CA User Activity Reporting Module

Handbuch zur API der virtuellen Automatisierung

Version 12.5.03

CA Technologies-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von 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
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Technischer Support – Kontaktinformationen

Wenn Sie technische Unterstützung für dieses Produkt benötigen, wenden Sie sich an den Technischen Support unter http://www.ca.com/worldwide. Dort finden Sie eine Liste mit Standorten und Telefonnummern sowie Informationen zu den Bürozeiten.

Inhalt

Kapitel 1: Über dieses Handbuch

Das *Handbuch zur API der virtuellen Automatisierung für CA User Activity Reporting Module* stellt Anweisungen bereit, um die REST-Architektur der API der virtuellen Automatisierung zu verwenden, mit der die Protokollerfassung von virtuellen Computern eingerichtet wird.

Das Handbuch wurde für Administratoren oder Webdesigner entwickelt, die mit der API-Grundstruktur und deren Verwendung sowie mit CA User Activity Reporting Module-Abfragen und Ereignisverfeinerung vertraut sind. Sie benötigen einen Administratorzugriff auf CA User Activity Reporting Module und andere Drittanbieter- oder CA-Produkte.

REST-Services verwenden das HTTP-Protokoll für die gesamte Kommunikation. Es ist erforderlich, dass Sie sowohl mit dem HTTP-Protokoll als auch mit der REST-Architektur (Representational State Transfer) vertraut sind.

Kapitel 2: Informationen zur API der virtuellen Automatisierung

Die API der virtuellen Automatisierung ermöglicht es Ihnen, Ereigniserfassung für virtuelle Computer mithilfe von CA User Activity Reporting Module bereitzustellen. Sie können die API verwenden, um ein voreingestelltes Erfassungsprofil auszulösen, das alle erforderlichen Informationen für die Bereitstellung der Ereigniserfassung enthält.

Sie können auch die API verwenden, um Anmeldedaten für Ereigniserfassung festzulegen, verfügbare Ressourcen und andere verwandte Funktionen zu identifizieren.

Weitere Informationen:

Übersicht zur API der virtuellen Automatisierung (siehe Seite 10)
Struktur der API der virtuellen Automatisierung (siehe Seite 11)

Übersicht zur API der virtuellen Automatisierung

Um die virtuelle API zu verwenden, rufen Sie HTTP-Methoden gegen Ressourcen auf, die jeweils über einen eigenen URI verfügen. Die API verwendet folgende HTTP-Methoden:

- POST - erstellt eine Ressource und stellt dabei die Ressourcenparameter in einem Nachrichtentext bereit. Sie können diese Methode verwenden, um Ereigniserfassung für einen virtuellen Computer bereitzustellen.
- GET - ruft eine aktuelle Darstellung einer Ressource ab. Sie können diese Methode verwenden, um eine Liste von Mandanten oder Informationen zur Bereitstellung abzurufen.
- PUT - aktualisiert eine Ressource, die aktuelle Ressourcendarstellung durch denjenigen ersetzend, den Sie im Meldungstext liefern. Sie können diese Methode verwenden, um vorhandene Anmeldeinformationen der Ereignisquellen zu ändern.
- DELETE - löscht eine Ressource. Sie können diese Methode verwenden, um Ereigniserfassung anzuhalten.

Geben Sie bei jedem API-Aufruf einen gültigen
CA User Activity Reporting Module-Benutzer und ein Kennwort oder einen Zertifikatnamen und ein Kennwort an. Verwenden Sie dafür eine HTTP-Standardauthentifizierung (Autorisierungsheader).

Sie können beispielsweise die verfügbaren Methoden verwenden, um die Ereigniserfassung bereitzustellen und auf diese Weise zu steuern:

1. Stellen Sie einen Connector bereit und starten Sie die Ereigniserfassung auf einem virtuellen Computer, indem Sie "POST" zur festen Ressource "/deploycollection" verwenden. "POST" erstellt eine Ressource, die Ihre Ereignisquelle darstellt.

