# High Availability Overview

The goal of any high availability solution is to ensure that all network services are resilient to failure. Such a solution aims to provide continuous access to network resources by addressing the potential causes of downtime through functionality, design, and best practices. The core of the Cisco SD-WAN high availability solution is achieved through a combination of three factors:

- Functional hardware device redundancy. The basic strategy consists of installing and provisioning redundant hardware devices and redundant components on the hardware. These devices are connected by a secure control plane mesh of Datagram Transport Layer Security (DTLS) connections among themselves, which allows for rapid failover should a device fail or otherwise become unavailable. A key feature of the Cisco SD-WAN control plane is that it is established and maintained automatically, by the Cisco IOS XE SD-WAN devices and software themselves.
- Robust network design.
- Software mechanisms ensure rapid recovery from a failure. To provide a resilient control plane, the Cisco SD-WAN Overlay Management Protocol (OMP) regularly monitors the status of all Cisco IOS XE SD-WAN devices in the network and automatically adjusts to changes in the topology as devices join and leave the network. For data plane resiliency, the Cisco SD-WAN software implements standard protocol mechanisms, specifically Bidirectional Forwarding Detection (BFD), which runs on the secure IPsec tunnels between routers.

Recovery from a failure is a function of the time it takes to detect the failure and then repair or recover from it. TheCisco SD-WAN solution provides the ability to control the amount of time to detect a failure in the network. In most cases, repair of the failure is fairly instantaneous.

### Hardware Support of High Availability

A standard best practice in any network setup is to install redundant hardware at all levels, including duplicate parallel routers and other systems, redundant fans, power supplies and other hardware components within these devices, and backup network connections. Providing high availability in the Cisco SD-WAN solution is no different. A network design that is resilient in the face of hardware failure should include redundant vBond orchestrators, vSmart controllers, and routers and any available redundant hardware components.

Recovery from the total failure of a hardware component in the Cisco SD-WAN overlay network happens in basically the same way as in any other network. A backup component has been preconfigured, and it is able to perform all necessary functions by itself.

### Robust Network Design

In addition to simple duplication of hardware components, the high availability of a Cisco SD-WAN network can be enhanced by following best practices to design a network that is robust in the face of failure. In one such network design, redundant components are spread around the network as much as possible. Design practices include situating redundant vBond orchestrators and vSmart controllers at dispersed geographical locations and connecting them to different transport networks. Similarly, the routers at a local site can connect to different transport networks and can reach these networks through different NATs and DMZs.

### Software Support of High Availability

The Cisco SD-WAN software support for high availability and resiliency in the face of failure is provided both in the control plane, using the standard DTLS protocol and the proprietary Cisco SD-WAN Overlay Management Protocol (OMP), and in the data plane, using the industry-standard protocols BFD, BGP, OSPF, and VRRP.

### Control Plane Software Support of High Availability

The Cisco SD-WAN control plane operates in conjunction with redundant components to ensure that the overlay network remains resilient if one of the components fails. The control plane is built on top of DTLS connections between the Cisco devices, and it is monitored by the Cisco SD-WAN OMP protocol, which establishes peering sessions (similar to BGP peering sessions) between pairs of vSmart controllers and routers, and between pairs of vSmart controllers. These peering sessions allow OMP to monitor the status of the Cisco devices and to share the information among them so that each device in the network has a consistent view of the overlay network. The exchange of control plane information over OMP peering sessions is a key piece in the Cisco SD-WAN high availability solution:

- vSmart controllers quickly and automatically learn when a vBond orchestrator or a router joins or leaves the network. They can then rapidly make the necessary modifications in the route information that they send to the routers.
- vBond orchestrators quickly and automatically learn when a device joins the network and when a vSmart controller leaves the network. They can then rapidly make the necessary changes to the list of vSmart controller IP addresses that they send to routers joining the network.
- vBond orchestrators learn when a domain has multiple vSmart controllers and can then provide multiple vSmart controller addresses to routers joining the network.
- vSmart controllers learn about the presence of other vSmart controllers, and they all automatically synchronize their route tables. If one vSmart controller fails, the remaining systems take over management of the control plane, simply and automatically, and all routers in the network continue to receive current, consistent routing and TLOC updates from the remaining vSmart controllers.

Let's look at the redundancy provided by each of the Cisco SD-WAN hardware devices in support of network high availability.

### Recovering from a Failure in the Control Plane

The combination of hardware component redundancy with the architecture of the Cisco SD-WAN control plane results in a highly available network, one that continues to operate normally and without interruption when a failure occurs in one of the redundant control plane components. Recovery from the total failure of a vSmart controller, vBond orchestrator, or router in the Cisco SD-WAN overlay network happens in basically the same way as the recovery from the failure of a regular router or server on the network: A preconfigured backup component is able to perform all necessary functions by itself.

In the Cisco SD-WAN solution, when a network device fails and a redundant device is present, network operation continues without interruption. This is true for all Cisco devices—vBond orchestrators, vSmart controllers, and routers. No user configuration is required to implement this behavior; it happens automatically. The OMP peering sessions running between Cisco devices ensure that all the devices have a current and accurate view of the network topology.

Let's examine failure recovery device by device.

### Data Plane Software Support for High Availability

For data plane resiliency, the Cisco SD-WAN software implements the standard BFD protocol, which runs automatically on the secure IPsec connections between routers. These IPsec connections are used for the data plane, and for data traffic, and are independent of the DTLS tunnels used by the control plane. BFD is used to detect connection failures between the routers. It measures data loss and latency on the data tunnel to determine the status of the devices at either end of the connection.

BFD is enabled, by default, on connections between  Cisco IOS XE SD-WAN devices and Cisco vEdge devices. BFD sends Hello packets periodically (by default, every 1 second) to determine whether the session is still operational. If a certain number of the Hello packets are not received, BFD considers that the link has failed and brings the BFD session down (the default dead time is 3 seconds). When BFD sessions goes down, any route that points to a next hop over that IPsec tunnel is removed from the forwarding table (FIB), but it is still present in the route table (RIB).

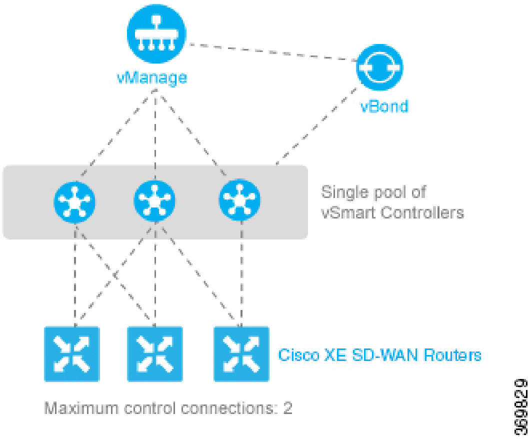
In the Cisco SD-WAN software, you can adjust the Hello packet and dead time intervals. If the timers on the two ends of a BFD link are different, BFD negotiates to use the lower value.

### Using Affinity To Manage Network Scaling

In the Cisco SD-WAN overlay network, all  Cisco IOS XE SD-WAN devices and Cisco vEdge devices establish control connections to all vSmart controllers, to ensure that the routers are always able to properly route data traffic across the network. As networks increase in size, with routers at thousands of sites and with vSmart controllers in multiple data centers managing the flow of control and data traffic among routers, network operation can be improved by limiting the number of vSmart controllers that a router can connect to. When data centers are distributed across a broad geography, network operation can also be better managed by having routers establish control connections only with the vSmart controllers collocated in the same geographic region.

Establishing affinity between vSmart controllers and  Cisco IOS XE SD-WAN devices allow you to control the scaling of the overlay network, by limiting the number of vSmart controllers that a Cisco IOS XE SD-WAN device can establish control connections (and form TLOCs) with. When you have redundant routers in a single data center, affinity allows you to distribute the vEdge control connections across the vSmart controllers. Similarly, when you have multiple data centers in the overlay network, affinity allows you to distribute the vEdge control connections across the data centers. With affinity, you can also define primary and backup control connections, to maintain overlay network operation in case the connection to a single vSmart controller or to a single data center fails.

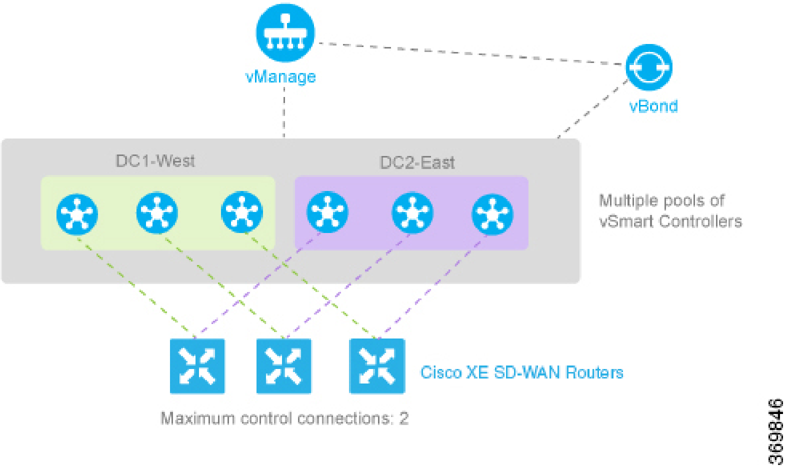
A simple case for using affinity is when redundant vSmart controllers are collocated in a single data center. Together, these vSmart controllers service all the  Cisco IOS XE SD-WAN devices in the overlay network. The figure below illustrates this situation, showing a scenario with three vSmart controllers in the data center and, for simplicity, showing just three of the many  Cisco IOS XE SD-WAN devices in the network.


vManage
vBond
Single pool of vSmart Controllers
Cisco XE SD-WAN Routers
Maximum control connections: 2
369829

