Configuring Cflowd Traffic Flow Monitoring

This article provides general procedures for configuring cflowd traffic flow monitoring.

You configure cflowd traffic flow monitoring using the basic components of centralized data policy. You configure cflowd template options, including the location of the cflowd collector (if you are sending the flow to a collector), and you must configure cflowd as an action in the data policy.

General vManage Configuration Procedure for Cflowd Traffic Flow Monitoring

To configure policy for cflowd traffic flow monitoring, use the vManage policy configuration wizard. The wizard consists of four sequential screens that guide you through the process of creating and editing policy components:

1. Create Applications or Groups of Interest—Create lists that group together related items and that you call in the match or action components of a policy.
2. Configure Topology—Create the network structure to which the policy applies.
3. Configure Traffic Rules—Create the match and action conditions of a policy.
4. Apply Policies to Sites and VPNs—Associate policy with sites and VPNs in the overlay network.

In the first three policy configuration wizard screens, you are creating policy components or blocks. In the last screen, you are applying policy blocks to sites and VPNs in the overlay network.

For the cflowd policy to take effect, you must activate the policy.

Start the Policy Configuration Wizard

To start the policy configuration wizard:

1. In vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy.

The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

Create Applications or Groups of Interest

To create lists of applications or groups to use in cflowd policy:

1. Start the policy configuration wizard as explained above.
2. Create new lists, as described in the following table:
<table>
<thead>
<tr>
<th>List Type</th>
<th>Procedure</th>
</tr>
</thead>
</table>
| Prefix    | 1. In the left bar, click Prefix.  
            2. Click New Prefix List.  
            3. Enter a name for the list.  
            4. In the Add Prefix field, enter one or more data prefixes separated by commas.  
            5. Click Add. |
| Site      | 1. In the left bar, click Site.  
            2. Click New Site List.  
            3. Enter a name for the list.  
            4. In the Add Site field, enter one or more site IDs separated by commas.  
            5. Click Add. |
| VPN       | 1. In the left bar, click VPN.  
            2. Click New VPN List.  
            3. Enter a name for the list.  
            4. In the Add VPN field, enter one or more VPN IDs separated by commas.  
            5. Click Add. |

4. Click Next to move to Configure Topology in the wizard. When you first open this screen, the Topology tab is selected by default.

---

**Configure the Network Topology**

To configure the network topology or a VPN membership to use in centralized policy:

1. If you are already in the policy configuration wizard, skip to Step 4. Otherwise, in vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.
3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.
4. Create a network topology, as described in the following table:

<table>
<thead>
<tr>
<th>Policy Type</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub and Spoke</td>
<td>Policy for a topology with one or more central hub sites and with spokes connected to a hub</td>
<td>1. In the Add Topology drop-down, select Hub and Spoke.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Enter a name for the hub-and-spoke policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Enter a description for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. In the VPN List field, select the VPN list for the policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. In the left pane, click Add Hub and Spoke. A hub-and-spoke policy component containing the text string My Hub-and-Spoke is added in the left pane.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Double-click the My Hub-and-Spoke text string, and enter a name for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7. In the right pane, add hub sites to the network topology:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add Hub Sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the Site List Field, select a site list for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Repeat Steps 7a, 7b, and 7c to add more hub sites to the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. In the right pane, add spoke sites to the network topology:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. Click Add Spoke Sites.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. In the Site List Field, select a site list for the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Click Add.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Repeat Steps 8a, 8b, and 8c to add more spoke sites to the policy component.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Repeat Steps 5 through 8 to add more components to the hub-and-spoke policy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Click Save Hub and Spoke Policy.</td>
</tr>
<tr>
<td>Policy Type</td>
<td>Description</td>
<td>Procedure</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Mesh       | Partial-mesh or full-mesh region | 1. In the Add Topology drop-down, select Mesh.  
2. Enter a name for the mesh region policy component.  
3. Enter a description for the mesh region policy component.  
4. In the VPN List field, select the VPN list for the policy.  
5. Click New Mesh Region.  
6. In the Mesh Region Name field, enter a name for the individual mesh region.  
7. In the Site List field, select one or more sites to include in the mesh region.  
8. Repeat Steps 5 through 7 to add more mesh regions to the policy.  
9. Click Save Mesh Region. |

5. To use an existing topology:
   1. In the Add Topology drop-down, click Import Existing Topology. The Import Existing Topology popup displays.  
2. Select the type of topology.  
3. In the Policy drop-down, select the name of the topology.  
4. Click Import.

