Global VLANs

Global VLANs

Cisco UCS Central enables you to define global VLANs in a LAN cloud at the domain group root, or at the domain group level. You can create a single VLAN or multiple VLANs in one operation.

Global VLAN resolution takes place in Cisco UCS Central prior to global service profiles deployment. If a global service profile references a global VLAN, and that VLAN does not exist, the global service profile deployment fails in the Cisco UCS domain due to insufficient resources. All global VLANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VLANs are pushed to Cisco UCS domain along with the global service profiles that reference them. Global VLAN information is visible to Cisco UCS Manager only if a global service profile with reference to a global VLAN is deployed in that Cisco UCS domain. When a global VLAN is deployed and becomes available in the Cisco UCS domain, locally-defined service profiles and policies can reference the global VLAN. A global VLAN is not deleted when a global service profile that references it is deleted.

If a global VLAN is part of a global service profile, or a global port configuration, automatic VLAN resolution takes place when the service profile is pushed down, and the VLANs are available for local consumption in the Cisco UCS domain. If the global VLANs are not associated to a global service profile, or a global port configuration, you must manually publish them to deploy them to Cisco UCS Manager. Cisco UCS Central provides a command to manually publish the global VLAN to sync with Cisco UCS Manager. For more information on Publishing VLANs see Cisco UCS Central CLI Reference Manual.

Note You must have created the VLAN in Cisco UCS Central prior to publishing it to push it down to Cisco UCS Manager.

Note If a VLAN group is used to allow VLANs on a Fabric Interconnect's uplink, the global VLAN must be manually published to Cisco UCS Manager and added to the VLAN group, prior to adding to the service profile assigned to the Cisco UCS domain. If the global VLAN is not published and added to the VLAN group, the vNIC will shut down as the uplink will not allow the global VLAN to pass through.

Note A global VLAN is not deleted when a global service profile that references it is deleted.

You cannot delete a global VLAN from Cisco UCS Manager. If you want to delete a global VLAN from Cisco UCS Manager, you have to localize the VLAN and then delete it.

VLAN Org Permission

All VLANs configured in Cisco UCS Central are common to the orgs in which they are created. You must assign organization permissions before the Cisco UCS Manager instances that are part of the organizations can consume the resources. When you assign org permission to a VLAN, the VLAN is visible to those organizations, and available to be referenced in service profiles maintained by the Cisco UCS Manager instances that are part of the organization.

VLAN name resolution takes place within the hierarchy of each domain group. If a VLAN with the same name exists in multiple domain groups, the organization permissions are applied to all VLANs with the same name across the domain groups.

You can create, modify or delete VLAN org permission.

Note Make sure to delete the VLAN org permission from the same org you created it in. On Cisco UCS Central GUI you can view the org structure where this VLAN is associated. But at the sub org level on the Cisco UCS Central CLI, you cannot view the VLAN org permission association hierarchy, so if you try to delete the VLAN at the sub org level on the Cisco UCS Central CLI the delete operation will fail.

Creating or Editing a VLAN

You can create a VLAN at the domain group root or at a specific domain group level, and specify the orgs that can access the VLAN.

You can edit the**VLAN ID**, **Multicast Policy** and access for control for any selected VLANs. After creating a VLAN in a domain group, you can not change the **Domain Group Location** or the **VLAN Name**.

To watch a video on creating a VLAN, see Video: Creating a VLAN and Assigning Org Permission.

Step 1 In the **Actions** bar, type **Create VLAN** and press Enter.

Step 2 In the **VLAN** dialog box, choose the type of VLAN that you want to create.

This can be one of the following:

- **LAN**—The VLAN is used for communication with an external LAN.

- **Appliance**—The VLAN is used for appliance ports and port channels only.

Step 3 In **Basic**, click **Domain Group Location** and select the location in which you want to create this VLAN.

Step 4 Enter a **Name** for this VLAN.

The VLAN name is case sensitive.

Important Do not use the name **default** when you create a VLAN in Cisco UCS Central. If you want to create a global default VLAN, you may use **globalDefault** for the name.

Step 5 Enter the **VLAN ID**.

A VLAN ID can:

- Be between 1 and 3967

  Note If the registeredCisco UCS Domain has Cisco UCS Manager version 2.2(4) or above the ID range can be between 1 an 4027.

- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Step 6 (Optional) Choose whether to enable **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 7 (Optional) If you want to associate a **Multicast Policy** with this VLAN, enter the multicast policy name.

Cisco UCS Central identifies the multicast policy and attaches it to the VLAN in the back end.

Step 8 In **Private VLAN**, click the **Sharing Type** to determine whether the VLAN is subdivided into private or secondary VLANs. This can be one of the following:

- **None**—This VLAN does not have any secondary or private VLANs.
- **Primary**—This VLAN can be associated with one or more secondary VLANs.
- **Isolated**—This is a private VLAN. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.
- **Community**—This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.

Step 9 In **Access Control**, click the plus sign to display available orgs.

Step 10 Select the organizations and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 11 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 12 In**Multicast Policy**, click **Manually Provision** and enter the specific multicast policy name that you want to associate with this VLAN.

Cisco UCS Central attaches it to the VLAN in the back end. If the multicast policy is associated with a global service profile, the Cisco UCS Central displays a Policy Conflict message when a multicast policy of the same name exists in Cisco UCS Manager.

Step 13 (Optional) Click **Global Policy** and then select the global multicast policy that you want to assign to this VLAN.

Step 14 Click **Create**.

Creating or Editing a VLAN Range

Step 1 In the **Actions** bar, type **Create VLAN Range** and press Enter.

Step 2 In the **VLAN Range** dialog box, click **Basic** and choose the **Domain Group Location** in which you want to create this VLAN.

Step 3 Enter a **Name Prefix** for this VLAN range.

Step 4 Enter **VLAN ID**.

A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Example:

For example, to create six VLANs with IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43.

Step 5 (Optional) Choose whether to enable **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 6 (Optional) if you want to associate a **Multicast Policy** with this VLAN range, enter the multicast policy name.

Cisco UCS Central identifies the multicast policy and attaches it to the VLAN range in the back end.

Step 7 In **Private VLAN**, click the **Sharing Type** to determine whether the VLAN is subdivided into private or secondary VLANs. This can be one of the following:

- **None**—This VLAN does not have any secondary or private VLANs.
- **Primary**—This VLAN can be associated with one or more secondary VLANs.
- **Isolated**—This is a private VLAN. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.
- **Community**—This VLAN can communicate with other ports on the same PVLAN as well as the promiscuous port. Select the primary VLAN with which it is associated in the Primary VLAN drop-down list.

Step 8 In **Access Control**, click the plus sign display available orgs.

Step 9 Select the orgs and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 10 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 11 In**Multicast Policy**, click **Manually Provision** and enter the specific multicast policy name that you want to associate with this VLAN.

Cisco UCS Central associates it to the VLAN in the back end. If the multicast policy is associated with a global service profile, the Cisco UCS Central displays a Policy Conflict message when a multicast policy of the same name exists in Cisco UCS Manager.

This feature is supported with the Cisco UCS Manager release 3.1(3) and later.

Step 12 (Optional) Click **Global Policy** and then select the global multicast policy that you want to assign to this VLAN.

Step 13 Click **Create**.

Managing VLAN Access

From the **Manage VLAN Access** dialog box, you can add or remove permissions to one or more VLANs at the same time.

Note You can only add or remove access each time you open the dialog box. If you want to do both actions, you will need to relaunch the dialog box.

Step 1 In the **Actions** bar, type **Manage VLAN Access** and press Enter.

Step 2 To add access permissions to VLANs, do the following in the **VLAN Access** dialog box:

a) Click **Add Org Permissions**.

b) Select the VLAN name or range that you want to use to filter the VLANs and click **Search**.

You can click specify a VLAN name to filter the results of VLANs displayed. You can search with a partial or full name of the VLAN that you want to select. For example, you can search for *VLAN100* to filter the list of VLANs with names containing VLAN100.

c) Click the check boxes for the VLANs that you want to change the permissions for, or select the top check box to select all VLANs on the page.

d) Click the Plus icon, and select the organizations for which you want to grant permissions.

