CA Enterprise Log Manager

API-Programmierhandbuch

r12.5

Diese Dokumentation, die eingebettete Hilfesysteme und elektronisch verteilte Materialien beinhaltet (im Folgenden als "Dokumentation" bezeichnet), dient ausschließlich zu Informationszwecken des Nutzers und kann von CA jederzeit geändert oder zurückgenommen werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung von CA weder vollständig noch auszugsweise kopiert, übertragen, vervielfältigt, veröffentlicht, geändert oder dupliziert werden. Diese Dokumentation enthält vertrauliche und firmeneigene Informationen von CA und darf vom Nutzer nicht weitergegeben oder zu anderen Zwecken verwendet werden als zu denen, die (i) in einer separaten Vereinbarung zwischen dem Nutzer und CA über die Verwendung der CA-Software, auf die sich die Dokumentation bezieht, zugelassen sind, oder die (ii) in einer separaten Vertraulichkeitsvereinbarung zwischen dem Nutzer und CA festgehalten wurden.

Ungeachtet der oben genannten Bestimmungen ist der Benutzer, der über eine Lizenz für das bzw. die in dieser Dokumentation berücksichtigten Software-Produkt(e) verfügt, berechtigt, eine angemessene Anzahl an Kopien dieser Dokumentation zum eigenen innerbetrieblichen Gebrauch im Zusammenhang mit der betreffenden Software auszudrucken, vorausgesetzt, dass jedes Exemplar diesen Urheberrechtsvermerk und sonstige Hinweise von CA enthält.

Dieses Recht zum Drucken oder anderweitigen Anfertigen einer Kopie der Dokumentation beschränkt sich auf den Zeitraum der vollen Wirksamkeit der Produktlizenz. Sollte die Lizenz aus irgendeinem Grund enden, bestätigt der Lizenznehmer gegenüber CA schriftlich, dass alle Kopien oder Teilkopien der Dokumentation an CA zurückgegeben oder vernichtet worden sind.

SOWEIT NACH ANWENDBAREM RECHT ERLAUBT, STELLT CA DIESE DOKUMENTATION IM VORLIEGENDEN ZUSTAND OHNE JEGLICHE GEWÄHRLEISTUNG ZUR VERFÜGUNG; DAZU GEHÖREN INSBESONDERE STILLSCHWEIGENDE GEWÄHRLEISTUNGEN DER MARKTTAUGLICHKEIT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET CA GEGENÜBER IHNEN ODER DRITTEN GEGENÜBER FÜR VERLUSTE ODER UNMITTELBARE ODER MITTELBARE SCHÄDEN, DIE AUS DER NUTZUNG DIESER DOKUMENTATION ENTSTEHEN; DAZU GEHÖREN INSBESONDERE ENTGANGENE GEWINNE, VERLORENGEGANGENE INVESTITIONEN, BETRIEBSUNTERBRECHUNG, VERLUST VON GOODWILL ODER DATENVERLUST, SELBST WENN CA ÜBER DIE MÖGLICHKEIT DIESES VERLUSTES ODER SCHADENS INFORMIERT WURDE.

Die Verwendung aller in der Dokumentation aufgeführten Software-Produkte unterliegt den entsprechenden Lizenzvereinbarungen, und diese werden durch die Bedingungen dieser rechtlichen Hinweise in keiner Weise verändert.

Diese Dokumentation wurde von CA hergestellt.

Zur Verfügung gestellt mit „Restricted Rights“ (eingeschränkten Rechten) geliefert. Die Verwendung, Duplizierung oder Veröffentlichung durch die US-Regierung unterliegt den in FAR, Absätze 12.212, 52.227-14 und 52.227-19(c)(1) bis (2) und DFARS, Absatz 252.227-7014(b)(3) festgelegten Einschränkungen, soweit anwendbar, oder deren Nachfolgebestimmungen.

Copyright © 2010 CA. Alle Rechte vorbehalten. Alle Marken, Produktnamen, Dienstleistungsmarken oder Logos, auf die hier verwiesen wird, sind Eigentum der entsprechenden Rechtsinhaber.

CA-Produktreferenzen

Dieses Dokument bezieht sich auf die folgenden Produkte von CA:

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

Technischer Support – Kontaktinformationen

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

Änderungen in der Dokumentation

Seit der letzten Version dieser Dokumentation wurden folgende Aktualisierungen vorgenommen:

- getObject - Dieses vorhandene Thema enthält eine Beschreibung des Befehls "getIncidentModel".
- getIncidentModel - Dieses neue Thema enthält ein Beispiel des Befehls "getIncidentModel".

Inhalt

Kapitel 1: Über dieses Handbuch

Das *CA Enterprise Log Manager-API-Programmierhandbuch* enthält Anweisungen zur Verwendung der CA Enterprise Log Manager-API, um mit den Abfrage- und Berichtsmechanismen auf Daten des Ereignis-Repositorys zuzugreifen und diese in einem Webbrowser anzuzeigen. Sie können die API auch verwenden, um CA Enterprise Log Manager-Abfragen oder -Berichte in eine CA-Benutzeroberfläche oder die Benutzeroberfläche eines Drittanbieters einzubetten.

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

Kapitel 2: Informationen zur CA Enterprise Log Manager-API

Die CA Enterprise Log Manager-API verwendet eine Webanwendung, die HTTPS-Post-Befehle akzeptiert, um die Abfrage- oder Berichtsinformationen zurückzugeben, die Sie benötigen. Die Webanwendung besteht aus einer dedizierten iGateway-Spindle.

Sie verwenden spezielle URLs, die Argumente enthalten, die steuern, welche Daten zurückgegeben und wie diese gefiltert werden. Jeder verfügbare URL/API-Befehl überprüft, ob der Aufrufer durch Überprüfung der Sitzungs-ID oder Zertifikatsanmeldeinformationen authentifiziert wurde. Alle HTTPS-Anforderungen müssen einen Typ dieser Authentifizierungsinformationen enthalten.

Zu den CA Enterprise Log Manager API-Funktionen zählen:

- Authentifizierte, sichere APIs
- Produktregistrierung für Single Sign-On (SSO)
- Abruf von nach Kennungen gefilterten Abfrage- oder Berichtslisten
- Anzeige einer Abfrage oder eines Berichts in der interaktiven CA Enterprise Log Manager-Benutzeroberfläche, die das Filtern und Einbetten in eine Benutzerschnittstelle zulässt

Für eine effektive Verwendung der CA Enterprise Log Manager API-Aufrufe müssen Sie mit der Föderationsstruktur Ihrer Umgebung, den verfügbaren Abfragen und Berichten sowie den Benutzerrollen und deren Zugriffsrechten vertraut sein.

Weitere Informationen

CA Enterprise Log Manager-API-Struktur (siehe Seite 13)
API-Authentifizierung (siehe Seite 15)
CA Enterprise Log Manager-API-Beispiele (siehe Seite 21)

API-Aufrufrückgaben

Alle API-Befehle, mit Ausnahme von "getQueryViewer" und "getReportViewer", geben ein Element im XML-Format zurück, das beschreibt, ob der Befehl erfolgreich war und den Grund nennt, wenn der Befehl erfolglos war.

Beispiel für eine API-Rückgabe

```
<?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>
```

In diesem Fall zeigt der Ergebniswert "true" die erfolgreiche Ausführung an, und die Beschreibung enthält den ausgeführten Befehl.

CA Enterprise Log Manager-API-Struktur

Ein CA Enterprise Log Manager-API-Aufruf verwendet das HTTPS-Protokoll, um den Ereignisprotokollspeicher zu kontaktieren. Der Aufruf gibt Ergebnisse im XML-Format oder in Form einer grafischen Abfrage- oder Berichtsanzeige aus, je nachdem welchen Aufruf Sie verwenden.

Jeder Aufruf hat eine definierte URL-Struktur, die aus mehreren gemeinsamen Elementen besteht. Ein API-Anmeldeaufruf sieht beispielsweise wie folgt aus:

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

Das erste Element legt den Zielserver fest:

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

Wenn Sie den Aufruf in Ihrer Umgebung verwenden möchten, ersetzen Sie den "ELMSERVER"-Teil der URL durch den Hostnamen oder die IP-Adresse des Servers, auf dem die Daten gespeichert sind, die Sie benötigen. Port 5250 ist der von CA Enterprise Log Manager verwendete Standardport. Der Text "/spin/calmapi/" bleibt bei allen Aufrufen gleich.

Das zweite Element definiert den API-Aufruf selbst und enthält alle Authentifizierungsdetails:

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

"calmapi_login.csp" ist der Anmeldeaufruf. Der zweite Teil "?username=xx&password=xx" legt die Anmeldeinformationen fest, die für die Anmeldung verwendet werden. In diesem Fall handelt es sich um einen CA Enterprise Log Manager-Benutzernamen und ein CA Enterprise Log Manager-Kennwort.

Weitere Informationen

API-Authentifizierung (siehe Seite 15)
API-Registrierung (siehe Seite 55)

Kapitel 3: API-Authentifizierung

Ihre API-Aufrufe müssen authentifiziert werden, um auf den CA Enterprise Log Manager-Ereignisprotokollspeicher zuzugreifen. Nachfolgenden finden Sie einige Möglichkeiten zum Einrichten der Authentifizierung:

- Verwenden eines gültigen CA Enterprise Log Manager-Benutzernamens und eines gültigen Kennworts als Teil der Authentifizierungs-URL. Überprüfen Sie bei der Erstellung eines Aufrufs, dass die gewünschten Informationen dem Benutzerkonto zur Verfügung stehen, das Sie für die Authentifizierung verwenden möchten.
- Verwenden eines Zertifikatnamens und eines Zertifikatkennworts als Teil der Authentifizierungs-URL. Auf der Registrierungsoberfläche des API-Produkts können Sie ein Zertifikat erstellen. Weitere Informationen zur Erstellung eines Zertifikats finden Sie in der *CA Enterprise Log Manager-API-Online-Hilfe*.
- Verwenden einer Sitzungs-ID als Teil der Authentifizierungs-URL. Diese Sitzungs-ID ist eine eindeutige ID, die nach einem erfolgreichen Authentifizierungsaufruf als Teil der XML-Antwort zurückgegeben wird. Verwenden Sie eine der anderen Authentifizierungsmethoden, um eine Sitzungs-ID zu erhalten, die Sie anschließend zum Erstellen einer anderen Sitzung verwenden können.