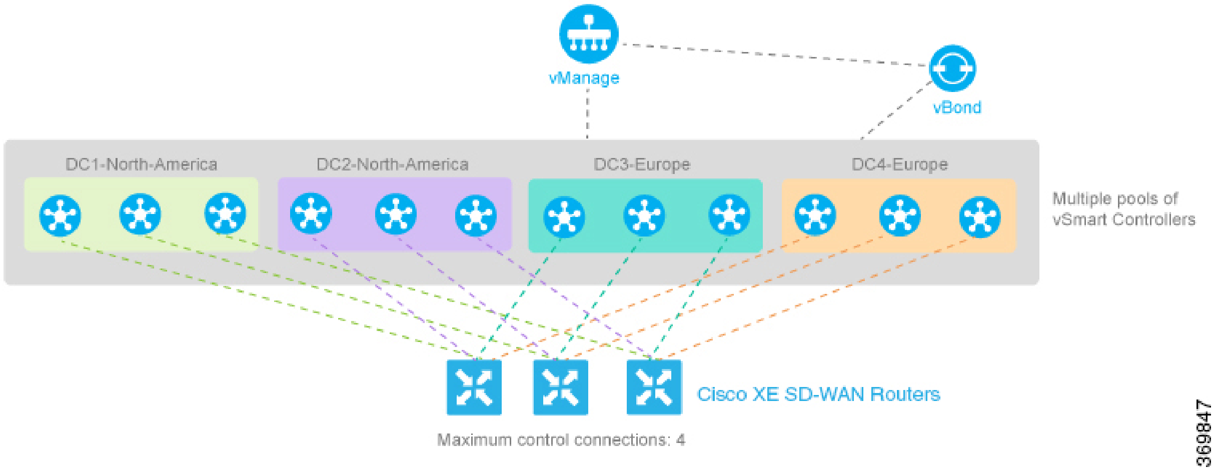
If you do not enable affinity, each Cisco IOS XE SD-WAN device establishes a control connection—that is, a TLOC—to each of the three vSmart controllers in the data center. Thus, a total of nine TLOCs are established, and each router exchanges OMP updates with each controller. Having this many TLOCs can strain the resources of both the vSmart controllers and the  Cisco IOS XE SD-WAN devices, and the strain increases in networks with larger numbers of  Cisco IOS XE SD-WAN devices.

Enabling affinity allows each Cisco IOS XE SD-WAN device to establish TLOC connections with only a subset of the vSmart controllers. The figure above shows each router connecting to just two of the three vSmart controllers, thus reducing the total number of TLOCs from nine to six. Both TLOC connections can be active, for a total of six control connections. It is also possible for one of the TLOC connections be the primary, or preferred, and the other to be a backup, to be used as an alternate only when the primary is unavailable, thus reducing the number of active TLOCs to three.

Affinity also enables redundancy among data centers, for a scenario in which multiple vSmart controllers are collocated in two or more data centers. Then, if the link between a Cisco IOS XE SD-WAN device and one of the data centers goes down, the vSmart controllers in the second data center are available to continue servicing the overlay network. The figure below illustrates this scenario, showing three vSmart controllers in each of two data centers. Each of the three  Cisco IOS XE SD-WAN devices establishes a TLOC connection to one controller in the West data center and one in the East data center.


vManage
vBond
DC1-West
DC2-East
Multiple pools of vSmart Controllers
Cisco XE SD-WAN Routers
Maximum control connections: 2
369846

You might think of the scenario in the figure above as one where there are redundant data centers in the same region of the world, such as in the same city, province, or country. For an overlay network that spans a larger geography, such as across a continent or across multiple continents, you can use affinity to limit the network scale either by restricting  Cisco IOS XE SD-WAN devices so that they connect only to local vSmart controllers or by having  Cisco IOS XE SD-WAN devices preferentially establish control connections with data centers that are in their geographic region. With geographic affinity,  Cisco IOS XE SD-WAN devices establish their only or their primary TLOC connection or connections with vSmart controllers in more local data centers, but they have a backup available to a more distant region to provide redundancy in case the closer data centers become unavailable. The figure below illustrates this scenario, Here, the  Cisco IOS XE SD-WAN devices in Europe have their primary TLOC connections to the two European data centers and alternate connections to the data centers in North America. Similarly, for the  Cisco IOS XE SD-WAN devices in North America, the primary connections are to the two North American data centers, and the backup connections are to the two European data centers.



As is the case with any overlay network that has multiple vSmart controllers, all policy configurations on all the vSmart controllers must be the same.

Before you cofigure High availability, to start with the configuration transaction, you can use the following command such as,

```
ntp server 198.51.241.229 source GigabitEthernet1 version 4
```

- vBond Orchestrator Redundancy, on page 5
- vManage NMS Redundancy, on page 7
- vSmart Controller Redundancy, on page 13
- Cisco IOS XE SD-WAN Device Redundancy, on page 15
- Configure Affinity between vSmart and Cisco IOS XE SD-WAN Devices, on page 16
- Configure Control Plane and Data Plane High Availability Parameters, on page 19
- Configure Disaster Recovery, on page 21
- High Availability CLI Reference, on page 28
- High Availability Configuration Examples, on page 29

# vBond Orchestrator Redundancy

The vBond orchestrator performs two key functions in the Cisco SD-WAN overlay network:

- Authenticates and validates all vSmart controllers and routers that attempt to join the Cisco SD-WAN network.
- Orchestrates the control plane connections between the vSmart controllers and routers, thus enabling vSmart controllers and routers to connect to each other in the Cisco SD-WAN network.

The vBond orchestrator runs as a VM on a network server.

Having multiple vBond orchestrators ensures that one of them is always available whenever a Cisco device such as a router or a vSmart controller is attempting to join the network.

### Configuration of Redundant vBond Orchestrators

A router learns that it is acting as a vBond orchestrator from its configuration. In the **system vbond** configuration command, which defines the IP address (or addresses) of the vBond orchestrator (or orchestrators) in the Cisco SD-WAN overlay network, you include the **local** option. In this command, you also include the local public IP address of the vBond orchestrator. (Even though on Cisco IOS XE SD-WAN device and vSmart controllers you can specify an IP address of vBond orchestrator as a DNS name, on the vBond orchestrator itself, you must specify it as an IP address.)

On vSmart controllers and Cisco IOS XE SD-WAN devices, when the network has only a single vBond orchestrator, you can configure the location of the vBond system either as an IP address or as the name of a DNS server (such as vbond.cisco.com). (Again, you configure this in the **system vbond** command.) When the network has two or more vBond orchestrators and they must all be reachable, you should use the name of a DNS server. The DNS server then resolves the name to a single IP address that the vBond orchestrator returns to the Cisco IOS XE SD-WAN device. If the DNS name resolves to multiple IP addresses, the vBond orchestrator returns them all to the Cisco IOS XE SD-WAN device, and the router tries each address sequentially until it forms a successful connection.

Note that even if your Cisco SD-WAN network has only a single vBond orchestrator, it is recommended as a best practice that you specify a DNS name rather than an IP address in the **system vbond** configuration command, because this results in a scalable configuration. Then, if you add additional vBond orchestrators to your network, you do not need to change the configurations on any of the routers or vSmart controllers in your network.

### Recovering from a vBond Orchestrator Failure

In a network with multiple vBond orchestrators, if one of them fails, the other vBond orchestrators simply continue operating and are able to handle all requests by Cisco devices to join the network. From a control plane point of view, each vBond orchestrator maintains a permanent DTLS connections to each of the vSmart controllers in the network. (Note however, that there are no connections between the vBond orchestrators themselves.) As long as one vBond orchestrator is present in the domain, the Cisco SD-WAN network is able to continue operating without interruption, because vSmart controllers and routers are still able to locate each other and join the network.

Because vBond orchestrators never participate in the data plane of the overlay network, the failure of any vBond orchestrator has no impact on data traffic. vBond orchestrators communicate with routers only when the routers are first joining the network. The joining router establishes a transient DTLS connection with a vBond orchestrator to learn the IP address of a vSmart controller. When the Cisco IOS XE SD-WAN device configuration lists the vBond address as a DNS name, the router tries each of the vBond orchestrators in the list, one by one, until it is able to establish a DTLS connection. This mechanism allows a router to always be able to join the network, even after one of a group of vBond orchestrators has failed.

# vManage NMS Redundancy

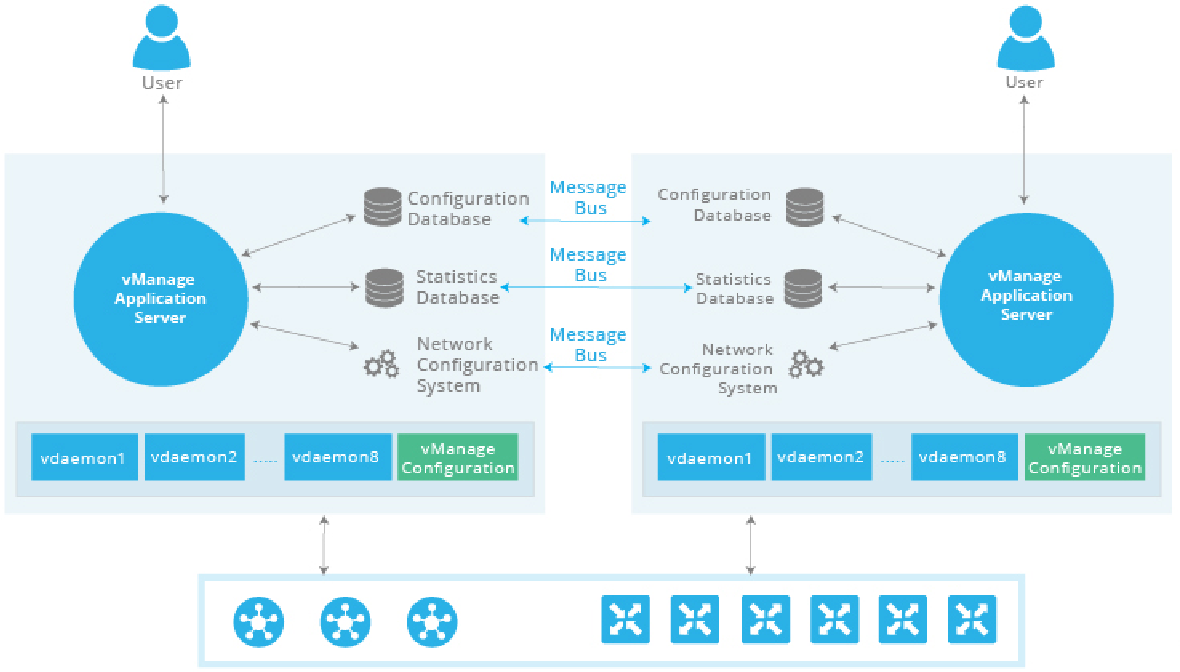
The vManage NMSs comprise a centralized network management system that enables configuration and management of the Cisco devices in the overlay network. It also provides a real-time dashboard into the status of the network and network devices. The vManage NMSs maintain permanent communication channels with all Cisco IOS XE SD-WAN devices in the network. Over these channels, the vManage NMSs push out files that list the serial numbers of all valid devices, they push out each device's configuration, and they push out new software images as part of a software upgrade process. From each network device, the vManage NMSs receive various status information that is displayed on the vManage Dashboard and other screens.

