Resource Management and Collectors in a Network Hierarchy

Feature history of resource management and collectors

Table 1: Feature History

Feature Name	Release Information	Description
Resource Management	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature enables you to create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. The network hierarchy and the associated resource IDs, including region IDs and site IDs, help you apply configuration settings to a device. In addition, the introduction of the resource manager in Cisco SD-WAN Manager automatically manages these resource IDs, thereby simplifying the overall user experience of Cisco Catalyst SD-WAN. You can create a network hierarchy in Cisco SD-WAN Manager to represent the geographical locations of your network. You can create a region, an area, and a site in a network hierarchy. In addition, you can assign a site ID and a region ID to a device.

Feature Name	Release Information	Description
Resource Management Enhancement	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The following enhancements are introduced in the Resource Management feature. • Creation of a system IP pool on the **Configuration** > **Network Hierarchy** page • Automatic assignment of site ID, system IP, and hostname to a device in the Quick Connect workflow • Display of detailed information on the **Configuration** > **Network Hierarchy** page, including site ID pool, region ID pool, and the list of devices associated with a site
Support for Traffic Flow Collectors	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature enables you to configure traffic flow collectors such as the Cflowd server and security logging server. Cflowd monitors service side traffic flowing through devices in the overlay network and exports flow information to the collector. Enable security logging and configure servers for high-speed logging (HSL) and collecting external syslogs. You can configure the traffic flow collectors by navigating to **Configuration** > **Network Hierarchy** > **Collectors**.

Resource management and collectors

The resource manager in Cisco SD-WAN Manager manages resource IDs, which include region IDs and site IDs. The resource manager automatically generates a region ID when you create a region on the **Configuration** > **Network Hierarchy** page. Similarly, it generates a site ID for a site if you do not specify it. You can assign a site ID and a region ID to a device.

When you upgrade from an earlier version of Cisco SD-WAN Manager to Cisco vManage Release 20.9.1, the resource manager automatically creates sites based on the site IDs of your devices. Each site is named SITE_. The sites appear under the global node on the **Configuration** > **Network Hierarchy** page, and Cisco SD-WAN Manager associates each device with its site in the network hierarchy.

Collectors

Collectors process traffic that flows through routers in the overlay network and export flow information to a server. They maintain flow data extracted from the IP headers of packets within the traffic.

You can configure the location of cflowd collectors and set how frequently sampled flows are sent to the collectors. The samples are sent to the collectors at specific intervals. You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Assign resource IDs to devices

The resource management feature enables you to assign site ID, region ID, system IP, and host names to a device.

Assign a site ID to a device using the quick connect workflow

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the site ID of the device.

Note

- You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.
- If you want Cisco SD-WAN Manager to automatically generate a site ID for the device, do not make any change to the default value, **AUTO**.

Assign a site ID to a device using a template

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.

Step 2 Check if a device is attached to a device template.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.

Step 4 Click **…** adjacent to the System feature template and choose **Edit**.

Step 5 Click the **Basic Configuration** tab and set the scope of the **Site ID** field to **Global** and enter the site ID.

If you set the scope of the **Site ID** field to **Device Specific**, do the following:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

b. Click **…** adjacent to the device template and choose **Edit Device Template**.

c. In the **Site ID** field, enter the site ID.

You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

d. Click **Update**.

e. Click **Configure Devices** to push the configuration to the device.

Step 6 Click **Update**.

Step 7 Click **Configure Devices** to push the configuration to the device.

Assign a site ID to a device using a configuration group

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Configuration Groups**.

Step 2 Click **…** adjacent to the configuration group name and choose **Edit**.

Step 3 Click **Associated Devices**.

Step 4 Choose a device that is associated with the configuration group and click **Deploy**.

The **Deploy Configuration Group** workflow starts.

Step 5 Follow the instructions provided in the workflow.

Step 6 On the **Add and Review Device Configuration** page, enter the site ID of the device.

You can use any of the existing site IDs that are available in the network hierarchy or enter a new site ID. If you enter a new site ID without creating a node in the network hierarchy, the site is automatically created and listed on the **Configuration** > **Network Hierarchy** page.

Assign a region ID to a device

Before you begin

- Have access to the **Multi-Region Fabric** feature.
- Ensure that the region is available in the network hierarchy.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** > **WAN Edge List**.

Step 2 Check if the corresponding device is attached to a device template.

Step 3 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Feature Templates**.

Step 4 Click **…** adjacent to the System feature template and choose **Edit**.

Step 5 Click the **Basic Configuration** tab and set the scope of the **Region ID** field to **Global** and enter the region ID.

You can use any of the existing region IDs that are available in the network hierarchy. If the specified region ID is not available in the network hierarchy, the template push operation to the devices fails.

If you set the scope of the **Region ID** field to **Device Specific**, do the following:

a. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates** > **Device Templates**.

b. Click **…** adjacent to the device template and choose **Edit Device Template**.

c. In the **Region ID** field, enter the region ID.

d. Click **Update**.

e. Click **Configure Devices** to push the configuration to the device.

Step 6 Click **Update**.

Step 7 Click **Configure Devices** to push the configuration to the device.

Assign a system IP to a device

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the system IP of the device. If you want Cisco SD-WAN Manager to automatically generate a system IP for the device, do not make any change to the default value, **AUTO**.