Beispiel für Name und Kennwort des Benutzers

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

Dieses Beispiel verwendet den Befehl "getQueryList", und die Authentifizierung erfolgt über einen CA Enterprise Log Manager-Benutzernamen und ein CA Enterprise Log Manager-Kennwort.

Beispiel für Name und Kennwort des Zertifikats

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

Dieses Beispiel verwendet den Befehl "getELMservers", und die Authentifizierung erfolgt über einen Zertifikatsnamen und ein Zertifikatskennwort.

Beispiel für eine Sitzungs-ID

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

Dieses Beispiel verwendet den Befehl "getQueryViewer" und authentifiziert mit Hilfe einer Sitzungs-ID.

Weitere Informationen

API-Anmeldung (siehe Seite 17)
Registrieren eines Produkts (siehe Seite 60)
API-Zertifikaterstellung (siehe Seite 56)

API-Anmeldung

Dieser Aufruf authentifiziert einen Benutzer anhand eines Satzes mit CA EEM-Anmeldeinformationen, eines Zertifikates oder einer Sitzungs-ID.

Da Sie Authentifizierungsinformationen in jede URL eines API-Aufrufs aufnehmen können, benötigen Sie in den meisten Fällen keinen separaten Anmeldeaufruf. Der Anmeldeaufruf ist besonders für das Ausgeben einer Sitzungs-ID nützlich, die anschließend für die Authentifizierung eines anderes Aufrufs, wie "getReportViewer", verwendet werden kann.

Für diesen Aufruf werden folgende Argumente verwendet:

username

Legt den gültigen CA Enterprise Log Manager-Benutzernamen für die Authentifizierung fest.

certname

Legt den Zertifikatsnamen für die Authentifizierung fest, wenn Sie das Produkt registriert haben, das auf CA Enterprise Log Manager zugreifen soll.

password

Legt entweder das CA Enterprise Log Manager-Benutzerkennwort oder das Zertifikatskennwort für die Authentifizierung fest, je nachdem welche Methode Sie für die Authentifizierung verwendet haben.

sessionid

Legt die Sitzungs-ID anhand einer vorhandenen authentifizierten Sitzung fest, die Sie für die Authentifizierung einer neuen Sitzung verwenden können.

Beispiele für API-Anmeldungen

Befehl:

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

Erfolgsmeldung:

```
  <?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>
```

Die von der Anmeldung geöffnete Sitzungs-ID wird im Tag <SessionID> angezeigt.

Fehlermeldung:

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

Weitere Informationen

API-Authentifizierung (siehe Seite 15)
Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)

API-Abmeldung

Dieser Aufruf beendet eine API-Sitzung, indem er einen Benutzer abmeldet, beendet eine Zertifikatssitzung oder eine mit der Sitzungs-ID erstellte Sitzung. Der Aufruf akzeptiert keine Argumente.

Beispiele für API-Abmeldungen

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

Erfolgsmeldung:

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

Fehlermeldung:

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

Informationen zu API-Sitzungen

Jedesmal, wenn Sie einen API-Aufruf verwenden, erstellt CA Enterprise Log Manager eine Sitzung. Die Persistenz dieser Sitzungen ist unterschiedlich, je nachdem welche Authentifizierungsmethode Sie verwenden:

- Benutzername und Kennwort oder mit der Sitzungs-ID authentifizierte Sitzungen laufen genauso ab wie CA Enterprise Log Manager-Sitzungen. Sie verwenden das Zeitlimit für Sitzungen, das standardmäßig auf 15 Minuten festgelegt ist. Sie können das Zeitlimit für Sitzungen auf der CA Enterprise Log Manager-Benutzeroberfläche festlegen.
- Durch Zertifikate authentifizierte Sitzungen laufen nicht ab, mit Ausnahme von ganz bestimmten Umständen. Das Zeitlimit für Sitzungen ist gesperrt, so dass Sie CA Enterprise Log Manager leichter über ein Webportal oder ein außerhalb befindliches Produkt integrieren können. Es können jedoch zusätzliche Aktionen gefordert werden, um eine unnötige Nutzung von Systemressourcen durch persistente Sitzungen zu vermeiden.

CA Enterprise Log Manager schließt durch Zertifikate authentifizierte Sitzungen unter folgenden Umständen:

- Schließen eines Browsers und Anzeigen einer Grafikkomponente, z. B. einer Abfrage
- Abmeldung bei einem außerhalb befindlichen Produkt
- Zulassen eines Ablaufs der Benutzersitzung eines außerhalb befindlichen Produkts

Der CA Enterprise Log Manager-Sitzungszeitgeber beginnt rückwärts zu zählen und beendet die Sitzung, nachdem der von Ihnen konfigurierte Zeitlimitwert abläuft.

Wenn viele "getQueryViewer"- oder "getReportViewer"-Aufrufe verwendet werden, können viele Sitzungen geöffnet und im Leerlauf sein. Um die von solchen Sitzungen verwendeten Systemressourcen zu reduzieren, beenden Sie eine Sitzung mit dem Abmeldebefehl, wenn sich der Benutzer eines außerhalb befindlichen Produkts abmeldet oder die Sitzung eines außerhalb befindlichen Produkts endet.

Weitere Informationen

Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)
API-Authentifizierung (siehe Seite 15)
API-Zertifikaterstellung (siehe Seite 56)
API-Anmeldung (siehe Seite 17)
API-Abmeldung (siehe Seite 19)

Kapitel 4: CA Enterprise Log Manager-API-Beispiele

Dieses Kapitel enthält folgende Themen:

Beispiele für Informationen zu API

Dieses Kapitel enthält Beispiele für API-Aufrufe. Jedes Beispiel beschreibt die benötigte URL und gibt die erwartete XML für Erfolg oder Fehlschlag zurück, falls vorhanden. Sie können diese Aufrufe testen, indem Sie die URL direkt in einen Browser eingeben und die XML-Antwort überwachen.

Die Aufrufe "getQueryViewer" und "getReportViewer" enthalten eher Benutzeroberflächenanzeigen von CA Enterprise Log Manager-Ereignissen und -Abfragen als XML. Diese werden in eigenen Abschnitten dieses Handbuchs behandelt.

GetObject

Sie können diese Befehlsdatei verwenden, um verschiedene Informationstypen abzurufen. Sie können die Datei verwenden, um eine Liste mit Abfragen, Berichten oder globalen Parametern und die ELM-Schemadefinition (CEG) abzurufen. Der Befehl "getObject" verwendet einen Qualifizierer oder ein Argument namens "type", um festzulegen, welche Daten, wie in nachfolgendem Beispiel, an den Aufrufer zurückgegeben werden:

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

Nachfolgende Liste enthält eine Zusammenfassung der Datentypen, die mit den Varianten dieses Befehls zurückgegeben wurden:

getQueryList

Gibt einen XML-String zurück, der alle Abfragen in CA Enterprise Log Manager anzeigt. "getQueryList" unterstützt viele Filterparameter, mit deren Hilfe Sie geeignete Abfragenamen auswählen und in Ihre API-Aufrufe aufnehmen können.

getReportList

Gibt einen XML-String zurück, der alle Berichte in CA Enterprise Log Manager anzeigt. "getReportList" unterstützt viele Filterparameter, mit deren Hilfe Sie geeignete Berichtsnamen auswählen und in Ihre API-Aufrufe aufnehmen können.

getDataModel

Gibt die ELM-Schemadefinition (CEG) im XML-Format zurück. Sie wählen CEG-Begriffe aus, die Sie in den API-Aufruf-Filter einschließen möchten.

getIdealModel

Gibt die Idealmodelle zurück, die in CEG definiert wurden. Sie wählen Begriffe aus großen Produktbereichen aus, die Sie in den Filter des API-Aufrufs einschließen möchten.

getIncidentModel

Gibt die verfügbaren CEG-Felder zurück, die in von der Ereigniskorrelation generierten Incidents verwendet werden.

getCombinedModel

Gibt die ELM-Schemadefinition (CEG) in XML-Format für die Felder "Ereignis" und "Incident" zurück. Sie wählen CEG-Begriffe aus, die Sie in den API-Aufruf-Filter einschließen möchten.

getGlobalSettings

Gibt die globalen Einstellungen des CA Enterprise Log Manager-Servers zurück, mit denen der Befehl ausgeführt wird. Sie erkennen, welcher Filter bereits für CA Enterprise Log Manager-Abfragen gesetzt sind, so dass Sie effektive API-Aufruf-Filter erstellen können.

getELMServers

Gibt eine Liste mit CA Enterprise Log Manager-Servern zurück. Dieser Befehl ist in einer föderierten Umgebung nützlich, da Sie mit dem Befehl über- oder untergeordnete Server erreichen können, die Sie abfragen möchten.

getTimeZones

Ermittelt eine Liste mit Zeitzonen, die in ausgeführten Abfragen als Argumente verwendet werden können.

getVersion

Gibt die ELM-Version zurück, die mit der Version der APIs identisch und für Diagnosezwecke nützlich ist.

getObjectDefinition

Gibt die Metadaten für einen Bericht oder eine Abfrage mit einer bestimmten Objekt-ID zurück. Zu den Metadaten zählen alle Formatierungsdaten, die festlegen, wie ein Bericht oder eine Abfrage dargestellt wird. Verwenden Sie die Metadaten, wenn Sie die Abfrage "runQuery" verwenden müssen, um CA Enterprise Log Manager-Daten für eine Anwendung zu erfassen, die den Abfrage- oder Berichts-Viewer nicht direkt einbetten kann.

getQueryViewer

Gibt die HTML zurück, die die Komponente des Abfrage-Viewers enthält, die mit einer bestimmten Abfrage vorab geladen wurde.

getReportViewer

Gibt die HTML zurück, die die Komponente des Berichts-Viewers enthält, die mit einem bestimmten Bericht vorab geladen wurde.