A highly available Cisco SD-WAN network contains three or more vManage NMSs in each domain. This scenario is referred to as a cluster of vManage NMSs, and each vManage NMS in a cluster is referred to as a vManage instance. Each vManage instance or device in a cluster can manage approximately 2000 devices, so a cluster of three vManage devices can manage up to 6000 devices. The vManage devices automatically load-balances the devices that they manage. With three devices, the vManage cluster remains operational if one of the devices in that cluster fail. A vManage cluster consists of the following architectural components:

- Application server—This provides a web server for user sessions. Through these sessions, a logged-in user can view a high-level dashboard summary of networks events and status, and can drill down to view details of these events. A user can also manage network serial number files, certificates, software upgrades, device reboots, and configuration of the vManage cluster itself from the vManage application server.
- Configuration database—Stores the inventory and state and the configurations for all Cisco IOS XE SD-WAN devices.
- Network configuration system—Stores all configuration information, policies, templates, certificates, and more.
- Statistics database—Stores the statistics information collected from all Cisco devices in the overlay network.
- Message bus—Communication bus among the different vManage instances. This bus is used to share data and coordinate operations among the vManage instances in the cluster.

The Statistics database and Configuration database services must run on an odd number of vManage instances, with a minimum of three. For these databases to be writeable, there must be a quorum of vManage instances running and they should be in sync. A quorum is a simple majority. For example, if you have a cluster of three vManage devices running these databases, then two must be running and in sync. Initially, all vManage devices run the same services. However, you can choose not to run some services on some devices. From the Cluster Management screen, you can select the services that can run on each vManage. You can add a fourth vManage device to load-balance more Cisco IOS XE SD-WAN devices. In such a case, disable the Statistics database and Configuration database on one of the vManage devices because those services need to run on an odd number of devices. Optionally, you can run the Configuration database on a single vManage device to reduce the amount of information shared between the devices and reduce load.

The following figure shows the interaction between vManage devices in a cluster, although a minimum of three devices are required. The figure illustrates the NMS services that synchronize between the vManage devices. Also in this figure, you see that each vManage instance resides on a virtual machine (VM). The VM can have from one to eight cores, with a Cisco SD-WAN software process (vdaemon) running on each core. In addition, the VM stores the actual configuration for the vManage NMS itself.



The vManage cluster implements an active-active architecture in the following way:

- Each vManage instance in the cluster is an independent processing node.
- All vManage instances are active simultaneously.
- All user sessions to the application server are load-balanced, using either an internal vManage load balancer or an external load balancer.
- All control sessions between the vManage application servers and the routers are load-balanced. A single vManage instance can manage a maximum of about 2000  Cisco IOS XE SD-WAN devices. However, all the controller sessions—the sessions between the vManage instances and the vSmart controllers, and the sessions between the vManage instances and the vBond orchestrators—are arranged in a full-mesh topology.
- The configuration and statistics databases can be replicated across vManage instances, and these databases can be accessed and used by all the vManage instances.
- If one of the vManage instances in the cluster fails or otherwise becomes unavailable, the network management services that are provided by the vManage NMS are still fully available across the network.

The message bus among the vManage instances in the cluster allows all the instances to communicate using an out-of-band network. This design, which leverages a third vNIC on the vManage VM, avoids using WAN bandwidth for management traffic.

You configure the vManage cluster from the vManage web application server. During the configuration process, you can configure each vManage instance that can run the following services:

- Application server—Each vManage server runs an application server instance.

- Configuration database—Within the vManage cluster, no more than three iterations of the configuration database can run.
- Load balancer—The vManage cluster requires a load balancer to distribute user login sessions among the vManage instances in the cluster. As mentioned above, a single vManage instance can manage a maximum of 2000 Cisco IOS XE SD-WAN devices. It is recommended that you use an external load balancer. However, if you choose to use a vManage instance for this purpose, all HTTP and HTTPS traffic directed to its IP address is redirected to other instances in the cluster.
- Messaging server—It is recommended that you configure each vManage instance to run the message bus so that all the instances in the cluster can communicate with each other.
- Statistics database—Within the vManage cluster, no more than three iterations of the statistics database can run.
- Coordination server: It is used internally by the Messaging server.

The following are the design considerations for a vManage cluster:

- A vManage cluster should consist of a minimum of three vManage instances.
- The application server and message bus should run on all vManage instances.
- Within a cluster, a maximum of three instances of the configuration database and three instances of the statistics database can run. Note, however, that any individual vManage instance can run both, one, or none of these two databases.
- To provide the greatest availability, it is recommended that you run the configuration and statistics databases on three vManage instances.

### Deploy vManage Cluster

Ensure that you have a minimum of three vManage devices in a vManage cluster.

**Note** This process requires multiple reboots and should be performed during a scheduled maintenance window.

1. Back up the vManage database. Use the following command to back up.

   **request nms configuration-db backup path /home/admin/<db _ backup _ filename>**

2. If the current vManage device has only two network interface cards (NICs), add a third NIC. Do not use Dynamic Host Configuration Protocol (DHCP) for addressing. This third NIC is used for cluster messaging between the vManage devices, within vpn 0. For the vManage device to detect the new interface, the device must be rebooted. Configure the interface and verify that it has connectivity.

3. In vManage GUI, click **Administration** > **Cluster Management**, edit the IP address to change localhost to the IP address of the third NIC, which is used for cluster messaging.

4. Restart the vManage NMS services. This may take some time. You can view the */var/log/nms/vmanage-server.log* for the log output to stabilize, and then use the **request nms all status** command to determine for how long the processes have been running. When it comes up, verify that vManage is operational and stable.

5. Provision the two additional vManage VMs in your virtual environment with the appropriate disk size and third NIC.

6. Configure the two additional vManage VMs with minimal system configuration and addressing for the NICs. Configure the admin user password to match that is configured on the original vManage device. If you are using enterprise certificates, ensure that you install the root certificate chain on the new vManage device as you did with the first vManage device. Also, ensure the clocks of the new vManage devices are in sync with the original vManage device.

   The following is a sample of a minimal configuration:

```
system
            host-name             vManage3
            system-ip             10.0.1.102
            site-id               1
            organization-name     cisco-sdwan1
            vbond vbond!
            vpn 0
                host vbond ip 198.51.100.103 192.51.100.104
                interface eth0
                ip address 198.51.100.102/24
                tunnel-interface
                no shutdown
                !
                interface eth1
                ip address 198.51.100.102/24
                no shutdown !
                ip route 10.0.0.1/0 10.0.1.254
                ip route 10.0.0.1/0 10.0.1.254
                !
                vpn 512
                interface eth2
                    ip address 198.56.101.102/24
                    no shutdown
                !
```

**Note** While a default gateway is given for the out of band vManage cluster interfaces, it is not required if the vManage cluster nodes are using addresses in the same subnet and are adjacent.

7. In vManage GUI, click **Administration** > **Cluster Management**, to add one of the new vManage VMs to the cluster by adding the IP address of the third NIC for database replication, click **Add vManage**. Select all services.

   vManage2 NMS processes restart. This process might take some time. View the */var/log/nms/vmanage-server.log* and then use the **request nms all status** command to determine process completion time.

8. View th new vManage device on the **Configuration** > **Certificates** > **Controllers** page.

9. Generate a certificate signing request (CSR), get the device signed, and install the signed device certificate for this new vManage device. See Cluster Management for more information.

   The cluster shows that the new vManage device is rebalancing and that NMS services are restarting on the previous vManage device. A new task appears in the task bar for the **Cluster Sync**. Although the task appears as Complete, view the */var/log/nms/vmanage-server.log* to resolve errors, if any.

vManage1 also restarts NMS services, which eventually resets the GUI session. It might take several minutes for the GUI to become available after the NMS services restarts. View the */var/log/nms/vmanage-server.log*, and then use the **request nms all status** command.

10. Wait for **Cluster Sync** to complete. View the *vmanage-server.log* to resolve errors, if any.
11. After the Cluster Sync is completed, add the second of the new vManage VMs to the cluster by adding the IP address of the third NIC for database replication. Select all services.

    vManage3 restarts NMS services. This might take some time. A new task appears in the task bar for the **Cluster Sync**. vManage1 and vManage2 also restarts NMS services, which eventually resets the GUI session. It may take several minutes for the GUI to become available after the NMS services restart. The new vManage device appears on the **Configuration** > **Certificates** > **Controllers** page. Perform steps 9 and 10 for this vManage device.

### Upgrade vManage Cluster

To upgrade a cluster, ensure that the services start in an orderly manner. After the upgrade steps, use the steps in the Restarting the NMS Processes section to start all the services in an orderly manner.

To get the software partitions prepared to be activated, upgrade the devices (without activating).