Assign a hostname to a device

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library**.

Step 2 Start the **Quick Connect** workflow.

Step 3 Follow the instructions provided in the workflow.

Step 4 On the **Add and Review Device Configuration** page, enter the hostname of the device. If you want Cisco SD-WAN Manager to automatically generate a hostname for the device, do not make any change to the default value, **AUTO**.

Configure cflowd

Before you begin

You can configure the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the samples are sent to the collectors (on Cisco SD-WAN Controllers only). You can configure a maximum of four cflowd collectors per Cisco IOS XE Catalyst SD-WAN device. To have a cflowd configuration take effect, apply it with the appropriate data policy.

Ensure that you specify the granular role-based access control (RBAC) for Cflowd and policy groups. With specific permissions to the user group, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**. For more information about configuring RBAC for policy groups, see Configure RBAC for policy groups in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** next to existing roles or click **Add Role** to create a new role.
3. Choose the desired permission for the **Cflowd** feature under **Network Settings** and click **Update**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.

Step 2 Enable Cflowd and configure the values in the following table for the collector server:

Field	Description
Add Collector Server	
VPN ID	VPN ID of the server. Range: 0 through 65536
IPv4/IPv6 Address	IPv4 or IPv6 address of the collector server.
UDP Port	UDP port number of the collector server. Range: 1024 through 65535
Export Spreading	Toggle to enable or disable the export spreading configuration.
BFD Metrics Exporting	Toggle to enable or disable Bidirectional Forwarding Detection (BFD) metrics.
Exporting Interval	Interval in seconds for sending BFD metrics. **Exporting Interval** appears if you have enabled **BFD Metrics Exporting**. The default BFD export interval is 600 seconds.
Advanced Settings	

Field	Description
Active Flow Timeout (Seconds)	Active flow timeout value. Range: 30 through 3600 Default: 600 seconds.
Inactive Flow Timeout (Seconds)	Inactive flow timeout value. Range: 1 through 3600 Default: 60 seconds.
Flow Refresh Time (Seconds)	Flow refresh time in seconds. Range: 60 through 86400 seconds. Default: 600 seconds.
Sampling Rate	Sample duration in seconds. Range: 1 through 65536. Default: 1 second.
Collect TLOC Loopback	Enable to collect information about the TLOC loopback.
Protocol	Traffic protocol type to apply the collector to. The options are: **IPv4**, **IPv6**, or **both**. The default protocol is **IPv4**.
TOS	Type of field in the IPv4 header.
Re-marked DSCP	Traffic output of the router's data policy.

You can configure up to four collector servers.

Step 3 Click **Save**.

The Cflowd settings that you configure are applied to the application priority and SLA policy when the policy is deployed to Cisco IOS XE Catalyst SD-WAN devices. You can monitor application traffic flow over IPv4, IPv6, or both network addresses. For more information about configuring additional settings, see **Monitor traffic flow** in Application Priority and SLA.

Configure security logging

You can set up security logging for Cisco IOS XE Catalyst SD-WAN devices by configuring the location of the destination IP address of the log server. You can configure up to four destination servers along with the source interface to collect the syslogs for High Speed Logging (HSL). The IP address for the destination server can be IPv4, IPv6, or both. For more information about configuring HSL, see Configure Firewall High-Speed Logging Using the CLI Template. You can configure the external syslog server to export UTD logs. For more information about UTD logging, see Create Unified Security Policy Summary page.

Before you begin

Ensure that you specify the granular role-based access control (RBAC) for security logging. Ensure that you are able to access policy groups from **Configuration** > **Policy Groups** by configuring specific permissions to the user group. For more information about configuring RBAC for policy groups, see "Configure RBAC for policy groups" in Prerequisites for Policy Groups.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Users and Access** > **Roles**.
2. Click **Edit** adjacent to existing roles or click **Add Role** to create a new role.
3. Choose the permission you wish to configure for the **Security Logging** feature under **Network Settings** and click **Update**.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Network Hierarchy** > **Collectors**.

Step 2 Enable **Security Logging** and configure the values in the following table for the high-speed logging and external syslog servers:

Field	Description
High Speed Logging	Configure the following values for the high-speed logging server: • **VPN**: VPN name of the high-speed logging server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the log collector server. • **Port**: Port number on which the log collector server is listening for incoming packets.
External Syslog Server	Configure the following values for the external syslog server: • **VPN**: VPN name of the external syslog server. The VPNs available in the drop-down list are ones that are previously configured in the configuration groups in Cisco SD-WAN Manager. • **Server IP**: IPv4 or IPv6 address of the external syslog server.

You can configure up to four high-speed logging servers.

Note
Starting from Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, server labels (**Server 1**, **Server 2**, **Server 3**, and **Server 4**) are added to the high-speed logging server and the syslog server.

For device-specific server settings, add the associated source interface in the **Additional Settings** of the NGFW policy. For more information about configuring additional settings in the policy groups, see Configure NGFW Additional Settings section.

For Global server settings, define the global NHM values. For more information about defining global values on NHM, see Network Hierarchy and Resource Management.

Step 3 Click **Save**.

The security logging settings that you configure are applied along with the embedded security policy when the policy is deployed to Cisco IOS XE Catalyst SD-WAN devices. For more information about configuring the embedded security policy, see Configure Embedded Security.