CA User Activity Reporting Module

Guía de la API de automatización virtual de UARM r12.5

r12.5.02

Referencias a productos de CA Technologies

En este documento se hace referencia a los siguientes productos de CA Technologies:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- Centro de comandos de seguridad de CA (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Información de contacto del servicio de Asistencia técnica

Para obtener asistencia técnica en línea, una lista completa de direcciones y el horario de servicio principal, acceda a la sección de Asistencia técnica en la dirección http://www.ca.com/worldwide.

Contenido

Capítulo 1: Acerca de esta guía

La *Guía* de la API de automatización virtual de
CA User Activity Reporting Module proporciona las instrucciones para la utilización de la API de automatización virtual de arquitectura REST en la configuración de la recopilación de registros desde máquinas virtuales.

Esta guía está diseñada para administradores o diseñadores Web que tengan conocimientos generales sobre el uso y la estructura de las API, consultas de CA User Activity Reporting Module y el refinamiento de eventos. Deberán disponer de acceso de administrador a CA User Activity Reporting Module y a otros productos de terceros o de CA necesarios.

Los servicios de REST utilizan el protocolo HTTP para toda la comunicación. Es necesario tener conocimientos tanto del protocolo HTTP como de la arquitectura REST (Transferencia de Estado Representacional).

Capítulo 2: Acerca de la API de automatización virtual

La API de automatización virtual permite implementar la recopilación de eventos en máquinas virtuales mediante CA User Activity Reporting Module. Puede utilizarse para activar un perfil de recopilación prestablecido que contenga toda la información necesaria para la recopilación de eventos.

También puede utilizarse para establecer credenciales de acceso para la recopilación de eventos, la identificación de recursos disponibles y para otras funciones relacionadas.

Más información:

Descripción general de la API de automatización virtual (en la página 10)
Estructura de la API de automatización virtual (en la página 11)

Descripción general de la API de automatización virtual

Para utilizar la API de automatización virtual, invoque métodos HTTP en los recursos, cada uno de los cuales tiene su propio URI. La API utiliza los métodos HTTP siguientes:

- POST: crea un recurso, proporcionando los parámetros del recurso en el cuerpo de un mensaje. Puede utilizarse este método para implementar la recopilación de eventos en máquinas virtuales.
- GET: recupera la representación actual de un recurso. Puede utilizarse este método para obtener una lista de clientes o información acerca de una implementación.
- PUT: actualiza un recurso reemplazando la representación del recurso actual por la representación proporcionada en el cuerpo del mensaje. Puede utilizarse para cambiar las credenciales existentes del origen del evento.
- DELETE: suprime un recurso. Puede utilizarse para detener la recopilación de eventos.

Proporcione un usuario y contraseña o un nombre de certificado y contraseña de CA User Activity Reporting Module válidos en cada llamada de la API. Realice esta acción mediante la autenticación básica de HTTP (el encabezado de autorización).

Por ejemplo, puede utilizar los métodos disponibles para implementar y controlar la recopilación de eventos del modo siguiente:

1. Implemente un conector e inicie la recopilación de eventos en una máquina virtual mediante el método POST en el recurso corregido "/deploycollection". POST crea un recurso que representa el origen del evento.

   Este método devuelve un URI para el nuevo recurso.
2. Compruebe el estado del origen del evento mediante GET en el URI del recurso.
3. Elimine el origen del evento, si es necesario, mediante DELETE en el mismo URI.

Algunos recursos son compatibles con varios métodos HTTP, otros son compatibles solamente con uno. La documentación de cada uno identifica los métodos compatibles.

Estructura de la API de automatización virtual

Todos los URI de los recursos para la API de automatización virtual tienen una estructura definida, como se muestra en el ejemplo siguiente:

```
https://nombre_host:8443/rest/am/1/collectionprofiles
```

La primera parte del URI identifica el servidor de destino. Reemplace nombre_host por el nombre del servidor de CA User Activity Reporting Module con el cual desea contactar.

La segunda parte del URI, /rest/am/1, es una parte común entre todos los recursos del servidor. 1 especifica la versión de la API a la cual desea acceder.

El tercer elemento define el recurso al cual desea acceder, en este caso /collectionprofiles.

Pueden devolverse o enviar datos en formato XML o JSON. Para especificar el formato de devolución de los datos, incluya valores en el encabezado de aceptación del método HTTP para especificar el formato deseado:

- Accept: application/xml
- Accept: application/json

Para especificar el formato de envío de los datos mediante PUT o POST, utilice el encabezado de tipo de contenido del método HTTP:

- Content-Type: application/xml
- Content-Type: application/json

Nota: Todos los ejemplos de la API presentes en esta guía se muestran mediante el cliente HTTP de la línea de comandos cURL.

Capítulo 3: Ejemplos de la API de automatización virtual

Esta sección contiene los siguientes temas:

Enumeración de clientes

La clasificación de clientes en el entorno virtual de
CA User Activity Reporting Module permite al usuario identificar los clientes disponibles para la implementación de la recopilación de eventos.

