号括起来 ({})	强制运算符集
用管道符 (|) 分隔的选项。	分隔可选运算符（选择一项）。 例如：下面的示例*既*可以表示用户名，*也*可以表示组名： `{username|groupname}`
...	指明前面的项或项组可以重复
下划线	默认值
前面带空格的行尾反斜杠 (\)	有时，在本指南中，一行无法容纳一个命令。 在这些情况下，行结尾处的空格加上反斜杠 (\) 就表示该命令延续到下一行。 **注意：**请勿复制反斜杠字符，并且请省略换行符。 这些不是实际命令语法的一部分。

示例：命令表示法约定

下面的代码说明了在本指南中使用命令约定的方式：

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

在该示例中：

- 命令名称 (ruler) 以常规等宽字体显示，必须按照显示内容键入。
- *className* 选项以斜体显示，因为它是一个类名（例如 USER）的占位符。
- 即使不带有方括号中的第二部分，您也可以运行该命令，方括号表示该运算符是可选的。
- 使用可选参数 (props) 时，可以选择关键字 *all*，也可以指定一个或多个属性名（以逗号分隔）。

文件位置约定

CA Access Control 文档使用以下文件位置约定：

- *ACInstallDir*—默认 CA Access Control 安装目录。
  - Windows—[set the Installation Path variable]
  - UNIX—[set the alternate Installation Path variable]

- *ACSharedDir*—CA Access Control for UNIX 使用的默认目录。
  - UNIX—/opt/CA/AccessControlShared
- *ACServerInstallDir*—默认 CA Access Control 企业管理 安装目录。
  - /opt/CA/AccessControlServer
- *DistServerInstallDir*—默认分发服务器安装目录。
  - /opt/CA/DistributionServer
- *JBoss_HOME*—默认 JBoss 安装目录。
  - /opt/jboss-4.2.3.GA

联系技术支持

要获取在线技术帮助以及办公地址、主要服务时间和电话号码的完整列表，请联系技术支持：http://www.ca.com/worldwide。

目录

第 1 章： 简介

此部分包含以下主题：

关于本指南

该指南向您说明如何将 CA Access Control 高级版 与 ObserveIT Enterprise 会话记录程序相集成。 该指南说明您要记录 PUPM 会话所执行的过程和步骤。

本指南面向要使用 CA Access Control 且想要充分利用 ObserveIT Enterprise 会话记录程序功能的安全管理员和系统管理员而编写。

为了简化术语，在本指南中我们将此产品称为 CA Access Control。

关于 ObserveIT 集成

CA Access Control 与 ObserveIT Enterprise 的 集成可扩展您对由特权帐户针对您组织中的服务器进行访问尝试的控制。 ObserveIT Enterprise 会话记录软件会记录目标系统上的用户活动。 当用户签出特权帐户密码并登录到端点时将开始记录，而在会话终止时（例如，当用户签入该特权帐户密码时）会结束记录。

已纪录的会话存储在您准备的专用数据库中。 您可以使用 ObserveIT 查看器，从 CA Access Control 企业管理 直接重放已纪录的会话。

您可以从以下链接中的 ObserveIT 系统获取 ObserveIT Enterprise 会话记录程序：

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

注意：有关 ObserveIT 的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 ObserveIT 文档。

第 2 章： 设置该集成

此部分包含以下主题：

如何设置该集成

将 CA Access Control 与 ObserveIT Enterprise 会话记录软件相集成需要您采取几个步骤。 在集成结束时，ObserveIT Enterprise 软件会记录所有的 PUPM 会话。

