CA Enterprise Log Manager

Manuel de programmation de l'API

r12.5

Produits CA référencés

Ce document fait référence aux produits CA suivants :

- 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)
- 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.

Modifications de la documentation

Les mises à jour suivantes ont été réalisées depuis la dernière version de la présente documentation.

- getObject : Rubrique existante contenant une description de la commande getObject
- getIncidentModel - Rubrique nouvelle contenant un exemple de la commande getIncidentModel

Table des matières

Chapitre 1 : A propos de ce manuel

Le *Manuel de programmation de l'API CA Enterprise Log Manager* contient les instructions nécessaires pour utiliser l'API CA Enterprise Log Manager afin d'accéder aux données du référentiel des événements à l'aide du mécanisme de création de requêtes et de rapports et de les afficher dans un navigateur Web. Vous pouvez également utiliser l'API pour intégrer des requêtes ou des rapports CA Enterprise Log Manager dans une interface CA ou d'un produit tiers.

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 Enterprise Log Manager, des fédérations et de l'ajustement d'événements. Ils doivent disposer de droits d'administrateur pour accéder à CA Enterprise Log Manager et aux autres produits tiers ou CA requis.

Chapitre 2 : A propos de l'API CA Enterprise Log Manager

L'API CA Enterprise Log Manager utilise une application Web qui accepte les commandes POST HTTPS pour renvoyer les informations provenant de requêtes ou de rapports dont vous avez besoin. L'application Web est constituée d'un axe iGateway dédié.

Vous pouvez utiliser des URL comprenant des arguments afin de définir les données à renvoyer et les filtrer. Chaque commande URL / API disponible vérifie si l'appelant est authentifié en validant l'ID de session ou les informations d'identification du certificat. Chaque requête HTTPS doit contenir un de ces types d'informations d'authentification.

Les fonctionnalités de l'API CA Enterprise Log Manager sont les suivantes :

- Appels API authentifiés et sécurisés
- Enregistrement de produits pour authentification unique
- Récupération d'une liste de requêtes ou de rapports filtrée à l'aide d'une balise
- Affichage d'une requête ou d'un rapport dans l'interface CA Enterprise Log Manager interactive afin de les filtrer et de les intégrer dans une interface utilisateur

Pour utiliser les appels API CA Enterprise Log Manager efficacement, familiarisez-vous avec la structure de fédération de votre environnement, les requêtes et les rapports disponibles ainsi qu'avec les rôles d'utilisateur et leurs droits d'accès.

Informations complémentaires :

Structure de l'API CA Enterprise Log Manager (page 13)
Authentification API (page 15)
Exemples API CA Enterprise Log Manager (page 21)

Résultats des appels API

Toutes les commandes API, à l'exception de getQueryViewer and getReportViewer, renvoient un élément dans le code XML indiquant la réussite ou l'échec de la commande, et dans ce cas la raison de l'échec.

Exemple de résultat d'appel API

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>true</Value>
<Description>Get Object Successful. Type [getQueryList]</Description>
<Items>
<Item edit="false">
       <Panel id="Subscription/panels/Unclassified_Event_Detail" name="Unclassified Event
Detail" shortname="Detail" subscription="true" type="EventViewer" version="12.0.46.5">
       <Description>Provides event details for unclassified event activity</Description>
```

Dans ce cas, la valeur du résultat est "true" indiquant le succès de la commande. La description contient le nom de la commande exécutée.

Structure de l'API CA Enterprise Log Manager

Un appel API CA Enterprise Log Manager utilise le protocole HTTPS pour contacter le magasin de journaux d'événements. Selon le type de l'appel utilisé, les résultats sont renvoyés au format XML ou sous forme de requête ou de rapport graphique.

Chaque appel a une structure d'URL définie qui comporte plusieurs éléments courants. Par exemple, un appel de connexion API se présente comme suit :

```
https://ELMSERVER:5250/spin/calmapi/calmapi_login.csp?username=xx&password=xx
```

Le premier élément définit le serveur cible :

```
https://ELMSERVER:5250/spin/calmapi/
```

Pour utiliser l'appel dans votre environnement, remplacez la partie "ELMSERVER" de l'URL par le nom d'hôte ou l'adresse IP du serveur contenant les données que vous recherchez. Le port 5250 est le port par défaut utilisé par CA Enterprise Log Manager. Le texte "/spin/calmapi/" reste le même quel que soit l'appel.

Le second élément définit l'API elle-même et fournit des informations d'authentification :

```
calmapi_login.csp?username=xx&password=xx
```

"calmapi_login.csp" est l'appel de connexion. La seconde partie, "?username=xx&password=xx" définit les informations d'identification utilisées pour la connexion. Dans ce cas, le nom d'utilisateur CA Enterprise Log Manager et le mot de passe.

Informations complémentaires :

Authentification API (page 15)
Enregistrement avec l'API (page 56)

Chapitre 3 : Authentification API

Les appels API doivent être authentifiés pour accéder au magasin de journaux d'événements CA Enterprise Log Manager. Il existe plusieurs manières de configurer l'authentification :

- En utilisant un nom d'utilisateur et un mot de passe CA Enterprise Log Manager valides dans l'URL d'authentification. Lorsque vous créez un appel, vérifiez que vous disposez des informations nécessaires pour le compte d'utilisateur à authentifier.
- En utilisant un nom de certificat et le mot de passe y afférent dans l'URL d'authentification. Vous pouvez créer un certificat dans l'interface d'enregistrement de produits de l'API. Consultez l'*aide en ligne de l'API CA Enterprise Log Manager* pour plus d'informations sur la création d'un certificat.
- En utilisant un ID de session dans l'URL d'authentification. Cet ID de session est un ID unique renvoyé dans la réponse XML à la suite d'un appel d'authentification réussi. Utilisez l'une des autres méthodes d'authentification pour obtenir un ID de session dérivé à utiliser pour créer une autre session.

Exemple de nom d'utilisateur et de mot de passe

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryList&username=xx&password=xx
```

Dans cet exemple la commande getQueryList est utilisée et l'appel est authentifié à l'aide d'un nom d'utilisateur et d'un mot de passe CA Enterprise Log Manager.

Exemple de nom et de mot de passe de certificat

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getELMServers&certname=xx&password=xx
```

Dans cet exemple la commande getELMservers est utilisée et l'appel est authentifié à l'aide d'un nom et d'un mot de passe de certificat.

Exemple d'ID de session

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_Event_Count_By_Event_Action&sessionID=xxxxx
```

Dans cet exemple la commande getQueryViewer est utilisée et l'appel est authentifié à l'aide d'un ID de session.

Informations complémentaires :

Connexion API (page 17)
Enregistrer un produit (page 61)
Création de certificats API (page 57)

Connexion API

Cet appel authentifie un utilisateur à partir d'un ensemble d'informations d'identification CA EEM, d'un certificat ou d'un ID de session.

Etant donné que vous pouvez inclure des informations d'authentification dans n'importe quelle URL d'appel API, vous n'avez pas besoin d'un appel de connexion distinct dans la plupart des cas. L'appel de connexion est particulièrement utile pour renvoyer un ID de session qui peut ensuite servir à authentifier un autre appel, tel que getReportViewer.

Les arguments utilisés pour cet appel sont répertoriés ci-dessous :

username

Définit le nom d'utilisateur CA Enterprise Log Manager valide à authentifier.

certname

Définit le nom du certificat à authentifier, si votre produit est déjà enregistré, accédez à CA Enterprise Log Manager.

password

Définit le mot de passe utilisateur CA Enterprise Log Manager ou le mot de passe du certificat à authentifier en fonction de la méthode d'authentification que vous avez utilisée.

sessionid

Définit l'ID d'une session authentifiée existante qui peut vous servir à authentifier une nouvelle session.

Exemples de connexion à l'API

Commande :

```
https://ELMSERVER:5250/spin/calmapi/calmapi_login.csp&username=xx&password=xx
```

Réponse en cas de réussite :

```
  <?xml version="1.0" encoding="UTF-8" ?>
 <Result>
  <Value>true</Value>
  <Description>Authentication Successful.</Description>
  <SessionId>spin=62e39751-computername.domain.com49b8a97e-9bfd318-1</SessionId>
  </Result>
```

L'ID de la session ouverte par la connexion apparaît dans la balise <SessionId>.