Métodos compatibles: GET

```
GET curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml"
"https://nombre_host:8443/rest/am/1/tenants"
```

Devuelve:

```
<tenants>

    <tenant>

        <name>Valor predeterminado</name>

        <description>El cliente predeterminado</description>

    </tenant>

    <tenant>

        <name>Cliente1</name>

        <description>Descripción del primer cliente</description>

    </tenant>

    <tenant>

        <name>Cliente 2</name>

        <description>Descripción del segundo cliente</description>

    </tenant>

</tenants>
```

Enumeración de perfiles de recopilación (/collectionprofiles)

Puede utilizarse esta llamada para devolver una lista de los perfiles de recopilación de eventos disponibles. Cada perfil contiene la información requerida para configurar la recopilación de eventos en un origen de evento específico.

Nota: Los perfiles de la recopilación de eventos se configuran desde la interfaz de usuario de CA User Activity Reporting Module. Para obtener más información acerca de los perfiles de recopilación de eventos, consulte la Ayuda en línea de CA User Activity Reporting Module.

Métodos compatibles: GET

```
GET curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml"
"https://nombre_host:8443/rest/am/1/collectionprofiles"
```

Devuelve:

```
<collectionProfiles>

    <collectionProfile>

        <name>Cliente 1 - Linux</name>

        <description>Recopila los eventos syslog de Linux para el primer
cliente</description>

        <credentialsRequired>falso</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Cliente 1 - Windows</name>

        <description>Recopila los eventos WinRM para el primer
cliente</description>

        <credentialsRequired>verdadero</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Cliente 2 - HPUX</name>

        <description>Recopila los eventos syslog de HPUX para el segundo
cliente</description>

        <credentialsRequired>falso</credentialsRequired>

    </collectionProfile>
```

```
</collectionProfiles>
```

El elemento credentialsRequired indica si debe enviarse el ID de usuario y la contraseña del origen del evento durante la implementación:

- El valor es verdadero en el caso de recopilación activa (o extracción). Por ejemplo los conectores WinRM obtienen los orígenes del evento como método de información.
- El valor es falso en el caso de recopilación pasiva (o inserción). Por ejemplo, el servidor de Syslog envía datos directamente a CA User Activity Reporting Module.

Implementación de la recopilación (/deploycollection)

Puede utilizarse la API para implementar la recopilación de eventos en máquinas virtuales. Incluye el cuerpo de un mensaje especificando el perfil del evento que desea utilizarse.

Nota: Los perfiles de la recopilación de eventos se configuran desde la interfaz de usuario de CA User Activity Reporting Module. Para obtener más información acerca de los perfiles de recopilación de eventos, consulte la Ayuda en línea de CA User Activity Reporting Module.

El procedimiento siguiente muestra cómo implementar una recopilación mediante la utilidad cURL.

Follow these steps:

1. Cree un archivo de texto llamado deploy.txt que contenga los parámetros de la implementación:

```
<deploymentRequest>
<tenant>Valor predeterminado</tenant><profile>prueba de
syslog</profile><host>syslogsource.ca.com</host><ip>10.0.0.0</ip><credentials
><user>root</user><password>contraseña_raíz</password></credentials></deploym
entRequest>
```

   Están disponibles los parámetros siguientes:

   <tenant>

   Nombra el cliente virtual en el cual desea implementarse la recopilación de eventos. Para obtener una lista de los clientes disponibles, utilice /tenants.

   <profile>

   Nombra el perfil de recopilación de eventos que desea utilizarse. Para obtener una lista de los perfiles disponibles, utilice /collectionprofiles.

   <host>

   Nombra el origen del evento para la recopilación de eventos.

   <ip>

   Especifica la dirección IP del origen del evento para la recopilación de eventos.

   <credentials>

Contiene los elementos que proporcionan el nombre del usuario y la contraseña para el acceso al origen del evento. Este elemento solamente es necesario para perfiles de conexión establecidos para el requerimiento de credenciales.

2. Abra una ventana de la línea de comandos y vaya al directorio donde guardó el archivo de texto.
3. Introduzca el comando siguiente:

   ```
   curl -u usuario_elm:contraseña_elm-k -H "Accept: application/xml" –H
   "Content-Type: application/xml" –X POST –d @deploy.txt
   "https://nombre_host:8443/rest/am/1/deploycollection"
   ```

   El elemento -d @deploy.txt proporciona el contenido del archivo de texto en el cuerpo de la solicitud.

Si la implementación es correcta, el usuario recibe un mensaje HTTP 201 (CREATED):

```
HTTP/1.1 201 Created
Location: http://myelmhost:8443/rest/agentgroups/Agents/agents/014589ec-4b97-
4179-8778-65b1671996f8/connectors/1cde5aa8-e11c-4c36-b7cc-
712477c9f52f/sources/10.0.0.0
Content-Type: application/xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<eventTarget>
    <host>10.0.0.0</host>
    <tcpPort>1468</tcpPort>
    <udpPort>40514</udpPort>
</eventTarget>
```

La respuesta muestra el URI del recurso implementado después de Location.