6. Click Next to move to Configure Traffic Rules in the wizard. When you first open this screen, the Application-Aware Routing tab is selected by default.

**Configure Traffic Rules**

To create the match and action rules to apply to traffic affected by the policy:

1. If you are already in the policy configuration wizard, skip this procedure. Otherwise, in vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed.

3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.

4. Click Next. The Configure Traffic Rules screen opens, and in the Application-Aware Routing bar, the Application-Aware Routing tab is selected by default.
To configure traffic rules for cflowd policy:

1. In the Application-Aware Routing bar, select the Cflowd tab.
2. Click the Add Policy drop-down.
4. Configure timer parameters for the cflowd template:
   1. In the Active Flow Timeout field, specify how long to collect a set of flows on which traffic is actively flowing, a value from 30 through 3,600 seconds. The default is 600 seconds (10 minutes).
   2. In the Inactive Flow Timeout field, specify how long to wait to send a set of sampled flows to a collector for a flow on which no traffic is flowing, a value from 1 through 3,600 seconds. The default is 60 seconds (1 minute).
   3. In the Flow Refresh Interval field, specify how often to send the cflowd template record fields to the collector, a value from 60 through 86,400 seconds (1 minute through 1 day). The default is 90 seconds.
   4. In the Sampling Interval field, specify how many packets to wait before creating a new flow, a value from 1 through 65,536 seconds. While you can configure any integer value, the software rounds the value down to the nearest power of 2.
5. Click Add New Collector, and configure the location of the cflowd collector. You can configure up to four collectors.
   1. In the VPN ID field, enter the number of the VPN in which the collector is located.
   2. In the IP Address field, enter the IP address of the collector.
   3. In the Port Number field, enter the collector port number. The default port is 4739.
   4. In the Transport Protocol drop-down, select the transport type to use to reach the collector, either TCP or UDP.
   5. In the Source Interface field, enter the name of the interface to use to send flows to the collector. It can be either a Gigabit Ethernet, a 10-Gigabit Ethernet interface (ge), or a loopback interface (loopbacknumber).
6. Click Save Cflowd Policy.

Click Next to move to Apply Policies to Sites and VPNs in the wizard.

---

**Apply Policies to Sites and VPNs**

In the last screen of the policy configuration wizard, you associate the policy blocks that you created on the previous three screens with VPNs and with sites in the overlay network.

To apply a policy block to sites and VPNs in the overlay network:

1. If you are already in the policy configuration wizard, skip to Step 6. Otherwise, in vManage NMS, select the Configure Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.
2. Click Add Policy. The policy configuration wizard opens, and the Create Applications or Groups of Interest screen is displayed
3. Click Next. The Network Topology screen opens, and in the Topology bar, the Topology tab is selected by default.

4. Click Next. The Configure Traffic Rules screen opens, and in the Application-Aware Routing bar, the Application-Aware Routing tab is selected by default.

5. Click Next. The Apply Policies to Sites and VPNs screen opens.

6. In the Policy Name field, enter a name for the policy. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.

7. In the Policy Description field, enter a description of the policy. It can contain up to 2048 characters. This field is mandatory, and it can contain any characters and spaces.

8. From the Topology bar, select the type of policy block. The table then lists policies that you have created for that type of policy block.

9. Click Add New Site List. Select one or more site lists, Click Add.

10. Click Preview to view the configured policy. The policy is displayed in CLI format.

11. Click Save Policy. The Configuration ► Policies screen opens, and the policies table includes the newly created policy.

**Activate a Centralized Policy**

Activating a cflowd policy sends that policy to all connected vSmart controllers. To activate a cflowd policy:

1. In vManage NMS, select the Configure ► Policies screen. When you first open this screen, the Centralized Policy tab is selected by default.

2. Select a policy.

3. Click the More Actions icon to the right of the row, and click Activate. The Activate Policy popup opens. It lists the IP addresses of the reachable vSmart controllers to which the policy is to be applied.