Réponse en cas d'échec :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>false</Value>
        <Description> EE_AUTHFAILED Authentication Failed</Description>
</Result>
```

Informations complémentaires :

Authentification API (page 15)
Appels de la visionneuse de requêtes et de rapports (page 38)

Déconnexion de l'API

Cet appel arrête une session API (en déconnectant l'utilisateur), une session de certificat ou une session créée à l'aide de l'ID de session. L'appel n'accepte aucun argument.

Exemples de déconnexion de l'API

```
https://ELMSERVER:5250/spin/calmapi/calmapi_logout.csp
```

Réponse en cas de réussite :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>true</Value>
        <Description>Logout Successful</Description>
</Result>
```

Réponse en cas d'échec :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>false</Value>
        <Description> User is not logged in</Description>
</Result>
UTHFAILED Authentication Failed</Description>
</Result>
```

A propos des sessions API

CA Enterprise Log Manager crée une session à chaque fois que vous utiliser un appel API. La persistance de ces sessions varie selon la méthode d'authentification que vous utilisez :

- Les sessions authentifiées par un nom d'utilisateur et un mot de passe ou par un ID de session ont la même durée que les sessions CA Enterprise Log Manager. L'expiration des sessions est fixée à 15 minutes par défaut. Vous pouvez définir la valeur de l'expiration des sessions dans l'interface CA Enterprise Log Manager.
- Les sessions authentifiées par un certificat n'expirent pas sauf dans certaines circonstances. En effet, la valeur de l'expiration des sessions est suspendue pour vous permettre d'intégrer CA Enterprise Log Manager à un portail Web ou à un produit extérieur plus facilement. Toutefois, une action supplémentaire peut être nécessaire pour éviter que les sessions persistantes utilisent inutilement les ressources du système.

CA Enterprise Log Manager ferme les sessions authentifiées par un certificat dans les circonstances suivantes :

- Fermeture d'un navigateur affichant un composant graphique tel qu'une requête
- Déconnexion d'un produit extérieur
- Expiration autorisée d'une session utilisateur d'un produit extérieur

Le temporisateur de la session CA Enterprise Log Manager commence le compte à rebours et arrête la session dès que la valeur d'expiration que vous avez configurée est atteinte.

Si plusieurs appels getQueryViewer ou getReportViewer sont en cours d'utilisation, il peut y avoir plusieurs sessions ouvertes mais inactives. Pour réduire l'utilisation des ressources système par ces sessions, utilisez la commande de déconnexion pour arrêter une session lorsque l'utilisateur d'un produit extérieur se déconnecte ou lorsque la session d'un produit extérieur se termine.

Informations complémentaires :

Appels de la visionneuse de requêtes et de rapports (page 38)
Authentification API (page 15)
Création de certificats API (page 57)
Connexion API (page 17)
Déconnexion de l'API (page 19)

Chapitre 4 : Exemples API CA Enterprise Log Manager

Ce chapitre traite des sujets suivants :

A propos des exemples API

Ce chapitre contient des exemples d'appels API. Chaque exemple décrit l'URL requise et montre le résultat attendu sous forme de code XML en cas de succès ou d'échec. Vous pouvez tester ces appels en entrant l'URL directement dans un navigateur. Examinez ensuite la réponse XML.

Les appels getQueryViewer et getReportViewer présentent les événements et les requêtes dans une interface CA Enterprise Log Manager et non au format XML. Une section leur est entièrement consacrée dans ce guide.

GetObject

Ce fichier de commande permet de récupérer divers types d'informations. Utilisez-le pour récupérer une liste de requêtes, de rapports ou de paramètres globaux, ou encore la grammaire commune aux événements (CEG). La commande getObject utilise un qualificateur ou un argument nommé "type" pour déterminer le type des données à renvoyer à l'appelant comme le montre cet exemple :

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=type&tag=tagname1&tag=tagnamen&taglogic=OR|AND
```

La liste suivante répertorie les types de données renvoyées selon les variations de cette commande :

getQueryList

Renvoie une chaîne XML contenant toutes les requêtes dans CA Enterprise Log Manager. getQueryList prend en charge de nombreux paramètres de filtrage qui vous permettent de sélectionner et d'inclure des noms de requête dans vos appels API.

getReportList

Renvoie une chaîne XML contenant tous les rapports dans CA Enterprise Log Manager. getReportList prend en charge de nombreux paramètres de filtrage qui vous permettent de sélectionner et d'inclure des noms de rapport dans vos appels API.

getDataModel

Renvoie la grammaire commune aux événements (CEG) au format XML. Cela vous permet de sélectionner les termes CEG à inclure dans le filtrage des appels API.

getIdealModel

Renvoie les modèles idéaux définis dans la CEG. Cela vous permet de sélectionner les termes de zone de produit à inclure dans le filtrage des appels API.

getIncidentModel

Renvoie les champs CEG disponibles utilisés dans les incidents générés par la corrélation d'événements.

getCombinedModel

Renvoie la grammaire commune aux événements (CEG) au format XML pour les champs d'événement et d'incident. Cela vous permet de sélectionner les termes CEG à inclure dans le filtrage des appels API.

getGlobalSettings

Renvoie les paramètres globaux pour le serveur CA Enterprise Log Manager sur lequel la commande est exécutée. Ces paramètres vous indiquent quel filtrage est activé pour les requêtes CA Enterprise Log Manager afin de créer des filtres d'appels API efficaces.

getELMServers

Renvoie une liste de serveurs CA Enterprise Log Manager. Cette commande est utile dans un environnement fédéré, car elle vous permet de cibler les serveurs parents ou enfants à interroger.

getTimeZones

Extrait une liste de fuseaux horaires pouvant être utilisés comme arguments dans les requêtes en cours d'exécution.

getVersion

Renvoie la version ELM, identique à celle des API et utile pour établir des diagnostics.

getObjectDefinition

Renvoie les métadonnées pour un rapport ou une requête selon l'ID d'objet indiqué. Les métadonnées correspondent aux données de formatage qui définissent la présentation d'un rapport ou d'une requête. Utilisez ces métadonnées lorsque vous devez utiliser l'appel runQuery pour obtenir les données CA Enterprise Log Manager d'une application qui ne peut pas intégrer directement une visionneuse de requêtes ou de rapports.

getQueryViewer

Affiche la page HTML contenant la visionneuse de requêtes avec une requête préchargée.

getReportViewer

Affiche la page HTML contenant la visionneuse de rapports avec un rapport préchargé.

Toutes les commandes GetObject, à l'exception de getQueryViewer et getReportViewer, produisent une erreur si la commande API ne comporte aucune session authentifiée :

```
Réponse en cas d'échec :
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>false</Value>
        <Description> User is not logged in</Description>
</Result>
```

Dans l'exemple précédent, la valeur du résultat est "false" ce qui indique un échec de la commande. La raison est indiquée dans la description, dans ce cas : "User is not logged in" (L'utilisateur n'est pas connecté).

Informations complémentaires :

Appels de la visionneuse de requêtes et de rapports (page 38)

getQueryList

Utilisez la commande getQueryList pour répertorier toutes les requêtes disponibles dans votre environnement CA Enterprise Log Manager. La réponse XML contient également les données de formatage et les critères de filtrage prédéfinis pour chaque requête.

Vous pouvez utiliser les paramètres facultatifs suivants avec la commande getQueryList.

tag

Définit une balise qui existe dans le système. Vous pouvez inclure une ou plusieurs balises à rechercher à l'aide de la commande getQueryList. Si vous spécifiez une balise inconnue, la commande produit une liste vide.

tagLogic

Indique comment la commande getQueryList traite plusieurs balises. Les valeurs valides sont AND et OR. La valeur par défaut est OR. Vous ne pouvez utiliser qu'une valeur tagLogic à la fois.

Exemple de balise non filtrée

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryList
```

Renvoie toutes les requêtes et les données de formatage associées à chacune d'elles.

Exemple de paramètre TagLogic avec la valeur OR

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryList&tag=Unknown
Category&tag=System
```

Renvoie toutes les requêtes associées aux balises "Unknown Category" OR "System" ("Catégorie inconnue" OU "Système")

Exemple de paramètre TagLogic avec la valeur AND

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryList&tag=Unknown
Category&tag=System&tagLogic=and
```

Renvoie toutes les requêtes associées aux balises "Unknown Category" AND "System" ("Catégorie inconnue" ET "Système")

Exemple de résultat

Cet exemple abrégé montre une seule requête , "System Event Count by Event Category" (Nombre d'événements du système par catégorie d'événement)..

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Get Object Successful. Type [getQueryList]</Description>
        <Items>
        <Item edit="false">
                <Panel id="Subscription/panels/System_Event_Count_by_Event_Category" name="System
Event Count by Event Category" subscription="true" version="12.0.46.8">
                        <Description>Ranks system event count activity by event
category</Description>
                        <Tags>
                                <Tag name="System" />
                        </Tags>
                        <Query id="">
                                <Table>view_event</Table>
                                <Args unique="false" />
                                <Column columnname="event_datetime" datatype="T" displayname="Date"
resultname="event_datetime" visible="true" />
                                <Column columnname="event_category" datatype="S"
displayname="Category" grouporder="1" notnull="true" resultname="event_category" sortdesc=""
visible="true" />
                                <Column columnname="event_count" datatype="I" displayname="Count"
functionname="sum" resultname="event_count" sortdesc="true" sortorder="1" visible="true" />
                        </Query>
                        <Display>
                                <X name="Category" resultname="event_category" />
                                <Y name="Count" resultname="event_count" />
                                <Visualization type="VizBarChart" />
                                <Visualization type="VizPieChart" />
                                <Visualization type="VizTable" />
                        </Display>
                </Panel>
        </Item>
        <Item edit="false">
```

"Panel id=" indique qu'il s'agit d'un rapport d'abonnement et indique son nom.

Remarque : Si la requête est une invite, la balise "Prompt id=" apparaît au lieu de la balise "Panel id=", par exemple "Prompt id=HostPrompt".

"Tag Name=" indique la balise System.

Les éléments "Column columname=" spécifient les colonnes d'événements dans lesquelles la requête a effectué la recherche et leur agencement.

Les éléments "Display" spécifient la forme sous laquelle les événements sont affichés.

Informations complémentaires :

getQueryViewer (page 39)
Requêtes d'invite (page 52)
runQuery (page 55)

getReportList

Utilisez la commande getReportList pour afficher tous les rapports disponibles dans l'environnement CA Enterprise Log Manager. La réponse XML contient également les données de formatage et l'ID de chaque requête utilisée dans le rapport.

