

Konfigurieren des CVIM OpenStack SSL-Zertifikats für den VIM Connector im Elastic Services Controller

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfung](#)

[Optionaler Schritt](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird das Verfahren zum Hinzufügen eines erneuerten OpenStack RESTAPI SSL-Zertifikats für die VIM-Verbindung (Virtualized Infrastructure Manager) zum Cisco Elastic Services Controller beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Elastic Services Controller
- Cisco VIM/OpenStack

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Elastic Services Controller 5.10.0.95
- Cisco VIM 4.2.2



Hinweis: Dieses Verfahren gilt auch für das Hinzufügen eines neuen Zertifikats beim Hinzufügen eines neuen VIM-Steckverbinders.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Nach der Verlängerung des OpenStack RESTAPI SSL-Zertifikats (HaProxy-Zertifikat für Cisco VIM-Umgebung) meldet der Elastic Services Controller, dass die VIM-Verbindung fehlgeschlagen ist.

```
[admin@lab-esc-1 ~]$ tail -100f /var/log/esc/yangesc.log
2024-04-09 10:35:36.148 WARN ===== SEND NOTIFICATION STARTS =====
```

```
2024-04-09 10:35:36.148 WARN Type: VIM_CONNECTION_STATE
2024-04-09 10:35:36.148 WARN Status: FAILURE
2024-04-09 10:35:36.148 WARN Status Code: 500
2024-04-09 10:35:36.148 WARN Status Msg: VIM Connection State Down
2024-04-09 10:35:36.148 WARN Vim connector id: cvim-openstack-lab
2024-04-09 10:35:36.148 WARN ===== SEND NOTIFICATION ENDS =====
```

```
[admin@lab-esc-1 ~]$ sudo escadm vim show
{
  "id":"cvim-openstack-lab",
  "type":"OPENSTACK",
  "last_checked":"2024-04-09T10:35:36.099",
  "status":"CONNECTION_FAILED",
  "status_message":"Unable to establish VIM connection",
}
```

Konfigurationen

Listen Sie die aktuellen Zertifikate auf, die im Elastic Services Controller-Vertrauensspeicher vorhanden sind:

```
[admin@lab-esc-1 ~]$ escadm truststore show --verbose
esc, Mar 30, 2024, trustedCertEntry,
cvim-openstack-lab, Apr 4, 2024, trustedCertEntry,
```

CA-Zertifikatsdatei in Elastic Services Controller-VM kopieren/übertragen

1. Für die Konfiguration des Active-Standby Elastic Services Controllers kopieren Sie das Zertifikat in Active VM.
2. Für die Active-Active ESC-Konfiguration kopieren Sie das Zertifikat in die VM für den geprimären Leiter.

```
[admin@lab-esc-1 ~]$ ls -l /home/admin
-rw-r--r--. 1 admin admin 1911 Apr 9 06:20 cvim-openstack-lab-renewed_haproxy.crt
```

Fügen Sie dem Elastic Services Controller-Vertrauensspeicher ein Zertifikat hinzu, indem Sie den Befehl ausführen `escadm truststore add`.

1. File-Argument bezieht sich auf die CA-Zertifikatsdatei des Typs X.509 v1, v2 und v3 und PKCS#7.

2. Das Alias-Argument ist eindeutig und bezieht sich auf den Namen dieses spezifischen Zertifizierungsstellen-Zertifikats.

```
[admin@lab-esc-1 ~]$ sudo escadm truststore add --alias cvim-openstack-lab-renewed --file cvim-openstack-lab-renewed.crt CA certificate "cvim-openstack-lab-renewed" added successfully.  
On ESC setup running ETSI, restart ETSI by running "sudo escadm etsi restart". All other components will be restarted.
```

Überprüfung

Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Überprüfen Sie, ob das Zertifikat dem Elastic Services Controller-Vertrauensspeicher erfolgreich hinzugefügt wurde.

```
[admin@lab-esc-1 ~]$ sudo escadm truststore show --verbose  
esc, Mar 30, 2024, trustedCertEntry,  
cvim-openstack-lab, Apr 4, 2024, trustedCertEntry,  
cvim-openstack-lab-renewed, Apr 9, 2024, trustedCertEntry,
```

Überprüfen Sie, ob die VIM-Verbindung aktiv ist.

```
[admin@lab-esc-1 esc]$ sudo escadm vim show  
{  
  "id":"cvim-openstack-lab",  
  "type":"OPENSTACK",  
  "last_checked":"2024-04-09T11:15:57.157",  
  "status":"CONNECTION_SUCCESSFUL",  
  "status_message":"Successfully connected to VIM"  
}
```

```
[admin@lab-esc-1 ~]$ tail -100f /var/log/esc/yangesc.log  
2024-04-09 11:15:57.188 INFO ===== SEND NOTIFICATION STARTS =====  
2024-04-09 11:15:57.188 INFO Type: VIM_CONNECTION_STATE  
2024-04-09 11:15:57.188 INFO Status: SUCCESS  
2024-04-09 11:15:57.188 INFO Status Code: 200  
2024-04-09 11:15:57.188 INFO Status Msg: VIM Connection State Up  
2024-04-09 11:15:57.189 INFO Vim connector id: cvim-openstack-lab  
2024-04-09 11:15:57.189 INFO ===== SEND NOTIFICATION ENDS =====
```

Optionaler Schritt

Bei einer Erneuerung des Zertifikats entfernen Sie das alte Zertifikat, nachdem Sie bestätigt haben, dass die VIM-Verbindung nach dem Hinzufügen eines neuen Zertifikats wieder besteht.

```
[admin@lab-esc-1 ~]$ sudo escadm truststore delete --alias cvim-openstack-lab --verbose  
CA certificate "cvim-openstack-lab" deleted successfully
```

```
[admin@lab-esc-1 ~]$ sudo escadm truststore show --verbose  
esc, Mar 30, 2024, trustedCertEntry,  
cvim-openstack-lab-renewed, Apr 9, 2024, trustedCertEntry,
```

Fehlerbehebung

In diesem Abschnitt erhalten Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Der Elastic Services Controller-TrustStore wird nach dem Hinzufügen eines neuen Services Controllers automatisch neu geladen. Daher muss die VIM-Verbindung automatisch aktiviert werden. Überprüfen Sie die Systemverwaltungsprotokolle, um im Fehlerfall eine Fehlerbehebung durchzuführen.

```
[admin@lab-esc-1 ~]$ tail -100f /var/log/esc/escamanager.log  
2024-04-09 11:15:55.369 INFO [SslManager.java:run:262] Change of type ENTRY_MODIFY is detected on trust  
2024-04-09 11:15:55.370 INFO [SslManager.java:loadESCTruststore:215] ESC truststore file loaded success  
2024-04-09 11:15:55.375 INFO [SslManager.java:loadESCTruststore:226] Added Java default Root CA certifi  
2024-04-09 11:15:55.376 INFO [VimUtils.java:reloadVimManagerTrustStore:1057] Starting request to reload  
2024-04-09 11:15:55.430 INFO [VimUtils.java:reloadVimManagerTrustStore:1065] Completed request to reloa  
2024-04-09 11:15:55.430 INFO [SslManager.java:run:270] Reloading of truststore is done.  
2024-04-09 11:15:57.183 INFO [VimAuthenticationService.java:updateVimStatusFromNotification:709] Vim st  
2024-04-09 11:15:57.183 INFO [VimAuthenticationService.java:processVimStatusNotification:784] Sending V  
2024-04-09 11:16:31.428 INFO [VimUtils.java:getAuthStatusById:1077] VIM ID - cvim-openstack-lab, VimInf
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.