Mit Ausnahme von "getQueryViewer" und "getReportViewer" geben alle "GetObject"-Befehle einen Fehler zurück, wenn im API-Befehl keine Authentifizierungssitzung vorhanden ist:

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

Im vorherigen Beispiel war der Ergebniswert "false", dies zeigt einen Fehler an, und die Beschreibung enthält den Grund, in diesem Fall: "User is not logged in" (Benutzer ist nicht angemeldet).

Weitere Informationen:

Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)

getQueryList

Verwenden Sie den Befehl "getQueryList", um eine Liste aller in Ihrer CA Enterprise Log Manager-Umgebung verfügbaren Abfragen anzuzeigen. Die XML-Antwort enthält auch die Formatierungsdaten und alle vorab definierten Filterkriterien für die einzelnen Abfragen.

Sie können folgende optionale Parameter mit dem Befehl "getQueryList" verwenden.

tag

Definiert eine Kennung, die im System vorhanden ist. Mit dem Befehl "getQueryList" können Sie nach einer Kennung oder nach mehreren Kennungen suchen. Falls Sie eine unbekannte Kennung angeben, gibt der Befehl eine leere Liste aus.

tagLogic

Gibt an, wie der Befehl "getQueryList" mehrere Kennungen behandelt. Die Werte AND und OR werden unterstützt. Der Standardwert ist OR. Sie können jeweils nur einen "tagLogic"-Wert verwenden.

Beispiel für eine ungefilterte Kennung

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

Gibt alle Abfragen und Formatierungsdaten zurück, die mit den einzelnen Kennungen verknüpft sind.

Beispiel für OR TagLogic

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

Gibt alle Abfragen zurück, die mit den Kennungen "Unknown Category" ODER "System" verknüpft sind.

Beispiel für AND TagLogic

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

Gibt alle Abfragen zurück, die mit den Kennungen "Unknown Category" UND "System" verknüpft sind.

Ergebnisbeispiel

Dieses abgekürzte Beispiel zeigt nur eine Abfrage "Systemereignisanzahl nach Ereigniskategorie".

```
<?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=" zeigt an, dass es sich um einen Sofwareaktualisierungsbericht und den Namen des Berichts handelt.

Hinweis: Wenn es sich bei der Abfrage um eine Eingabeaufforderungsabfrage handelt, wird eher die Kennung "Prompt id=" als "Panel id=" angezeigt, z. B. "Prompt id=HostPrompt".

"Tag Name=" zeigt an, dass es sich um die Systemkennung handelt.

Die Elemente "Column columname=" geben die Ereignisspalten an, die von der Abfrage durchsucht werden, sowie deren Gruppierung und Sortierung.

Die Elemente "Display" geben an, wie die Ereignisse grafisch dargestellt werden.

Weitere Informationen

getQueryViewer (siehe Seite 39)
Eingabeaufforderungsabfragen (siehe Seite 51)
runQuery (siehe Seite 54)

getReportList

Verwenden Sie den Befehl "getReportList", um eine Liste aller in Ihrer CA Enterprise Log Manager-Umgebung verfügbaren Berichte anzuzeigen. Die XML-Antwort enthält auch die Formatierungsdaten und IDs aller im Bericht verwendeten Abfragen.

Sie können folgende optionale Parameter mit dem Befehl "getReportList" verwenden.

tag

Definiert eine Kennung, die im System vorhanden ist. Mit dem Befehl "getReportList" können Sie nach einer Kennung oder nach mehreren Kennungen suchen. Falls Sie eine unbekannte Kennung angeben, gibt der Befehl eine leere Liste aus.

tagLogic

Gibt an, wie der Befehl "getReportList" mehrere Kennungen behandelt. Die Werte AND und OR werden unterstützt. Der Standardwert ist OR. Sie können jeweils nur einen "tagLogic"-Wert verwenden.

Beispiel für eine ungefilterte Kennung

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

Gibt alle Abfragen und alle Formatierungs- und Anzeigedaten zurück, die mit den einzelnen Kennungen verknüpft sind.

Beispiel für OR TagLogic

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

Gibt alle Berichte zurück, die mit den Kennungen "Unknown Category" ODER "System" verknüpft sind.

Beispiel für AND TagLogic

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

Gibt alle Berichte zurück, die mit den Kennungen "Unknown Category" UND "System" verknüpft sind.

getObjectDefinition

Verwenden Sie den Befehl "getObjectDefinition", um spezifische Formatierungs- und Layoutdaten einer Abfrage oder eines Berichts im XML-Format anzuzeigen. Sie können Formatierungsdaten in vorhandenen Berichten anzeigen, um eine benutzerdefinierte Formatierung zu erstellen, insbesondere wenn Sie den Befehl "runQuery" verwenden. Sie können "getObjectDefinition" verwenden, um Daten sowohl zu automatischen Software-Updates als auch zu benutzerdefinierten Berichten oder Abfragen zurückzugeben.

Beispiel für "getObjectDefinition"

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

Gibt folgende XML zurück:

```
?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>
```

Dieses Beispiel zeigt die Formatierungsdaten für die Abfrage "Nicht klassifiziertes Ereignis - Trend". Der Parameter "objectId" im Aufruf gibt an, welche Abfrage- oder Berichtsformatierung angezeigt wird. In diesem Fall ist es die Abfrage "Nicht klassifiziertes Ereignis - Trend" im Ordner "Software-Update-Abfragen".

Weitere Informationen

runQuery (siehe Seite 54)

getDataModel

Verwenden Sie den Befehl "getDataModel", um die typischen Formatierungsdaten der ELM-Schemadefinition (CEG) anzuzeigen. CED enthält alle möglichen Ereignisfelder des Schemas, eine Beschreibung der einzelnen Felder und mögliche Werte für die einzelnen Felder (falls zutreffend). Sie können CEG-Felder für alle Filtervorgänge korrekt identifizieren, die Sie in einen Aufruf einbeziehen möchten.

Beispiel für "getDataModel"

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

Gibt folgende XML zurück:

```
<?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>
```

Das Element "field name=" zeigt das CEG-Feld an, in diesem Fall "event_logname".

Jedes CEG-Feld hat einen Typ, der im Element "type=" angezeigt wird.

getCombinedModel

Verwenden Sie den Befehl "getCombinedModel", um die typischen Formatierungsdaten der ELM-Schemadefinition (CEG) für Ereignisse und Incidents anzuzeigen. CED enthält alle möglichen Ereignisfelder des Schemas, eine Beschreibung der einzelnen Felder und mögliche Werte für die einzelnen Felder (falls zutreffend). Sie können CEG-Felder für alle Filtervorgänge korrekt identifizieren, die Sie in einen Aufruf einbeziehen möchten.

Beispiel für "getCombinedModel"

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

Gibt folgende XML zurück:

```
                        <?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"
```

Das Element "field name=" zeigt das CEG-Feld an, in diesem Fall "incident_id".

Das Element "dbtable=" identifiziert den Datenbanktyp, in diesem Fall die Incident-Datenbank.

getIncidentModel

Verwenden Sie den getIncidentModel-Befehl, um die Felder der ELM-Schemadefinition (CEG) anzuzeigen, die spezifisch sind für Incidents in Ihrer Umgebung. CEG enthält alle möglichen Ereignisfelder, eine Beschreibung der einzelnen Felder und mögliche Werte für die einzelnen Felder (falls zutreffend). Sie können CEG-Felder für alle Filtervorgänge korrekt identifizieren, die Sie in einen Aufruf einbeziehen möchten.

Beispiel für "getIncidentModel"

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

Gibt folgende XML zurück:

```
<?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" />
```

Das Element "field name=" zeigt das CEG-Feld "Incident" an.

getELMServers

Verwenden Sie den Befehl "getELMServers", um eine Liste aller verfügbaren CA Enterprise Log Manager-Server auszugeben, auf denen Abfragen ausgeführt werden können.

Beispiel für "getELMServers"

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

Gibt folgende XML zurück:

```
<?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>
```

Dieses Beispiel zeigt nur einen Server, bei dem das Attribut "type=host" einen CA Enterprise Log Manager-Server-Hostnamen angibt, in diesem Fall "machinename". Es können einzelne oder mehrere Hosts angegeben werden. Jedes XML-"Dienst"-Element steht für einen einzelnen CA Enterprise Log Manager-Server.

getGlobalSettings

Verwenden Sie den Befehl "getGlobalSettings", um globale Einstellungen für den CA Enterprise Log Manager-Zielserver anzuzeigen. Sie können die globalen Einstellungen anzeigen und entscheiden, ob diese für API-Abfrageaufrufe oder -Berichtsaufrufe geeignet sind, die Sie erstellen möchten. Die Einstellungen werden von der CA Enterprise Log Manager-Benutzeroberfläche gesteuert.

Beispiel für "getGlobalSettings"

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

Gibt folgende XML zurück:

```
<?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>Global Configuration</DisplayName>
  <CalmType>service</CalmType>
  <AppInstance>CAELM</AppInstance>
  <ELMPath>/opt/CA/LogManager</ELMPath>
  <Updated>1269421754</Updated>
  <KeyFile>@APP_NAME@Cert.key</KeyFile>
  <UpdateInterval label="Update Interval (seconds)" def="300" prompt="Update
interval in seconds at which components checks for updated configurations"
type="number" min="30" max="86400" global="true">30</UpdateInterval>
  <SessionTimeout label="Session Timeout (minutes)" def="15" prompt="Session
timeout in minutes" type="number" min="10" max="600">15</SessionTimeout>
  <AutoRefreshAllowed type="bool" label="Allow Auto Refresh" prompt="Allow users
to set auto refresh of reports" def="false">true</AutoRefreshAllowed>
  <AutoRefreshFrequency type="number" label="Auto Refresh Frequency (minutes)"
prompt="Auto refresh frequency in minutes" min="1" max="60"
def="10">10</AutoRefreshFrequency>
  <AutoRefreshEnabled type="bool" label="Enable Auto Refresh" prompt="Enable auto
refresh of reports" def="false">false</AutoRefreshEnabled>
  <AlertAuthentication def="true" label="Viewing Action Alerts Requires
Authentication" prompt="Requires authentication for Viewing action alerts"
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="Default Report"
prompt="The default report to run"
type="combo">Collection_Monitor_by_Log_Manager</DefaultReport>
  <EnableDefaultReport type="bool" label="Enable default report launch"
prompt="Enable automatic launch of default report"
def="true">true</EnableDefaultReport>
```

```
  <HiddenReportTags type="shuttle" prompt="Hide selected report tags view in the
application." icon="tagIcon" label="Hide Report Tags"
EEMsource="/CALM_Configuration/Content/Reports/Tags/Report" orderedlist="false"
/>
  <HiddenQueryTags type="shuttle" prompt="Hide selected query tags view in the
application." icon="tagIcon" label="Hide Query Tags"
EEMsource="/CALM_Configuration/Content/Reports/Tags/Panel" orderedlist="false"
global="true" />
  <EnableDefaultProfile group="Profiles" type="bool" label="Enable default
profile" prompt="Enable automatic launch of default profile"
def="false">false</EnableDefaultProfile>
  <DefaultProfile group="Profiles" EEMDisplay="calmName"
EEMsource="/CALM_Configuration/Content/Profiles/Subscription,/CALM_Configuration/
Content/Profiles/User" calmType="profile" label="Default Profile" prompt="The
default profile to run" type="combo"
global="true">CA_Access_Control</DefaultProfile>
  <HiddenProfiles group="Profiles" EEMDisplay="calmName" type="shuttle"
prompt="Hide selected profiles view in the application." icon="profileIcon"
label="Hide Profiles"
EEMsource="/CALM_Configuration/Content/Profiles/Subscription,/CALM_Configuration/
Content/Profiles/User" orderedlist="false"
global="true">CA_Identity_Manager</HiddenProfiles>
  </iSponsor>
  </Result>
```

getTimeZones

Verwenden Sie den Befehl "getTimeZones", um Zeitzonen anzuzeigen, die als Abfrageparameter unterstützt werden. Sie können den Befehl verwenden, um eine Liste mit Zeitzonen anzuzeigen, so dass die Abfragedaten mit der richtigen Zeitzonenformatierung zurückgegeben werden.

Hinweis: Wenn Sie für "getQueryViewer", "getReportViewer" und "runQuery" keine gültige Zeitzone angeben, werden die Daten mit der Zeitzone des CA Enterprise Log Manager-Servers zurückgegeben.

Beispiele für "getTimeZones"

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

Gibt folgende XML zurück:

```
<?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

Sie können den Befehl "getVersion" verwenden, um die API-Version anzuzeigen, die auf dem CA Enterprise Log Manager-Zielserver ausgeführt wird. Die Versionen müssen identisch sein. Verwenden Sie diesen Befehl für die Fehlerbehebung.

Hinweis: Die API-Version kann von den Versionen anderer CA Enterprise Log Manager-Komponenten abweichen, wie der Agenten, je nachdem für welche Aktualisierungen sich Ihr Administrator entschieden hat.

Beispiel für "getVersion"

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

Gibt folgende XML zurück:

```
<?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>
```

Aufrufe des Abfrage- und Berichts-Viewers

"GetQueryViewer" und "getReportViewer" geben ein Fenster mit der grafischen Viewer-Oberfläche zurück, das der CA Enterprise Log Manager-Benutzeroberfläche ähnlich ist. In diesem Fenster können Sie viele der Aufgaben durchführen, die mit Berichten oder Abfragen zusammenhängen. Weitere Informationen zu den verfügbaren Aufgaben finden Sie in der *CA Enterprise Log Manager-API-Online-Hilfe*.

Diese Aufrufe bieten externe Integrationspunkte für Portale von Drittanbietern und andere Anwendungen. Bedenken Sie bei der Verwendung folgendes:

- Die Verwendung der Zertifikatsauthentifizierung bedeutet, dass die Sitzung des Berichts- oder Abfrage-Viewers nicht wie eine CA Enterprise Log Manager-Sitzung beendet wird. Die Anwendung, von der Sie den Ereignis- oder Abfrage-Viewer aufrufen, und nicht die CA Enterprise Log Manager-Anwendung, steuert das Zeitlimit.
- Aus Sicherheitsgründen führen diese Aufrufe wieder zur Anmeldeseite, wenn Sie das Produkt eines Drittanbieters nicht mit CA Enterprise Log Manager registriert haben. Sie können die Umleitung zur Anmeldeseite vermeiden, wenn Sie eine der folgenden Techniken verwenden:
  - Beziehen Sie die Attribute der Anmeldeinformationen als verborgenes Feld in jeden Befehl ein. Die API-Spindle authentifiziert automatisch und arbeitet mit einigen Portalen, die die Einstellung verborgener Felder zulassen.
  - Führen Sie einen Befehl, wie "getVersion", vor dem Starten oder Einbetten der Benutzeroberflächenkomponente durch, und ergreifen Sie bei Bedarf geeignete Maßnahmen (wie die erneute Authentifizierung hinter den Kulissen).

Weitere Informationen

Informationen zu API-Sitzungen (siehe Seite 19)
getQueryViewer (siehe Seite 39)
getReportViewer (siehe Seite 52)
API-Authentifizierung (siehe Seite 15)

getQueryViewer

Verwenden Sie diesen Aufruf, um den grafischen Viewer für eine bestimmte Abfrage anzuzeigen. Der Viewer ist ein voll funktionsfähiger CA Enterprise Log Manager-Abfrage-Viewer, der als Standalone-Komponente geliefert wird. Sie können bestimmte Abfragen in eine sich außerhalb befindende Anwendungsoberfläche oder ein externes Portal einbetten, indem Sie die URL in einen iFrame einbetten.

Hinweis: Die hier gezeigte Lösung arbeitet mit webbasierten Anwendungen, wie JSPs, JavaScript und HTML. Die Lösung funktioniert möglicherweise *nicht* in C++- oder Java Swing-Anwendungen, je nach Verfügbarkeit und Unterstützung einer eingebetteten HTML-Seite und des notwendigen FLASH Plugin-Supports der Anwendungen. Bei Anwendungen ohne FLASH-Support empfehlen wir die Verwendung von "runQuery", um die Rohdaten abzurufen und anschließend mit Hilfe einer Ihrer Umgebung angemessenen Methode zu erzeugen.

Beispiel für "getQueryViewer"

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

Zeigt die Abfrage "Systemereignisanzahl nach Ereignisaktion" an.

"getObject.csp?type=getQueryViewer" gibt den Typ des Aufrufs "getObject" an, in diesem Fall den Abfrage-Viewer.

"&objectId=Subscription/panels/System_Event_Count_By_Event_Action" identifiziert die entsprechende Abfrage, in diesem Fall die Software-Update-Abfrage "Systemereignisanzahl nach Ereignisaktion". Sie können einen beliebigen Abfragenamen angeben, indem Sie den Titel, wie an der Benutzeroberfläche angezeigt, durch Unterstriche getrennt eingeben.

Weitere Informationen

getQueryList (siehe Seite 25)
Eingabeaufforderungsabfragen (siehe Seite 51)
runQuery (siehe Seite 54)

Abfragespezifikationen

Sie können die Ergebnisse der Aufrufe "getQueryViewer", "rungetReportViewer" oder "runQuery" vorqualifizieren, indem Sie Spezifikationen hinzufügen. Sie können vorhandene Detailinformationen festlegen. Hierbei kann es sich um die Teilmenge einer vorhandenen Abfrage oder um Informationen handeln, die für bestimmte Verbraucher gelten. Sie können Spezifikationen beispielsweise verwenden, um bei einem Server nur bestimmte Ereignistypen des Vortags abzufragen.

Sie können die folgenden Spezifikationen festlegen:

server

Gibt den abgefragten CA Enterprise Log Manager-Server an. Der Standardwert ist "localhost", der im Aufruf "getQuery" genannte Server. Mit dieser Spezifikation können Sie einen anderen Server als Ziel auswählen.

timezone

Legt die Zeitzone fest, in der die Abfrage auftritt. Der Standardwert ist die Zeitzone, in der der CA Enterprise Log Manager-Server ausgeführt wird. Sie können diese Spezifikation verwenden, um Ihre Ergebnisse in einer anderen Zeitzone festzulegen.

federated

Gibt (mit "true" oder "false") an, ob die Abfrage auf geeignete föderierte Server angewendet wird. Der Standardwert ist "true", damit wird die Abfrage auf alle föderierten Server angewendet. Dieses Verhalten wendet die normalen CA Enterprise Log Manager-Regeln für die Abfrage von Föderationshierarchien an.

filterXml

Definiert die auf die Abfrage angewendeten Datenfilter im XML-Format. Sie können diese Spezifikation verwenden, um nach dem Hostnamen oder nach anderen CEG-Feldern zu filtern.