Vous pouvez utiliser les paramètres facultatifs suivants avec la commande getReportList :

tag

Définit une balise qui existe dans le système. Vous pouvez inclure une ou plusieurs balises à rechercher à l'aide de la commande getReportList. Si vous spécifiez une balise inconnue, la commande produit une liste vide.

tagLogic

Indique comment la commande getReportList traite plusieurs balises. Les valeurs valides sont AND et OR. La valeur par défaut est OR. Vous ne pouvez utiliser qu'une valeur tagLogic à la fois.

Exemple de balise non filtrée

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getReportList
```

Renvoie tous les rapports et les données de formatage et d'affichage associées à chacun d'eux.

Exemple de paramètre TagLogic avec la valeur OR

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type= getReportList&tag=Unknown
Category&tag=System
```

Renvoie tous les rapports associés aux balises "Unknown Category" OR "System" ("Catégorie inconnue" OU "Système")

Exemple de paramètre TagLogic avec la valeur AND

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type= getReportList&tag=Unknown
Category&tag=System&tagLogic=and
```

Renvoie tous les rapports associés aux balises "Unknown Category" AND "System" ("Catégorie inconnue" ET "Système")

getObjectDefinition

Utilisez la commande getObjectDefinition pour afficher les données de formatage et de disposition associées à une requête ou un rapport au format XML. Vous pouvez afficher les données de formatage dans les rapports existants pour créer un formatage personnalisé, surtout si vous souhaitez utiliser la commande runQuery. La commande getObjectDefinition vous permet également de renvoyer des données portant sur les rapports ou les requêtes d'abonnement et définis par l'utilisateur.

Exemple de commande getObjectDefinition

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getObjectDefinition&objectId=Subscription/
panels/Unclassified_Event_Trend
```

Renvoie le code XML suivant :

```
?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Get Object Successful. Type [getObjectDefinition]</Description>
        <Panel id="Subscription/panels/Unclassified_Event_Trend" name="Unclassified Event Trend"
shortname="Trend" subscription="true" version="12.0.46.5">
                <Description>Provides Trending for unclassified event activity</Description>
                <Tags>
                        <Tag name="Unclassified Event" />
                        <Tag name="Unknown Category" />
                </Tags>
                <Params />
                <Query>
```

Cet exemple montre les données de formatage pour la requête Unclassified Event Trend (Tendance de l'événement non classé). Le paramètre "objectId" dans l'appel spécifie le formatage à afficher selon la requête ou le rapport. Dans ce cas, il s'agit de la requête Unclassified Event Trend dans le dossier de requêtes Subscription (Abonnement).

Informations complémentaires :

runQuery (page 55)

getDataModel

Utilisez la commande getDataModel pour afficher les données de formatage spécifiques à la grammaire commune aux événements (CEG). La CEG contient tous les champs d'événement figurant dans le schéma, la description de chaque champ et leurs valeurs possibles (le cas échéant). Vous pouvez ainsi correctement identifier les champs CEG pour chaque filtrage que vous souhaitez inclure dans un appel.

Exemple de commande getDataModel

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getDataModel
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>true</Value>
<Description>Get Object Successful. Type [getDataModel]</Description>
<CommonEventGrammar version="12.0.45.4">
                    ....
<field name="event_logname" type="S" class="" category="event" index="y" desc="The name of the
log expressed in the event information.">
<values>
                    <value>ACF2</value>
                    <value>Apache</value>
                    <value>AuditEngine</value>
```

L'élément "field name=" affiche le champ CEG, dans ce cas event_logname.

Le type de chaque champ CEG est indiqué dans l'élément "type=".

getCombinedModel

Utilisez la commande getCombinedModel pour afficher les données de formatage spécifiques à la grammaire commune aux événements (CEG), pour les événements et les incidents. La CEG contient tous les champs d'événement figurant dans le schéma, la description de chaque champ et leurs valeurs possibles (le cas échéant). Vous pouvez ainsi correctement identifier les champs CEG pour chaque filtrage que vous souhaitez inclure dans un appel.

Exemple de commande getCombinedModel

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getCombinedModel
```

Renvoie le code XML suivant :

```
                        <?xml version="1.0" encoding="UTF-8" ?>
- <Result>
  <Value>true</Value>
  <Description>Get Object Successful. Type [getCombinedModel]</Description>
- <CEGFields>
+ <events>
- <incidents>
- <CommonEventGrammar version="12.1.5109.0">
  <SchemaVersion value="1" desc="Incident Schema version, integer, incremented
starting at 1 (no version=0)" />
  <field internal="true" name="" type="" class="" category="" index="" desc=""
dbtable="version" dbname="value" dbtype="INTEGER" dbindex="NOT NULL" />
  <field internal="true" name="" type="" class="" category="" index="" desc=""
dbtable="version" dbname="timestamp" dbtype="INTEGER" dbindex="NOT NULL" />
  <field name="incident_id" type="S" class="" category="" index="y" desc=""
dbtable="incidents"
```

L'élément "field name=" affiche le champ CEG, dans ce cas incident_id.

L'élément "dbtable=" identifie le type de base de données, dans ce cas la base de données des incidents.

getIncidentModel

Utilisez la commande getIncidentModel pour afficher les champs Grammaire commune aux événements (CEG) spécifiques aux incidents de votre environnement. La CEG contient tous les champs d'événement possibles, une description de chacun d'eux et les valeurs possibles, le cas échéant. Vous pouvez ainsi correctement identifier les champs CEG pour chaque filtrage que vous souhaitez inclure dans un appel.

Exemple de commande getIncidentModel

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getIncidentModel
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Result>
  <Value>true</Value>
  <Description>Get Object Successful. Type [getIncidentModel]</Description>
- <CommonEventGrammar version="12.1.5109.0">
  <SchemaVersion value="1" desc="Incident Schema version, integer, incremented starting at 1 (no
version=0)" />
  <field internal="true" name="" type="" class="" category="" index="" desc="" dbtable="version"
dbname="value" dbtype="INTEGER" dbindex="NOT NULL" />
  <field internal="true" name="" type="" class="" category="" index="" desc="" dbtable="version"
dbname="timestamp" dbtype="INTEGER" dbindex="NOT NULL" />
  <field name="incident_id" type="S" class="" category="" index="y" desc="" dbtable="incidents"
dbname="producer_msg_id" dbindex="UNIQUE NOT NULL" SnmpOID="1.3.6.1.4.1.791.9845.2.1001" />
  <field name="incident_createtime_gmt" type="T" class="" category="" index="y" desc=""
dbtable="incidents" dbname="createtime" SnmpOID="1.3.6.1.4.1.791.9845.2.1002" />
  <field name="incident_name" type="S" class="" category="" index="y" desc="" dbtable="incidents"
dbname="name" SnmpOID="1.3.6.1.4.1.791.9845.2.1003" />
  <field name="incident_rule_id" type="S" class="" category="" index="y" desc=""
dbtable="incidents" dbname="rule_id" SnmpOID="1.3.6.1.4.1.791.9845.2.1004" />
  <field name="incident_rule_version" type="S" class="" category="" index="y" desc=""
dbtable="incidents" dbname="rule_version" SnmpOID="1.3.6.1.4.1.791.9845.2.1005" />
  <field name="incident_rule_grouppath" type="S" class="" category="" index="y" desc=""
dbtable="incidents" dbname="rule_grouppath" SnmpOID="1.3.6.1.4.1.791.9845.2.1006" />
```

L'élément "field name=" affiche le champ CEG de l'incident.

getELMServers

Utilisez la commande getELMServers pour renvoyer une liste des serveurs CA Enterprise Log Manager disponibles sur lesquels exécuter des requêtes.

Exemple de commande getELMServers

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getELMServers
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Get Object Successful. Type [getELMServers]</Description>
        <service type="service" name="Event Log Store"
id="/CALM_Configuration/Modules/logDepot/Config" edit="true" updated="1232571794"
global_config="true">
        <service type="host" name="machinename"
id="/CALM_Configuration/Modules/logDepot/machinename/Config" edit="true" service_name="Event Log
Store" updated="1232571795" />
        </service>
</Result>
```

Cet exemple montre un seul serveur pour lequel l'attribut "type=host" indique le nom du serveur hôte CA Enterprise Log Manager, dans ce cas "machinename" (nom de la machine). Plusieurs hôtes peuvent être spécifiés. Chaque élément XML "service" représente un serveur CA Enterprise Log Manager.

getGlobalSettings

Utilisez la commande getGlobalSettings pour afficher les paramètres globaux pour le serveur CA Enterprise Log Manager cible. Vous pouvez ainsi afficher les paramètres globaux et décider s'ils conviennent pour les appels de requête ou de rapport API que vous souhaitez créer. Définissez ensuite les paramètres dans l'interface CA Enterprise Log Manager.

