CA User Activity Reporting Module

Manuel de l'API virtuelle d'automatisation

Version 12.5.03

La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2011 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA Access Control
- CA Audit
- CA Technologies ACF2™
- CA Directory
- CA Technologies Embedded Entitlements Manager (CA Technologies EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- Poste de service CA
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1 : A propos de ce manuel

Le Manuel *API virtuelle d'automatisation de CA User Activity Reporting Module* fournit des instructions pour l'utilisation de l'API d'automatisation virtuelle de l'architecture REST pour configurer la collecte de journaux à partir d'ordinateurs virtuels.

Ce manuel est destiné aux administrateurs ou aux concepteurs de sites Web ayant une bonne connaissance de la structure de base des API et de leur utilisation ainsi que des requêtes CA User Activity Reporting Module et de l'ajustement d'événements. Ils doivent disposer de droits d'administrateur pour accéder à CA User Activity Reporting Module et aux autres produits tiers ou CA requis.

Les services REST utilisent le protocole HTTP pour l'ensemble des communications. Une bonne connaissance du protocole HTTP et de l'architecture REST (Representational State Transfer) est requise.

Chapitre 2 : A propos de l'API virtuelle d'automatisation

L'API virtuelle d'automatisation permet de déployer la collecte d'événements pour des ordinateurs virtuels exécutant CA User Activity Reporting Module. Cette API permet de déclencher un profil de collecte prédéfini, contenant toutes les informations nécessaires au provisionnement de la collecte d'événements.

Vous pouvez également utiliser l'API pour définir des informations d'identification d'accès pour la collecte d'événements, identifier les ressources disponibles et exécuter d'autres fonctions associées.

Informations complémentaires :

Présentation de l'API virtuelle d'automatisation (page 10)
Structure de l'API virtuelle d'automatisation (page 11)

Présentation de l'API virtuelle d'automatisation

Pour utiliser l'API virtuelle, appelez des méthodes HTTP par rapport aux ressources, chacune disposant de son propre URI. L'API utilise les méthodes HTTP suivantes :

- POST : crée une ressource, en indiquant les paramètres de ressource dans le corps du message. Vous pouvez utiliser cette méthode pour déployer la collecte d'événements pour un ordinateur virtuel.
- GET : récupère la représentation en cours d'une ressource. Vous pouvez utiliser cette méthode pour obtenir une liste de clients hébergés ou des informations concernant un déploiement.
- PUT : met à jour une ressource, en remplaçant sa représentation actuelle par celle indiquée dans le corps du message. Cette méthode permet de changer les informations d'identification de sources d'événements existantes.
- DELETE : supprime une ressource. Vous pouvez utiliser cette méthode pour arrêter la collecte d'événements.

Indiquez un utilisateur et un mot de passe CA User Activity Reporting Module valides, ou un nom de certificat et un mot de passe, lors ce chaque appel d'API, à l'aide de l'authentification de base HTTP (en-tête de l'autorisation).

Par exemple, vous pouvez utiliser les méthodes disponibles pour déployer et contrôler la collecte d'événements comme suit :

1. Déployez un connecteur et lancez la collecte d'événements sur un ordinateur virtuel à l'aide de la méthode POST vers la ressource spécifique "/deploycollection". La méthode POST crée une ressource qui représente votre source d'événements

   et renvoie un URI à cette nouvelle ressource.
2. Vérifiez le statut de la source d'événements, à l'aide de la méthode GET avec l'URI de la ressource.
3. Supprimez la source d'événements, si nécessaire, à l'aide de la méthode DELETE avec le même URI.

Certaines ressources prennent en charge plusieurs méthodes HTTP, d'autres uniquement une. La documentation de chacune d'elles identifie les méthodes prises en charge.

Structure de l'API virtuelle d'automatisation

Tous les URI de ressource de l'API virtuel disposent d'une structure définie, comme dans l'exemple suivant :
`https://nomd'hôte:8443/rest/am/1/profilsdecollecte`

La première partie de l'URI identifie le serveur cible. Remplacez nomd'hôte par le nom du serveur CA User Activity Reporting Module que vous voulez contacter.

La deuxième partie de l'URI, "/rest/am/1" est commune à toutes les ressources sur ce serveur. "1" spécifie la version de l'API à laquelle vous voulez accéder.

Le troisième élément définit la ressource à laquelle vous voulez accéder, dans ce cas "/profil de collecte".