Esta información puede utilizarse para modificar o suprimir la implementación. En el ejemplo anterior, el recurso implementado es un conector pasivo, de modo que aparece el elemento eventTarget. EventTarget muestra el puerto y la dirección IP del conector, permitiendo así la configuración del origen del evento para la transmisión de los eventos al destino correcto.

Si no hay suficiente capacidad en el grupo de agentes seleccionado, aparece un mensaje de error (HTTP 507).

Llamadas al ID de origen (/<sourceid>)

El recurso <sourceid> representa un origen de evento de CA User Activity Reporting Module. Puede devolverse la información acerca del recurso o eliminarla. Esta última acción detiene la recopilación de eventos desde el origen de evento correspondiente.

Métodos compatibles: GET y DELETE.

Más información:

Identificación de recursos (en la página 20)
Eliminación de recursos (en la página 21)

Identificación de recursos

GET permite identificar recursos que representan orígenes de evento y obtener información acerca de ellos. Esta llamada devuelve información acerca del origen en el URI especificado. Esta ruta se obtiene del resultado de una llamada /deploycollection.

```
GET curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml"
"https://nombre_host:8443/rest/am/1/agentgroups/<groupid>/agents/<agentid>/connec
tors/<connid>/sources/<sourceid>
```

En su entorno, reemplace la ruta del URI de muestra /agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid> por la ruta del recurso deseado.

Esta llamada devuelve:

```
<connectorSource>
    <id>e94523c9-65a3-4510-87cb-fc693ffce966</id>
    <integration>Syslog</integration>
    <integrationVersion>12.5.5203.0</integrationVersion>
    <deploymentPending>falso</deploymentPending>
    <target>
        <host>calmdev06</host>
        <tcpPort>1468</tcpPort>
        <udpPort>40514</udpPort>
    </target>
</connectorSource>
```

Cuando el valor deploymentPending es verdadero, significa que se ha vuelto a configurar el agente y que actualmente no está disponible para la realización de algunas operaciones.

Eliminación de recursos

Puede eliminarse un recurso que representa el origen de un evento mediante DELETE. Esta llamada suprime el recurso especificado y detiene la recopilación de eventos. La ruta del URI se obtiene del resultado de una llamada /deploycollection.

```
DELETE curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml"
"https:/nombre_host:8443/rest/am/1//agentgroups/<groupid>/agents/<agentid>/connec
tors/<connid>/sources/<sourceid>
```

En su entorno, reemplace la ruta del URI de muestra /agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid> por la ruta del recurso deseado.

Una vez realizada la supresión, la llamada devuelve una confirmación (HTTP 200).

Llamadas de credenciales (/credentials)

El recurso /credentials representa el nombre de usuario y la contraseña que utiliza un conector para acceder al origen de un evento. Puede recuperarse información acerca de las credenciales o actualizarla.

Métodos compatibles: GET y PUT.

Más información:

Enumeración de credenciales (en la página 22)
Reemplazo de credenciales (en la página 23)

Enumeración de credenciales

Pueden recuperarse las credenciales utilizadas por un conector implementado para acceder al origen de un evento. La respuesta muestra el nombre del usuario y la contraseña. Esta llamada solamente es válida para conectores activos. En el caso de conectores pasivos, aparece el error HTTP 404.

```
GET curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml"
"https://nombre_host:8443/rest/am/1/agentgroups/<groupid>/agents/<agentid>/connec
tors/<connid>/sources/<sourceid>/credentials
```

En su entorno, reemplace la ruta del URI de muestra /agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid> por la ruta del recurso deseado.

Esta llamada devuelve:

```
<credentials>
    <user>root</user>
    <password>contraseña</password>
    <domain>nombre_dominio</domain>
</credentials>
```

El valor del dominio opcional solamente se utiliza para credenciales de Windows.

Reemplazo de credenciales

Pueden reemplazarse las credenciales existentes. Esta llamada solamente es válida para conectores activos. En el caso de conectores pasivos, aparece el error HTTP 404.

```
curl -u usuario_elm:contraseña_elm -k -H "Accept: application/xml" –H "Content-Type: application/xml" –X PUT –d <credentials><user>root</user><password>contraseña</password><domain>nombre_dominio</domain></credentials> "https://nombre_host:8443/rest/am/1/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>/credentials
```

En su entorno, reemplace la ruta del URI de muestra /agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid> por la ruta del recurso deseado.

En este caso, la opción -d especifica la nueva representación para el recurso directamente en la línea de comandos.

Nota: Este ejemplo contiene el valor del dominio que solamente se requiere para credenciales de Windows.