4. Click Activate.

**General Cflowd Routing Policy CLI Configuration Procedure**

Following are the high-level steps for configuring a cflowd centralized data policy to perform traffic monitoring and to export traffic flows to a collector:

1. Create a list of overlay network sites to which the cflowd centralized data policy is to be applied (in the apply-policy command):
   
   ```
   vSmart(config)# policy
   vSmart(config-policy)# lists site-list list-name
   vSmart(config-lists-list-name)#& site-id site-id
   ```

   The list can contain as many site IDs as necessary. Include one site-id command for each site ID. For contiguous site
IDs, you can specify a range of numbers separated with a dash (–). Create additional site lists, as needed.

2. Create a list of VPN for which the cflowd centralized data policy is to be configured (in the `policy data-policy` command):
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# vpn-list list-name
   vSmart(config-lists-list-name)# vpn vpn-id
   ```

3. Create lists of IP prefixes, as needed:
   ```
   vSmart(config)# policy lists
   vSmart(config-lists)# prefix-list list-name
   vSmart(config-lists-list-name)# ip-prefix prefix/length
   ```

4. Configure a cflowd template, and optionally, configure template parameters, including the location of the cflowd collector, the flow export timers, and the flow sampling interval:
   ```
   vSmart(config)# policy cflowd-template template-name
   vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address port port-number transport-type (transport_tcp | transport_udp) source-interface interface-name
   vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
   vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
   vSmart(config-cflowd-template-template-name)# flow-sampling-interval number
   vSmart(config-cflowd-template-template-name)# template-refresh seconds
   ```
   You must configure a cflowd template, but it need not contain any parameters. With no parameters, the data flow cache on vEdge nodes is managed using default settings, and no flow export occurs.
   You can configure one cflowd template per vEdge router, and it can export to a maximum of four collectors. By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields (the three timer values) are sent to the collector every 90 seconds. Also by default, a new flow is created immediately after an existing flow has ended.
   If you modify the configuration of the template record fields, the changes take effect only on flows that are created after the configuration change has been propagated to the vEdge router. Because an existing flow continues indefinitely, to have configuration changes take effect, clear the flow with the `clear app cflowd flows` command.

5. If you configure a logging action, configure how often to log packets to the syslog files:
   ```
   vEdge(config)# policy log-frequency number
   ```

6. Create a data policy instance and associate it with a list of VPNs:
   ```
   vSmart(config)# policy data-policy policy-name
   vSmart(config-data-policy-policy-name)# vpn-list list-name
   ```

7. Create a sequence to contain a single match–action pair:
   ```
   vSmart(config-vpn-list-list-name)# sequence number
   vSmart(config-sequence-number)#
   ```
   The match–action pairs are evaluated in order, by sequence number, starting with the lowest numbered pair and ending when the route matches the conditions in one of the pairs. If no match occurs, the default action is taken.

8. Define match parameters for the data packets:
9. In the action, enable cflowd:
   vSmart(config-sequence-number)# action cflowd

10. In the action, count or log data packets:
   vSmart(config-sequence-number)# action count counter-name
   vSmart(config-sequence-number)# action log

11. Create additional numbered sequences of match–action pairs within the data policy, as needed.

12. If a route does not match any of the conditions in one of the sequences, it is rejected by default. If you want
    nonmatching prefixes to be accepted, configure the default action for the policy:
   vSmart(config-policy-name)# default-action accept

13. Apply the policy and the cflowd template to one or more sites in the overlay network:
   vSmart(config)# apply-policy site-list list-name data-policy policy-name
   vSmart(config)# apply-policy site-list list-name cflowd-template template-name

---

**Structural Components of Policy Configuration for Cflowd**

Here are the structural components required to configure cflowd on a vSmart controller. Each component is explained in
more detail in the sections below.