IncidentFilterXml

Definiert die Datenfilter, die auf eine Incident-Abfrage in einem Bericht in XML-Format angewendet werden. Sie können diese Spezifikation verwenden, um nach dem Zeitpunkt der Erstellung des Incidents oder anderen CEG-Feldern zu filtern. Diese Spezifikation bezieht sich nur auf den Aufruf "getReportViewer".

accessfilterXml

Definiert die auf die Abfrage angewendeten Datenfilter im XML-Format. Sie können mit dieser Spezifikation z. B. eine Abfrage oder ein Berichtsergebnis entsprechend Ihrer Rolle filtern, wenn Sie sich mit Zertifikatsnamen und Zertifikatskennwort authentifizieren.

params

Definiert die auf die Abfrage angewendeten Ergebnisbedingungen im XML-Format.

Aufforderung

Steuert (mit Hilfe von "true" oder "false), ob die zusätzlichen Eingabeaufforderungs-Steuerelemente angezeigt werden. Der Standardwert ist "false". Dieser Wert ist nur gültig, wenn die Abfrage eine Eingabeaufforderung ist. Der Wert wird ignoriert, wenn es sich bei der Abfrage nicht um eine Eingabeaufforderung handelt.

Nachfolgende Spezifikationen werden nur verwendet, wenn Sie "prompt=true" festgelegt haben:

promptvalue

Legt den Filterwert für eine Eingabeaufforderungsabfrage fest.

col

Zeigt eine Liste der Ereignisspalten an, nach denen die Eingabeaufforderungsabfrage sucht. Sie können mehrere col-Begriffe verwenden, um mehr als eine Zielspalte zu identifizieren.

Weitere Informationen:

getQueryViewer (siehe Seite 39)
Eingabeaufforderungsabfragen (siehe Seite 51)
runQuery (siehe Seite 54)

Server-Spezifikationen

Sie können den Ereignisprotokollspeicher eines nicht standardmäßigen CA Enterprise Log Manager-Servers nach Name oder IP-Adresse als Abfrageziel angeben. Der Standardwert ist "localhost", der im API-Aufruf genannte Server.

Sie können "getELMServers" verwenden, um eine Liste mit geeigneten Servernamen abzurufen.

Beispiel für die Spezifikation eines Servernamens

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

In diesem Beispiel gibt "&server=" den Namen des Servers für die Abfrage an. Der von Ihnen gewünschte Servername ersetzte "ELMSERVER2". Da der Localhost (ELMSERVER) standardmäßig verwendet wird, muss das Element "&server" nicht verwendet werden, es sei denn, Sie möchten einen nicht standardmäßigen Zielserver angeben.

Hinweis: Wenn Sie einen ungültigen Servernamen eingeben, gibt der Aufruf Daten des Standard-CA Enterprise Log Manager-Servers zurück, den der ELMSERVER-Wert identifiziert hat.

Weitere Informationen

getELMServers (siehe Seite 33)
runQuery (siehe Seite 54)

Spezifikationen der Zeitzone

Sie können Ihren Aufrufen "getQuery" oder "runQuery" eine Zeitzonenspezifikation hinzufügen. Mit "getTimeZones" können Sie eine Liste der verfügbaren Zeitzonen abrufen.

Beispiel für eine Zeitzonenspezifikation

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

In diesem Fall gibt "&timezone=" den Namen, der von Ihnen gewünschten Zeitzone an. Ihr Zeitzonenname ersetzt "TIMEZONENAME", wie in der vom Aufruf "getTimeZones" zurückgegebenen Liste angezeigt.

Hinweis: Die Antwort auf eine ungültige Zeitzone ist unterschiedlich, abhängig davon, in welchem Aufruf sie enthalten ist:

- Wenn eine ungültige Zeitzone im Aufruf "runQuery" verwendet wird, werden GMT-Zeitstempel zurückgegeben. Wenn keine Zeitzonen passiert werden, ist die Zeitzone der Standardwert, in der der Server ausgeführt wird.
- Wenn keine oder eine ungültige Zeitzone im "getQueryViewer" oder "getReportViewer" verwendet wird, ist die Zeitzone des Zielservers der Standardwert.

Weitere Informationen

getTimeZones (siehe Seite 36)
runQuery (siehe Seite 54)

Weitere Informationen:

IncidentFilter XML-Spezifikationen (siehe Seite 47)

Filter-XML-Spezifikationen

Sie können CA Enterprise Log Manager-Filter für Ihren Bericht im XML-Format voreinstellen und den URLs "getQueryViewer", "getReportViewer", "getIncidentViewer" oder "runQuery" mit dem Begriff "filterXML" hinzufügen. Sie können mehrere Filter verschachteln, indem Sie die Begriffe AND und OR und Klammern verwenden. Im Wesentlichen erstellen Sie erweiterte CA Enterprise Log Manager-Filter in XML.

Wichtig! FilterXml-Begriffe sind komplex, und die API führt keine Validierung durch. Ungültige Filterbegriffe führen zu einem Abfragefehler. Wir empfehlen deshalb, bei der Erstellung der Filterbegriffe besonders sorgfältig vorzugehen.

Folgende Filterelemente sind verfügbar. Die Auflistung erfolgt in der Reihenfolge, in der die Elemente verwendet werden müssen:

lparens

Legt die Anzahl linker Klammern fest. Gültige Werte sind 0 oder mehr.

Logik

Legt die Verbindungsfilter AND oder OR der logischen Begriffe fest. Lassen Sie den logischen Wert beim ersten Filterbegriff immer leer.

col

Definiert die abgefragten Ereignisspalten. Verwenden Sie "getDataModel", um die Liste der verfügbaren Spalten zu erhalten.

oper

Definiert einen Operator für den Filter. Folgende Werte sind gültig (Groß- und Kleinschreibung muss beachtet werden):

- EQUAL - Gleich
- NEQ - Ungleich
- LESS - Kleiner als
- GREATER - Größer als
- LEQ - Kleiner als oder gleich
- GREATEQ - Größer als oder gleich
- LIKE - Wie
- NOTLIKE - Nicht wie

- INSET - Im Satz
- NOTINSET - Nicht im Satz
- MATCH - Stimmt überein
- KEYED - Mit Schlüssel
- NOTKEYED - Ohne Schlüssel

val

Legt den Wert fest, nach dem der Filter sucht.

rparens

Legt die Anzahl rechter Klammern fest. Gültige Werte sind 0 oder mehr. Die Gesamtanzahl rechter Klammern stimmt mit der Anzahl linker Klammern überein.

Wenn Sie eine grafische Abfrage oder einen grafischen Bericht anzeigen, können Sie die FilterXML-Begriffe, die Sie im Abschnitt mit den erweiterten Filtern des Dialogfelds "Lokale Filter" festgelegt haben, auf der Benutzeroberfläche des Viewers anzeigen.

Beispiel einer Filter-XML-Spezifikation

Dieses Beispiel zeigt den Aufruf "getQueryViewer" mit einer Filteranweisung. Die Filterbegriffe werden zur Verdeutlichung in voller Länge angezeigt.

```
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=" gibt an, dass eine Filteranweisung folgt.

Die Filteranweisung legt die Abfrage fest, mit der die Spalte "source_username" nach "su" und die Spalte "event_logname" nach "CALM" durchsucht wird. Da eine AND-Anweisung die beiden Begriffe verbindet (Filterlogik="AND"), werden nur Ereignisse zurückgegeben, bei denen jeder Wert in seiner entsprechenden Spalte gefunden wurde.

Zugriffsfilter-XML-Spezifikationen

Sie können CA Enterprise Log Manager-Filter für Ihre Abfragen oder Berichte im XML-Format voreinstellen, wenn Sie sich mit Zertifikatsnamen und Zertifikatskennwort authentifizieren. Eine in einem Anmeldeaufruf übergebene Zugriffsfilter-XML wird auf alle Abfragen und Berichte angewendet, die in der entsprechenden jener Sitzung ausgeführt werden. Wenn Sie in der Abfrage oder dem Bericht eine Filter-XML übergeben, nachdem Sie sich mit Zugriffsfilter-XML angemeldet haben, wendet CA Enterprise Log Manager für das Abrufen von Ergebnissen beide Filter an.

Die Elemente der Zugriffsfilter-XML sind jenen der Filter-XML ähnlich.

Beispiel einer Zugriffsfilter-XML-Spezifikation ohne Filter-XML

Dieses Beispiel zeigt den Aufruf "getQueryViewer" mit einer Zugriffsfilter-XML-Anweisung. Die Filterbegriffe werden zur Verdeutlichung in voller Länge angezeigt.

```
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=" gibt an, dass eine Zugriffsfilteranweisung folgt.

Beispiel einer Zugriffsfilter-XML-Spezifikation mit Filter-XML

Dieses Beispiel zeigt den Aufruf "objectId" mit einer Filter- und einer Zugriffsfilter-XML-Anweisung.

```
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=" gibt an, dass eine Filteranweisung folgt.

"&accessFilterXml=" gibt an, dass eine Zugriffsfilteranweisung folgt.

IncidentFilter XML-Spezifikationen

Sie können CA Enterprise Log Manager-Filter für Ihren Bericht im XML-Format voreinstellen und der URL "getReportViewer" mit dem Begriff "IncidentFilterXML" hinzufügen. Sie können mehrere Filter verschachteln, indem Sie die Begriffe AND und OR und Klammern verwenden. IncidentFilter-Spezifikationen funktionieren gleich wie Filterspezifikationen und nutzen die gleichen Elemente und Operatoren.

IncidentFilter XML-Spezifikationen gelten nur für Incident-Abfragen, die in Berichten enthalten sind. Allerdings kann ein Bericht sowohl Ereignisse als auch Incident-Abfragen enthalten. Um auf diese Berichte zuzugreifen und sie zu filtern, kann Ihre API URL sowohl Filter XML- als auch IncidentFilter XML-Spezifikationen enthalten.

Wichtig! Die Begriffe "IncidentFilterXml" sind komplex, und die API führt keine Validierung durch. Ungültige Filterbegriffe führen zu einem Abfragefehler. Wir empfehlen deshalb, bei der Erstellung der Filterbegriffe besonders sorgfältig vorzugehen.

Beispiel einer IncidentFilter XML-Spezifikation

Dieses Beispiel zeigt den Aufruf "getReportViewer" mit einer Filteranweisung. Die Filterbegriffe werden zur Verdeutlichung in voller Länge angezeigt.

