CISCO SD-WAN Cloud Ramp Colocation User Guide

Contents

1 CISCO SD-WAN Cloud Ramp Colocation User Guide
2 Overview of Colocation Multitenancy
3 Roles and Functionalities in a Multitenant Environment
4 Recommended Specifications in a Multitenant Environment
5 Assumptions and Restrictions in Colocation Multitenancy
6 Service Provider Functionalities
7 Provision a New Tenant
8 Manage Tenant Colocation Clusters
9 c-tenant-functionalities
10 Monitor Colocation ClusterDevices and Cisco SD-WANDevices in Comanaged Multitenant Environment
11 Documents / Resources
11.1 References
12 Related Posts

CISCO SD-WAN Cloud Ramp Colocation User Guide

Cisco SD-WAN Cloud onRamp for Colocation Multitenancy

Table 1: Feature History

Feature Name	Release Information	Description
Colocation Multitenancy UsingRole-Based Access Control	Cisco IOS XE Release 17.5.1aCisco SD-WAN Release 20.5.1Cisco vManage Release 20.5.1	This feature enables a service provider to manage multiple colocation clusters and share these clusters across tenants by using multiplecolocation groups. In a multitenant setup, service providers don’t need to deploy a unique colocation cluster for each tenant. Instead, the hardware resources of a colocation cluster are shared across multiple tenants. With multitenancy, service providers ensure that tenants view only their data by restricting access based on roles of individual tenant users.

Overview of Colocation Multitenancy

In Cisco SD-WAN Cloud onRamp for Colocation multitenancy, a service provider can manage multiple colocation clusters using Cisco vManage in single-tenant mode. A service provider can bring up a multitenant cluster in the same way as bringing up a cluster in a single-tenant mode. A multitenant cluster can be shared across multiple tenants. See Create and Activate Clusters.
The tenants share the hardware resources such as the Cisco Cloud Services Platform (CSP) devices and Cisco Catalyst 9500 devices of a colocation cluster. The following are the key points of this feature.

- A service provider deploys and configuresthe CiscoSD-WAN Controllers(Cisco vManage, Cisco vBond Orchestrator, and Cisco vSmart Controller) with valid certificates.
- A service provider sets up colocation clusters after onboarding the Cisco CSPdevices and Cisco Catalyst 9500 switches.
- Cisco SD-WAN operates in a single-tenant mode and Cisco vManage appears in a single-tenant mode.
- In a colocation multitenant deployment, a service provider ensures that tenants see only their service chains by, creating roles. A service provider creates roles for each tenant in a colocation group. These tenants are permitted to access and monitor the service chains based on their roles. However, they can’t configure theirservice chains or change the system-levelsettings. The roles ensure that tenants can access only the information that they are authorized to view.
- Each tenant traffic is segmented using VXLAN across the compute devices, and VLAN across the Cisco Catalyst switch fabric.
- A service provider can provision service chains on a specific cluster

The following are the two scenarios of a colocation multitenant setup:

- **Service provider owned Cisco SD-WAN devices:** In this scenario, the Cisco SD-WAN devices used in a service chain belong to the corresponding service provider. The CSPdevices and Catalyst 9500 switches are owned, monitored, maintained by the service provider. The virtual machine (VM) packages are owned, uploaded, and maintained by a service provider. See Monitor **Colocation Cluster Devices and Cisco SD WAN Devices in Comanaged Multitenant Environment, on page 9.**
- **Comanaged Cisco SD-WAN devices:** In this scenario, the Cisco SD-WAN devices that are used in a service chain belong to a tenant overlay network. The colocation cluster devices are owned by the service provider, whereas the Cisco SD-WAN devices of a service chain are controlled by the Cisco SD-WAN Controllers (Cisco vManage, Cisco vBond Orchestrator, and Cisco vSmart Controller) of a tenant. The CSP devices and Catalyst 9500 switches are owned, monitored, maintained by the service provider. The VM packages are owned, uploaded, and maintained by a service provider.See **Monitor Colocation Cluster Devices and Cisco SD-**