Vous pouvez renvoyer ou envoyer des données au format XML ou JSON. Pour spécifier le format de renvoi des données, incluez des valeurs dans l'en-tête d'acceptation HTTP :

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

Pour spécifier le format d'envoi de données que vous envoyez à l'aide de la méthode PUT ou POST, utilisez l'en-tête de type de content HTTP :

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

Remarque : Tous les exemples d'API de ce manuel sont affichés à l'aide du client HTTP de la ligne de commande cURL.

Chapitre 3 : Exemples d'API virtuelle d'automatisation

Ce chapitre traite des sujets suivants :

Liste de clients hébergés

Vous pouvez répertorier les clients hébergés de votre environnement virtuel CA User Activity Reporting Module, afin d'identifier ceux disponibles pour le déploiement de la collecte d'événements.

Méthodes prises en charge : GET

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

Renvoie :

```
<clients hébergés>

    <client hébergé>

        <nom>valeur par défaut</nom>

        <description>client hébergé</description>

    </client hébergé>

    <client hébergé>

        <name>Tenant1</name>

        <description>Texte de description du premier client hébergé</description>

    </client hébergé>

    <client hébergé>

        <Nom>client hébergé 2</nom>

        <description>Texte de description du deuxième client
hébergé</description>

    </client hébergé>

</clients hébergés>
```

Liste de profils de collecte (/collectionprofiles)

Cet appel permet de renvoyer une liste des profils de collecte d'événements disponibles. Chaque profil contient les informations requises pour la configuration d'une collecte d'événements sur une source d'événements spécifique.

Remarque : Les profils de collecte d'événements sont configurés à partir de l'interface utilisateur CA User Activity Reporting Module. Pour plus d'informations sur la configuration des profils de collecte d'événements, consultez l'Aide en ligne de CA User Activity Reporting Module .

Méthodes prises en charge : GET

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

Renvoie :

```
<collectionProfiles>

    <collectionProfile>

        <name> Client hébergé1 - Linux</name>

        <description>Collecte les événements Syslog pour Linux du premier client
hébergé</description>

        <credentialsRequired>false</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Client hébergé1 Windows</name>

        <description>Collecte les événements WinRM du premier client
```

```
hébergé</description>

        <credentialsRequired>true</credentialsRequired>

    </collectionProfile>

    <collectionProfile>

        <name>Client hébergé2 HPUX</name>

        <description>Collecte les événements HPUX du deuxième client
hébergé</description>

        <credentialsRequired>false</credentialsRequired>

    </collectionProfile>

</collectionProfiles>
```

L'élément credentialsRequired indique si vous devez soumettre l'ID d'utilisateur et le mot de passe de la source d'événements pendant le déploiement :

- Cette valeur est définie sur true dans le cas d'une collecte active (ou de réception) par exemple un connecteur WinRM qui interroge des sources d'événements pour obtenir des informations.
- Cette valeur est définie sur false dans le cas d'une collecte passive (ou de distribution), par exemple d'un serveur Syslog qui envoie des données directement à CA User Activity Reporting Module.

Déploiement d'une collecte (/deploycollection)

Vous pouvez utiliser l'API pour déployer la collecte d'événements pour un ordinateur virtuel. Spécifiez un corps de message indiquant le profil d'événement que vous voulez utiliser.

Remarque : Les profils de collecte d'événements sont configurés à partir de l'interface utilisateur CA User Activity Reporting Module. Pour plus d'informations sur la configuration des profils de collecte d'événements, consultez l'Aide en ligne de CA User Activity Reporting Module .

La procédure suivante illustre la méthode de déploiement d'une collecte à l'aide de l'utilitaire cURL.

Procédez comme suit:

1. Créez un fichier texte appelé deploy.txt contenant les paramètres de déploiement :

```
<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>
```

   Les paramètres suivants sont disponibles :

   <client hébergé>

   Attribut un nom au client hébergé virtuel sur lequel vous voulez déployer la collecte d'événements. Vous pouvez obtenir une liste de clients hébergés disponibles à l'aide de /tenants.

   <profile>

   Nomme le profil de collection d'événement que vous voulez utiliser. Vous pouvez obtenir une liste de profils disponibles à l'aide de /collectionprofiles.

   <host>

   Nomme la source d'événements à partir de laquelle vous voulez collecter des événements.

   <ip>

   Spécifie l'adresse IP de la source d'événements à partir de laquelle vous voulez collecter des événements.

   <credentials>

Contient les éléments qui fournissent le nom d'utilisateur et le mot de passe pour accéder à la source d'événements. Cet élément est uniquement requis pour des profils de connexion définis pour requérir les informations d'identification.