   Diese Methode gibt einen URI für die neue Ressource zurück.
2. Überprüfen Sie den Status der Ereignisquelle, indem Sie "GET" gegen den Ressource-URI verwenden.
3. Entfernen Sie im Bedarfsfall die Ereignisquelle, indem Sie "DELETE" gegen den gleichen URI verwenden.

Einige Ressourcen unterstützen mehrere HTTP-Methoden, andere unterstützen nur eine. Die Dokumentation identifiziert die unterstützten Methoden.

Struktur der API der virtuellen Automatisierung

Alle Ressourcen-URIs für die virtuelle API haben eine definierte Struktur, wie im folgenden Beispiel illustriert:

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

Der erste Teil des URI identifiziert den Zielserver. Ersetzen Sie "hostname" durch den Namen des CA User Activity Reporting Module-Servers, zu dem Sie eine Verbindung herstellen möchten.

Der zweite Teil des URI, "/rest/am/1" ist für alle Ressourcen auf diesem Server gebräuchlich. Die "1" gibt die API-Version an, auf die Sie zugreifen möchten.

Das dritte Element definiert die Ressource, auf die Sie zugreifen möchten, in diesem Fall "/collectionprofiles".

Sie können Daten entweder im XML- oder JSON-Format zurückgeben oder senden. Um das Format der Datenrückgabe festzulegen, schließen Sie Werte in den HTTP-Accept-Header ein, um das von Ihnen gewünschte Format anzugeben:

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

Um das Datenformat festzulegen, das Sie mithilfe von "PUT" oder "POST" gesendet haben, verwenden Sie den HTTP-Content-Type-Header:

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

Hinweis: Alle API-Beispiele in diesem Handbuch werden mithilfe des HTTP-Client der cURL-Befehlszeile angezeigt.

Kapitel 3: API der virtuellen Automatisierung - Beispiele

Dieses Kapitel enthält folgende Themen:

Auflisten von Mandanten

Sie können Mandanten in Ihrer virtuellen CA User Activity Reporting Module-Umgebung auflisten und somit die verfügbaren Mandanten für die Bereitstellung der Ereigniserfassung identifizieren.

Unterstützte Methoden: GET

```
GET curl -u elm_user:elm_password -k -H "Accept: application/xml"
"https://hostname:8443/rest/am/1/tenants"
```

Gibt Folgendes zurück:

```
<tenants>

    <tenant>

        <name>Default</name>

        <description>The default Tenant</description>

    </tenant>

    <teant>

        <name>Tenant1</name>

        <description>Text description of the first tenant</description>

    </tenant>

    <tenant>

        <name>Tenant 2</name>

        <description>Text description of the second tenant</description>

    </tenant>

</tenants>
```

Auflisten von Erfassungsprofilen (/collectionprofiles)

Sie können diesen Aufruf verwenden, um eine Liste der verfügbaren Ereigniserfassungsprofile zurückzugeben. Jedes Profil enthält die erforderlichen Informationen, um die Ereigniserfassung auf einer spezifischen Ereignisquelle zu konfigurieren.

Hinweis: Ereigniserfassungsprofile werden über die CA User Activity Reporting Module-Benutzeroberfläche konfiguriert. Weitere Informationen zur Konfiguration der Ereigniserfassungsprofile finden Sie in der CA User Activity Reporting Module-Online-Hilfe.

Unterstützte Methoden: GET

```
GET curl -u elm_user:elm_password -k -H "Accept: application/xml"
"https://hostname:8443/rest/am/1/collectionprofiles"
```

Gibt Folgendes zurück:

```
<collectionProfiles>

    <collectionProfile>

        <name>Tenant1 - Linux</name>

        <description>Collects Linux syslog events for the first
tenant</description>

        <credentialsRequired>false</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Tenant1 Windows</name>

        <description>Collects WinRM events for the first tenant</description>

        <credentialsRequired>true</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Tenant2 HPUX</name>

        <description>Collects HPUX syslog events for the second
tenant</description>

        <credentialsRequired>false</credentialsRequired>

    </collectionProfile>
```

```
</collectionProfiles>
```

Das Element "credentialsRequired" zeigt an, ob Sie während der Bereitstellung eine Benutzer-ID der Ereignisquelle und ein Kennwort übermitteln müssen:

- Dieser Wert ist "true", wenn eine aktive (oder Pull-) Erfassung vorliegt, wie z. B. ein WinRM-Connector, der Ereignisquellen für Informationen abfragt.
- Dieser Wert ist "false", wenn eine passive (oder Push-) Erfassung vorliegt, wie z B. ein Syslog-Server, der Daten direkt an CA User Activity Reporting Module sendet.