```
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=" gibt an, dass eine Incident-Filteranweisung folgt.

Der Filter gibt alle Incidents an, die innerhalb eines bestimmten Zeitraums erstellt wurden.

Weitere Informationen:

Filter-XML-Spezifikationen (siehe Seite 44)

Spezifikationen der Ergebnisbedingung

Verwenden Sie "param"-Begriffe, um Ergebnisbedingungen für die Aufrufe "getQueryViewer", "getReportViewer" oder "runQuery call" festzulegen.

Folgende "param"-Begriffe sind verfügbar:

ARG_limit

Legt die Anzahl der Zeilen fest, die von der Abfrage ausgegeben werden.

ARG_show_other

Legt fest, ob die Spalte "Andere anzeigen" im Display eines Abfrage-Viewers mit "true" oder "false" angezeigt wird. Diese Option wird für Diagramme mit Top-N-Abfragen verwendet (aggregierte Abfragen mit festgelegter Zeilenbegrenzung, die auf Basis von "event_count" aggregiert wurden). Wenn diese Option ausgewählt wird, werden die ersten N -1-Ereignisse normal angezeigt (wobei N die Zeilenbegrenzung ist). Das N.-Ereignis ist jedoch das "Andere Ereignis". Dabei handelt es sich um ein aggregiertes Ereignis, das auf den restlichen Ereignissen basiert.

ARG_event_datetime

Legt den Detailgrad des in der Abfrageanzeige für Trendabfragen verwendeten Zeitraums fest. Die verfügbaren Werte sind:

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

ARG_start

Legt die dynamische Startzeit für die Abfrage fest.

ARG_stop

Legt die dynamische Endzeit für die Abfrage fest.

ARG_minduring

Definiert das früheste Gruppenereignis, das nach einer festgelegten dynamischen Zeit datiert wurde. Nur für Gruppenabfragen relevant.

ARG_maxduring

Definiert das späteste gruppierte Ereignis, das nach einer festgelegten dynamischen Zeit datiert wurde. Nur für Gruppenabfragen relevant.

ARG_maxbefore

Definiert das späteste gruppierte Ereignis, das vor einer festgelegten dynamischen Zeit datiert wurde. Nur für Gruppenabfragen relevant.

ARG_sumatleast

Legt die Mindestanzahl an Ereignissen für die Gruppierung fest. Nur für Gruppenabfragen relevant.

ARG_sumatmost

Legt die maximale Anzahl an Ereignissen in der Gruppierung fest. Nur für Gruppenabfragen relevant.

Beispiel für eine Spezifikation der Ergebnisbedingung

Zur Verdeutlichung werden die "params"-Begriffe in diesem Beispiel in voller Länge angezeigt.

```
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>
```

Der "ARG_limit"-Wert "200" legt fest, dass in der Abfrage nur die ersten 200 Zeilen angezeigt werden.

Dynamische Zeitbegriffe

Verwenden Sie dynamische Zeitparameterbegriffe (params), um die Zeiträume anzugeben, für die eine Abfrage gilt, indem Sie diese bestimmten Spezifikationen der Ergebnisbedingungen hinzufügen.

Folgende dynamische Zeitparameterbegriffe (params) sind verfügbar:

Begriff	Beschreibung
now	Die aktuelle Uhrzeit
start of day	Start des aktuellen Tages

weekday <number>	Nummerierter Wochentag ■ Sonntag 0 ■ Montag 1 ■ Dienstag 2 ■ Mittwoch 3 ■ Donnerstag 4 ■ Freitag 5 ■ Samstag 6
start of month	Start des aktuellen Monats
start of year	Start des aktuellen Jahres
<number> seconds	Anzahl der Sekunden
<number> minutes	Anzahl der letzten Minuten
<number> hours	Anzahl der Stunden
<number> days	Anzahl der Tage

Sie können Ergebnisbedingungen für eine Abfrage- oder eine Berichtsdefinition angeben. In diesem Fall überschreiben alle Zeitangaben, die Sie dem Aufruf hinzufügen, die in der Basisabfrage oder dem Basisbericht angegebenen Werte.

In beiden Fällen bleiben alle Werte unverändert, die nicht in der URL angegeben sind.

Beispiel für die Spezifikation dynamischer Zeitbegriffe

Zur Verdeutlichung werden die "param"-Begriffe in diesem Beispiel in voller Länge angezeigt.

```
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>
```

Die "ARG_start"-Werte 'now' und '-12 hours' legen fest, dass die Abfrage vor 12 Stunden begann.

Der "ARG_stop"-Wert 'now' legt fest, dass die Abfrage zum jetzigen Zeitpunkt endet, so dass diese Abfrage nur Daten der vergangenen 12 Stunden erfasst.

Weitere Informationen

Spezifikationen der Ergebnisbedingung (siehe Seite 48)
runQuery (siehe Seite 54)

Eingabeaufforderungsabfragen

Eingabeaufforderungen sind spezialisierte Abfragen, mit denen Sie bestimmte Filterwerte eingeben können, bevor Sie die Abfrage ausführen. Sie können die verfügbaren Eingabeaufforderungsabfragen mit "getQueryList" anzeigen. Das Element "Prompt id" identifiziert eine Eingabeaufforderungsabfrage, die auf der Position des Elements "Panel id" angezeigt wird, das Standardabfragen identifiziert Sie können die Begriffe "prompt", "promptvalue" und "col" zum Definieren von Eingabeaufforderungsabfragen verwenden, die Sie aufrufen möchten.

Sie können ohne angegebene Filterwerte auf die grafische Eingabeaufforderungsabfrage zugreifen oder die Filterwerte vorab in der URL angeben. Falls die URL keine Spalten enthält, werden alle Spalten der Eingabeaufforderung ausgewählt.

Beispiel für eine ungefilterte Host-Eingabeaufforderung

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

Zeigt die Host-Eingabeaufforderung ohne eingegebene Filterwerte, jedoch mit allen ausgewählten Spalten der Eingabeaufforderung an.

Beispiel für eine gefilterte IP-Eingabeaufforderung

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

Führt die IP-Eingabeaufforderung aus und sucht dabei in der Zieladressspalte nach der IP-Adresse 255.255.255.0

"&prompt=true" zeigt die Eingabeaufforderungssteuerungen an, mit denen Sie die die Werte der Eingabeaufforderungsabfrage nach der Ausführung ändern und die Abfrage bei Bedarf erneut ausführen können.

"&promptvalue=" gibt die von Ihnen gewünschte IP-Adresse an.

"&col=dest_address" wählt die von Ihnen gewünschte Ereignisspalte aus.

Weitere Informationen

getQueryList (siehe Seite 25)
runQuery (siehe Seite 54)

getReportViewer

Sie können den Befehl "getReportViewer" verwenden, um den grafischen Viewer für einen bestimmten Bericht anzuzeigen. Der Berichts-Viewer ist so ähnlich wie der Berichts-Viewer der CA Enterprise Log Manager-Benutzeroberfläche und wird als Standalone-Komponente geliefert. Sie können bestimmte Berichte in eine sich außerhalb befindende Anwendungsoberfläche oder ein externes Portal einbetten, dies geschieht normalerweise, indem Sie die URL in einen iFrame oder ein Portlet einbetten.

Hinweis: Die hier gezeigte Lösung arbeitet mit webbasierten Anwendungen, wie JSPs, JavaScript und HTML. Die Lösung funktioniert möglicherweise *nicht* in C++- oder Java Swing-Anwendungen, je nach Verfügbarkeit und Unterstützung einer eingebetteten HTML-Seite und des notwendigen FLASH Plugin-Supports solcher Anwendungen. Für die Anwendungen, in denen FLASH nicht unterstützt werden kann, empfehlen wir die Verwendung von "getReportList", um festzulegen, welche Abfragen in den Berichts eingeschlossen werden. Verwenden Sie anschließend für jeden Bericht "runQuery" um die Rohdaten abzurufen und anschließend mit Hilfe einer Ihrer Umgebung angemessenen Methode zu erzeugen.

Beispiel für "getReportViewer"

Dieses Beispiel ruft den Bericht "Erfassungsüberwachung nach Protokollmanager" auf.

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

Sie können Filter und andere Spezifikationen für "getReportViewer" genauso verwenden wie für "getQueryViewer".

Sie können einen beliebigen Berichtsnamen angeben, indem Sie den Titel, wie an der Benutzeroberfläche angezeigt, durch Unterstriche getrennt eingeben.

Weitere Informationen

getReportList (siehe Seite 28)
runQuery (siehe Seite 54)

getIncidentViewer

Sie können den Befehl "getIncidentViewer" verwenden, um eine grafische Incident-Ansicht anzuzeigen. Der Viewer ähnelt dem Incident-Viewer der CA Enterprise Log Manager-Benutzeroberfläche und wird als Standalone-Komponente geliefert. Die in der CA Enterprise Log Manager-Benutzeroberfläche verfügbaren Verwaltungsfunktionen, wie Zusammenführen oder Löschen von Incidents, können nicht mithilfe dieses Viewers ausgeführt werden.