注意：有关如何完成步骤 1 - 5 的更多信息，请参阅 ObserveIT 安装介质上的 ObserveIT Enterprise 文档。

执行以下操作来设置集成：

1. 查看 ObserveIT Enterprise 系统和安装要求。

   确认您使用的服务器满足安装 ObserveIT Enterprise 的最低系统要求。

2. 准备中央数据库

   已纪录的会话存储在专用的 Microsoft SQL Server 上。

3. 配置 Internet Information Server (IIS)。

   ObserveIT Enterprise 应用程序服务器使用 IIS 来处理代理发送的元数据。

4. 安装 ObserveIT Enterprise 服务器组件。

   ObserveIT 应用程序服务器、代理和管理控制台也进行安装。

5. 配置 ObserveIT Enterprise 应用程序服务器。

   配置记录设置。

6. 在企业管理服务器上部署会话记录脚本。

   脚本会启用触发会话记录的 PUPM 自动登录。

7. 创建服务帐户。

   创建要使用的企业管理服务器服务帐户

8. 定义到 CA Access Control 企业管理 中的 ObserveIT Enterprise 应用程序服务器的连接。

   配置连接设置来启用会话记录。

如何准备集成

在完成 ObserveIT Enterprise 应用程序服务器的安装后，准备用于 CA Access Control 集成的服务器。 在准备 ObserveIT Enterprise 应用程序服务器后，服务器已配置为开始记录和保存 PUPM 会话。

执行以下操作来准备集成：

1. 打开管理控制台。
2. 创建服务帐户。

   CA Access Control 使用服务帐户连接到 ObserveIT Enterprise 应用程序服务器。

打开管理控制台

在安装和开始 ObserveIT Enterprise 之后，您可以启动基于 Web 的管理控制台。

打开管理控制台

1. 使用浏览器打开 ObserveIT Enterprise 管理控制台。 输入以下 URL：

   http://observeit_server_name:port/ObserveIT

   示例：

   http://observeit_server:4884/ObserveIT

2. 使用您在安装过程中指定的管理员凭据进行登录。

   此时打开 ObserveIT Enterprise 管理控制台。

注意：您也可以通过依次单击“开始”、“程序”、“ObserveIT”、“ObserveIT WebConsole”打开 ObserveIT Enterprise 管理控制台。

创建服务帐户

CA Access Control 企业管理 使用服务帐户来验证 ObserveIT Enterprise 应用程序服务器以便记录用户活动。 当在 CA Access Control 企业管理 中配置 ObserveIT Enterprise 应用程序服务器连接设置时，提供服务帐户凭据。

创建服务帐户

1. 在 ObserveIT Enterprise 管理控制台中，依次选择“配置”、“控制台用户”。

   此时打开控制台用户屏幕。

2. 选择“创建用户”。

   此时打开“添加控制台用户”窗口。

3. 输入用户名、密码，然后确认密码。
4. 将身份验证方法设为“ObserveIT.Authentication”，将用户角色设为“Admin”。
5. 单击“添加”。

   服务帐户即被创建。

注意：有关用户管理的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

部署会话记录脚本

用户会话记录与 PUPM 自动登录协同工作。 当用户签出特权帐户密码并选择登录到端点时，会打开一个远程管理软件并自动让用户登录。 CA Access Control 企业管理 通过使用基于端点类型的会话记录脚本来控制远程管理程序。

例如，当用户选择登录到 Windows 端点时，CA Access Control 企业管理 使用的脚本会打开远程桌面软件来连接到端点。

要记录 ObserveIT Enterprise 应用程序服务器上的会话，您要在企业管理服务器上部署会话记录脚本。

部署会话记录脚本

1. 从 CA 支持网站中下载会话记录脚本，并将其保存在临时目录中。
2. 在企业管理服务器上，导航到以下目录，其中 *JBoss_HOME* 指定了安装 JBoss 的目录：

   JBoss_HOME/server/default/deploy/IdentityMinder.ear/config/sso_scripts

3. 将会话记录脚本复制到 sso_scripts 目录。

   建议您在覆盖该目录中的文件之前先进行备份。

4. 选择使用新文件覆盖现有文件。

现在，您可以配置到 ObserveIT Enterprise 应用程序服务器的连接设置。

定义到 ObserveIT 的连接

为了完成与 ObserveIT Enterprise 的集成，您配置 CA Access Control 企业管理 中到 ObserveIT Enterprise 应用程序服务器的连接设置。