1. Collect an NMS backup. This can take a while. If Cisco hosts the controllers and there is a recent snapshot, this step can be skipped.

   ```
   request nms configuration-db backup path/home/admin/<db _ backup _ filename>
   ```

2. Stop NMS services on all vManage devices in the cluster by using the following command on each device.

   ```
   request nms all stop
   ```

3. Activate the new version on each device. This activation causes each device to reload.

   ```
   request software activate <version>
   ```

4. If you do the upgrade from CLI, ensure that you manually confirm the upgrade from the CLI after the reload and before it reverts to the previous version.

   ```
   request software upgrade-confirm
   ```

5. After the vManage devices reboot, stop NMS services on all vManage devices in the cluster.

   ```
   request nms all stop
   ```

Next, ensure that you perform the steps of restarting the NMS process manually.

### Restarting the NMS Processes Manually

When the cluster is in a bad state as part of the upgrade, you should manually restart the NMS processes. Restart the processes one at a time in an orderly manner instead of using **request nms all restart** or a similar command. The following manual restart order might vary for your cluster, depending on what services you are running on the vManage devices in the cluster. The following order is based on a basic cluster with three vManage devices.

**Note** Consider bringing up the services manually as mentioned in the following method whenever you have to reboot a vManage device or after an upgrade.

1. On each vManage device, stop all NMS services.

   ```
   request nms all stop
   ```

2. Verify that all services have stopped. It is normal for the above command to give some message about failing to stop a service if it takes too long, so use the following command to verify that everything is stopped before proceeding.

   ```
   request nms all status
   ```

3. Start the Statistics database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next vManage device.

   ```
   request nms statistics-db start
   ```

4. Verify that the service is started before proceeding to start it on the next vManage. After service starts, perform step 3 to start the Statistics database on the next vManage device. Once all the vManage devices have the Statistics database running, proceed to the next step.

   ```
   request nms statistics-db status
   ```

5. Start the Configuration database on each device that is configured to run it. Wait for the service to start each time before proceeding to the next vManage device.

   ```
   request nms configuration-db start
   ```

6. Verify that the service has started before proceeding to start it on the next vManage device. Go to vshell and tail a log file to look for a database is online message. When confirmed, go to step 5 to start the Configuration database on the next vManage device. After all vManage devices have the Configuration database running, proceed to the next step.

   ```
   tail -f -n 100 /var/log/nms/vmanage-orientdb-database.log
   ```

7. Start the Coordination server on each device. Wait for the service to start each time before proceeding to the next vManage device.

   ```
   request nms coordination-server start
   ```

8. Verify that the service is started before proceeding to start it on the next vManage device. After verifying, go to step 7 to start the Coordination server on the next vManage device. After the Coordination server runs on all the vManage devices, proceed to the next step.

   ```
   request nms coordination-server status
   ```

9. Start the Messaging server on each device. Wait for the service to start each time before proceeding to the next vManage device.

   ```
   request nms messaging-server start
   ```

10. Verify that the service has started before proceeding to start it on the next vManage device. After verifying, go to step 9 to start the Messaging server on the next vManage device. After the Messaging server runs on all vManage devices, proceed to the next step.

    ```
    request nms messaging-server status
    ```

11. Start the Application server on each device. Wait for the service to start each time before proceeding to the next vManage device.

    ```
    request nms application-server start
    ```

12. Verify that the service has started before proceeding to start it on the next vManage device. To verify if the service is fully started, open the GUI of that vManage device. After the GUI is fully loaded and you are able to log in, go to step 11 to start the Application server on the next vManage device.

13. Restart the NMS cloud services on each device. Wait for the service to start each time before proceeding to the next vManage device.

    ```
     request nms cloud-agent start
    ```

14. Verify that the service has started before proceeding to start it on the next vManage device. After verifying, go to step 12 to start the cloud services on the next vManage device. After the cloud services run on all vManage devices, proceed to the next step.

    ```
    request nms cloud-agent status
    ```

15. To verify that there are no errors and everything has loaded cleanly, tail the log files.

Check the vManage GUI to verify that all devices appear as online and reachable, and that the statistics exist.

### vManage Backups

Cisco manages vManage by taking regular snapshots of the vManage devices for the purpose of recovery due to a catastrophic failure or corruption. The frequency and retention of these snapshots are set for each overlay. Generally, the snapshots are taken daily and retained for up to 10 days. For certain scheduled maintenance activities, such as the upgrade of the vManage devices, another snapshot can be taken before the scheduled activity. In all other cases, it is your responsibility to take regular backups of the vManage configuration database and snapshots of the vManage virtual machine, and follow the example of frequency and retention that is followed by Cisco.

### vManage Database Backup

Although the vManage cluster provides high availability and a level of fault tolerance, regular backup of the configuration database should be taken and stored securely off-site. vManage does not have a mechanism of automating the collection of a configuration database backup on a schedule and copying it to another server. The greater the time between the backup and when it is needed for a recovery, the greater the risk that data might be lost. Perform configuration database backups often. Use the following command to create a configuration database backup file.

```
request nms configuration-db backup path <path>
```

# vSmart Controller Redundancy

### vSmart Controller Redundancy

The vSmart controllers are the central orchestrators of the control plane. They have permanent communication channels with all the Cisco devices in the network. Over the DTLS connections between the vSmart controllers and vBond orchestrators and between pairs of vSmart controllers, the devices regularly exchange their views of the network, to ensure that their route tables remain synchronized. The vSmart controllers pass accurate and timely route information over DTLS connections to Cisco IOS XE SD-WAN device.

A highly available Cisco SD-WAN network contains two or more vSmart controllers in each domain. A Cisco SD-WAN domain can have up to 20 vSmart controllers, and each router, by default, connects to two of them. When the number of vSmart controllers in a domain is greater than the maximum number of controllers that a domain's routers are allowed to connect to, the Cisco SD-WAN software load-balances the connections among the available vSmart controllers.

While the configurations on all the vSmart controllers must be functionally similar, the control policies must be identical. This is required to ensure that, at any time, all  Cisco IOS XE SD-WAN devices receive consistent views of the network. If the control policies are not absolutely identical, different vSmart controllers might give different information to a Cisco IOS XE SD-WAN device, and the likely result will be network connectivity issues.

**Note** To reiterate, the Cisco SD-WAN overlay network works properly only when the control policies on all vSmart controllers are identical. Even the slightest difference in the policies will result in issues with the functioning of the network.

To remain synchronized with each other, the vSmart controllers establish a full mesh of DTLS control connections, as well as a full mesh of OMP sessions, between themselves. Over the OMP sessions, the vSmart controllers advertise routes, TLOCs, services, policies, and encryption keys. It is this exchange of information that allows the vSmart controllers to remain synchronized.

You can place vSmart controllers anywhere in the network. For availability, it is highly recommended that the vSmart controllers be geographically dispersed.

Each vSmart controller establishes a permanent DTLS connection to each of the vBond orchestrators. These connections allow the vBond orchestrators to track which vSmart controllers are present and operational. So, if one of the vSmart controller fails, the vBond orchestrator does not provide the address of the unavailable vSmart controller to a router that is just joining the network.

To reiterate, the Cisco SD-WAN overlay network works properly only when the control policies on all vSmart controllers are identical. Even the slightest difference in the policies result in issues with the functioning of the network.

### Recovering from a vSmart Controller Failure

The vSmart controllers are the primary controllers of the network. To maintain this control, they maintain permanent DTLS connections to all the vBond orchestrators and Cisco IOS XE SD-WAN devices and Cisco vEdge devices. These connections allow the vSmart controllers to be constantly aware of any changes in the network topology. When a network has multiple vSmart controllers:

- There is a full mesh of OMP sessions among the vSmart controllers.
- Each vSmart controller has a permanent DTLS connection to each vBond orchestrator.
- The vSmart controllers have permanent DTLS connections to the Cisco IOS XE SD-WAN devices and Cisco vEdge devices. More specifically, each router has a DTLS connection to one of the vSmart controllers.

If one of the vSmart controllers fails, the other vSmart controllers seamlessly take over handling control of the network. The remaining vSmart controllers are able to work with Cisco IOS XE SD-WAN devices and Cisco vEdge devices joining the network and are able to continue sending route updates to the routers. As long as one vSmart controller is present and operating in the domain, the Cisco SD-WAN network can continue operating without interruption.

To configure graceful restart for OMP on Cisco IOS XE SD-WAN device by setting the timer for six hours, see the following:

```
ISR4331(config)# sdwan omp graceful-restart timers graceful-restart-timer 21600
ISR4331(config-timers)# commit
Commit complete.
ISR4331(config-timers)# end
```

```
ISR4331#show sdwan running-config | section sdwan
tunnel mode sdwan
sdwan
interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  exit
exit
omp
  no shutdown
  graceful-restart
  timers
   graceful-restart-timer 21600
  exit
  address-family ipv4
   advertise connected
   advertise static
  !
!
```

# Cisco IOS XE SD-WAN Device Redundancy

### Cisco IOS XE SD-WAN Device Redundancy

The Cisco IOS XE SD-WAN devices are commonly used in two ways in the Cisco SD-WAN network: to be the Cisco SD-WAN routers at a branch site, and to create a hub site that branch routers connect to.

A branch site can have two Cisco IOS XE SD-WAN devices in a branch site for redundancy. Each of the router maintains:

- A secure control plane connection, via a DTLS connection, with each vSmart controller in its domain
- A secure data plane connection with the other routers at the site

Because both the routers receive the same routing information from the vSmart controllers, each one is able to continue to route traffic if one fails, even if they are connected to different transport providers.

When using  Cisco IOS XE SD-WAN devices and Cisco vEdge devices in a hub site, you can provide redundancy by installing two Cisco IOS XE SD-WAN devices. The branch routers need to connect to each of the hub routers by using separate DTLS connections.

