Cisco SD-WAN Cloud onRamp for Colocation Multitenancy

Table 1: Feature History

Feature Name	Release Information	Description
Colocation Multitenancy Using Role-Based Access Control	Cisco IOS XE Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature enables a service provider to manage multiple colocation clusters and share these clusters across tenants by using multiple colocation 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 configures the Cisco SD-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 CSP devices 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 their service chains or change the system-level settings. 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 CSP devices 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-WAN Devices in Comanaged Multitenant Environment, on page 9.

Roles and Functionalities in a Multitenant Environment

Multitenant environments include a service provider and multiple tenants. Each role has distinct responsibilities and associated functions.

Service Provider

A service provider owns all the hardware infrastructure and manages the clusters. The service provider also onboards tenants by creating their roles, provisions the service chains for tenants, and can view all the service chains of all the tenants.

A service provider logs in to Cisco vManage as the **admin** user or a user who has the write permission for the manage users permission. A service provider can add, edit, or delete users and user groups from the Cisco vManage server, and is typically responsible for the following activities:

- Create and manage clusters for tenants.
- Upload prepackaged VM image packages and Cisco Enterprise NFV Infrastructure Software (NFVIS) software images on the CSP devices.

- Create custom colocation groups and role-based access control (RBAC) users.
- Create service groups and associate a colocation group to multiple service groups.
- Upgrade CSP devices and Catalyst 9500 switches.
- Monitor service chains and VMs of all the tenants.
- Start, stop, or restart operations on any of the tenant virtual network functions (VNFs).
- Administer Cisco vManage and record system-wide logging of Cisco SD-WAN devices.

Tenants

Tenants can initiate operations on the VNFs for the service chains that belong to themselves, but they can't view, access, or initiate operations on VNFs for the service chains that belong to another tenant. Tenants are responsible for the following activities:

- Monitor all the service groups and the health status of the service chains that belong to themselves.
- Monitor event or alarms for VNFs that are a part of the service chains that belong to themselves.
- Initiate start, stop, or restart operations on VNFs that are a part of the service chains that belongs to themselves.
- Collaborate with the corresponding service provider for issues, if any, on cluster, service chains, or VNFs.

Recommended Specifications in a Multitenant Environment

We recommend that service providers use the following information to decide on the number of tenants, clusters, service chains per tenant, and VLANs for various colocation sizes:

Table 2: Specifications for a Multitenant Environment

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

Tenants	Clusters (CPUs)	Service Chains (CPUs) per Tenant	VLANs
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 CSP devices. Each of these tenants or service chains requires 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 Cisco SD-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 comanaged multitenant 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 vBond Orchestrator IP address, tenant site ID, system IP address, and so on, out of band. See Create Service Chain in a Service Group.

Restrictions

- Altering a colocation cluster from a single-tenant mode to a multitenant mode and conversely isn’t supported.
- Sharing VNF devices across multiple tenants isn't supported.
- Service providers can provision multiple service groups for a tenant. But, the same service group can’t be provisioned for multiple tenants.

- Upgrading from Cisco SD-WAN Cloud onRamp for Colocation Release 20.4.1 having a single-tenant mode, to Release 20.5.1 or later having a multitenant mode isn't supported. This restriction means you can't upgrade from a single-tenant mode to multitenant mode.
- Multitenancy in single-root IO virtualization enabled (SR-IOV-enabled) physical network interface cards (PNICs) isn't supported; only open virtual switch (OVS) for VNF VNICs is supported. All the PNICs in the CSP devices are in OVS mode because the current SR-IOV drivers don't support VXLAN. The VNF VNICs are connected to OVS networks, and the ability to forward traffic at the desired speed might reduce.
- Managing billing and subscription of the resources utilized by tenants isn't supported.
- In a comanaged multitenant setup, a tenant can monitor only the VNF devices that the tenant owns.

Service Provider Functionalities

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

Provision a New Tenant

The service provider can provision a new tenant by creating a colocation group, and then provide access to a tenant by creating an RBAC user for the user group associated with the colocation group. RBAC users can perform limited administrative duties within their own tenant environment.