Hinweis: Die hier gezeigte Lösung arbeitet mit webbasierten Anwendungen, wie JSPs, JavaScript und HTML. Die Lösung funktioniert möglicherweise *nicht* in C++- oder Java Swing-Anwendungen, je nach Verfügbarkeit und Unterstützung einer eingebetteten HTML-Seite und des notwendigen FLASH Plugin-Supports solcher Anwendungen.

Beispiel für "getIncidentViewer"

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

Mit diesem Aufruf wird der Incident-Viewer angezeigt, der die in den letzten sechs Stunden erstellten Incidents anzeigt.

Sie können Zeitbegriffe, Filter und andere Spezifikationen für "getIncidentViewer" genauso verwenden wie für "getQueryViewer".

runQuery

Verwenden Sie "runQuery", um eine Abfrage auszuführen und die Ergebnisse in XML statt im grafischen Abfrage-Viewer zurückzugeben. Sie können diese Methode verwenden, um CA Enterprise Log Manager-Daten für eine Anwendung zu erfassen, die den Abfrage- oder Berichts-Viewer nicht direkt einbetten kann, wie die Anwendungen ohne Flash-Support.

Fügen Sie der URL Abfragespezifikationen hinzu, um die Basisabfrage wie beim "getQueryViewer" zu filtern.

Formatieren Sie nach der Verwendung von "runQuery" die XML-Daten, damit diese in Ihrer Umgebung richtig angezeigt werden. Sie können beispielsweise den Aufruf "runQuery" in ein Webportal einbetten und ein Stylesheet anwenden, um die Daten anzuzeigen.

Beispiel für runQuery

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

Gibt folgende XML zurück:

```
<?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>
```

Weitere Informationen

getQueryViewer (siehe Seite 39)
getReportViewer (siehe Seite 52)

API-Registrierung

Dieser Abschnitt enthält Informationen zur Produktregistrierung mit CA Enterprise Log Manager. Sie können die API-Produktregistrierungsseite verwenden, um Registrierungszertifikate zu erstellen, mit denen Sie sich über das Single Sign-On von außerhalb befindlichen Produkten anmelden können. Sie können mehrere Produkte über eine einzelne Schnittstelle registrieren, ohne individuelle Registrierungsaufrufe erstellen zu müssen. Auf der Produktregistrierungsseite können Sie in fast allen Fällen ein Zertifikat erstellen.

Dieser Abschnitt enthält auch Aufrufe, die registriert werden können, ohne dass die Verwendung der Produktregistrierungsseite oder die einfache Authentifizierung ratsam oder möglich ist.

Weitere Informationen

API-Zertifikaterstellung (siehe Seite 56)
Registrieren eines Produkts (siehe Seite 60)
Aufheben von Produktregistrierungen (siehe Seite 61)

API-Zertifikaterstellung

Sie können auf die API-Produktregistrierungsschnittstelle zugreifen, um Single Sign-On-Registrierungszertifikate zu erstellen, eine Liste der registrierten Produkte anzuzeigen oder Produktregistrierungen durch das Löschen vorhandener Zertifikate aufzuheben.

Sie können der URL Authentifizierungsinformationen hinzufügen. Wenn Sie nicht authentifiziert werden, werden Sie zur CA Enterprise Log Manager-Anmeldeseite umgeleitet. Dieses Verhalten stimmt mit allen anderen API-Aufrufen überein, die eine Benutzeroberfläche zurückgeben.

Note: Verwenden Sie zum Erstellen eines Registrierungszertifikats den Benutzernamen und das Kennwort "EiamAdmin". Für das Anzeigen von Produktlisten oder Aufheben von Produktregistrierungen *können* Sie die EiamAdmin-Anmeldeinformationen verwenden, die Administrator-Anmeldeinformationen sind jedoch ausreichend.

Beispiel für die Anzeige einer Zertifizierungsseite

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

Zeigt die CA Enterprise Log Manager-Anmeldeseite an. Wenn Sie die passenden Anmeldeinformationen eingeben, wird die Produktregistrierungsseite angezeigt.

Weitere Informationen zur Erstellung von Zertifikaten finden Sie in der *CA Enterprise Log Manager-API-Hilfe*, auf die Sie von der Produktregistrierungsseite zugreifen können.

Weitere Informationen

Registrieren eines Produkts (siehe Seite 60)
Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)
API-Authentifizierung (siehe Seite 15)

Registrieren eines Produkts für die Verwendung mit CA Enterprise Log Manager

Sie haben die Möglichkeit, ein Produkt für die Verwendung mit CA Enterprise Log Manager zu registrieren, um Single Sign-On nutzen können. So können Sie je nach Bedarf über das Kennwort-Management, das Zugriffs-Management oder von einer anderen Anwendung aus auf CA Enterprise Log Manager-Abfragen und -Berichte zugreifen. Der Registrierungsprozess umfasst zwei Schritte:

1. Erstellen eines Registrierungszertifikats in CA Enterprise Log Manager
2. Verwenden des Zertifikatnamens und des zugehörigen Kennworts innerhalb des Fremdprodukts, um die Registrierung für Single Sign-On abzuschließen

   Bei diesem Schritt richtet sich die genaue Vorgehensweise jeweils nach dem Produkt, das Sie für die Verwendung mit CA Enterprise Log Manager registrieren möchten. Folgende Informationen sollten Sie jedoch bereithalten, um die Registrierung abschließen zu können:

   - Hostname oder IP-Adresse des CA Enterprise Log Manager-Servers, auf dem Sie das Produkt registrieren möchten
   - Zertifikatname wie in Schritt 1 erstellt
   - Kennwortname wie in Schritt 1 erstellt

Weitere Informationen

Erstellen eines Registrierungszertifikats (siehe Seite 58)

Erstellen eines Registrierungszertifikats

Sie können ein Registrierungszertifikat erstellen, um von anderen CA- oder Drittanbieter-Produkten aus Single Sign-On nutzen zu können.

So erstellen Sie ein Registrierungszertifikat

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

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

   Ersetzen Sie "calmserver" mit dem Servernamen oder der IP-Adresse des CA Enterprise Log Manager-Servers, auf dem Sie Produkte registrieren möchten.

   Sofern Sie nicht bereits als EiamAdmin-Benutzer authentifiziert sind, wird der Anmeldebildschirm angezeigt. Wenn Sie bereits authentifiziert sind, wird die Seite "Produktregistrierung" angezeigt.

2. Geben Sie den Benutzernamen "Eiamadmin" und das zugehörige Kennwort ein.

   Eine Liste mit allen aktuellen Registrierungszertifikaten wird angezeigt.

   Hinweis: Sie benötigen die Anmeldeinformationen für den "EiamAdmin"-Benutzer, um ein Zertifikat zu erstellen. Zum Auflisten von Produkten oder Aufheben von Produktregistrierungen reichen die Administrator-Anmeldeinformationen aus.

3. Klicken Sie im linken Fenster oberhalb der Liste "Registrierte Produkte" auf den Link "Registrieren".

4. Geben Sie für das zu registrierende Produkt einen Namen und ein Kennwort ein.

   Hinweis: Schreiben Sie sich den Zertifikatnamen und das Kennwort unbedingt auf. Diese Daten benötigen Sie, um den Registrierungsprozess vom Fremdprodukt aus abzuschließen.

5. Klicken Sie im rechten Fensterbereich auf die Schaltfläche "Registrieren".

   Eine Bestätigungsmeldung wird eingeblendet, und der Zertifikatname wird in der Liste "Registrierte Produkte" angezeigt.

Aufheben von Produktregistrierungen

Sie können eine Produktregistrierung aufheben, indem Sie das Registrierungszertifikat löschen.

So heben Sie eine Produktregistrierung auf

1. Öffnen Sie einen Webbrowser, und geben Sie die folgende URL ein:

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

   Ersetzen Sie "calmserver" mit dem Servernamen oder der IP-Adresse des CA Enterprise Log Manager-Servers, auf dem Sie Produktregistrierungen aufheben möchten.

   Der Anmeldebildschirm wird angezeigt.

2. Geben Sie für eine Administratorrolle einen Benutzernamen mit Kennwort ein.

   Eine Liste mit allen aktuellen Registrierungszertifikaten wird angezeigt.

3. Klicken Sie auf das zu löschende Registrierungszertifikat.

4. Klicken Sie auf "Registrierung aufheben".

   Ein Bestätigungsdialogfeld wird angezeigt.

5. Klicken Sie auf "OK".

   Eine Bestätigungsmeldung wird angezeigt, und der Zertifikatname wird aus der Liste "Registrierte Produkte" gelöscht.

Registrieren eines Produkts

Sie können den Aufruf "registerProduct" verwenden, um ein Produkt für Single Sign-On-Zwecke zu registrieren. Die Registrierung eines Produkts erstellt ein Zertifikat, das in der Management-Datenbank gespeichert wird. Sie können diesen Aufruf verwenden, wenn Sie nicht auf die Registrierungsoberfläche des Produkts zugreifen können oder dies nicht ratsam ist.

Wenn Sie beispielsweise das Produkt eines Drittanbieters integrieren, möchten Sie das Kennwort "EiamAdmin" möglicherweise für die Zertifikatserstellung nicht weiter verbreiten. In diesem Fall können Sie ein Zertifikat und ein Kennwort erstellen und an die Benutzer des betreffenden Programms verteilen, um die Integrationen einzurichten.

Beispiele für "registerProduct"

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

In diesem Fall legt "&certname=YourProductName" das Produkt fest, das Sie registrieren möchten. Ersetzen Sie "YourProductName" durch den Namen des Produkts, das Sie registrieren möchten.

"&certname=xxxxx" gibt den gültigen Zertifikatsnamen und das Kennwort an.