You can also have Cisco IOS XE SD-WAN device provide redundancy by configuring up to tunnel interfaces on a single router. Each tunnel interface can go through the same or different firewalls, service providers, and network clouds, and each maintains a secure control plane connection, by means of a DTLS tunnel, with the vSmart controllers in its domain.

### Recovering from a Cisco IOS XE SD-WAN Device Failure

The route tables on  Cisco IOS XE SD-WAN devices and Cisco vEdge devices are populated by OMP routes received from the vSmart controllers. For a site or branch with redundant routers, the route tables on both routers remain synchronized, so if either of the routers fail, the other one continues to be able to route data traffic to its destination.

# Configure Affinity between vSmart and Cisco IOS XE SD-WAN Devices

One way to manage network scale is to configure affinity between vSmart controllers and Cisco IOS XE SD-WAN devices. To do this, you place each vSmart controller into a controller group, and then you configure which group or groups a Cisco IOS XE SD-WAN device can establish control connections with. The controller groups are what establishes the affinity between vSmart controllers and Cisco IOS XE SD-WAN devices.

### Configure the Controller Group Identifier on vSmart Controllers

To participate in affinity, each vSmart controller must be assigned a controller group identifier:

```
vSmart(config)#system controller-group-id number
```

The identifier number can be from 0 through 100.

When vSmart controllers are in different data centers, it is recommended that you assign different controller group identifiers to the vSmart controllers. Doing this provides redundancy among data centers, in case a data center becomes unreachable.

For vSmart controllers in the same a data center, they can have the same controller group identifier or different identifiers:

- If the vSmart controllers have the same controller group identifier, a Cisco IOS XE SD-WAN device establishes a control connection to any one of them. If that vSmart controller becomes unreachable, the router simply establishes a control connection with another one of the controllers in the data center. As an example of how this might work, if one vSmart controller becomes unavailable during a software upgrade, the Cisco IOS XE SD-WAN device immediately establishes a new TLOC with another vSmart controller, and the router's network operation is not interrupted. This network design provides redundancy among vSmart controllers in a data center.
- If the vSmart controllers have different controller group identifiers, a Cisco IOS XE SD-WAN device can use one controller as the preferred and the other as backup. As an example of how this might work, if you are upgrading the vSmart controller software, you can upgrade one controller group at a time. If a problem occurs with the upgrade, a Cisco IOS XE SD-WAN device establishes TLOCs with the vSmart controllers in the second, backup controller group, and the router's network operation is not interrupted. When the vSmart controller in the first group again becomes available, the Cisco IOS XE SD-WAN device switches its TLOCs back to that controller. This network design, while offerring redundancy among the vSmart controllers in a data center, also provides additional fault isolation.

### Configure Affinity on Cisco IOS XE SD-WAN Devices

For a Cisco IOS XE SD-WAN device to participate in affinity, you configure the vSmart controllers that the router is allowed to establish control connections with, and you configure the maximum number of control connections (or TLOCs) that the Cisco IOS XE SD-WAN device itself, and that an individual tunnel on the router, is allowed to establish.

### Configure a Controller Group List

Configuring the vSmart controllers that the router is allowed to establish control connections is a two-part process:

- At the system level, configure a single list of all the controller group identifiers that are present in the overlay network.
- For each tunnel interface in VPN 0 (sdwan), you can choose to restrict which controller group identifiers the tunnel interface can establish control connections with. To do this, configure an exclusion list.

At a system level, configure the identifiers of the vSmart controller groups:

```
ISR4331(config)#system controller-group-list numbers
```

List the vSmart controller group identifiers that any of the tunnel connections on the Cisco IOS XE SD-WAN device might want to establish control connections with. It is recommended that this list contain the identifiers for all the vSmart controller groups in the overlay network.

If, for a specific tunnel interface in VPN 0 (sdwan), you want it to establish control connections to only a subset of all the vSmart controller groups, configure the group identifiers to exclude:

```
ISR4331(config-interface-GigabitEthernets0/0/1)#tunnel-interface exclude-controller-group-list
 numbers
```

Or

```
ISR4331(config-sdwan)# interface GigabitEthernets0/0/1 tunnel-interface
exclude-controller-group-list numbers
```

In this command, list the identifiers of the vSmart controller groups that this particular tunnel interface should never establish control connections with. The controller groups in this list must be a subset of the controller groups configured with the **system controller-group-list** command.

To display the controller groups configured on a Cisco IOS XE SD-WAN device, use the **show sdwan control connections** command.

### Configure the Maximum Number of Control Connections

Configuring the maximum number of control connections for the Cisco IOS XE SD-WAN device is a two-part process:

- At the system level, configure the maximum number of control connections that the Cisco IOS XE SD-WAN device can establish to vSmart controllers.
- For each tunnel interface in VPN 0 (sdwan), configure the maximum number of control connections that the tunnel can establish to vSmart controllers.

By default, a Cisco IOS XE SD-WAN device can establish two OMP sessions for control connections to vSmart controllers. To modify the maximum number of OMP sessions:

```
ISR4331(config)#system max-omp-sessions number
```

The number of OMP sessions can be from 0 through 100.

A Cisco IOS XE SD-WAN device establishes OMP sessions as follows:

- Each DTLS and and each TLS control plane tunnel creates a separate OMP session.

- It is the Cisco IOS XE SD-WAN device as a whole, not the individual tunnel interfaces in VPN 0 (sdwan), that establishes OMP sessions with vSmart controllers. When different tunnel interfaces on the router have affinity with the same vSmart controller group, the Cisco IOS XE SD-WAN device creates a single OMP session to one of the vSmart controllers in that group, and the different tunnel interfaces use this single OMP session.

By default, each tunnel interface in VPN 0 (sdwan) can establish two control connections. To change this:

```
ISR4331(config)#sdwan interface interface-name tunnel-interface max-control-connections
number
```

The number of control connections can be from 0 through 100. The default value is the maximum number of OMP sessions configured with the **system max-omp-sessions** command.

When a Cisco IOS XE SD-WAN devices has multiple WAN transport connections, and hence has multiple tunnel interfaces in VPN 0 (sdwan), the sum of the maximum number of control connections that all the tunnels can establish cannot exceed the maximum number allowed on the router itself.

To display the maximum number of control connections configured on an interface, use the **show sdwan control local-properties** command.

To display the actual number of control connections for each tunnel interface, use the **show sdwan control affinity config** command.

To display a list of the vSmart controllers that each tunnel interface has established control connections with, use the **show sdwan control affinity status** command.

### Best Practices for Configuring Affinity

- In the **system controller-group-list** command on the Cisco IOS XE SD-WAN device, list all the controller groups available in the overlay network. Doing so ensures that all the vSmart controllers in the overlay network are available for the affinity configuration, and it provides additional redundancy in case connectivity to the preferred group or groups is lost. You manipulate the number of control connections and their priority based on the maximum number of OMP sessions for the router, the maximum number of control connections for the tunnel, the controller groups a tunnel should not use. A case in which listing all the controller groups in the **system controller-group-list** command provides additional redundancy is when the Cisco IOS XE SD-WAN device site is having connectivity issues in reaching the vSmart controllers in the controller group list. To illustrate this, suppose, in a network with three controller groups (1, 2, and 3), the controller group list on a Cisco IOS XE SD-WAN device contains only groups 1 and 2, because these are the preferred groups. If the router learns from the vBond controller that the vSmart controllers in groups 1 and 2 are up, but the router is having connectivity issues to both sites, the router loses its connectivity to the overlay network. However, if the controller group list contains all three controller groups, even though group 3 is not a preferred group, if the router is unable to connect to the vSmart controllers in group 1 or group 2, it is able to fall back and connect to the controllers in group 3. Configuring affinity and the order in which to connect to vSmart controllers is only a preference. The preference is honored whenever possible. However, the overarching rule in enforcing high availability on the overlay network is to use any operational vSmart controller. The network ceases to function only when no vSmart controllers are operational. So it might happen that the least preferred vSmart controller is used if it is the only controller operational in the network at a particular time. When a Cisco IOS XE SD-WAN device boots, it learns about all the vSmart controllers in the overlay network, and the vBond orchestrator is continuously communicating to the router which vSmart controllers are up. So, if a Cisco IOS XE SD-WAN device cannot reach any of the preferred vSmart controllers in the configured controller group and another vSmart controller is up, the router connects to that controller. Put another way, in a network with multiple vSmart controllers, as a last resort, a Cisco IOS XE SD-WAN device connects to any of the controllers, to ensure that the overlay network remains operational, whether or not these controllers are configured in the router's controller group list.

- The controller groups listed in the **exclude-controller-group-list** command must be a subset of the controller groups configured for the entire router, in the **system controller-group-list** command.
- When a data center has multiple vSmart controllers that use the same controller group identifier, and when the overlay network has two or more data centers, it is recommended that the number of vSmart controllers in each of the controller groups be the same. For example, if Data Center 1 has three vSmart controllers, all with the same group identifier (let's say, 1), Data Center 2 should also have three vSmart controllers, all with the same group identifier (let's say, 2), and any additional data centers should also have three vSmart controllers.
- When a data center has vSmart controllers in the same controller group, the hardware capabilities—specifically, the memory and CPU—on all the vSmart controllers should be identical. More broadly, all the vSmart controllers in the overlay network, whether in one data center or in many, should have the same hardware capabilities. Each vSmart controller should have equal capacity and capability to handle a control connection from any of the Cisco IOS XE SD-WAN devices in the network.
- When a router has two tunnel connections and the network has two (or more) data centers, it is recommended that you configure one of the tunnel interfaces to go to one of the data centers and the other to go to the second. This configuration provides vSmart redundancy with the minimum number of OMP sessions.
- Whenever possible in your network design, you should leverage affinity configurations to create fault-isolation domains.

# Configure Control Plane and Data Plane High Availability Parameters

This topic discusses the configurable high availability parameters for the control plane and the data plane.