Step 3 To remove access permissions to VLANs, do the following:

a) Click **Remove Org Permissions**.

b) Select the organization for which you want to remove access permissions.

c) Select the VLAN name or range that you want to use to filter the VLANs and click **Search**.

d) Click the check boxes for the VLANs that you want to remove the permissions for, or select the top check box to select all VLANs on the page.

Step 4 Click **Apply** to save and apply your changes.

VLAN Groups

A VLAN Group is a logical entity created to configure VLANs on uplink ports and port channels, and vNICs in a Global Service Profile. Starting Cisco UCS Central 2.0, you can create a VLAN Group to logically group VLANs on Ethernet uplink ports by function, or by VLANs that belong to a specific network. You can apply these VLAN Groups to Ethernet uplink ports or service profile vNICs. VLAN Groups for Ports and Service Profiles are supported for Cisco UCS Manager 3.1(3) and later releases. However, Global VLAN Groups are

not supported on Cisco UCS Manager releases prior to 3.1(3) even though they are supported locally in Cisco UCS Central.

Creating or Editing a VLAN Group

You can create a VLAN Group under **LAN Cloud** per Domain-Group.

- For a Global Service profile, all associated VLAN Groups are resolved when the service profile is associated to a server. Depending on the server location in Cisco UCS Central, the VLANs get dynamically resolved and get deployed to the domain.
- For VLAN Groups on a Port, all associated VLANs are resolved when you save the port configuration depending on the domain group membership of the domain in **Cisco UCS Central**.

VLAN Groups have Org permission configured, and are accessible only from those Global Service Profiles that are created under the **Orgs** with the corresponding org permission. After you assign a VLAN to a VLAN group, all changes you make are applied to all Ethernet uplink ports and vNICs that are configured in the VLAN Group. You can configure multiple VLAN Groups for a vNIC (in the case of the Global Service Profile), and for uplink ports or port-channels. More than one VLAN Group can co-exist with other ungrouped VLANs that are configured on a vNIC or a port or port-channel.

When you add a VLAN Group to an uplink port, all the VLANs assigned before to the port are removed and re-added once the configuration is complete. Also, the uplink port allows the newly added VLANs instead. An uplink port on a particular Cisco UCS Domain that is not associated with the VLAN Group does not support the VLANs that are part of the configured VLAN Group.

You can configure VLAN Groups on the vNICs in the following ways:

- Directly modifying the vNIC
- Modifying through the LAN Connectivity Policy
- Modifying through the vNIC template

Step 1 In the **Actions** bar, type **Create VLAN Group** and press Enter.

Step 2 In the **VLAN Group** dialog box, choose the domain group to create the VLAN group.

Step 3 Choose the **Organization** where you want to create the VLAN group, and enter the **Name** and optional **Description**.

The name is case-sensitive.

Step 4 In **VLANs**, select the VLAN you want to add to the VLAN group. Optionally, you can choose any VLAN from the following VLAN types and **Set as Native** VLAN by checking the **Set as Native** check box:

- Primary
- Community
- isolated
- *Name*-VLAN

Step 5 In **Access Controls**, select the Organization permission.

Step 6 Click **Create**.

Step 7 In **Access Control**, click the plus sign to display available organizations.

Step 8 Select the organizations and click the checkmark to apply the selected organizations as **Permitted Orgs** for this VLAN.

You must configure the permitted Orgs for VLAN Groups for a Global Service Profile. Configuring Access controls is optional for Port groups.

Viewing a VLAN Group

Step 1 From **VLAN Groups Container** view, select a **VLAN Group** you want to view and press Enter.

Step 2 The VLAN Group view displays the following details:

- VLANs associated with the VLAN group, and native VLANs configured on the VLAN group
- Size of the VLAN group
- Permitted organizations and Location of the VLAN group

From the **VLAN Group** view, you can **Edit**, **Delete**, **Share**, **Favorite**, and **Tag** the VLAN Group you created.

VLAN Group Container View

A **VLAN Group Container** view displays a list of all VLAN groups in a domain. You can view the following details in the VLAN Group Container view:

- **Name**—Lists the VLAN group names present in a domain group
- **Native VLAN**—Lists the Native VLANs associated with the VLAN groups

You can filter the VLAN group Containers by Domain Group, **Export**, **Delete**, **Tag**, and **Search** for a specific VLAN group on this page.