Cisco ACI and SDWAN Integration

New and Changed 2

About SDWAN Integration 2

Connecting to a vManage Controller and Applying WAN SLA Policies Using the Cisco APIC GUI 3

Connecting to a vManage Controller and Applying WAN SLA Policies Using the CLI 6

Connecting to a vManage Controller and Applying WAN SLA Policies Using the REST API 7

Removing the vManage Controller Registration 9

Revised: June 21, 2022,

New and Changed

The following table provides an overview of the significant changes up to the current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Table 1: New Features in Cisco APIC

Cisco APIC Release Version	Feature	Description
Release 4.1(1i)	Support was added to configure an SDWAN controller as an external device manager with SD WAN capability.	This guide was created for the Cisco ACI and SDWAN integration.
Release 4.2(1)	Provides support for enabling reverse traffic that is destined for the ACI data center to receive differentiated services over the WAN.	See *About SDWAN Integration* for more information.

About SDWAN Integration

Cisco ACI release 4.1(1i) adds support for WAN SLA policies. This feature enables tenant admins to apply preconfigured policies to specify the levels of packet loss, jitter, and latency for the tenant traffic over the WAN. When you apply a WAN SLA policy to the tenant traffic, the Cisco APIC sends the preconfigured policies to a vManage controller. The vManage controller, which is configured as an external device manager that provides Cisco Software-Defined Wide Area Network (SDWAN) capability, chooses the best possible WAN link that meets the loss, jitter, and latency parameters specified in the SLA policy.

You apply the WAN SLA policies to the tenant traffic though contracts. Before applying the WAN SLA policies, you must first establish a connection between the vManage controller and the Cisco APIC.

Note

- There are four preconfigured WAN SLA policies.
- The loss, latency, and jitter parameter values of the preconfigured WAN SLA policies can be modified from vManage. For more information, see the Policies Configuration Guide:

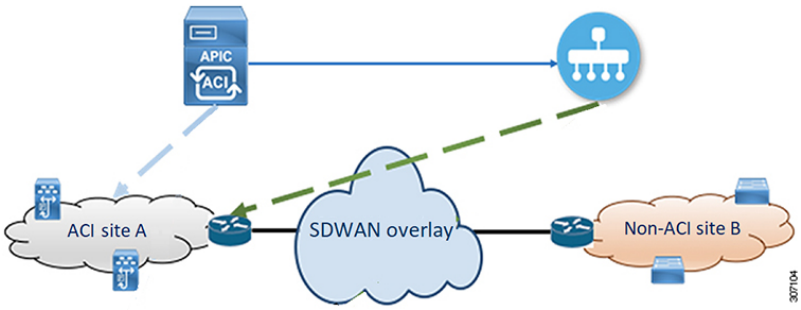
  https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html
- You apply the WAN SLA policies using the Cisco APIC GUI, CLI, or REST API.

Cisco APIC release 4.2(1) adds support for enabling returning traffic from a remote site that is destined for the ACI data center to receive differentiated services over the WAN. After the tenant admin registers the Cisco APIC to vManage, the Cisco APIC pulls the WAN-SLA policies and the WAN-VPN from vManage. Then, the Cisco APIC assigns DSCP to each WAN-SLA policy and pushes a prefix list. The prefix list, which is taken from the EPG if the contract between this EPG and L3Out has WAN-SLA configured, enables quality of service on the returning traffic. The WAN-SLA policy and WAN-VPN are both available in the tenant common. Tenant admins map the WAN-VPNs to VRFs on remote sites.

Note If you configure a subnet prefix under an EPG, the Cisco APIC pushes the subnet prefixes. If you configure a subnet and host prefix under an EPG, the Cisco APIC pushes only the subnet prefixes.

This document explains how to use the Cisco APIC GUI, CLI, and REST API to connect a preexisting vManage controller to the Cisco APIC, to apply the preconfigured WAN SLA policies, and to use a VPN to map VRFs on remote sites. For information about setting up the vManage controller, see the *Integrate Cisco XE SD-WAN Router with Cisco ACI* chapter of the *Policies Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html.

Figure 1: Ecosystem of the ACI-SDWAN Platform



Connecting to a vManage Controller and Applying WAN SLA Policies Using the Cisco APIC GUI

Connecting to a vManage Controller Using the Cisco APIC GUI

This task explains how to connect an SDWAN controller (vManage controller) to the Cisco APIC.

Before you begin

You have already configured a vManage controller. For information, see the *Integrate Cisco XE SD-WAN Router with Cisco ACI* chapter of the *Policies Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html.