### Control Plane High Availability

A highly available Cisco SD-WAN network contains two or more vSmart controllers in each domain. A Cisco SD-WAN domain can have up to 20 vSmart controllers, and each Cisco IOS XE SD-WAN device, by default, connects to two of them. You change this value on a per-tunnel basis:

```
ISR4331(config)# sdwan interface interface-name  tunnel-interface max-control-connections
  number
```

When the number of vSmart controllers in a domain is greater than the maximum number of controllers that a domain's Cisco IOS XE SD-WAN devices are allowed to connect to, the SD-WAN software load-balances the connections among the available vSmart controllers.

**Note** To maximize the efficiency of the load-balancing among vSmart controllers, use sequential numbers when assigning system IP addresses to the Cisco IOS XE SD-WAN devices in the domain. One example of a sequential numbering schemes is 172.1.1.1, 172.1.1.2, 172.1.1.3, and so forth. Another is 172.1.1.1, 172.1.2.1, 172.1.3.1, and so forth.

### Data Plane High Availability

BFD, which detects link failures as part of the Cisco SD-WAN high availability solution, is enabled by default on all Cisco devices. BFD runs automatically on all IPsec data tunnels between Cisco IOS XE SD-WAN devices. It does not run on the control plane (DTLS or TLS) tunnels that vSmart controllers establish with all Cisco devices in the network.

You can modify the BFD Hello packet interval and the number of missed Hello packets (the BFD interval multiplier) before BFD declares that a link has failed.

#### Change the BFD Hello Packet Interval

BFD sends Hello packets periodically to detect faults on the IPsec data tunnel between two Cisco IOS XE SD-WAN devices. By default, BFD sends these packets every 1000 milliseconds (that is, once per second). To change this interval on one or more traffic flow, use the **hello-interval** command:

```
ISR4331(config)#bfd color color hello-interval milliseconds
```

The interval can be a value from 100 to 300000 milliseconds (5 minutes).

Configure the interval for each tunnel connection, which is identified by a color. The color can be **3g**, **biz-internet**, **blue**, **bronze**, **custom1**, **custom2**, **custom3**, **default**, **gold**, **green**, **lte**, **metro-ethernet**, **mpls**, **private1**, **private2**, **public-internet**, **red**, or **silver**.

#### Change the BFD Packet Interval Multiplier

After BFD has not received a certain number of Hello packets on a link, it declares that the link has failed. This number of packets is a multiplier of the Hello packet interval time. By default, the multiplier is 7 for hardware routers and 20 for Cloud software routers. This means that if BFD has not received a Hello packet after 7 seconds, it considers that the link has failed and implements its redundancy plan.

To change the BFD packet interval multiplier, use the **multiplier** command:

```
ISR4331(config)#bfd color color multiplier integer
```

Multiplier range: 1 to 60 (integer)

You configure the multiplier for each tunnel connection, which is represented by a color.

#### Control PMTU Discovery

On each transport connection (that is, for each TLOC, or color), the Cisco SD-WAN BFD software performs path MTU (PMTU) discovery, which automatically negotiates the MTU size in an effort to minimize or eliminate packet fragmentation on the connection. BFD PMTU discovery is enabled by default, and it is recommended that you use BFD PMTU discovery and not disable it. To explicitly enable it:

```
ISR4331(config)#bfd color color pmtu-discovery
```

With PMTU discovery enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. With PMTU discovery enabled, 16 bytes might be required by PMTU discovery, so the effective tunnel MTU might be as low as 1452 bytes. From an encapsulation point of view, the default IP MTU for GRE is 1468 bytes, and for IPsec it is 1442 bytes because of the larger overhead. Enabling PMTU discovery adds to the overhead of the BFD packets that are sent between the Cisco IOS XE SD-WAN devices, but does not add any overhead to normal data traffic.

If PMTU discovery is disabled, the expected tunnel MTU is 1472 bytes (tunnel MTU of 1500 bytes less 4 bytes for the GRE header, 20 bytes for the outer IP header, and 4 bytes for the MPLS header). However, the effective tunnel MTU might be 1468 bytes, because the software might sometimes erroneously add 4 bytes to the header.

# Configure Disaster Recovery

*Table 1: Feature History*

| Feature Name | Release Information | Feature Description |
|---|---|---|
| Disaster Recovery for Cisco vManage | Cisco IOS XE SD-WAN Release 16.12.1b<br>Cisco vManage Release 19.2.1 | This feature helps you configure Cisco vManage in an active or standby mode to counteract hardware or software failures that may occur due to unforeseen circumstances. |

You want to deploy the Cisco SD-WAN controllers across two data centers, and if a data center goes down due to a disaster, you want the network to be available. Out of the three controllers that make up theCisco SD-WAN solution, vManage is the only one that is stateful and cannot be deployed in an active/active mode. The goal of the disaster recovery solution is to deploy vManage across two data centers in some sort of primary/secondary mode.

The disaster recovery option provides automatic failover of the primary cluster to the secondary cluster. Data is replicated from the primary cluster to the secondary cluster.

There are two available disaster recovery options:

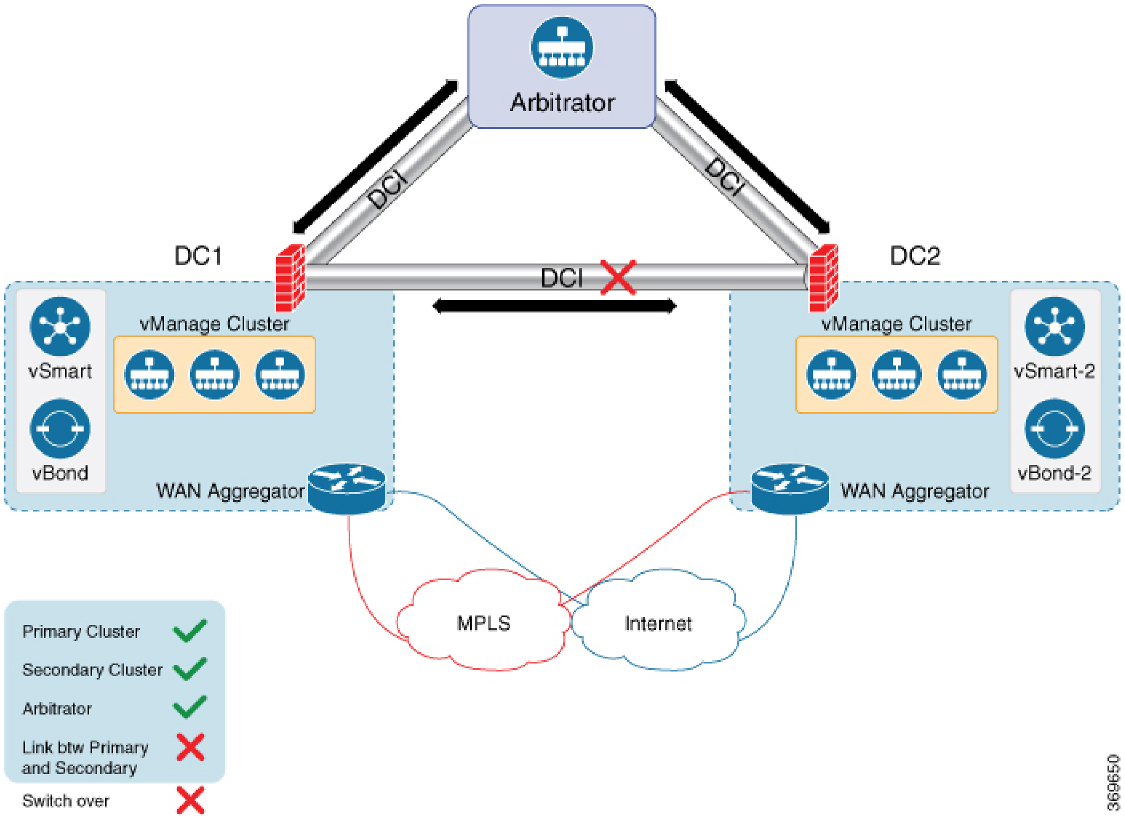
- Manual—If you want to make the clusters active, you can do it manually rather than having the arbitrator do the switchover. You can specify the switchover threshold.
- Automated —Arbitrator does the monitoring of the cluster and performs the necessary action.

  A highly available Cisco SD-WAN network contains three or more vManage NMSs in each domain. This scenario is referred to as a cluster of vManage NMSs, and each vManage NMS in a cluster is referred to as a vManage instance.

### Architecture Overview

The following diagram describes the high-level architecture of the disaster recovery solution.

The arbitrator is an additional vManage cluster that runs in arbitrator mode. The arbitrator monitors the health of the primary and the secondary clusters and performs the necessary actions.



## Prerequisites

Prior to configuring disaster recovery, make sure you have met the following requirements:

- You must have two vManage clusters with three nodes in each cluster. If automated recovery option is selected, then another vManage node is required.
- You must be able to reach the primary and the secondary cluster using HTTPS on a transport VPN (VPN 0).
- Make sure that vSmart and vBond devices on the secondary cluster are connected to the primary cluster.

## Best Practices and Recommendations

- Ensure that you use a netadmin user privilege for Disaster Recovery registration. We recommend that you modify the factory-default password, admin before you start the registration process.
- To change user credentials, we recommend that you use the Cisco vManage GUI, and not use the CLI of a Cisco SD-WAN device.
- If Cisco SD-WAN devices are configured using feature templates, ensure that you create separate feature templates for both primary data center and secondary data center.
- When primary cluster is switched over to the secondary cluster, Cisco vManage detaches the Cisco SD-WAN devices from the feature templates. Therefore, ensure that you reattach the devices to the specific feature templates.

- For an on-premises deployment, ensure that you regularly take backup of the Configuration database from the active Cisco vManage instance.

### Changing the Cisco vManage or Cisco vBond Orchestrator Administrator Password

If you need to change the administrator password for Cisco vManage or Cisco vBond Orchestrator, first change the password, then deregister disaster recovery from the Cisco vManage cluster, and then re-register disaster recovery on the cluster.

### Enable Disaster Recovery on Day-0:

You need to bring up two separate clusters with no devices being shared, which means do not share any vSmart, vBond, or vManage devices.