Exemple de commande getGlobalSettings

```
https://ELMSERVER:5250/spin/calmapi/
getObject.csp?type=getIGlobalSetthttps://ELMSERVER:5250/spin/calmapi/getObject.cs
p?type=getGlobalSettingsings
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
- <Result>
  <Value>true</Value>
  <Description>Get Object Successful. Type [getGlobalSettings]</Description>
- <iSponsor>
  <Name>CALM</Name>
  <Version>12.1.xxx.1</Version>
  <EEMServer>etr851l1-blade3</EEMServer>
  <EEMAdmin>EiamAdmin</EEMAdmin>
  <Certificate>/opt/CA/SharedComponents/iTechnology/CAELMCert.p12</Certificate>
  <Password>BhUXVFhQCFxEDA==</Password>
  <DisplayName>Configuration globale</DisplayName>
  <CalmType>service</CalmType>
  <AppInstance>CAELM</AppInstance>
  <ELMPath>/opt/CA/LogManager</ELMPath>
  <Updated>1269421754</Updated>
  <KeyFile>@APP_NAME@Cert.key</KeyFile>
  <UpdateInterval label="Mettre à jour l'intervalle (en secondes)" def="300"
prompt="Mettre à jour l'intervalle (en secondes) auquel les composants vérifie la
présence de configurations actualisées" type="number" min="30" max="86400"
global="true">30</UpdateInterval>
  <SessionTimeout label="Expiration de la session (en minutes)" def="15"
prompt="Expiration de la session (en minutes)" type="number" min="10"
max="600">15</SessionTimeout>
  <AutoRefreshAllowed type="bool" label="Autoriser l'actualisation automatique"
prompt="Autoriser les utilisateurs à définir l'actualisation automatique des
rapports" def="false">true</AutoRefreshAllowed>
  <AutoRefreshFrequency type="number" label="Fréquence de l'actualisation
automatique (en minutes)" prompt="Fréquence de l'actualisation automatique (en
minutes)" min="1" max="60" def="10">10</AutoRefreshFrequency>
  <AutoRefreshEnabled type="bool" label="Activer l'actualisation automatique"
prompt="Fréquence de l'actualisation automatique des rapports"
def="false">false</AutoRefreshEnabled>
  <AlertAuthentication def="true" label="Authentification requise pour
l'affichage des alertes d'action" prompt="L'affichage des alertes d'action
requiert l'authentification de l'utilisateur" type="bool"
global="true">false</AlertAuthentication>
  <DefaultReport EEMDisplay="calmName"
EEMsource="/CALM_Configuration/Content/Reports/Subscription/scorecards,/CALM_Conf
iguration/Content/Reports/User" calmType="scorecard" label="Rapport par défaut"
prompt="Rapport à exécuter par défaut"
type="combo">Collection_Monitor_by_Log_Manager</DefaultReport>
```

```
  <EnableDefaultReport type="bool" label="Activer le lancement du rapport par
défaut" prompt="Activer le lancement automatique du rapport par défaut"
def="true">true</EnableDefaultReport>
  <HiddenReportTags type="shuttle" prompt="Masquer les balises du rapport
sélectionné dans l'application" icon="tagIcon" label="Masquer les balises du
rapport" EEMsource="/CALM_Configuration/Content/Reports/Tags/Report"
orderedlist="false" />
  <HiddenQueryTags type="shuttle" prompt="Masquer les balises de la requête
sélectionnée dans l'application" icon="tagIcon" label="Masquer les balises de la
requête" EEMsource="/CALM_Configuration/Content/Reports/Tags/Panel"
orderedlist="false" global="true" />
  <EnableDefaultProfile group="Profils" type="bool" label="Activer le profil par
défaut" prompt="Activer le lancement automatique du profil par défaut"
def="false">false</EnableDefaultProfile>
  <DefaultProfile group="Profiles" EEMDisplay="calmName"
EEMsource="/CALM_Configuration/Content/Profiles/Subscription,/CALM_Configuration/
Content/Profiles/User" calmType="profile" label="Profil par défaut"
prompt="Profil à exécuter par défaut" type="combo"
global="true">CA_Access_Control</DefaultProfile>
  <HiddenProfiles group="Profiles" EEMDisplay="calmName" type="shuttle"
prompt="Masquer les profils sélectionnés dans l'application" icon="profileIcon"
label="Masquer les profils"
EEMsource="/CALM_Configuration/Content/Profiles/Subscription,/CALM_Configuration/
Content/Profiles/User" orderedlist="false"
global="true">CA_Identity_Manager</HiddenProfiles>
  </iSponsor>
  </Result>
```

getTimeZones

Utilisez la commande getTimeZones pour afficher les fuseaux horaires pris en charge en tant que paramètres de requête. Cette commande vous permet d'obtenir une liste des fuseaux horaires pour que le format de fuseau horaire correct figure sur les données des requêtes obtenues.

Remarque : Si vous n'indiquez pas un fuseau horaire valide pour getQueryViewer, getReportViewer et runQuery, le fuseau horaire du serveur CA Enterprise Log Manager figurera sur les données.

Exemple de commande getTimeZones

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getTimeZones
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Get Object Successful. Type [getTimeZones]</Description>
        <tz>
                <TimeZone isDefault="false">Etc/GMT+12</TimeZone>
                <Offset>720.0</Offset>
        </tz>
        <tz>
                <TimeZone isDefault="false">Etc/GMT+11</TimeZone>
                <Offset>660.0</Offset>
        </tz>
        ....
```

getVersion

Utilisez la commande getVersion pour afficher la version des API exécutées sur le serveur CA Enterprise Log Manager. Il n'est pas obligatoire que les versions soient les mêmes. Utilisez cette commande pour la résolution des problèmes.

Remarque : La version des API peut différer de celle des autres composants CA Enterprise Log Manager tels que les agents, selon les choix de votre administrateur concernant les mises à jour.

Exemple de commande getVersion

```
https://ELMSERVER:5250/spin/calmapi/ getObject.csp?type=getVersion
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Get Object Successful. Type [getVersion]</Description>
        <Version>v12.0.48.14</Version>
</Result>
```

Appels de la visionneuse de requêtes et de rapports

GetQueryViewer et getReportViewer affichent une visionneuse graphique dans une fenêtre d'interface similaire à l'interface CA Enterprise Log Manager. Cette fenêtre vous permet d'effectuer de nombreuses tâches associées aux rapports et aux requêtes. Pour plus d'informations sur les tâches disponibles, consultez l'*aide en ligne de l'API CA Enterprise Log Manager*.

Ces appels fournissent des points d'intégration externes avec des portails tiers et d'autres applications. Lorsque vous les utilisez, tenez compte de ce qui suit :

- L'utilisation de l'authentification de certificat empêche la session de la visionneuse de rapports ou de requêtes d'expirer comme c'est le cas avec une session CA Enterprise Log Manager. C'est l'application à partir de laquelle vous appelez la visionneuse d'événements ou de requêtes qui détermine le délai d'expiration de la session et non l'application CA Enterprise Log Manager.
- Pour des raisons de sécurité, si vous n'avez pas enregistré un produit tiers avec CA Enterprise Log Manager, ces appels vous redirigent vers la page de connexion. Pour éviter cela, vous avez deux possibilités :
  - Incluez les attributs d'informations d'identification en tant que champ masqué dans chaque commande. L'axe de l'API procède automatiquement à l'authentification des appels. Cela fonctionne sur les portails qui acceptent les champs masqués.
  - Exécutez une commande telle que getVersion avant de lancer ou d'intégrer le composant d'interface approprié et d'effectuer l'action nécessaire (comme la réauthentification en arrière-plan).

Informations complémentaires :

A propos des sessions API (page 19)
getQueryViewer (page 39)
getReportViewer (page 53)
Authentification API (page 15)

getQueryViewer

Utilisez cet appel pour afficher la visionneuse graphique pour une requête. La visionneuse de requêtes CA Enterprise Log Manager est un composant autonome entièrement fonctionnel. Vous pouvez intégrer des requêtes dans une interface d'application externe ou un portail externe en saisissant l'URL dans un cadre intégré.

Remarque : La solution fournie ici fonctionne avec les applications Web (JSP, JavaScript et HTML). Il est en revanche possible que la solution *ne* fonctionne pas dans les applications C++ ou Java Swing si celles-ci ne prennent pas en charge l'intégration de pages HTML ni le plug-in FLASH nécessaire. Dans le cas des applications ne prenant pas en charge le plug-in FLASH, nous vous conseillons d'utiliser runQuery pour récupérer les données brutes et les restituer graphiquement selon une méthode appropriée à votre environnement.

Exemple d'appel getQueryViewer

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_Event_Count_By_Event_Action
```

Affiche la requête System Event Count by Event Action (Nombre d'événements du système par action d'événement).

"getObject.csp?type=getQueryViewer" spécifie le type de l'appel getObject, dans ce cas la visionneuse de requêtes.

"&objectId=Subscription/panels/System_Event_Count_By_Event_Action" identifie la requête, dans ce cas la requête d'abonnement (Subscription) appelée System Event Count by Event Action. Pour spécifier le nom d'une requête, il suffit d'entrer son nom tel qu'il apparaît dans l'interface, en séparant les mots par des caractères de soulignement.

Informations complémentaires :

getQueryList (page 25)
Requêtes d'invite (page 52)
runQuery (page 55)

Spécifications de requête

Vous pouvez préqualifier les résultats d'un appel getQueryViewer, getReportViewer ou runQuery en ajoutant des spécifications. Vous pouvez définir des informations détaillées qui peuvent être un sous-ensemble d'une requête existante ou pertinentes pour certains clients. Par exemple, vous pouvez utiliser des spécifications afin de rechercher sur un serveur un certain type d'événements s'étant produits uniquement lors du jour précédent.

Vous pouvez définir les spécifications suivantes :

server

Spécifie le serveur CA Enterprise Log Manager interrogé. Le serveur par défaut est l'hôte local, le serveur nommé dans l'appel getQuery. Vous pouvez utiliser cette spécification pour cibler un autre serveur.

timezone

Définit le fuseau horaire dans lequel la requête apparaît. La valeur par défaut est le fuseau horaire dans lequel le serveur CA Enterprise Log Manager fonctionne. Vous pouvez utiliser cette spécification pour définir vos résultats dans un autre fuseau horaire.

federated

Indique (avec la valeur true ou false) si la requête est appliquée aux serveurs fédérés appropriés. La valeur par défaut est true. La requête est alors appliquée à tous les serveurs fédérés. Ce comportement applique les règles CA Enterprise Log Manager normales pour interroger les hiérarchies de fédérations.

filterXml

Définit les filtres de données appliquées à la requête au format XML. Vous pouvez utiliser cette spécification pour filtrer sur le nom d'hôte ou sur d'autres champs CEG.