2. Ouvrez une fenêtre d'invite de commande, puis accédez au répertoire dans lequel vous avez enregistré le fichier texte.
3. Entrez la commande suivante:

   ```
   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"
   ```

   L'élément "-d @deploy.txt" diffuse le contenu du fichier texte dans le corps de la demande.

Si le déploiement est correctement effectué, vous recevrez un message HTTP 201 (CREATED) :

```
HTTP/1.1 201 Created
Emplacement : 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 réponse indique l'URI de la ressource déployée, précédé de "Emplacement".

Vous pouvez utiliser ces informations pour modifier ou supprimer le déploiement. Dans l'exemple précédant, la ressource déployée est un connecteur passif, c'est pourquoi l'élément eventTarget s'affiche. EventTarget affiche le port et l'adresse IP des informations pour le connecteur, ce qui vous permet de configurer la source d'événements pour transmettre des événements à la cible correcte.

Si la capacité disponible n'est pas suffisante dans le groupe d'agents sélectionné, un message d'erreur (HTTP 507) s'affiche.

Appels d'ID de sources (/<sourceid>)

La ressource <sourceid> représente une source d'événements de CA User Activity Reporting Module. Vous pouvez renvoyer les informations sur la ressource, ou les supprimer, ce qui arrêtera la collecte d'événements à partir de la source d'événements correspondante.

Méthodes prises en charge (GET, DELETE)

Informations complémentaires :

Identification de ressources (page 20)
Supprimer une ressource (page 21)

Identification de ressources

Vous pouvez identifier des ressources représentant des sources d'événements et obtenir des informations les concernant à l'aide de la méthode GET. Cet appel renvoie des informations sur la source au chemin d'accès URI spécifié. Ce chemin d'accès est dérivé du résultat d'un appel /deploycollection.

```
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>
```

Dans votre environnement, remplacez le chemin d'accès d'URI "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<so urceid>" par le chemin d'accès à la ressource de votre choix.

Cet appel renvoie les éléments suivants :

```
<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>
```

Si la valeur de deploymentPending est définie sur true, cela signifie que l'agent est en cours de reconfiguration et actuellement indisponible pour de nombreuses d'opérations.

Supprimer une ressource

Vous pouvez supprimer une ressource représentant une source d'événements à l'aide de la méthode DELETE. Cet appel supprime la ressource spécifiée et la collecte d'événements s'arrête. Le chemin d'accès URI est dérivé du résultat d'un appel /deploycollection.

```
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>
```

Dans votre environnement, remplacez le chemin d'accès d'URI "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<so urceid>" par le chemin d'accès à la ressource de votre choix.

L'appel renvoie une confirmation (HTTP 200) à l'issue de l'opération de suppression.

Appels d'Informations d'Identification (/credentials)

La ressource /credentials représente le nom d'utilisateur et le mot de passe utilisé par un connecteur pour accéder à une source d'événements. Vous pouvez récupérer ces informations ou les mettre à jour.

Méthodes prises en charge (GET, PUT)

Informations complémentaires :

Liste d'informations d'identification (page 22)
Remplacement des informations d'identification (page 23)

Liste d'informations d'identification

Vous pouvez récupérer les informations d'identification utilisées par un connecteur déployé pour accéder à une source d'événements. La réponse affiche le nom d'utilisateur et le mot de passe. Cet appel est uniquement valide pour les connecteurs actifs. Une erreur HTTP 404 s'affiche pour les connecteurs passifs.

```
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
```

Dans votre environnement, remplacez le chemin d'accès d'URI "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" par le chemin d'accès à la ressource de votre choix.

Cet appel renvoie les éléments suivants :

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

La valeur du domaine facultative est uniquement utilisée pour des informations d'identification de Windows.

Remplacement des informations d'identification

Vous pouvez remplacer des informations d'identification existantes. Cet appel est uniquement valide pour les connecteurs actifs. Une erreur HTTP 404 s'affiche pour les connecteurs passifs.

```
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
```

Dans votre environnement, remplacez le chemin d'accès d'URI "/agentgroups/<groupid>/agents/<agentid>/connectors/<connid>/sources/<sourceid>" par le chemin d'accès à la ressource de votre choix.

Dans ce cas l'option "-d spécifie la nouvelle représentation de la ressource directement dans la ligne de commande.

Remarque : Cet exemple contient la valeur du domaine, uniquement requise pour les informations d'identification de Windows.