On both clusters, configure the following:

| Item | Action |
|---|---|
| Secondary cluster | Bring up the secondary vManage cluster with three vManage clusters. |
| Arbitrator | To assign an IP address for the OOB network, navigate to **Administration > Cluster Management**. |
| | Ensure reachability between the primary, secondary clusters, and arbitrator on VPN (0) using HTTPS. |
| | Ensure reachability between the primary cluster, secondary cluster, and vBond orchestrators. |

### Verify after Registering for Disaster Recovery on Day-1

- Replication from the primary cluster to the secondary cluster happens at the configured intervals.
- Status check: **Administration > Disaster Recovery**.
- Arbitrator:
  - First health check after 15 minutes. This check provides enough time for all the nodes to be up and running with the configured disaster recovery processes.
  - Health check of the primary cluster, secondary cluster, and the arbitrator every five minutes.
  - Check the */var/log/nms/vmanage-server.log* for the status information on the arbitrator cluster.

### Configure Disaster Recovery

1. From the Cisco vManage dashboard, select **Administration > Disaster Recovery**.
2. On the **Administration > Disaster Recovery** page, select **Manage Disaster Recovery**.
3. To configure primary and secondary cluster, on the vManage Disaster Recovery screen, select an IP address for any vManage node within the respective cluster.

   If a cluster is behind a load balancer, specify the IP address of the load balancer.

4. Specify the following: **Start Time**, **Replication Interval**, and **Delay Threshold** for replicating data from the primary to the secondary cluster.

   The default value for **Delay Threshold** is 30 minutes.

   The default value for **Replication Interval** is 15 minutes.

5. Click **Administration** > **Disaster Recovery**, and for Cluster 2 (Secondary), click **Make Primary**.

   It can take 10 to 15 minutes to push all changes from all the devices.

6. You can also decide to pause disaster recovery, pause replication, or delete your disaster recovery configuration.

   After disaster recovery is configured and you have replicated data, you can view the following:

   - when your data was last replicated, how long it took to replicate, and the size of the data that was replicated.
   - when the primary cluster was switched over to the secondary cluster and the reason for the switchover.
   - the replication schedule and the delay threshold.

### Disaster Recovery Striking the Primary Data Center

- Switchover happens only when all the nodes in the primary data center are lost.
- The arbitrator detects the loss of all the primary data center members and initiates switchover to the secondary data center.
- Secondary data center updates the vBond:
  - Invalidates old Cisco vManage systems.
  - New Cisco vManage systems from the secondary data center are updated, as valid.
  - Routers reach vBond after losing control connections.
  - Routers start forming control connections with the new valid Cisco vManage systems.

### Troubleshooting Tips

If disaster recovery registration fails, verify the following:

- Reachability to the vBond orchestrator from all cluster members on the secondary cluster.
- Reachability between the secondary cluster, primary cluster, and the arbitrator on the transport interface (VPN 0).
- Check that you have the correct username and password.

If disaster recovery registration fails due to arbitrator reachability, check the following:

- You must configure the arbitrator in cluster mode. Navigate to **Administration** > **Cluster Management**, and add a Cisco vManage as the arbitrator.
- If the IP address is not assigned to the correct arbitrator, log on to the arbitrator cluster and do the following:

- Navigate to **Administration > Cluster Management**.
- Edit the Cisco vManage.
- Select the correct IP address from the drop-down list and save the configuration.

The disaster recovery consul process uses this IP address for disaster recovery communication. This is set once you configure the Cisco vManage in cluster mode.

# Disaster Recovery with Manual Switchover

This section provides information about setting up and registering disaster recovery in a Cisco SD-WANdeployment, and about performing a manual switchover. Disaster recovery has been validated for a three-node cluster

### Prerequisites for Setting up Disaster Recovery with Manaual Switchover

Before you set up disaster recovery for your SD-WAN deployment, perform the following tasks:

- Configure an out-of-band or cluster interface on the VPN 0 of each Cisco vManage node that is to be used for disaster recovery. This interface is the same one that Cisco vManage uses to communicate with its peers in a cluster.
- Make sure that all Cisco vManage nodes can reach each other through the out-of-band interface.
- Make sure that all services (application-server, configuration-db, messaging server, coordination server, and statistics-db) are enabled on all Cisco vManage nodes in the cluster.
- Make sure that all Cisco vManage nodes in a cluster reside on the same LAN segment.
- Make sure that all Cisco vManage nodes are running same Cisco vManage software version.
- To allow Cisco vManage clusters to communicate with each other across data centers, enable TCP ports 8443 and 830 on your data center firewalls.
- Spin all controllers, including Cisco vBond Orchestrators, across both primary and secondary data centers. Ensure that these controllers are reachable by Cisco vManage nodes that are spun across these data centers. The controllers connect only to the primary Cisco vManagecluster.
- Distribute each Cisco vManage VM on a separate physical server so that a single physical server outage does not affect the Cisco vManage cluster in a data center.

### Disaster Recovery Registration

Disaster Recovery must be registered on the primary Cisco vManage cluster. Before you start the registration process, make sure that no other operations in process in the active (primary) and the standby (secondary)Cisco vManage cluster. For example, make sure that no servers are in the process of upgrading or no templates are in the process of attaching templates to devices.

You can use the out-of-band IP address of a reachable Cisco vManage node in the cluster for disaster recovery registration.

Before you start the registration process, go to the **Tools** > **Rediscover Network** page on the primary Cisco vManage node and rediscover the Cisco vBond Orchestrators.

Disaster recovery registration is a day 1 operation. The registration can take up to 30 minutes to complete. After the registration starts, the message “No Data Available” may display for a short time in the Disaster Registration Task View. During the registration process, the message “In-progress” displays.

If you see the message “Error occurred retrieving status for action disaster_recovery_registration,” click the **Reload** button in your browser after the last active Cisco vManage node restarts.

If you need to upgrade your Cisco vManage software in the future, pause disaster recovery, perform the upgrade, and then resume disaster recovery. When upgrading Cisco vManage, follow the best practices as described in Cisco SD-WAN vManageCluster Creation and Troubleshooting.

### Scheduled Disaster Recovery

Performing a manually scheduled switchover let you test the operation of disaster recovery.

Detach templates from Cisco vManage devices in the primary cluster before you perform a switchover.

To manually perform a scheduled switchover, follow these steps:

1. Shut off the tunnel interfaces on the primary Cisco vManage cluster to prevent devices from toggling during the switchover.
2. From a Cisco vManage system on the secondary cluster, select **Administration** > **Disaster Recovery**.
3. Wait for data replication to complete, then click **Make Primary**.

   Devices and controllers converge to the secondary cluster and that cluster assumes the role of the primary cluster. When this process completes, the original primary cluster assumes the role of the secondary cluster. Then data replicates from the new primary cluster to the new secondary cluster.

To move back to the original primary cluster, repeat these steps.

### Disaster Recovery Operations

This sections explains how to perform disaster recovery in a variety of situations.

#### Loss of Primary Cisco vManage Cluster

If your primary Cisco vManage cluster goes down, follow these steps for disaster recovery:

1. From a Cisco vManage system on the secondary cluster, select **Administration** > **Disaster Recovery**.
2. Click **Make Primary**.

   Devices and controllers converge to the secondary cluster and that cluster assumes the role of the primary cluster.

   When the original primary cluster recovers and is back on line, it assumes the role of the secondary cluster and begins to receive data from the primary cluster.

#### Loss of Primary Data Center

If your primary data center cluster goes down, follow these steps for disaster recovery:

1. From a Cisco vManage system on the secondary cluster, select **Administration** > **Disaster Recovery**.
2. Click **Make Primary**.

The switchover process begins. During the process, only the Cisco vBond Orchestrators in the secondary data center are updated with a new valid Cisco vManage list. Devices and controllers that are on line converge to the secondary cluster and that cluster assumes the role of the primary cluster.

After the original primary data center recovers and all VMs, including controllers, are back on line, the controllers are updated with a new valid Cisco vManage and converge to the new primary Cisco vManage cluster. The original primary cluster assumes the role of secondary cluster and begins to receive data from the primary cluster.

**Partial Loss of Primary Cisco vManage Cluster**

If you experience a partial loss of the primary Cisco vManage cluster, we recommend that you try to recover that cluster instead of switching over to the secondary cluster.

A cluster with N nodes is considered to be operational if (N/2)+1 nodes are operational.

A cluster with N nodes becomes read only if (N/2)+1 or more nodes are lost.

**Loss of Enterprise Network Between Data Centers**

If a link failure occurs between your data centers but the WAN in the primary data center is operational, data replication fails. In this situation, attempt to recover the link so that data replication can resume.

To avoid a possible split brain scenario, do not perform a switchover operation.

### Delete Disaster Recovery

If you want to delete disaster recovery, we recommend that you initiate the delete operation on the primary cluster. Before deleting, make sure that there is no data replication session in pending state, and make sure that the secondary cluster is not importing data.

If the primary Cisco vManage cluster is down, you can perform the delete operation on the secondaryCisco vManage cluster.

If any Cisco vManage cluster that was offline during the disaster recovery delete operation come on line, execute the following POST request on that cluster to complete the delete disaster recovery operation:

**POST /dataservice/disasterrecovery/deleteLocalDC**

After you delete disaster recovery, makes sure that the primary and secondary clusters are operating correctly. To do so, go to the **Administration** > **Cluster Management** page and make sure that all Cisco vManage nodes are present in the cluster. If the nodes are not present, restart the application server. Also go to the **Administration** > **Disaster Recovery** page and make sure that no nodes appear.

Data centers must be deleted from disaster recovery before you can reregister disaster recovery for the data centers.

### Guidelines and Best Practices

- The disaster recovery functionality does not replace the best practices of taking database backups and VM snapshots on the primary Cisco vManage cluster. We recommend that you to take these backups and snapshots.
- In some situations, The **Administration** > **Disaster Recovery** page displays the message “Disaster recovery not configured.” This message represents the transient issue data replication occurring on the secondary cluster.