IncidentFilterXml

Définit les filtres de données appliqués à une requête d'incident incluse dans un rapport au format XML. Vous pouvez utiliser cette spécification pour appliquer un filtre dans le champ de l'heure de création ou d'autres champs CEG. Cette spécification s'applique uniquement à l'appel getReportViewer.

accessfilterXml

Définit les filtres de données appliquées à la requête au format XML. Cette spécification permet de filtrer un résultat de requête ou de rapport en fonction du rôle, lors de l'authentification à l'aide d'un nom et d'un mot de passe de certificat.

params

Définit les conditions de résultat appliquées à la requête au format XML.

invite

Détermine (avec la valeur true ou false) si les contrôles d'invite supplémentaires sont affichés. La valeur par défaut est false. Cette valeur est uniquement valide si la requête est une invite. Si ce n'est pas le cas, la valeur est ignorée.

Les spécifications sont uniquement utilisées si vous avez défini "prompt=true":

promptvalue

Définit la valeur de filtre pour une requête d'invite.

col

Répertorie les colonnes d'événements dans lesquelles la requête d'invite recherche des informations. Vous pouvez utiliser plusieurs termes col pour identifier plusieurs colonnes cibles.

Informations complémentaires :

getQueryViewer (page 39)
Requêtes d'invite (page 52)
runQuery (page 55)

Spécifications de serveur

Vous pouvez spécifier le magasin de journaux d'événements d'un serveur CA Enterprise Log Manager non défini par défaut comme cible de la requête, en indiquant le nom ou l'adresse IP du serveur. Le serveur par défaut est l'hôte local, le serveur nommé dans l'appel API.

Pour récupérer une liste des noms de serveurs éligibles, utilisez getELMServers.

Exemple de spécification de nom de serveur

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Su
bscription/panels/System_Event_Count_By_Event_Action&server=ELMSERVER2
```

Dans cet exemple, "&server=" spécifie le nom du serveur pour la requête. Le nom du serveur voulu remplace "ELMSERVER2". Etant donné que le serveur par défaut est l'hôte local (ELMSERVER), il n'est pas nécessaire d'utiliser l'élément &server, sauf si vous souhaitez spécifier un serveur cible non défini par défaut.

Remarque : Si vous entrez un nom de serveur non valide, l'appel renvoie les données du serveur CA Enterprise Log Manager par défaut qui est identifié par la valeur ELMSERVER.

Informations complémentaires :

getELMServers (page 33)
runQuery (page 55)

Spécifications de fuseau horaire

Vous pouvez ajouter une spécification de fuseau horaire à votre appel getQuery ou runQuery. Pour récupérer une liste des fuseaux horaires disponibles, utilisez getTimeZones.

Exemple de spécification de fuseau horaire

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_Event_Count_By_Event_Action&timezone=TIMEZONENAME
```

Dans ce cas, "&timezone=" spécifie le nom du fuseau horaire voulu. Le nom du fuseau horaire, tel qu'il apparaît dans la liste renvoyée par l'appel getTimeZones, remplace "TIMEZONENAME".

Remarque : La réponse à un fuseau horaire non valide varie selon l'appel dans lequel celui-ci est inclus :

- Si un fuseau horaire non valide est utilisé dans l'appel runQuery, des heures GMT sont renvoyées. Si aucun fuseau horaire n'est transmis, alors le fuseau horaire par défaut est celui dans lequel le serveur fonctionne.
- Si l'appel getQueryViewer ou getReportViewer comporte un fuseau horaire non valide ou s'il n'en comporte aucun, le fuseau horaire par défaut est celui du serveur cible.

Informations complémentaires :

getTimeZones (page 36)
runQuery (page 55)

Informations complémentaires :

Spécifications IncidentFilter au format XML (page 47)

Spécifications de filtre au format XML

Vous pouvez prédéfinir des filtres CA Enterprise Log Manager pour les rapports au format XML et les ajouter à l'URL d'un appel getQueryViewer, getReportViewer, getIncidentViewer, ou runQuery à l'aide du terme filterXML. Pour imbriquer plusieurs filtres, utilisez les termes AND et OR et des parenthèses. Les filtres CA Enterprise Log Manager que vous créez au format XML sont des filtres avancés.

Important : Les termes FilterXml sont complexes et l'API ne procède à aucune validation. Les termes de filtre non valides produisent une erreur de requête. Pour cette raison, nous vous conseillons de procéder avec précaution pour créer des termes de filtre.

Les éléments de filtre disponibles, présentés dans l'ordre dans lequel ils doivent être utilisés, sont les suivants :

lparens

Définit le nombre de parenthèses de gauche. Les valeurs valides sont 0 et plus.

Logique

Définit le terme logique reliant les filtres, à savoir AND ou OR. Pour le premier terme de filtre, il convient de toujours laisser la valeur logique vide.

col

Définit les colonnes d'événements interrogés. Pour obtenir la liste des colonnes disponibles, utilisez getDataModel.

oper

Définit un opérateur pour le filtre. Les valeurs valides distinguant les majuscules des minuscules sont :

- EQUAL - Egal à
- NEQ - Différent de
- LESS - Inférieur à
- GREATER - Supérieur à
- LEQ - Inférieur ou égal à
- GREATEQ - Supérieur ou égal à

- LIKE - Similaire à
- NOTLIKE - Distinct de
- INSET - Dans l'ensemble
- NOTINSET - Hors ensemble
- MATCH - Correspond
- KEYED - A clés
- NOTKEYED - Sans clé

val

Définit la valeur sur laquelle la recherche est filtrée.

rparens

Définit le nombre de parenthèses de droite. Les valeurs valides sont 0 et plus. Le nombre total de parenthèses de droite correspond toujours au nombre de parenthèses de gauche.

Lorsque vous affichez une requête ou un rapport graphique, vous pouvez vérifier ou ajuster les termes FilterXML que vous avez définis dans la section de filtre avancé de la boîte de dialogue Filtre local de l'interface de la visionneuse.

Exemple de spécification de filtre au format XML

Cet exemple montre un appel getQueryViewer avec une instruction de filtre. Les termes de filtre sont présentés dans leur forme développée pour plus de clarté.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panel
s/System_Event_Count_By_Event_Action&server=ELMSERVER&filterXml=
  <Filter logic="" lparens="1" col="source_username" oper="LIKE" val="su" rparens="0"/>
  <Filter logic="AND" lparens="0" col="event_logname" oper="LIKE" val="CALM" rparens="1"/>
</Scope>
```

"&filterxml=" spécifie qu'une instruction de filtre suit.

L'instruction de filtre définit la requête pour rechercher "su" dans la colonne source_username et "CALM" dans la colonne event_logname. Etant donné que l'instruction AND joint les deux termes (Filter logic="AND"), seuls les événements pour lesquels chaque valeur est trouvée dans sa colonne respective sont renvoyés.

Spécifications de filtre d'accès au format XML

Lors de l'authentification à l'aide du mécanisme du nom et du mot de passe du certificat, vous pouvez prédéfinir des filtres CA Enterprise Log Manager de requêtes ou de rapports au format XML. Un filtre XML d'accès transmis dans un appel de connexion est appliqué à toutes les requêtes et tous les rapports exécutés dans la même session. Si vous transmettez un filtre XML à la requête ou au rapport suite à une connexion avec un filte d'accès au format XML, CA Enterprise Log Manager appliquera les deux filtres pour obtenir des résultats.

Les éléments du filtre d'accès au format XML sont identiques à ceux du filtre XML.

Exemple de spécification de filtre d'accès au format XML sans filtre XML

Cet exemple illustre un appel getQueryViewer à l'aide d'une instruction de filtre XML. Les termes de filtre sont présentés dans leur forme développée pour plus de clarté.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panel
s/System_Event_Count_by_Event_Source&certname=test&password=test&accessFilterXml=<AccessScope><Fi
lter logic="" lparens="0" col="event_logname"oper="LIKE" val="CALM" rparens="0"/></AccessScope>
```

"&accessFilterXml=" spécifie qu'une instruction de filtre d'accès suit.

Exemple de spécification de filtre d'accès au format XML avec filtre XML

Cette exemple illustre un appet objectId à l'aide d'instructions de filtre XML et de filtre d'accès au format XML.

```
https://ELMSERVER:5250/spin/calmapi/runQuery.csp?objectId=Subscription/panels/System_Event_Count_
by_Event_Source&filterXml=<Scope><Filter logic="" lparens="1"  col="event_logname" oper="INSET"
val="'CALM','Unix'"
rparens="1"/></Scope>&certname=test&password=test&accessFilterXml=<AccessScope><Filter logic=""
lparens="1" col="event_logname" oper="LIKE" val="CALM" rparens="1"/></AccessScope>
```

"&filterXml=" spécifie qu'une instruction de filtre suit.

"&accessFilterXml=" spécifie qu'une instruction de filtre d'accès suit.

Spécifications IncidentFilter au format XML

Vous pouvez prédéfinir des filtres CA Enterprise Log Manager pour les rapports d'incidents au format XML et les ajouter à l'URL d'un appel getReportViewer à l'aide du terme IncidentFilterXML. Pour imbriquer plusieurs filtres, utilisez les termes AND et OR et des parenthèses. Les spécifications IncidentFilter fonctionnent de la même manière que les spécifications Filter et partagent les mêmes éléments et opérateurs.