Bereitstellen von Erfassungen (/deploycollection)

Sie können diese API verwenden, um Ereigniserfassung auf einem virtuellen Computer bereitzustellen. Fügen Sie einen Nachrichtentext ein, in dem Sie angeben, welches Ereignisprofil Sie verwenden möchten.

Hinweis: Ereigniserfassungsprofile werden über die CA User Activity Reporting Module-Benutzeroberfläche konfiguriert. Weitere Informationen zur Konfiguration der Ereigniserfassungsprofile finden Sie in der CA User Activity Reporting Module-Online-Hilfe.

Der folgende Vorgang veranschaulicht, wie eine Erfassung mithilfe des cURL-Hilfsprogramms bereitgestellt wird.

Gehen Sie wie folgt vor:

1. Erstellen Sie eine Textdatei mit dem Namen "deploy.txt", die die Bereitstellungsparameter enthält:

   ```
   <deploymentRequest>
   <tenant>Default</tenant><profile>syslog
   test</profile><host>syslogsource.ca.com</host><ip>10.0.0.0</ip><credentials><
   user>root</user><password>rootpw</password></credentials></deploymentRequest>
   ```

   Folgende Parameter sind verfügbar:

   <tenant>

   Benennt den virtuellen Mandanten, auf dem Sie die Ereigniserfassung bereitstellen möchten. Sie können mithilfe von "/tenants" eine Liste der verfügbaren Mandanten abrufen.

   <profile>

   Benennt das Ereigniserfassungsprofil, das Sie verwenden möchten. Sie können mithilfe von "/collectionprofiles" eine Liste der verfügbaren Mandanten abrufen.

   <host>

   Benennt die Ereignisquelle, von der Sie Ereignisse erfassen möchten.

   <ip>

   Gibt die IP-Adresse der Ereignisquelle an, von der Sie Ereignisse erfassen möchten.

   <credentials>

   Enthält die Elemente, die den Benutzernamen und das Kennwort für den Zugriff auf die Ereignisquelle bereitstellen. Dieses Element ist nur für Verbindungsprofile erforderlich, die festgelegt werden, um Anmeldeinformationen zu erfordern.

2. Öffnen Sie eine Eingabeaufforderung, und wechseln Sie in das Verzeichnis, in dem die Textdatei gespeichert haben.

3. Geben Sie folgenden Befehl ein:

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

   Das Element "-d @deploy.txt" stellt den Inhalt der Textdatei im Nachrichtentext der Anforderung bereit.

Wenn die Bereitstellung erfolgreich ist, erhalten Sie eine HTTP 201-Nachricht (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>
```

Die Antwort zeigt nach "Location:" den URI der bereitgestellten Ressource an.

Diese Informationen können verwendet werden, um die Bereitstellung zu ändern oder zu löschen. Im vorangehenden Beispiel ist die bereitgestellte Ressource ein passiver Connector, sodass das Element "eventTarget" angezeigt wird. "EventTarget" zeigt Informationen des Ports und der IP-Adresse für den Connector an und ermöglicht es Ihnen, die Ereignisquelle zu konfigurieren, um Ereignisse zum richtigen Ziel zu übertragen.

Wenn in der ausgewählten Agentengruppe nicht genügend Kapazität vorhanden ist, wird eine Fehlermeldung (HTTP 507) angezeigt.

Quellen-ID-Aufrufe (/<sourceid>)

Die Ressource "<sourceid>" stellt eine CA User Activity Reporting Module-Ereignisquelle dar. Sie können Informationen über die Ressource zurückgeben, oder sie entfernen, wodurch die Ereigniserfassung von der entsprechenden Ereignisquelle angehalten wird.

Unterstützte Methoden: GET, DELETE

Weitere Informationen:

Identifizieren einer Ressource (siehe Seite 19)
Ressource löschen (siehe Seite 20)

Identifizieren einer Ressource

Sie können Ressourcen, die Ereignisquellen darstellen, identifizieren und Informationen zur Verwendung von "GET" abrufen. Dieser Aufruf gibt Informationen zur Quelle an den angegebenen URI-Pfad zurück. Dieser Pfad wird aus dem Ergebnis eines "/deploycollection"-Aufruf abgeleitet.

