Replace a cEdge RMA Router

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Step 1. Upgrade Spare or RMA Device into an SDWAN Compatible Image with the Controllers
- Step 2. Use Basic Configuration in order for the cEdge to Reach the vBond, vManage, and vSmart
- Step 3. Copy and Install the Root CA Certificate into Spare or RMA cEdge
- Step 4. Sync/Upload the Device List Under the vManage

Replacement Process if the cEdge Uses a Template

- Step 1. Backup the Current Values Used Under the Device Template
- Step 2. Remove the Failed Device from the Device Template Attached
- Step 3. Invalidate the Old/Failed Router
- Step 4. Send to the Controllers
- Step 5. Push the Template into a Spare or RMA Router

Replacement Process if the cEdge is Configured Through CLI

- Step 1. Backup the Current Configuration
- Step 2. Invalidate the Old/Failed Router
- Step 3. Send to the Controllers
- Step 4. Place the Configuration into the Router

Related Information

Introduction

This document describes how to replace a failed cEdge unit with another one.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Software-defined Wide Area Network (SD-WAN)

Components Used

The information in this document is based on these software and hardware versions:

- cEdge version 17.3.3
- vManage version 20.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This process consists of using a copy of the configuration from the failed router to the replacement router, the removal of this cEdge, and the addition of the new router into the network. This process is similar to vEdge replacement, however, the copy option is missed in vManage for cEdges.

Usually, the replacement of a failed cEdge unit with a new one is done when an RMA router is received due to the old cEdge router failing completely or a component in the router failing, and Cisco TAC must proceed with an RMA.

Before the cEdge replacement, verify some points in order for the new cEdge router to successfully establish control connections.

Step 1. Upgrade Spare or RMA Device into an SDWAN Compatible Image with the Controllers

Note: Ensure the current cEdge version is compatible with the controller versions. Refer to Compatibility matrix.

Note: For more information on the cEdge upgrade process through CLI, please refer to Software Installation and Upgrade for Cisco IOS XE Routers.

Step 2. Use Basic Configuration in order for the cEdge to Reach the vBond, vManage, and vSmart

Confirm that the cEdge in question has been configured properly. It includes:

- Valid Certificate that has been installed.
- Configure under the system block:

```
System-IP
Site-ID
Organization-Name
vBond address
```

- VPN 0 Transport interface that is configured with Tunnel option and IP address.
- System Clock that is configured correctly on the cEdge and those that match with other devices/controllers.

The command **show clock** confirms the current time set and use **clock set** to set the right time on the device.

```
show clock
clock set
```

- Ensure that cEdge reaches the vBond. If a Frequently Qualified Domain Name (FQDN) is used for the vBond, ensure that DNS is configured under VPN 0 and it resolves the vBond.

⚠ **Caution**: For the new cEdge, use a different System IP than the one present in the original/failed router. In the final steps, the system-IP is changed to the same as the original cEdge.

Step 3. Copy and Install the Root CA Certificate into Spare or RMA cEdge

The Root CA is grabbed by the CLI of any controller like vBond, vSmart or vManage. Locate the certificate in the vshell.

Example from vBond:

```
vshell
cd /usr/share/viptela
```

Display the content of the certificate and copy all the content.

```
ls -l root*
cat root-ca.crt
```

In order to copy the certificate into the boot flash of the cEdge, use FTP, SFTP, or a USB drive. If this is not possible, copy the certificate manually as the last resort.

Create the **file** for the new Root CA in the RMA cEdge.

⚠ **Caution**: The command lines have comments that start with "!". Remove all the **comments**.

```
tclsh !Hit enter
puts [open "bootflash:root-ca-new.cert" w+] { !Hit enter
!Paste-all-the-previous-content-from-vBond-or-vManage-certificaet-WITHOUT-spaces
}!Hit enter
exit
```

Under newer versions of Cisco IOS® XE SD-WAN, the **tclsh** command is disabled by default. In order to enable it temporarily, the **service internal** command is needed.

```
config-t
(config)# service internal
(config)# commit
(config)# end
debug platform software sdwan unlock-ios-cl
```

Uninstall the **old Root CA** and install the just **added Root CA**.

```
request platform software sdwan root-cert-chain uninstall
request platform software sdwan root-cert-chain install bootflash:<RootCAFile>
```

Check **show control connections** in order to validate device has established connections again with controllers.

Step 4. Sync/Upload the Device List Under the vManage

The RMA router has to be displayed under “vManage > Devices ”. If the device is not under the vManage, ensure that the device is added to the PnP portal.

At this point, the cEdge has control connections up to the controllers.

Replacement Process if the cEdge Uses a Template

Step 1. Backup the Current Values Used Under the Device Template

Backup current values used for the device under the template. Navigate to **vManage > Device Template > Template > … > Export CSV**.

Step 2. Remove the Failed Device from the Device Template Attached

Back up the variable values first.

Note: After the device template removal, all the variable values from the template are lost. The only way to recover them is to check the configuration of the failed or original unit. Furthermore, it is not possible to detach a device template if the WAN Edge router is in an unreachable state. The message "Please fix DTLS, NETCONF connectivity between device and vManage before template attempt workflow" is presented in the vManage GUI. In this situation, please invalidate the device first (**Configuration> Certificate**) and then proceed to detach the template.

Remove the device from any device template attached.

Step 3. Invalidate the Old/Failed Router

Invalidate the failed router under **vManage > Certificates > Devices.**

Note: All control connections are lost on these steps.

Step 4. Send to the Controllers

Select the **Send to controllers** in order to push the changes to the controllers.

Caution: If invalidated router's info is no longer needed and same system-ip needs to be reused on RMA router, please delete **invalidated router** from vManage.

Step 5. Push the Template into a Spare or RMA Router

Push the template into a spare or RMA router.

Note: Use the CSV file from step 1 to fill in all the values requested when the device template is attached.

Replacement Process if the cEdge is Configured Through CLI

Step 1. Backup the Current Configuration

Back up the current configuration. Navigate to **vManage > Device > … > Running Config**.

If the device is offline, try to select the **Local Configuration**, in order to check if there is a backup of the device configuration.

If any configuration is saved at the vManage, pull this configuration from the device itself.

Use these commands under CLI to create a file in Bootflash with all the current configurations:

```
show running-config | redirect bootflash:sdwan/ios.cli
show sdwan running-config | redirect bootflash:sdwan/sdwan.cli
```

Step 2. Invalidate the Old/Failed Router

Invalidate the old/failed Router in **vManage > Certificates > Devices.**

Note: After the device is invalidated, the configuration is lost. There is no way to recover the configuration from the vManage. The configuration is still available at the failed or original device.

Note: All control connections are lost on these steps.

Caution: If invalidated router's info is no longer needed and same system-ip needs to be reused on RMA router, please delete invalidated router from vManage.

Step 3. Send to the Controllers

Select the **Send to controllers** in order to push the changes to the controllers.

Step 4. Place the Configuration into the Router

Place all the configurations into the router. At this point, it is safe to change the system IP to use the system IP from the failed or original router.

Related Information

- Replace a vEdge Router
- Technical Support & Documentation - Cisco Systems