Les spécifications IncidentFilter au format XML s'appliquent uniquement aux requêtes d'incidents contenues dans des rapports. Toutefois, un rapport peut contenir des requêtes d'incident et d'événement. Pour accéder à un rapport et lui appliquer un filtre, l'URL D'API peut contenir les deux spécifications FilterXML et IncidentFilterXml.

Important : Les termes IncidentFilterXml sont complexes et l'API ne procède à aucune validation. Les termes de filtre non valides produisent une erreur de requête. Pour cette raison, nous vous conseillons de procéder avec précaution pour créer des termes de filtre.

Exemple de spécification IncidentFilter au format XML

Cet exemple montre un appel getReportViewer avec une instruction de filtre. Les termes de filtre sont présentés dans leur forme développée pour plus de clarté.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/Incidents_by_Priority=ELMSERVER&incidentfilterXml=

<Filter logic="AND" lparens="1" col="incident_createtime_gmt" colfunc="" oper="GREATEQ"
val="1285854741" rparens="0" filterTag="" substituteValue="false" isDynamic="true"/>

<Filter logic="AND" lparens="0" col="incident_createtime_gmt" colfunc="" oper="LEQ"
val="1285876341" rparens="1" filterTag="" substituteValue="false" isDynamic="true"/>
```

"&incidentfilterxml=" spécifie qu'une instruction de filtre d'accès suit.

Le filtre spécifie tous les incidents créés sur une période de temps spécifique.

Informations complémentaires :

Spécifications de filtre au format XML (page 44)

Spécifications de conditions de résultat

Utilisez les termes param pour définir les conditions de résultat pour un appel getQueryViewer, getReportViewer ou runQuery call.

Les termes param suivants sont disponibles :

ARG_limit

Définit le nombre de lignes renvoyées par la requête.

ARG_show_other

Indique à l'aide de la valeur true ou false si show other column (afficher l'autre colonne) apparaît dans une visionneuse de requête. Cette option est utilisée pour les graphiques ayant des requêtes de type N premiers (requêtes cumulées avec une limite de lignes définie et cumulées selon le nombre d'événements (event_count)). Si cette option est sélectionnée, les premiers événements N -1 (N étant la limite de lignes) sont affichés normalement. Toutefois, le Nième événement est l'"autre événement" qui est un événement cumulé basé sur le reste des événements.

ARG_event_datetime

Définit le niveau de détail de la période utilisée dans l'affichage des requêtes pour les requêtes de tendance. Les valeurs disponibles sont :

- event_datetime
- event_day_datetime
- event_minute_datetime
- event_hour_datetime
- event_month_datetime
- event_year_datetime

ARG_start

Définit l'heure de début dynamique de la requête.

ARG_stop

Définit l'heure de fin dynamique de la requête.

ARG_minduring

Définit l'événement regroupé le plus ancien dont la date est ultérieure à une période dynamique spécifiée. Uniquement pertinent pour les requêtes groupées.

ARG_maxduring

Définit le dernier événement regroupé dont la date est ultérieure à une période dynamique spécifiée. Uniquement pertinent pour les requêtes groupées.

ARG_maxbefore

Définit le dernier événement regroupé dont la date est antérieure à une période dynamique spécifiée. Uniquement pertinent pour les requêtes groupées.

ARG_sumatleast

Définit le nombre minimal d'événements à regrouper. Uniquement pertinent pour les requêtes groupées.

ARG_sumatmost

Définit le nombre maximal d'événements dans le regroupement. Uniquement pertinent pour les requêtes groupées.

Exemple de spécification de condition de résultat

Dans cet exemple, les termes params sont présentés dans leur forme développée pour plus de clarté.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panel
s/System_Event_Count_By_Event_Action
<Params>
  <Param id="ARG_limit" val="'200'"/>
</Params>
```

La définition de valeur "ARG_limit" sur 200 permet d'afficher uniquement les 200 premières lignes.

Termes de période dynamique

Utilisez les termes params de période dynamique pour spécifier les périodes auxquelles une requête s'applique. Il suffit pour cela de les ajouter à certaines spécifications de condition de résultat.

Les termes params de période dynamique sont les suivants :

Terme	Description
now	Heure courante
start of day	Début du jour courant

weekday <number>	Jour numéroté de la semaine ■ Dimanche 0 ■ Lundi 1 ■ Mardi 2 ■ Mercredi 3 ■ Jeudi 4 ■ Vendredi 5 ■ Samedi 6
start of month	Début du mois courant
start of year	Début de l'année courante
<number> seconds	Nombre de secondes
<number> minutes	Nombre de minutes
<number> hours	Nombre d'heures
<number> days	Nombre de jours

Vous pouvez spécifier des conditions de résultats pour une définition de requête ou de rapport. Dans ce cas, les spécifications de période que vous ajoutez à l'appel remplacent les valeurs spécifiées dans la requête ou le rapport de base.

Dans les deux cas, les valeurs non spécifiées dans l'URL restent inchangées.

Exemple de spécification de termes de période dynamique

Dans cet exemple, les termes params sont présentés dans leur forme développée pour plus de clarté.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Su
bscription/panels/System_Event_Count_By_Event_Action
<Params>
  <Param id="ARG_start" val="'now', '-12 hours'"/>
  <Param id="ARG_stop" val="'now'"/>
</Params>
```

Les valeurs 'now' et '-12 hours' de "ARG_start" définissent la requête de façon à ce qu'elle commence 12 heures plus tôt par rapport à l'heure courante.

La valeur 'now' de "ARG_stop" définit la requête de sorte qu'elle se termine à l'heure courante. Par conséquent, cette requête recueillera des données uniquement pour les 12 dernières heures.

Informations complémentaires :

Spécifications de conditions de résultat (page 48)
runQuery (page 55)

Requêtes d'invite

Les invites sont des requêtes spécialisées qui vous permettent d'entrer certaines valeurs de filtre avant de les exécuter. Utilisez la commande getQueryList pour afficher les requêtes d'invite disponibles. L'élément "Prompt id" identifie les requêtes d'invite, l'élément "Panel id", quant à lui, identifie les requêtes standard. Vous pouvez utiliser les termes prompt, promptvalue et col pour définir les requêtes d'invite que vous voulez appeler.

Vous pouvez accéder à la requête d'invite graphique sans spécifier les valeurs de filtre, ou les préspécifier dans l'URL. Si aucune colonne n'est indiquée dans l'URL, toutes les colonnes d'invite sont sélectionnées.

Exemple d'invite Hôte non filtrée

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/HostPrompt
```

Affiche l'invite Hôte sans aucune valeur de filtre entrée mais avec toutes les colonnes d'invite sélectionnées.

Exemple d'invite IP filtrée

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/IPPrompt&prompt=true&promptvalue=255.255.255.0&col=dest_address
```

Exécute l'invite IP afin de rechercher l'adresse IP 255.255.255.0 dans la colonne des adresses de destination.

"&prompt=true" indique les contrôles d'invite vous permettant de modifier les valeurs de la requête d'invite après son exécution et de l'exécuter de nouveau si besoin.

"&promptvalue=" spécifie l'adresse IP voulue.

"&col=dest_address" sélectionne la colonne d'événements voulue.

Informations complémentaires :

getQueryList (page 25)
runQuery (page 55)

getReportViewer

Utilisez la commande getReportViewer pour afficher la visionneuse graphique d'un rapport. La visionneuse de rapports est similaire à l'interface d'affichage de rapports CA Enterprise Log Manager fournie en tant que composant autonome. Vous pouvez intégrer des rapports dans une interface d'application externe ou un portail externe en intégrant leur URL dans un cadre intégré ou un portlet.

Remarque : La solution fournie ici fonctionne avec les applications Web (JSP, JavaScript et HTML). Il est en revanche possible que la solution *ne* fonctionne pas dans les applications C++ ou Java Swing si celles-ci ne prennent pas en charge l'intégration de pages HTML ni le plug-in FLASH nécessaire. Dans le cas des applications ne prenant pas en charge le plug-in FLASH, nous vous conseillons d'utiliser getReportList pour déterminer quelles requêtes sont incluses dans les rapports, puis d'utiliser runQuery pour chaque rapport afin de récupérer les données brutes et les restituer graphiquement selon une méthode appropriée à votre environnement.

Exemple d'appel getReportViewer

Dans cet exemple le rapport Collection Monitor by Log Manager (Contrôleur de collecte par gestionnaire de journaux) est appelé.

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getReportViewer&objectId=Subscription/scorecards/Collection_Monitor_by_Log_Manager
```

Vous pouvez utiliser le filtre et d'autres spécifications pour getReportViewer comme pour getQueryViewer.

Pour spécifier le nom d'un rapport, il suffit d'entrer son nom tel qu'il apparaît dans l'interface, en séparant les mots par des caractères de soulignement.

Informations complémentaires :

getReportList (page 28)
runQuery (page 55)

getIncidentViewer

La commande getIncidentViewer permet d'afficher une visionneuse d'incidents graphiques. Celle-ci est similaire à la visionneuse d'incidents de l'interface CA Enterprise Log Manager, fournie comme composant autonome. Les fonctions de gestion disponibles à partir de l'interface de CA Enterprise Log Manager (fusion, suppression d'incidents) ne sont pas exécutables à partir de cette visionneuse.

Remarque : La solution fournie ici fonctionne avec les applications Web (JSP, JavaScript et HTML). Il est en revanche possible que la solution *ne* fonctionne pas dans les applications C++ ou Java Swing si celles-ci ne prennent pas en charge l'intégration de pages HTML ni le plug-in FLASH nécessaire.