Erfolgsmeldung:

```
<?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>
```

Fehlermeldung:

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

Hinweis: Häufig tritt ein Fehler auf, wenn das Zertifikat mit dem in der URL gegebenen Namen bereits erstellt wurde. Eine andere gängige Fehlerbeschreibung ist "EE_AUTHFAILED Authentication failed", die anzeigt, dass das Kennwort falsch war.

Aufheben von Produktregistrierungen

Mit dem Befehl zum Aufheben der Registrierung können Sie die Produktregistrierung aufheben. Sie können diesen Aufruf verwenden, wenn Sie nicht auf die Registrierungsoberfläche des Produkts zugreifen können oder dies nicht ratsam ist, um ein Registrierungszertifikat zu entfernen.

Beispiel für das Aufheben einer Produkt-URL:

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

In diesem Fall gibt "&username=Administrator" einen CA Enterprise Log Manager-Benutzer mit Administratorrolle an. Ersetzen Sie "Administrator" durch einen geeigneten Benutzer mit Administratorrechten.

"&password=adminpassword" gibt das Kennwort für den Administrator an. Ersetzen Sie "adminpassword" durch das Kennwort des Benutzers, den Sie unter "&username=" angegeben haben.

Hinweis: Verwenden Sie zum Registrieren eines Produkts den Benutzernamen und das Kennwort "EiamAdmin". Für das Anzeigen von Produktlisten oder Aufheben von Produktregistrierungen *können* Sie die EiamAdmin-Anmeldeinformationen verwenden, die Administrator-Anmeldeinformationen sind jedoch ausreichend.

Erfolgsmeldung:

```
<?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>
```

Fehlermeldung:

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

Hinweis: Häufig tritt ein Fehler auf, wenn die Produktregistrierung bereits aufgehoben wurde oder nicht vorhanden ist. Eine andere gängige Fehlerbeschreibung ist "EE_AUTHFAILED Authentication failed", die anzeigt, dass das Kennwort falsch war.

Kapitel 5: Einbetten von CA Enterprise Log Manager in ein Webportal

Sie können CA Enterprise Log Manager-Abfragen oder Berichte in ein Webportal einbetten, um den gewünschten Inhalt anzuzeigen. Der Vorgang läuft wie folgt ab:

1. Identifizieren Sie den CA Enterprise Log Manager-Inhalt, den Sie anzeigen möchten, und erstellen Sie den API-Aufruf, um diesen zu identifizieren und zurückzugeben.
2. Einbetten des ausgewählten Inhalts in das Webportal.

Weitere Informationen

Identifizieren von Inhalten (siehe Seite 64)
Einbetten von Inhalten in ein Liferay Portal (siehe Seite 65)
Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)

Identifizieren von Inhalten

Beginnen Sie mit der Einbettung des CA Enterprise Log Manager-Inhalts, indem Sie entscheiden, welchen Inhalt Sie anzeigen möchten. Überprüfen Sie die CA Enterprise Log Manager-Benutzeroberfläche, um den Bericht oder die Abfrage mit den Informationen zu finden, die Sie benötigen.

Verwenden Sie für die Anzeige von CA Enterprise Log Manager-Abfragen oder -Berichten in einem Webportal die Aufrufe "getQueryViewer" oder "getReportViewer", um interaktive Berichte und Abfragen mit allen innerhalb der CA Enterprise Log Manager-Benutzeroberfläche verfügbaren Funktionen anzuzeigen

Sie können für die Rückgabe von XML-Inhalten auch den Bericht "runQuery" verwenden und den XML-Inhalt durch Anwenden eines Stylesheets anzeigen. Die Anzeige ist nicht interaktiv, und Sie können die Daten ohne Flash anzeigen.

In diesem Beispiel wird der Bericht "Alle Ereignisse des Systems - Details" mit "getQueryViewer" aufgerufen, um eine Ereignis-Viewer-Tabelle mit allen Ereignissen anzuzeigen. Der API-Aufruf für diesen Bericht hat folgende Syntax:

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

- Wenn Sie den Aufruf in Ihrer Umgebung verwenden möchten, ersetzen Sie den "ELMSERVER"-Teil der URL durch den Hostnamen oder die IP-Adresse des Servers, auf dem die Daten gespeichert sind, die Sie benötigen.
- Dieses Beispiel authentifiziert mit einem CA Enterprise Log Manager-Benutzernamen und einem CA Enterprise Log Manager-Kennwort: "&username=xxx&password=xxx". Die Verwendung dieser Authentifizierungsmethode wird für das Einbetten von CA Enterprise Log Manager-Inhalten empfohlen. Ersetzen Sie "xxx" durch einen passenden CA Enterprise Log Manager-Benutzernamen und ein passendes CA Enterprise Log Manager-Kennwort. Wenn Sie nicht möchten, dass der Benutzername und das Kennwort in der URL sichtbar sind, können Sie diese als ausgeblendete Werte einstellen, falls Ihr Webportal dies zulässt.

Sie können die endgültige Syntax testen, indem Sie die in einem Browser erstellte URL eingeben und bestätigen, dass der gewünschte Bericht oder die gewünschte Abfrage angezeigt wird.

Weitere Informationen

API-Authentifizierung (siehe Seite 15)
Aufrufe des Abfrage- und Berichts-Viewers (siehe Seite 38)
getQueryViewer (siehe Seite 39)
getReportViewer (siehe Seite 52)
runQuery (siehe Seite 54)

Einbetten von Inhalten in ein Liferay Portal

Wenn Sie einen API-Aufruf haben, der die von Ihnen gewünschte Abfrage oder den von Ihnen gewünschten Bericht zurückgibt, betten Sie den Aufruf mit einem iFrame oder Portlet in Ihr Webportal ein, und zeigen Sie den CA Enterprise Log Manager-Inhalt an.

Dieses Beispiel verwendet das Liferay Portal, das davon ausgeht, dass Sie ein Portal mit Installations- und Konfigurationsanweisungen von Liferay erstellt haben. Ihr eigenes Webportal verfügt unter Umständen über ähnliche Steuerelemente. Informationen zur Erstellung von iFrames oder Portlets finden Sie in der Dokumentation Ihres Webportals.

So betten Sie Inhalte in ein Liferay Portal ein:

1. Erstellen Sie eine Seite, oder öffnen Sie eine Seite, die Sie in Liferay ändern möchten.
2. Klicken Sie in der oberen rechten Ecke der Seite auf das Symbol des Tools neben der Begrüßungsmeldung.
3. Wählen Sie im Menü "Anwendung hinzufügen" aus.

   Das Dialogfeld "Anwendung hinzufügen" wird mit den Anwendungskategorien angezeigt.
4. Erweitern Sie die Beispielkategorie, und klicken Sie neben der iFrame-Anwendung auf "Hinzufügen".

   Auf der Seite wird ein neues iFrame-Portlet angezeigt.
5. Klicken Sie auf den Konfigurationslink im Portlet, und geben Sie den Text des API-Aufrufs in das Feld der Quell-URL ein.
6. Klicken Sie auf "Speichern".

   Der ausgewählte Inhalt wird im iFrame angezeigt.
7. Konfigurieren Sie andere iFrames, oder veröffentlichen Sie das Webportal gemäß der Liferay-Dokumentation.

Kapitel 6: API-Fehlerbehebung

Falls Ihre API-Aufrufe nicht wie erwartet funktionieren, führen Sie die Fehlerbehebung anhand nachfolgender Schritte durch, und überprüfen Sie nach jedem Schritt, ob die richtigen Ergebnisse angezeigt werden.

1. Überprüfen Sie die Syntax des URL-Aufrufs:
   a. Vergleichen Sie Ihre Syntax mit dem Beispiel im Handbuch, und überprüfen Sie, ob Sie Ihren eigenen richtigen CA Enterprise Log Manager-Servernamen oder Ihre eigene richtige IP-Adresse verwendet haben.
   b. Falls Sie Abfrage- oder Berichtsspezifikationen hinzugefügt haben, überprüfen Sie, ob der Hauptteil des Aufrufs (vor den Spezifikationsparametern) mit einem Fragezeichen (?) endet, bevor Parameter hinzugefügt werden. Beispiel:

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

2. Wenn die URL-Syntax richtig ist und keine Daten angezeigt werden, überprüfen Sie die Filter. Falls Sie "getQueryViewer" oder "getReportViewer" verwenden, überprüfen Sie die Filter und Ergebnisbedingungseinstellungen in der Schnittstelle. Falls Sie "runQuery" verwenden, überprüfen Sie die Parameterspezifikationen, die Sie der URL hinzugefügt haben:
   a. **Filter überprüfen** - Überprüfen Sie, ob die Basisfilter die von Ihnen gewünschten Daten anzeigen. Beispielsweise, ob der Name der von Ihnen gefilterten Ereignisquelle richtig eingegeben wurde.
   b. **Syntax** - Überprüfen Sie, ob die Filtersyntax richtig ist, insbesondere wenn Sie Filter erstellt haben, die Spezifikationsparameter verwenden.
   c. **Zeitfilter** – Überprüfen Sie, ob der Zeitraum lang genug ist, und stellen Sie sicher, dass die Zeitzone Ihres Betriebssystems und die Zeitzone von CA Enterprise Log Manager identisch sind.
   d. **Zugriffsfilter-XML-Filter** – Stellen Sie sicher, dass Sie sich erfolgreich von einer Sitzung abgemeldet haben.
   e. **LogDepot log** - Überprüfen Sie, ob Ereignisse empfangen und in der Datei "logDepot_sponsor.log" angezeigt werden.
3. Überprüfen Sie die Protokolleinstellungen für die API-Komponente. Überprüfen Sie, ob folgende Dateien und Einstellungen vorhanden sind:
   - Eigenschaftendatei: epSIM_logging.properties

- Die Standardstufe ist WARN.
- Protokollierung: logmanager.ui.calmapi
- Protokolldatei: calm.log