Procedure

Step 1 On the menu bar, choose **Integrations** > **Create Group** .

The **Create Integrations Group** dialog appears.

Step 2 Enter the appropriate values in the **Create Integrations Group** dialog.

Note For an explanation of each field, click the help icon (**?**) in the top-right corner of the **Create Integrations Group** dialog

Step 3 Click **Submit**.

You are now in the **Integrations** window, which displays the name of the integrations group as a row in a summary table.

Step 4 Click the row in the summary table that contains the name of the group you created.

The **Integration Groups** window appears in the **Work** pane, and the **UCSM** and **vManage** icons appear as sub-nodes under the group icon in the **Navigation** pane.

Step 5 Right-click **vManage** and choose **Create Integration Manager**.

The **Create Integration** dialog appears.

Step 6 Enter the appropriate values in the **Create Integration** dialog fields.

Note For an explanation of each field, click the help icon (**?**) in the top-right corner of the **Create Integration** dialog

Step 7 Click **Submit** when finished.

You return to the **Integrations** window.

What to do next

Confirm that the SDWAN controller configuration was successful.

Confirming the vManage Controller is Connected Using the Cisco APIC GUI

This section explains how to use the Cisco APIC GUI to confirm that the SDWAN controller (vManage controller) connection was successful.

Before you begin

You must first configure a vManage controller and establish a connection to the Cisco APIC.

For information about establishing a connection between the Cisco APIC and the vManage controller using the Cisco APIC GUI, see Connecting to a vManage Controller Using the Cisco APIC GUI, on page 3

Procedure

Step 1 On the menu bar, choose **Integrations**.

The names of the previously created integration groups appear as subtabs.

Step 2 Click on the name of the group with the SDWAN controller configuration you want to confirm.

The group appears as an icon in the **Navigation** pane.

Step 3 From the **Navigation** pane, expand the group name node icon.

The **UCSM** and **vManage** icons appear in the **Navigation** pane.

Step 4 Expand the **vManage** icon.

The ***Integration_Name*** node appears in the **Navigation** pane.

Step 5 Click the ***Integration_Name*** node.

The **Integration** window appears in the **Work** pane with the **System Info**, **Policy**, **Faults**, and **History** tabs.

Step 6 Click the **System Info** tab.

The **System Info** properties appear in the **Work** pane. The **Status** field contains a message indicating that the SDWAN configuration was successful or if it failed. If the configuration was successful, the **Partner ID** property is also populated with a value.

What to do next

If not already specified, associate a WAN SLA policy with a contract associated between the tenant EPG traffic and the L3Out. For more information, see Associating a WAN SLA Policy with a Contract Using the Cisco APIC GUI, on page 5

Associating a WAN SLA Policy with a Contract Using the Cisco APIC GUI

This section explains how to associate a preconfigured WAN SLA policy with a contract using the Cisco APIC GUI.

Note The contract you associate with preconfigured WAN SLA policies must be associated “between the tenant EPG and the external EPG defined in the L3Out.

Before you begin

You must first create a contract with a subject. For information on creating contracts, see the *Cisco APIC Basic Configuration Guide*.

Procedure

Step 1 On the menu bar, choose **Tenant** and the tenant name on which you want to operate.

Step 2 In the **Navigation** pane, expand the *tenant-name* and **Contracts** > **Standard**.

The standard contracts appear in the **Navigation** pane.

Step 3 In the **Navigation** pane, expand the contract that you want to associate with the SDWAN controller.

The contract subjects appear in the **Navigation** pane.

Step 4 In the **Navigation** pane, click a subject icon.

The **Contract Subject** window appears in the **Work** pane.

Step 5 Click the **WAN SLA Policy** drop-down arrow and choose a policy.

Step 6 If the **QoS Priority** value is set to **Unspecified**, click the **QoS Priority** drop-down arrow and choose a level.

Note The **QoS Priority** value must be set to any value other than **Unspecified**. The WAN SLA policies will not work if the **QoS Priority** value is set to **Unspecified**.

Matching a WAN VPN to a Tenant VRF Using the GUI

This task demonstrates how to match a WAN VPN to a tenant VRF using the GUI.

Procedure

Step 1 On the menu bar, choose **Tenant** and the tenant name on which you want to operate.

Step 2 In the **Navigation** pane, expand the *tenant-name* and **Networking** > **VRFs**.

The configured VRFs appear in the **Navigation** pane.

Step 3 From the **Navigation** pane, click the VRF you want to match with a WAN VPN.