Exemple de commande getIncidentViewer

```
https://elmserver:5250/spin/calmapi/getObject.csp?type=getIncidentViewer
```

Cet appel permet d'afficher la visionneuse d'incidents, qui contient les incidents créés au cours des six dernières heures.

Vous pouvez utiliser des termes de période, des filtres et d'autres spécifications pour getIncidentViewer comme pour getQueryViewer.

runQuery

Utilisez runQuery pour exécuter une requête qui affichera les résultats au format XML et non dans la visionneuse de requêtes graphique. De cette manière, vous pouvez obtenir des données CA Enterprise Log Manager pour une application qui ne peut pas intégrer directement la visionneuse de requêtes ou de rapports, comme c'est le cas avec les applications ne prenant pas en charge le plug-in Flash.

Ajoutez des spécifications à l'URL pour filtrer la requête de base comme pour getQueryViewer.

Après avoir utilisé runQuery, formatez les données XML de manière à les afficher de la manière appropriée pour votre environnement. Par exemple, vous pouvez intégrer un appel runQuery dans un portail Web et appliquer une feuille de style pour afficher les données.

Exemple d'appel runQuery

```
https://ELMSERVER:5250/spin/calmapi/runQuery.csp?objectId=Subscription/panels/Collection_Monitor_by_Log_Manager_By_Log_Name
```

Renvoie le code XML suivant :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
        <Value>true</Value>
        <Description>Query run successful</Description>
        <QueryResults>
                <Version>1</Version>
                <Row number="1">
                        <event_logname>CALM</event_logname>
                        <event_count>581</event_count>
                </Row>
                <Row number="2">
                        <event_logname>EiamSdk</event_logname>
                        <event_count>131</event_count>
                </Row>
                <Result totalrows="2" returnedrows="2" startrow="1" endrow="2" executems="2382"
mstofirst="2382" mstolast="2382" />
                <DbResult numberdbsqueried="1" numberdbsresponding="1" numberdbsnotresponding="0"
listdbsresponding="../../LogManager/data/hot/machinename_1232571874.hot" listdbsnotresponding=""
/>
                <HostResult numbberhostsqueried="0" numberhostsresponding="0"
numberhostsnotresponding="0" listhostsresponding="" listhostsnotresponding="" />
        </QueryResults>
```

```
       SQL ServerSELECT event_logname , SUM(event_count) AS FUNC_SUM_event_count FROM view_event
WHERE ( ( datetime(event_time_gmt, 'unixepoch') >= datetime('now', '-6 hours') and
datetime(event_time_gmt, 'unixepoch') < datetime('now') ) AND ( event_category = ? ) ) GROUP BY
event_logname ORDER BY FUNC_SUM_event_count DESC LIMIT 10 ; [Operational Security]</Sql>
</Result>
```

Informations complémentaires :

getQueryViewer (page 39)
getReportViewer (page 53)

Enregistrement avec l'API

Cette section contient des informations sur l'enregistrement de produits avec CA Enterprise Log Manager. La page d'enregistrement des produits de l'API vous permet de créer des certificats d'enregistrement qui permettent l'authentification unique de produits externes. Vous pouvez enregistrer plusieurs produits dans une seule interface, ce qui vous évite de devoir créer plusieurs appels d'enregistrement. Les pages d'enregistrement de produits permettent de créer des certificats dans presque tous les cas.

Cette section décrit également des appels d'enregistrement que vous pouvez utiliser lorsqu'il n'est pas possible ou qu'il n'est pas conseillé d'utiliser la page d'enregistrement des produits ou l'authentification unique.

Informations complémentaires :

Création de certificats API (page 57)
Enregistrer un produit (page 61)
Annuler l'enregistrement d'un produit (page 62)

Création de certificats API

Accédez à la page de l'interface d'enregistrement des produits de l'API pour créer des certificats d'enregistrement à authentication unique, afficher une liste des produits enregistrés ou annuler l'enregistrement de produits en supprimant des certificats existants.

Si nécessaire, vous pouvez ajouter des informations d'authentification à l'URL. Si vous n'êtes pas authentifié, vous êtes redirigé vers la page de connexion CA Enterprise Log Manager. Ce comportement est le même pour tous les autres appels API qui affichent une interface utilisateur.

Remarque : Utilisez le nom d'utilisateur et le mot de passe EiamAdmin pour créer un certificat d'enregistrement. Pour afficher les produits enregistrés ou annuler l'enregistrement de certains produits, vous *pouvez* utiliser les informations d'identification EiamAdmin mais les informations d'identification de l'administrateur suffisent.

Exemple d'affichage de page de certification

```
URL: https://ELMSERVER:5250/spin/calmapi/products.csp
```

Affiche la page de connexion CA Enterprise Log Manager. Lorsque vous entrez les informations d'identification appropriées, la page d'enregistrement de produits apparaît.

Consultez *l'aide de l'API CA Enterprise Log Manager*, accessible à partir de la page d'enregistrement des produits, pour plus d'informations sur la création de certificats.

Informations complémentaires :

Enregistrer un produit (page 61)
Appels de la visionneuse de requêtes et de rapports (page 38)
Authentification API (page 15)

Comment enregistrer un produit avec CA Enterprise Log Manager

Vous pouvez enregistrer un produit avec CA Enterprise Log Manager pour autoriser l'authentification unique. Vous pouvez accéder aux requêtes et aux rapports CA Enterprise Log Manager par la gestion des mots de passe, par la gestion des accès ou par toute autre application en fonction de vos besoins. Le processus d'enregistrement est composé de deux étapes.

1. Création d'un certificat d'enregistrement avec CA Enterprise Log Manager.
2. Utilisation du nom du certificat d'enregistrement et du mot de passe à partir de votre produit tiers pour terminer l'enregistrement à authentification unique.

   La procédure exacte concernant cette étape diffère selon le produit que vous souhaitez enregistrer avec CA Enterprise Log Manager. Cependant, il vous faut les informations suivantes pour terminer l'enregistrement.

   - Le nom d'hôte ou l'adresse IP du serveur CA Enterprise Log Manager sur lequel vous souhaitez effectuer l'enregistrement
   - Le nom du certificat créé à l'étape 1
   - Le mot de passe du certificat créé à l'étape 1

Informations complémentaires :

Créer un certificat d'enregistrement (page 59)

Créer un certificat d'enregistrement

Vous pouvez créer un certificat d'enregistrement pour permettre l'authentification unique à partir d'autres produits CA ou tiers.

Pour créer un certificat d'enregistrement

1. Ouvrez un navigateur Web et entrez l'URL ci-dessous.

   ```
   https://calmserver:5250/spin/calmapi/products.csp
   ```

   Remplacez "calmserver" par le nom du serveur ou l'adresse IP du serveur CA Enterprise Log Manager sur lequel vous souhaitez enregistrer des produits.

   Si vous n'êtes pas déjà authentifié en tant qu'utilisateur EiamAdmin, l'écran de connexion s'affiche. Si vous êtes déjà authentifié, la page Enregistrement du produit s'affiche.

2. Entrez le nom d'utilisateur EiamAdmin et son mot de passe.

   Une liste de tous les certificats d'enregistrement actuels s'affiche.

   Remarque : Pour créer un certificat, vous devez avoir les informations d'identification de l'utilisateur EiamAdmin. Les informations d'identification de l'administrateur suffisent pour lister les produits et annuler leur enregistrement.

3. Cliquez sur le lien Enregistrer au-dessus de la liste Produits enregistrés dans le volet de gauche.

4. Saisissez un nom ainsi qu'un mot de passe pour le produit que vous souhaitez enregistrer.

   Remarque : Assurez-vous de conserver le nom du certificat ainsi que le mot de passe. Vous en aurez besoin pour terminer le processus d'enregistrement à partir du produit tiers.

5. Dans le volet de droite, cliquez sur le bouton Enregistrer.

   Un message de confirmation s'affiche et le nom du certificat apparaît dans la liste Produits enregistrés.

Annuler l'enregistrement d'un produit

Vous pouvez annuler l'enregistrement d'un produit en supprimant le certificat d'enregistrement.

Pour annuler l'enregistrement d'un produit

1. Ouvrez un navigateur Web et entrez l'URL ci-dessous.

   `https://calmserver:5250/spin/calmapi/products.csp`

   Remplacez "calmserver" par le nom ou l'adresse IP du serveur CA Enterprise Log Manager sur lequel vous souhaitez annuler l'enregistrement de produits.

   L'écran Connexion s'affiche.

2. Saisissez un nom d'utilisateur du rôle Administrator et un mot de passe.

   Une liste de tous les certificats d'enregistrement actuels s'affiche.

3. Cliquez sur le certificat d'enregistrement à supprimer.

4. Cliquez sur Annuler l'enregistrement.

   Une boîte de dialogue de confirmation s'affiche.

5. Cliquez sur OK.

   Un message de confirmation s'affiche et le nom du certificat disparaît de la liste Produits enregistrés.

Enregistrer un produit

Utilisez l'appel registerProduct pour enregistrer un produit à des fins d'authentification unique. Lorsque vous enregistrez un produit, un certificat est créé et enregistré dans la base de données de gestion. Utilisez cet appel lorsqu'il n'est pas possible ou qu'il n'est pas conseillé d'accéder à l'interface d'enregistrement des produits.

Par exemple, si vous intégrez un produit tiers, il n'est pas conseillé de transmettre le mot de passe EiamAdmin le plus largement possible pour permettre la création de son certificat. Dans ce cas, il est préférable de créer un certificat et un mot de passe et de les transmettre uniquement aux utilisateurs du produit pour qu'ils puissent procéder à son intégration.

Exemples d'appel registerProduct