```
policy
lists
  prefix-list list-name
  ip-prefix prefix
  site-list list-name
  site-id site-id
  vpn-list list-name
  vpn-id vpn-id
log-frequency number
  cflowd-template template-name
  collector vpn vpn-id address ip-address port port-number transport transport-type source-interface
interface-name
  flow-active-timeout seconds
  flow-inactive-timeout seconds
  flow-sampling-interval number
  template-refresh seconds
data-policy policy-name
  vpn-list list-name
  sequence number
  match
    match-parameters
  action
  cflowd
  count counter-name
  drop
  log
  default-action
    (accept | drop)
apply-policy site-list list-name
data-policy policy-name
cflowd-template template-name
```

---

**Lists**

Centralized data policy uses the following types of lists to group related items. You configure lists under the `policy lists` command hierarchy on vSmart controllers.
<table>
<thead>
<tr>
<th>List Type</th>
<th>Description</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>List of one or more IP prefixes. To configure multiple prefixes in a single list, include multiple <em>ip-prefix</em> options, specifying one prefix in each option.</td>
<td><code>data-prefix-list list-name ip-prefix prefix/length</code></td>
</tr>
<tr>
<td>Sites</td>
<td>List of one or more site identifiers in the overlay network. To configure multiple sites in a single list, include multiple <em>site-id</em> options, specifying one site number in each option. You can specify a single site identifier (such as <em>site-id 1</em>) or a range of site identifiers (such as <em>site-id 1-10</em>).</td>
<td><code>site-list list-name site-id site-id</code></td>
</tr>
<tr>
<td>VPNs</td>
<td>List of one or more VPNs in the overlay network. To configure multiple VPNs in a single list, include multiple <em>vpn</em> options, specifying one VPN number in each option. You can specify a single VPN identifier (such as <em>vpn-id 1</em>) or a range of VPN identifiers (such as <em>vpn-id 1-10</em>).</td>
<td><code>vpn-list list-name vpn vpn-id</code></td>
</tr>
</tbody>
</table>

**Logging Frequency**

If you configure a logging action, by default, the vEdge router logs all data packet headers to a syslog file. To log only a sample of the data packet headers:

```
vEdge(config)# policy log-frequency number
```

`number` specifies how often to log packet headers. For example, if you configure `log-frequency 20`, every sixteenth packet is logged. While you can configure any integer value for the frequency, the software rounds the value down to the nearest power of 2.

**Cflowd Templates**

For each cflowd data policy, you must create a template that defines the location of the flow collector:

```
vSmart(config)# policy cflowd-template template-name
```

The template can specify cflowd parameters or it can be empty. With no parameters, the data flow cache on vEdge nodes is managed using default settings, and no flow export occurs.

In the cflowd template, you can define the location of the flow collection:

```
vSmart(config-cflowd-template-template-name)# collector vpn vpn-id address ip-address port port-number transport transport-type source-interface interface-name
```

You can configure one cflowd template per vEdge router, and it can export to a maximum of four collectors.
You can configure flow export timers:

```
vSmart(config)# policy cflowd-template template-name
vSmart(config-cflowd-template-template-name)# flow-active-timeout seconds
vSmart(config-cflowd-template-template-name)# flow-inactive-timeout seconds
vSmart(config-cflowd-template-template-name)# flow-sampling-interval number
vSmart(config-cflowd-template-template-name)# template-refresh seconds
```

By default, an actively flowing data set is exported to the collector every 600 seconds (10 minutes), a data set for a flow on which no traffic is flowing is sent every 60 seconds (1 minute), and the cflowd template record fields are sent to the collector every 90 seconds. For flow sampling, by default, a new flow is started immediately after an existing flow ends.

For a single vEdge router, you can configure a maximum of four collectors.

### Data Policy Instance

For each centralized data policy, you create a named container for that policy with a `policy data-policy policy-name` command. For a single vEdge router, you can configure a maximum of four cflowd policies.

### VPN Lists

Each centralized data policy instance applies to the VPNs contained in a VPN list. Within the policy, you specify the VPN list with the `policy data-policy vpn-list list-name` command. The list name must be one that you created with a `policy lists vpn-list list-name` command.

### Sequences

Within each VPN list, a centralized data policy contains sequences of match–action pairs. The sequences are numbered to set the order in which data traffic is analyzed by the match–action pairs in the policy. You configure sequences with the `policy data-policy vpn-list sequence` command.

Each sequence in a centralized data policy can contain one `match` command and one `action` command.

### Match Parameters

Centralized data policy can match IP prefixes and fields in the IP headers. You configure the match parameters under the `policy data-policy vpn-list sequence match` command.

For data policy, you can match these parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group of destination prefixes</td>
<td><code>destination-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list.</td>
</tr>
<tr>
<td>Individual destination prefix</td>
<td><code>destination-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Destination <code>port number</code></td>
<td><code>destination-port number</code></td>
<td>0 through 65535</td>
</tr>
<tr>
<td>Description</td>
<td>Command</td>
<td>Value or Range</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>---------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>DSCP value</td>
<td><code>dscp number</code></td>
<td>0 through 63</td>
</tr>
<tr>
<td>Internet Protocol number</td>
<td><code>protocol number</code></td>
<td>0 through 255</td>
</tr>
<tr>
<td>Group of source prefixes</td>
<td><code>source-data-prefix-list list-name</code></td>
<td>Name of a <code>data-prefix-list</code> list</td>
</tr>
<tr>
<td>Individual source prefix</td>
<td><code>source-ip prefix/length</code></td>
<td>IP prefix and prefix length</td>
</tr>
<tr>
<td>Source <code>port number</code></td>
<td><code>source-port address</code></td>
<td>0 through 255</td>
</tr>
</tbody>
</table>

### Action Parameters

When data traffic matches the conditions in the match portion of a centralized data policy, the packet can be accepted or rejected, and you can configure a counter for the accepted or rejected packets. You configure the action parameters under the `policy data-policy vpn-list sequence action` command.

<table>
<thead>
<tr>
<th>Description</th>
<th>Command</th>
<th>Value or Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Count the accepted or dropped packets.</td>
<td><code>count counter-name</code></td>
<td>Name of a counter. To display counter information, use the <code>show policy access-lists counters</code> command on the vEdge router.</td>
</tr>
<tr>
<td>Enable cflowd.</td>
<td><code>cflowd</code></td>
<td>—</td>
</tr>
<tr>
<td>Log the packet headers into the messages and vsyslog system logging (syslog) files. In addition to logging the packet headers, a syslog message is generated the first time a packet header is logged and then every 5 minutes thereafter, as long as the flow is active.</td>
<td><code>log</code></td>
<td>To display logging information, use the <code>show app log flow-all</code>, <code>show app log flows</code>, and <code>show log</code> commands on the vEdge router.</td>
</tr>
</tbody>
</table>

For a packet that is accepted, configure the parameter `cflowd` to enable packet collection.

### Default Action

If a data packet being evaluated does not match any of the match conditions in a control policy, a default action is applied to this route. By default, the route is rejected. To modify this behavior, include the `policy data-policy vpn-list default-action accept` command.
Applying Cflowd Policy

For a centralized data policy to take effect, you must apply it to a list of sites in the overlay network:

```
  vSmart(config)# apply-policy site-list list-name data-policy policy-name
```

To activate the cflowd template, associate it with the data policy:

```
  vSmart(config)# apply-policy cflowd-template template-name
```

For all `data-policy` policies that you apply with `apply-policy` commands, the site IDs across all the site lists must be unique. That is, the site lists must not contain overlapping site IDs. An example of overlapping site IDs are those in the two site lists `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`. Here, sites 70 through 100 are in both lists. If you were to apply these two site lists to two different `data-policy` policies, the attempt to commit the configuration on the vSmart controller would fail.

The same type of restriction also applies to the following types of policies:

- Application-aware routing policy (`app-route-policy`)
- Centralized control policy (`control-policy`)
- Centralized data policy (`data-policy`)

You can, however, have overlapping site IDs for site lists that you apply for different types of policy. For example, the sites lists for `control-policy` and `data-policy` policies can have overlapping site IDs. So for the two example site lists above, `site-list 1 site-id 1-100` and `site-list 2 site-id 70-130`, you could apply one to a control policy and the other to a data policy.

As soon as you successfully activate the configuration by issuing a `commit` command, the vSmart controller pushes the data policy to the vEdge routers located in the specified sites. To view the policy as configured on the vSmart controller, use the `show running-config` command on the vSmart controller. To view the policy that has been pushed to the vEdge router, use the `show policy from-vsmart` command on the vEdge router.

To display the centralized data policy as configured on the vSmart controller, use the `show running-config` command:

```
  vSmart# show running-config policy
  vSmart# show running-config apply-policy
```

To display the centralized data policy that has been pushed to the vEdge router, issue the `show omp data-policy` command on the vEdge router:

```
  vEdge# show policy from-vsmart
```

Enable Cflowd Visibility on vEdge Routers

You can enable cflowd visibility directly on vEdge routers, without configuring data policy, so that you can perform traffic flow monitoring on traffic coming to the router from all VPNs in the LAN. To do this, configure cflowd visibility on the router:
To monitor the applications, use the `show app cflowd flows` and `show app cflowd statistics` commands on the vEdge router.

**Additional Information**

- Cflowd Traffic Flow Monitoring Configuration Example
- Traffic Flow Monitoring with Cflowd