The Policy tab appears in the **Work** pane.

Step 4 Click the **Policy** tab.

The VRF properties appear in the **Work** pane.

Step 5 **WAN VPN** drop-down arrow and choose the VPN.

Note The VPN options appear in the drop-down menu as a list of numbers. The number of VPN options that appear in the menu depends on how many are created in the manager.

Connecting to a vManage Controller and Applying WAN SLA Policies Using the CLI

Connecting to a vManage Controller Using the CLI

This task demonstrates how to connect an SDWAN controller (vManage controller) to the Cisco APIC using the CLI.

Before you begin

You have already configured a vManage controller. For information, see the *Integrate Cisco XE SD-WAN Router with Cisco ACI* chapter of the *Policies Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html.

Procedure

Connect a vManage controller:

```
apic1# conf t
apic1(config)# integrations-group MyExtDevGroupClassic
apic1(config-integrations-group)# integrations-mgr External_Device Cisco/vManage
apic1(config-integrations-mgr)# device-address 172.31.209.198
apic1(config-integrations-mgr)# user admin
Password:
Retype password:
apic1(config-integrations-mgr)#
```

What to do next

Apply WAN SLA policies to a contract subject

Applying WAN SLA Policies to a Contract Subject Using the CLI

This task demonstrates how to apply WAN SLA policies to a contract subject using the CLI.

Before you begin

You must first create a contract with a subject. For information on creating contracts, see the *Cisco APIC Basic Configuration Guide*.

Note The contract you associate with preconfigured WAN SLA policies must be associated between the tenant EPG and the external EPG defined in the L3Out.

Procedure

Apply WAN SLA policies to a contract subject:

```
apic1# conf t
apic(config)# tenant tenant_1
apic(config)# contract contract_c1_1
apic(config)# subject subj_c1_1
apic(config)# access-group Filter_c1_1 both
apic(config)# set qos-class level1
apic(config)# set target-dscp CS2
apic(config)# sdwan-sla Voice
```

Matching a WAN VPN to a Tenant VRF Using the CLI

This task demonstrates how to match a WAN VPN to a tenant VRF using the CLI.

Procedure

Matching a WAN VPN to a tenant VRF:

```
apic1# conf t
apic1(config)# tenant TENANT_1
apic1(config-tenant)# vrf context vrf1
apic1(config-tenant)# sdwan-vpn 1
apic1(config-tenant)# exit
```

What to do next

Connecting to a vManage Controller and Applying WAN SLA Policies Using the REST API

Connecting a vManage Controller Using the REST API

This task demonstrates how to connect to a preexisting SDWAN controller (vManage controller) to the Cisco APIC using the REST API.

Before you begin

You have already configured a vManage controller. For information, see the *Integrate Cisco XE SD-WAN Router with Cisco ACI* chapter of the *Policies Configuration Guide*: https://www.cisco.com/c/en/us/support/routers/sd-wan/tsd-products-support-series-home.html.

Procedure

Specify the vManage controller as an external device manager with SD WAN capability.

```
POST  https://<apic>/api/policydist/mo/uni.xml
<extdevGroupP name="MyExtDevGroupClassic" status="">
<extdevMgrP name="MyExtDevMgrClassic" deviceAddress="172.31.209.198" inventoryTrigSt="triggered"
status="" usr="admin" pwd="admin" srcDevType="uni/infra/devCont/devt-Cisco-vManage"/>
</extdevGroupP>
```

What to do next

Apply WAN SLA policies to a contract subject (See Applying WAN SLA Policies to a Contract Subject Using the REST API, on page 8).

Applying WAN SLA Policies to a Contract Subject Using the REST API

This task demonstrates how to associate a WAN SLA policy with a subject in a contract.

Note The contract you associate with preconfigured WAN SLA policies must be associated between the tenant EPG and the external EPG defined in the L3Out.

Before you begin

You must first create a contract with a subject. For information on creating contracts, see the *Cisco APIC Basic Configuration Guide*.

Procedure

Add a relation to a WAN SLA policy from a subject in a contract that can be between a tenant EPG and an L3Out.

```
POST https://<apic>/api/node/mo/.xml
<polUni>
<fvTenant dn="uni/tn-coke1" name="TENANT_1" >
   <vzFilter name="Filter_c1_1" >
      <vzEntry  etherT="ip" name="filter_c1_1"  />
   </vzFilter>
   <vzBrCP intent="install" name="contract_c1_1">
      <vzSubj name="subj_c1_1" prio="level1" targetDscp="CS2">
         <vzRsSubjFiltAtt action="permit"  tnVzFilterName="Filter_c1_1" />
         <vzRsSdwanPol  tDn="uni/tn-common/sdwanpolcont/sdwanslapol-Voice" />
      </vzSubj>
   </vzBrCP>
</fvTenant>
</polUni>
```

Matching a WAN VPN to a Tenant VRF Using the REST API

This section demonstrates how to match a WAN VPN to a tenant VRF and how to delete the match using the REST API.