```
GET curl -u elm_user:elm_password -k -H "Accept: application/xml"
"https://hostname:8443/rest/am/1/agentgroups/<groupid>/agents/<agentid>/connector
s/<connid>/sources/<sourceid>
```

Ersetzen Sie in Ihrer Umgebung den URI-Beispielpfad "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" mit dem Pfad für die gewünschte Ressource.

Dieser Aufruf gibt Folgendes zurück:

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

Wenn der Wert "deploymentPending" "true" ist, bedeutet dies, dass der Agent neu konfiguriert wird und für viele Vorgänge gegenwärtig nicht verfügbar ist.

Ressource löschen

Sie können eine Ressource, die eine Ereignisquelle darstellt, mithilfe von "DELETE" entfernen. Dieser Aufruf löscht die angegebene Ressource und hält die Ereigniserfassung zurück. Der URI-Pfad wird aus dem Ergebnis des Aufrufs "/deploycollection" abgeleitet.

```
DELETE curl -u elm_user:elm_password -k -H "Accept: application/xml"
"https://hostname:8443/rest/am/1//agentgroups/<groupid>/agents/<agentid>/connecto
rs/<connid>/sources/<sourceid>
```

Ersetzen Sie in Ihrer Umgebung den URI-Beispielpfad "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" mit dem Pfad für die gewünschte Ressource.

Der Aufruf gibt eine Bestätigung (HTTP 200) zurück, wenn die Löschung abgeschlossen ist.

Aufrufe der Anmeldeinformationen (/credentials)

Die Ressource "/credentials" stellt den Benutzernamen und das Kennwort dar, das von einem Connector verwendet wird, um auf eine Ereignisquelle zuzugreifen. Sie können Informationen zur Anmeldung abrufen oder aktualisieren.

Unterstützte Methoden: GET, PUT

Weitere Informationen:

Auflisten von Anmeldeinformationen (siehe Seite 21)
Ersetzen der Anmeldeinformationen (siehe Seite 22)

Auflisten von Anmeldeinformationen

Sie können Anmeldeinformationen abrufen, die von einem bereitgestellten Connector verwendet werden, um auf eine Ereignisquelle zuzugreifen. Die Antwort zeigt den Benutzernamen und das Kennwort an. Dieser Aufruf ist nur für aktive Connectors zulässig. Ein HTTP 404-Fehler wird für passive Connectors angezeigt.

```
GET curl -u elm_user:elm_password -k -H "Accept: application/xml"
"https://hostname:8443/rest/am/1/agentgroups/<groupid>/agents/<agentid>/connector
s/<connid>/sources/<sourceid>/credentials
```

Ersetzen Sie in Ihrer Umgebung den URI-Beispielpfad "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" mit dem Pfad für die gewünschte Ressource.

Dieser Aufruf gibt Folgendes zurück:

```
<credentials>
    <user>root</user>
    <password>password</password>
    <domain>domain_name</domain>
</credentials>
```

Der optionale Domänenwert wird nur für Anmeldeinformationen von Windows verwendet.

Ersetzen der Anmeldeinformationen

Sie können vorhandene Anmeldeinformationen ersetzen. Dieser Aufruf ist nur für aktive Connectors zulässig. Ein HTTP 404-Fehler wird für passive Connectors angezeigt.

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

Ersetzen Sie in Ihrer Umgebung den URI-Beispielpfad "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" mit dem Pfad für die gewünschte Ressource.

In diesem Fall legt die Option "–d" die neue Darstellung für die Ressource direkt in der Befehlszeile fest.

Hinweis: Dieses Beispiel enthält den Domänenwert, der nur für Anmeldeinformationen von Windows erforderlich ist.