Tenants	Clusters (CPUs)	Service Chains (CPUs) per Tenant	VLANs
150	2 (608)	1 (4)–Small	~300
75-150	2 (608)	2-3 (4-8)–Medium	300-450
25-50	2 (608)	4-6 (12-24)–Large	~400
300	4 (1216)	Small	~600
150-300	4 (1216)	Medium	600-900
50-100	4 (1216)	Large	~800
600	8 (2432)	Small	~1200
300-600	8 (2432)	Medium	900-1200
100-200	8 (2432)	Large	~1050
750	10 (3040)	Small	~1500
375-750	10 (3040)	Medium	600-1500
125-230	10 (3040)	Large	~1250

For example, if a service provider provisions four vCPUs per tenant for a service chain that consists of a single VM, the service provider can onboard approximately 150 tenants on two clusters with eight CSPdevices. Each of these tenants orservice chainsrequires 300 hand-off VLANs, one ingress, and one egress VLAN per service chain. For information about the number of VMs per service chain for various colocation sizes,see **Sizing Requirements of CiscoSD-WAN Cloud onRamp for Colocation Solution Devices.**

Assumptions and Restrictions in Colocation Multitenancy

The following sections provide detailed information about the assumptions and restrictions in a colocation multitenant environment.

Assumptions

- The wiring between Cisco CSP devices and Cisco Catalyst 9500 switches is completed as per the prescriptive connections or flexible topology. To bring up multiple clusters, ensure that the wiring between the CSP devices and Catalyst 9500 switches of a cluster are in the same way as a single cluster. For more information about wiring, see Wiring Requirements.
- Each Cisco CSP device has two 1-GB management ports that are manually configured as port channels to the out of band (OOB) management switch.
- A tenant can only monitor the event or alarms from the Monitor window for the VNFs that are a part of the service chains that they own. The tenant-monitoring windows display the corresponding colocation group when a tenant is viewing a service chain.

Note

In a co managed multi tenant setup, the service provider provisions service chains for tenants by gathering the required information from tenants. For example, a tenant provides the tenant organization name, tenant Cisco v

In a single-tenant Cisco vManage, a colocation cluster can be shared across multiple tenants by using colocation groups. The colocation groups are a mechanism to associate a service chain to a particular tenant. The RBAC users created for the tenants are called the colocation groups. These users can log in to Cisco vManage using their credentials to view only their tenant-specific service chains and VNFinformation. If the service provider chooses to use a service group for a tenant, the colocation group needs to be created prior to creating a service group so that the colocation group can be associated with the service group.

Step 1 From the Cisco vManage menu, choose Administration > Colo Groups.
Step 2 Click Add Colo Group.
Step 3 Enter a colocation group name, name of a user group with which the colocation group must be associated with, and description.
Note The colocation group name you provide here is displayed when you create a service group for a multitenant setup.
Step 4 Click Add

View Permissions of a User Group

Step 1 From the Cisco vManage menu, choose Administration > Manage Users.
Step 2 Click User Groups.
Step 3 To view the permissions of a user group, in theGroup Name list, and click the name of the user group that you created.
Note The user group and their permissions are displayed. To know about the list of user group permissions in a multitenant environment, see the Manage Users Using Cisco vManage topic in the Cisco SD-WAN Systems and Interfaces Configuration Guide.

Create an RBAC User and Associate to Colocation Group

Step 1 From the Cisco vManage menu, choose Administration > Manage Users.
Step 2 Click Add User.
Step 3 In the Add User dialog box, enter the full name, username, and password for the user.
Note You can’t enter uppercase characters for usernames.
Step 4 From the User Groups drop-down list, add the groups that the user must belong to, by choosing one group after another, for example, a user group that you created for the colocation feature. By default, the resource group global is chosen.
Step 5 Click Add.

Cisco vManage now lists the user is in the Users table.

Note The RBAC users who are created for tenants or colocation groups can log in to Cisco vManage using their credentials. These users can view their tenant-specific service chains and VNF information after the service group associated with a tenant is attached to a cluster.

Delete an RBAC User from a Colocation User Group

To delete an RBAC user, remove the RBAC user from a colocation group if the user is configured using Cisco vManage. If the user is authenticated using the TACACS server, disassociate the user from the user group in the TACACS server.
After an RBAC user is deleted, the user can no longer access or monitor the devices of the cluster. If an RBAC user is logged into Cisco vManage, deleting the user doesn’t log out the RBAC user.