Before you begin

A service provider should bring up clusters in shared mode by establishing control connections with the CSP devices and activating the cluster. The service provider can create several clusters, and each of these clusters can have between two to eight CSP devices and two Catalyst 9500 switches. The cluster-creation operation supports an option to choose if the cluster is for a multitenant or a single-tenant deployment. See Create and Activate Clusters.

Step 1 To onboard a tenant, create a colocation group. For more information, see Create Colocation Group . This group provides access to tenants to monitor their service groups and VMs.

Step 2 Add an RBAC user and associate it with the colocation group created in Step 1. For more information, see Create an RBAC User and Associate to Colocation Group.

Note Don't add an RBAC user if you're authenticating the user using the TACACS server instead of Cisco vManage. If you're authenticating a user using a TACACS server, associate the user with the colocation group created in Step 1.

Step 3 Create a service group, associate it with the colocation group, and attach the service group to a specific cluster. See Create Service Chain in a Service Group.

When a tenant requires a new service chain, use the handoff VLANs that are specific to the tenant.

Create Colocation Group

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 VNF information. 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 the**Group 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 colocation 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 packages into 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 CSP devices: 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

All tenants must monitor the service chains and VMs associated with the service chains, and collaborate with service providers if any health issues arise with the service chains. Tenants can only monitor those events or alarms for VNFs that are a part of the service chains that belongs to the tenant.

Tenants don’t have any administrative privileges and can only see the service chains that service providers create. The tenant-monitoring windows display the corresponding colocation group when a tenant is viewing service chains. Tenants can perform the following tasks:

1. Log in to Cisco vManage as a tenant by entering the RBAC username and password.
2. View and monitor the health of the tenant service chains along with the health of the VNFs. To know more about the different service chain health statuses, see Monitor Cloud onRamp Colocation Clusters.

   In the **Monitor. Network** window, click **Diagram** for a service chain to view all the tenant service groups along with the service chains and VNFs in the design view.
3. View the VNF health of a tenant:
   a. In the Monitor window, click **Network Functions**.

b. Click a VNF name from the **Virtual NF** table.

In the left pane, click **CPU Utilization**, **Memory Utilization**, and **Disk Utilization** to monitor the resources utilization of a VNF.

You can also view the VM-specific alarms and events from the left pane.

4. Start, stop, or reboot a VNF:

a. In the Monitor window, click a VNF name from the **Virtual NF** table.

b. For the clicked VNF name, click **...** and choose one of the following operations:

- **Start**
- **Stop**
- **Restart**

Monitor Colocation Cluster Devices and Cisco SD-WAN Devices in Comanaged Multitenant Environment

Before you begin

- When creating a service chain using a service provider Cisco vManage, the service provider should ensure that the correct UUID, and device OTP for the Cisco SD-WAN VM in a service chain are entered. The service provider has no access to the tenant overlay, and therefore, a tenant should provide this information.
- When a service provider detaches a service group from a colocation cluster, the service provider should notify the tenant that the corresponding VM devices must be decommissioned using the tenant Cisco vManage.
- If a service provider needs to reattach a service group to a colocation cluster, a new OTP of the Cisco SD-WAN VM should be entered. This OTP is provided by the tenant. The service group in the service provider Cisco vManage should be edited to save the new OTP of the Cisco SD-WAN VM.

Step 1 Associate the tenant Cisco SD-WAN devices with the service provider service group when creating a service chain. See Create Service Chain in a Service Group.

Step 2 Monitor the VNFs from the service provider Cisco vManage. See Monitor Cloud OnRamp Colocation Clusters.

Step 3 Monitor the information about the Cisco SD-WAN devices of the VNFs from the tenant Cisco vManage.

Note The service provider can't view information about the Cisco SD-WAN devices of the VNFs from the service provider **Cisco vManage** > **Configuration** > **Devices** window under **WAN Edge List**, because these devices are controlled by the tenant.