定义到 ObserveIT 的连接

1. 在 CA Access Control 企业管理 中，依次选择“系统”、“连接管理”、“会话记录”、“创建连接”。

   将显示“创建连接”屏幕。

2. 输入以下详细信息：

   连接说明

   定义连接的自由文本说明

   播放 URL

   定义 ObserveIT Enterprise 应用程序服务器 URL

   示例： http://observeit_host:4884/observeit/

   用户 ID

   定义服务帐户用户名

   密码

   定义服务帐户密码

   高级

   指定以下高级连接设置：

   查看器页面

   指定是否显示一条消息，表示该会话记录在屏幕的顶端

   查看器参数

   指定 ObserveIt 查看器窗口的宽度和高度

ActiveX URL

指定 ObserveIT Enterprise ActiveX 文件所在位置的完整路径名。 默认情况下，指定到 ObserveIT 应用程序服务器的 URL。

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

服务器 URL

指定 ObserveIT Enterprise 应用程序服务器存储已纪录会话的位置的完整路径名。默认情况下，指定到 ObserveIT 应用程序服务器的 URL。

示例： http://observeit_host:4884/ObserveITApplicationServer

3. 单击“提交”。

CA Access Control 企业管理 将创建连接。

第 3 章： 记录 PUPM 会话

此部分包含以下主题：

如何记录会话

每个 PUPM 会话都被记录下来并存储在 ObserveIT Enterprise 数据库上。每个会话都被分为单个的片段，您可以从整个纪录的会话中分别播放。

以下过程说明了如何记录 PUPM 会话：

1. 用户从 CA Access Control 企业管理 中签出特权帐户密码，并选择自动登录到端点。

   如果这是首次使用该选项，用户需要安装 ActiveX。
2. 此时打开一个远程管理会话，而用户无需输入密码即可登录。
3. 安装在端点上的 ObserveIT 代理开始记录用户活动，并将片段发送到 ObserveIT Enterprise 应用程序服务器，该服务器将数据保存在数据库中。
4. 用户关闭远程管理会话，而 ObserveIT 代理也停止记录。
5. 已纪录的会话在 CA Access Control 企业管理 中显示。

重要说明！ 要使 Internet Explorer 能够下载 ActiveX，请在“本地 Intranet 区域”或“受信任区域”中指定 ObserveIT Enterprise 主机名，然后将“下载已签名的 ActiveX 控件”安全选项设为“启用”。

注意：有关会话记录的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

记录会话的位置

ObserveIT Enterprise 应用程序服务器将 PUPM 会话记录到专用的 Microsoft SQL Server 上。 ObserveIT 数据库服务器使用两个专用的数据库。 第一个数据库命名为 ObserveIT，承载着配置和元数据。 第二个数据库命名为 ObserveIT_Data，存储 ObserveIT 代理在已纪录会话期间收集的快照。

注意：有关会话记录的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

播放会话

从 CA Access Control 企业管理 播放已纪录的 PUPM 会话。 当选择播放会话时，CA Access Control 企业管理 在新窗口中播放已纪录的会话。 播放器窗口中包含用来导航该会话的控制按钮。 您还可以在已纪录的会话中执行自由的文本搜索。

注意：有关自由文本搜索的更多信息，请参阅位于 ObserveIT Enterprise 安装介质上的 *ObserveIT 文档*。

播放会话

1. 在 CA Access Control 企业管理 中，依次选择“特权帐户”、“审核子任务”。

   此时“审核特权帐户”任务显示在可用任务的列表中。

2. 选择“审核特权帐户”

   此时打开“审核特权帐户”搜索窗口。

   注意：确认已为您分配了 PUPM 审核管理员角色。

3. 指定搜索标准、输入要显示的行数，然后单击“搜索”。

   将显示满足您搜索标准的任务。

4. 单击会话详细信息列中的播放图标可播放该会话。

   此时打开播放器窗口，从会话的开头播放该会话。

   注意：使用窗口底部的控件可导航该会话。