Step 1 From the Cisco vManage menu, choose Administration > Manage Users.
Step 2 Click an RBAC user you want to delete.
Step 3 For the RBAC user you want to delete, click … and choose Delete.
Step 4 Click OK to confirm the deletion of the RBAC user.

Delete Tenants
To delete a tenant, remove the service groups associated with the tenant and then remove the collocation group for the tenant.

Step 1 Locate the list of service groups associated with the tenant that you want to delete. See View Service Groups.
Note A tenant is a colocation group having one or more RBAC users associated to the same colocation group. In the service group configuration page, you can view the colocation group of the tenant.
Step 2 Detach the service group from the cluster for the tenant that you want to delete. See Attach or Detach a Service Group in a Cluster.
Note To reuse the service group for another tenant, change the colocation group associated with the service group.
If you delete the service group, you need to re-create it.
Step 3 Delete the colocation group for the tenant. See the Manage a User Group topic in the Cisco SD-WAN Systems and Interfaces Configuration Guide.

Manage Tenant Colocation Clusters

A service provider can perform the following managing tasks:

- **Activate clusters:** A service provider can configure devices, resource pool, system settings, and activate a cluster in the multitenant or shared mode. See **Create and Activate Clusters.**
- Create service groups and associate RBAC users to colocation groups: A service provider can create a colocation group, associate RBAC users to the colocation group, create a service group, associate the service group with the colocation group for the multitenant mode, and attach the service group to a specific cluster. See **Create Service Chain in a Service Group**

 **Note** A service provider must associate specific service groups for each tenant.

- Create VM packages: A service provider can create and upload the VM packagesinto the Cisco vManage repository. The same packages can be used to provision VNFs in service chains for multiple tenants.

   **Note**

  When a service group is associated with a colocation group, the SR-IOV option in the VM package creation that is used for configuring the VNF, is ignored. In a multitenant mode, VNF packages support only OVS-DPDK with VXLAN.
- Monitor service chains and VNFs of tenants: A service provider can monitor all the tenant service chains and identify the service chains that are unhealthy along with the tenants associated with these service chains. The service providers can also collect logs from Cisco vManage or CSP devices and notify the tenants.
- Add and remove Cisco CSPdevices: To manage colocation clusters, a service provider can add or remove CSP devices.

c-tenant-functionalities

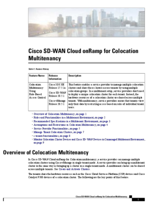
The following sections provide information about the tasks that tenants can perform.

Manage Colocation Clusters as Tenants

provider Cisco vManage > Configuration > Devices window under WAN Edge List, because these devices are controlled by the tenant.

Cisco SD-WAN Cloud onRamp for Colocation Multitenancy

Documents / Resources

	CISCO SD-WAN Cloud Ramp Colocation [pdf] User Guide SD-WAN Cloud Ramp Colocation, SD-WAN, Cloud Ramp Colocation, Ramp Colocation, Colocation

References

- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Configure Cisco SD-WAN Cloud onRamp for Colocation Solution Devices from vManage [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Configure Cisco SD-WAN Cloud onRamp for Colocation Solution Devices from vManage [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Configure Cisco SD-WAN Cloud onRamp for Colocation Solution Devices from vManage [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Cisco SD-WAN Cloud onRamp for Colocation Multitenancy [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Cisco SD-WAN Cloud onRamp for Colocation Multitenancy [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Monitor Cisco SD-WAN Cloud onRamp for Colocation Solution Devices [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Prerequisites and Requirements of Cisco SD-WAN Cloud onRamp for Colocation Solution [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco

- Cisco SD-WAN Cloud OnRamp for Colocation Solution Guide, Release 20.5.1 - Prerequisites and Requirements of Cisco SD-WAN Cloud onRamp for Colocation Solution [Cisco SD-WAN Cloud OnRamp for Co-Location] - Cisco
- Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - Configure User Access and Authentication [Cisco SD-WAN] - Cisco
- Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x - Configure User Access and Authentication [Cisco SD-WAN] - Cisco
- User Manual