Procedure

Step 1 To match a WAN VPN to a tenant VRF:

```
POST https://<apic>/api/node/mo/.xml
<polUni>
   <fvTenant annotation="" descr="" dn="uni/tn-TENANT_1" name="TENANT_1" nameAlias="" ownerKey=""
ownerTag="">
      <fvCtx annotation="" bdEnforcedEnable="no" descr="" ipDataPlaneLearning="enabled"
knwMcastAct="permit" name="vrf1" nameAlias="" ownerKey="" ownerTag="" pcEnfDir="ingress"
pcEnfPref="enforced">
         <fvRsCtxToSDWanVpn annotation="" tDn="uni/tn-common/sdwanvpncont/sdwanvpnentry-1" />
      </fvCtx>
   </fvTenant>
</polUni>
```

Step 2 To delete a WAN VPN match to a tenant VRF:

```
POST https://<apic>/api/node/mo/.xml
<polUni>
   <fvTenant annotation="" descr="" dn="uni/tn-TENANT_1" name="TENANT_1" nameAlias="" ownerKey=""
ownerTag="">
      <fvCtx annotation="" bdEnforcedEnable="no" descr="" ipDataPlaneLearning="enabled"
knwMcastAct="permit" name="vrf1" nameAlias="" ownerKey="" ownerTag="" pcEnfDir="ingress"
pcEnfPref="enforced">
         <fvRsCtxToSDWanVpn annotation="" tDn="uni/tn-common/sdwanvpncont/sdwanvpnentry-1"
status="deleted"/>
      </fvCtx>
   </fvTenant>
</polUni>
```

Removing the vManage Controller Registration

Removing the vManage Controller Registration Using the Cisco APIC GUI

This task explains how to remove the SDWAN controller (vManage controller) registration from the Cisco APIC.

Note When the vManage controller is registered with the Cisco APIC, a conduit is created from inside Cisco ACI. When the registration is removed, that channel is disconnected.

Before you begin

You have connected a vManage controller to the Cisco APIC that you want to disconnect.

Procedure

Step 1 On the menu bar, choose **Integrations** > **Integration_group_name** .

The **Integration Groups** window appears in the work pane.

Step 2 From the navigation pane, expand the nodes representing the **Integration_group_name** > **vManage** > **vManage_controller_name**.

Step 3 Right-click the **vManage_controller_name** and choose **Delete**.

A **Delete** dialog appears.

Step 4 Click **Yes**.

The vManage controller is now disconnected.

Removing the vManage Controller Registration Using the Cisco APIC CLI

This task explains how to remove the SDWAN controller (vManage controller) registration from the Cisco APIC.

Note When the vManage controller is registered with the Cisco APIC, a conduit is created from inside Cisco ACI. When the registration is removed, that channel is disconnected.

Before you begin

You have connected a vManage controller that you want to disconnect from the Cisco APIC.

Procedure

Disconnect the vManage controller from the Cisco APIC:

```
apic1# conf t
apic1(config)# integrations-group MyExtDevGroup
apic1(config-integrations-group)# show running-config
# Command: show running-config integrations-group MyExtDevGroup
# Time: Thu Feb 14 13:35:44 2019
  integrations-group MyExtDevGroup
    integrations-mgr External_Device Cisco/vManage
      device-address 172.31.209.198
      # user admin
      exit
    exit
apic1(config-integrations-group)# no integrations-mgr External_Device
```

Removing the vManage Controller Registration Using the REST API

This task explains how to remove the SDWAN controller (vManage controller) registration from the Cisco APIC.

Note When the vManage controller is registered with the Cisco APIC, a conduit is created from inside Cisco ACI. When the registration is removed, that channel is disconnected.

Before you begin

You have connected a vManage controller to the Cisco APIC that you want to disconnect.

Procedure

To remove the vMange controller registration:

```
POST: https://<mgmt0_IP>/api/policydist/mo/uni.xml
<extdevGroupP name="MyExtDevGroup">
<extdevMgrP deviceAddress="<mgmt0_IP>" name="External_Device" status='deleted'/>
</extdevGroupP>
```

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.