```
https://ELMSERVER:5250/spin/calmapi/calmapi/registerProduct.csp?action=register&c
ertname=YourProductName&certpassword=CertPassword&certname=xxxxx&password=xxxxxx
```

Dans ce cas "&certname=YourProductName" définit le produit que vous voulez enregistrer. Remplacez "YourProductName" par le nom du produit que vous voulez enregistrer.

"&certname=xxxxx" indique le nom du certificat et le mot de passe valides.

Réponse en cas de réussite :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>true</Value>
        <Description>The product has been registered successfully.   The default
access rights on the ELM application have been provided.</Description>
</Result>
```

Réponse en cas d'échec :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>false</Value>
        <Description> EE_POZERROR Repository Error</Description>
</Result>
```

Remarque : Une erreur se produit souvent lorsque le certificat avec le nom indiqué dans l'URL a déjà été créé. "EE_AUTHFAILED Authentication failed" est une erreur courante qui indique que le mot de passe est incorrect.

Annuler l'enregistrement d'un produit

Utilisez la commande d'annulation d'enregistrement pour annuler l'enregistrement d'un produit. Utilisez cet appel lorsqu'il n'est pas possible ou qu'il n'est pas conseillé d'accéder à l'interface d'enregistrement des produits pour supprimer un certificat d'enregistrement.

Exemples d'URL d'annulation d'enregistrements :

```
https://ELMSERVER:5250/spin/calmapi/calmapi/registerProduct.csp?action=unregister
&certname=YourProductName&username=Administrator&password=adminpassword
```

Dans ce cas "&username=Administrator" indique un utilisateur CA Enterprise Log Manager avec le rôle Administrateur. Remplacez "Administrator" par l'utilisateur disposant du privilège Administrateur.

"&password=adminpassword" indique le mot de passe de l'utilisateur Administrateur. Remplacez "adminpassword" par le mot de passe de l'utilisateur que vous avez spécifié dans "&username=".

Remarque : Utilisez le nom d'utilisateur et le mot de passe EiamAdmin pour enregistrer un produit. Pour afficher les produits enregistrés ou annuler l'enregistrement de certains produits, vous *pouvez* utiliser les informations d'identification EiamAdmin mais les informations d'identification de l'administrateur suffisent.

Réponse en cas de réussite :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>true</Value>
        <Description>The product has been unregistered successfully. The default
access rights have been revoked. </Description>
</Result>
```

Réponse en cas d'échec :

```
<?xml version="1.0" encoding="UTF-8" ?>
<Result>
<Value>false</Value>
        <Description> EE_POZERROR Repository Error</Description>
</Result>
```

Remarque : Une erreur se produit souvent lorsque l'enregistrement d'un produit a déjà été annulé ou si ce produit n'existe pas. "EE_AUTHFAILED Authentication failed" est une erreur courante qui indique que le mot de passe est incorrect.

Chapitre 5 : Intégration de CA Enterprise Log Manager dans un portail Web

Vous pouvez intégrer des requêtes ou des rapports CA Enterprise Log Manager dans un portail Web pour afficher le contenu que vous souhaitez consulter. La procédure est la suivante :

1. Identifiez le contenu CA Enterprise Log Manager que vous voulez afficher et créez l'appel API pour l'obtenir.
2. Intégrez le contenu sélectionné dans le portail Web.

Informations complémentaires :

Identification du contenu (page 66)
Intégration du contenu dans un portail Liferay (page 67)
Appels de la visionneuse de requêtes et de rapports (page 38)

Identification du contenu

Avant de commencer la procédure d'intégration de contenu CA Enterprise Log Manager, déterminez le contenu que vous souhaitez afficher. Dans l'interface CA Enterprise Log Manager, recherchez le rapport ou la requête qui contient les informations dont vous avez besoin.

Pour afficher des requêtes ou des rapports CA Enterprise Log Manager dans un portail Web, utilisez l'appel getQueryViewer ou getReportViewer. Les requêtes et les rapports interactifs seront alors affichés avec la plupart des fonctionnalités disponibles de l'interface CA Enterprise Log Manager.

Vous pouvez également utiliser le rapport runQuery pour obtenir le contenu au format XML. Il suffit alors de lui appliquer une feuille de style pour l'afficher. L'affichage n'est pas interactif, ce qui vous permet d'afficher les données sans devoir recourir au plug-in Flash.

Dans cet exemple, le rapport System All Events Detail (Détail de tous les événements du système) est appelé à l'aide de getQueryViewer pour afficher une table de tous les événements dans une visionneuse. La syntaxe de l'appel API pour ce rapport est la suivante :

```
https://ELMSERVER:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_All_Events_Detail&username=xxx&password=xxx
```

- Pour utiliser l'appel dans votre environnement, remplacez la partie "ELMSERVER" de l'URL par le nom d'hôte ou l'adresse IP du serveur contenant les données que vous recherchez.
- Dans cet exemple, l'appel est authentifié avec un nom d'utilisateur et un mot de passe CA Enterprise Log Manager : "&username=xxx&password=xxx". Cette méthode d'authentification est recommandée pour l'intégration de contenu CA Enterprise Log Manager dans une page Web. Remplacez 'xxx' par un nom d'utilisateur et un mot de passe CA Enterprise Log Manager. Si vous ne voulez pas que le nom d'utilisateur et le mot de passe soient visibles dans l'URL, vous pouvez les définir comme valeurs masquées si votre portail Web le permet.

Pour tester la syntaxe finale, entrez l'URL que vous avez créée dans un navigateur et vérifiez que la requête ou le rapport voulu apparaît.

Informations complémentaires :

Authentification API (page 15)
Appels de la visionneuse de requêtes et de rapports (page 38)
getQueryViewer (page 39)
getReportViewer (page 53)
runQuery (page 55)

Intégration du contenu dans un portail Liferay

Après avoir créé l'appel API vous permettant d'obtenir la requête ou le rapport voulu, intégrez-le dans le portail Web à l'aide d'un cadre intégré ou d'un portlet qui affichera le contenu CA Enterprise Log Manager.

Cet exemple utilise le portail Liferay créé selon les instructions d'installation et de configuration de Liferay. Le portail Web que vous utilisez peut comporter des contrôles similaires. Consultez la documentation de ce portail Web pour créer des cadres intégrés ou des portlets.

Pour intégrer du contenu dans un portail Liferay

1. Créez une page ou ouvrez une page que vous voulez modifier dans Liferay
2. Cliquez sur l'icône des outils dans l'angle supérieur droit de la page, à côté du message de bienvenue.
3. Sélectionnez Add Application (Ajouter une application) dans le menu.

   La boîte de dialogue Add Application apparaît et affiche les catégories d'application.
4. Développez la catégorie Sample (Echantillon) et cliquez sur Add (Ajouter) en regard de l'application de cadre intégré.

   Un nouveau portlet de cadre intégré apparaît dans la page.
5. Cliquez sur le lien de configuration dans le portlet et entrez le texte de l'appel API dans le champ de l'URL source.
6. Cliquez sur Enregistrer.

   Le contenu que vous avez sélectionné apparaît dans le cadre intégré.
7. Configurez d'autres cadres intégrés ou publiez le portail Web en suivant les instructions de la documentation Liferay.

Chapitre 6 : Dépannage API

Si vos appels API ne fonctionnent pas de manière satisfaisante, suivez les instructions de dépannage ci-dessous pour tester chacun d'eux et vérifier qu'ils produisent les résultats attendus.

1. Vérifiez la syntaxe de l'URL d'appel :
   a. Comparez la syntaxe que vous avez créée à l'exemple approprié dans le manuel pour vérifier que le nom ou l'adresse IP du serveur CA Enterprise Log Manager est correcte.
   b. Si vous avez ajouté des spécifications de requête ou de rapport, vérifiez que la partie principale de l'appel (avant les paramètres de spécification) se termine par le caractère ? avant d'ajouter d'autres paramètres. Exemple :

      ```
      ?param1=val1&param2=val2
      ```

2. Si aucune donnée n'apparaît alors que la syntaxe de l'URL est correcte, vérifiez les filtres. Si vous utilisez getQueryViewer ou getReportViewer, vérifiez les filtres et les paramètres de condition de résultat dans l'interface. Si vous utilisez runQuery, vérifiez les spécifications de paramètre que vous avez ajoutées à l'URL :
   a. **Vérification des filtres** - Vérifiez que les filtres de base affichent les données voulues. Par exemple, vérifiez que le nom de la source d'événement utilisé comme filtre est correct.
   b. **Syntaxe** - Vérifiez que la syntaxe des filtres est correcte, surtout si vous avez utilisé des paramètres de spécification pour créer les filtres.
   c. **Filtres de période** : Assurez-vous d'indiquer une période suffisamment longue et que le fuseau horaire de votre système d'exploitation est identique à celui de CA Enterprise Log Manager.
   d. **Filtre d'accès au format XML** : Assurez-vous de fermer correctement votre session.
   e. **Journal LogDepot** - Vérifiez que les événements sont reçus et qu'ils figurent dans le fichier logDepot_sponsor.log.
3. Vérifiez les paramètres de journalisation pour le composant API. Vérifiez que les fichiers et les paramètres suivants existent :
   - Fichier des propriétés : epSIM_logging.properties
   - Le niveau par défaut est WARN
   - Enregistreur : logmanager.ui.calmapi

- Fichier journal : calm.log