- The time that it takes for devices to converge to new primary Cisco vManage cluster after a switchover depends on the number of devices that are involved in the switchover. For example, a switchover of 10 devices might take less than 30 seconds, but the switchover of 100 devices can take few minutes.
- After a switchover, the old primary cluster requires reachability to the new primary cluster to update the states of both clusters. It can take up to 5 minutes for the update to complete.
- After you complete the registration process, wait for the first data replication cycle between clusters to complete before you perform any action on the primary Cisco vManage cluster. You can verify the replication status in the **Administration** > **Disaster Recovery** page.
- After switching over, do not update disaster recovery settings until the first data replication cycle between clusters completes. You can verify the replication status in the **Administration** > **Disaster Recovery** page.
- To avoid a split brain scenario, do not perform a make-primary operation from a secondary data center when the tunnel interfaces of the Cisco vManage nodes in the primary data center are up and accessible from other controllers and devices. Bring down the tunnel interfaces for the primary Cisco vManage cluster before you perform the make primary operation for the secondary cluster.
- If the **Make Primary** button in the **Administration** > **Disaster Recovery** page becomes dim after you click it, click the **Reload** button in your browser.
- In a deployment in which Cisco vManage acts as the certificate authority (CA) for Cisco edge devices, devices that you add to the overlay network after performing a switchover from one data center to another do not join the overlay network after you switch back. In this situation, manually synchronize root certificates between the data centers after you perform the first switchover.
- Periodically check the Cisco vBond Orchestrator information on the Cisco vManage Dashboard in the secondary cluster. If you see an issue, go to the **Tools** > **Rediscover Network** page on the primary Cisco vManage node and rediscover the Cisco vBond Orchestrators. The updated discovery information replicates to the secondary Cisco vManage cluster during the next replication cycle.
- After a switchover completes, review the replication information in the **Administration** > **Disaster Recovery** page to ensure that data is transferred from the primary cluster to the secondary cluster.
- If replication fails, verify that the primary cluster can reach the secondary cluster.
- For related disaster recovery troubleshooting tips and information, see the “High Availability Overview” chapter in Network Optimization and High Availability Configuration Guide.

# High Availability CLI Reference

CLI commands for configuring and monitoring high availability.

### High Availability Configuration Commands

Use the following commands to configure high availability on a Cisco IOS XE SD-WAN device:

```
bfd
  app-route
    multiplier number
    poll-interval milliseconds
  color color
    hello-interval milliseconds
    multiplier number
    pmtu-discovery
```

### High Availability Monitoring Commands

**show sdwan bfd sessions**—Display information about the BFD sessions running on the local Cisco IOS XE SD-WAN device.

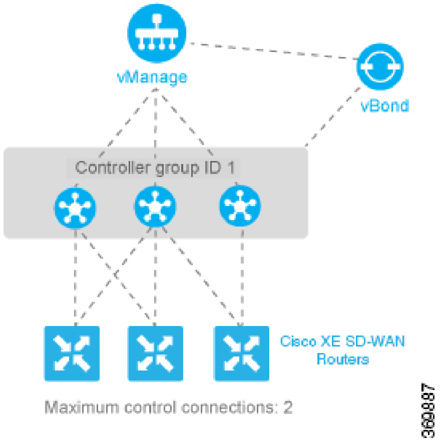
# High Availability Configuration Examples

This topic provides examples of configuring high availability, specifically, of configuring affinity between vSmart controllers and Cisco IOS XE SD-WAN device.

### Configure Affinity to vSmart Controllers in a Single Data Center

In an overlay network with a single data center that has multiple vSmart controllers, if you want the Cisco IOS XE SD-WAN device to establish a single control connection to one of vSmart controllers, there is no need to configure affinity because this situation is the default behavior.

However, if you want the Cisco IOS XE SD-WAN device to establish control connections to more than one vSmart controllers, to provide redundancy in case one of the controllers becomes unavailable, you configure affinity. You generally place the vSmart controllers in the same controller group.



Let's say that all the vSmart controllers use the same controller group identifier, 1. You configure the identifier on all three controllers as follows:

```
vSmart(config)# system controller-group-id 1
```

To verify the configuration, use the **show running-config** command:

```
vSmart# show running-config system
system
 description          "vSmart in data center 1"
 host-name            vSmart
 gps-location latitude 37.368140
 gps-location longitude -121.913658
 system-ip            172.16.255.19
 site-id              100
 controller-group-id 1
 organization-name    "Cisco"
 clock timezone America/Los_Angeles
```

We want the three Cisco IOS XE SD-WAN devices to establish two control connections to two of the three vSmart controllers. We do this for purposes of redundancy, in case one of the controllers becomes available. Because all the vSmart controllers are in the same controller group, we cannot specify or influence which of the two controllers the Cisco IOS XE SD-WAN devices connect to. The configurations on all three routers are effectively identical. We show here the configuration for router Cisco IOS XE SD-WAN device-1.

First, configure the available vSmart controller groups. This scenario has just one group:

```
ISR4331-1(config)# system controller-group-list 1
```

By default, a Cisco IOS XE SD-WAN device can establish two control connections. Because we want each Cisco IOS XE SD-WAN device and each tunnel interface to connect to two vSmart controllers, no configuration is required here. However, if you want to explicitly configure these parameters, you configure the maximum number of OMP sessions at the system level and the maximum number of control connections per tunnel:

```
ISR4331-1(config)# system max-omp-sessions 2
ISR4331-1(config)# sdwan interface GigabitEthernets0/0/1 tunnel-interface
ISR4331-1(config-tunnel-interface)# max-control-connections 2
```

Here are the relevant configuration snippets from Cisco IOS XE SD-WAN device-1:

```
ISR4331-1# show sdwan running-config | section system
system
 host-name              ISR4331-1
gps-location latitude 43.0
gps-location longitude -75.0
system-ip             172.16.255.11
site-id               100
max-omp-sessions      2
controller-group-list 1
admin-tech-on-failure
organization-name     Cisco
 ...
ISR4331-1# show running-config | section sdwan
...
 interface GigabitEthernets0/0/1
  tunnel-interface
   encapsulation ipsec
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
exit
…
```

To display the control connections with the vSmart controllers, use the **show sdwan control connections** command. The last column, Controller Group ID, lists the vSmart controller group that a router is in.

```
ISR4331-1# show sdwan control connections

                                                                                       PEER
PEER                                    CONTROLLER
PEER    PEER PEER           SITE       DOMAIN PEER                                    PRIV  PEER
PUB                                     GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                              PORT  PUBLIC IP                               PORT
LOCAL COLOR     PROXY STATE UPTIME      ID
----------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------
vsmart  dtls 10.255.2.120     1          1      10.2.1.120                               12346 10.2.1.120                               12346
```

```
default               up     0:00:06:17  1
vmanage dtls 10.255.2.100  1    1          0      10.2.1.100                              12346 10.2.1.100
12346 default               up     0:00:06:13  0
```

To display the maximum number of control connections allowed on the router, use the **show sdwan control local-properties** command. The last line of the output lists the maximum controllers. The following is the abbreviated output for this command:

```
ISR4331-1# show sdwan control local-properties

personality                  vedge
organization-name            Cisco
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Sep 27 03:14:18 2016 GMT
certificate-not-valid-after  Sep 27 03:14:18 2026 GMT
...

                         PUBLIC          PUBLIC PRIVATE         PRIVATE                                 PRIVATE                             MAX
 RESTRICT/           LAST         SPI
TIME    NAT  VM
INTERFACE                IPv4            PORT   IPv4            IPv6                                    PORT    VS/VM COLOR            STATE CNTRL
 CONTROL/     LR/LB  CONNECTION
REMAINING   TYPE CON
STUN                                              PRF
--------------------------------------------------------------------------------------------------------------------------------------------------
-------------------
GigabitEthernet0/0/1     2.2.1.17        12406  2.2.1.17        ::                                      12406    2/1  default          up     2
   no/yes/no   No/No  17:15:53:07
0:08:02:33  N    5
```

Two commands display information about the control connections established by the affinity configuration. To see, for each interface, which controller groups are configured and which the interface is connected to, use the **show sdwan control affinity config** command:

```
ISR4331-1# show sdwan control affinity config
EFFECTIVE CONTROLLER LIST FORMAT - G(C),...     - Where G is the Controller Group ID
                                                        C is the Required vSmart Count

CURRENT CONTROLLER LIST FORMAT   - G(c)s,...    - Where G is the Controller Group ID
                                                        c is the current vSmart count
                                                        s Status Y when matches, N when
does not match


                EFFECTIVE
                REQUIRED
                                                           LAST-RESORT
INDEX INTERFACE VS COUNT  EFFECTIVE CONTROLLER LIST                               CURRENT
CONTROLLER LIST                               EQUILIBRIUM  INTERFACE
------------------------------------------------------------------------------------------
0     GigabitEthernet0/0/11         1(1)
  1(1)Y                                                 Yes          No
```

The command output above shows that affinity is configured on interface GigabitEthernet 0/0/11.

- The **Effective Required** and **Count** column shows that the interface is configured to create two control connections, and, in fact, two control connections have been established. You configure the number of control connections for the tunnel interface with the **max-control-connections** command.
- The Effective Controller List column shows that affinity on the interface is configured to use Cisco vSmart Controller identifier 1 and that the router supports two OMP sessions. You configure the affinity controller identifiers with the **controller-group-list** command (at the **system** level) and, for the tunnel interface, the **exclude-controller-group-list** command.
- The Current Controller List column lists the actual affinity configuration for the interface. The output here shows that the interface has two control connections with Cisco vSmart Controllers in group 1. The

check mark indicates that the current and effective controller lists match each other. If, for example, the tunnel had established only one TLOC connection to a vSmart controller, this column would show "1(1)X".

- The Equilibrium column indicates that the current controller lists matches what is expected from the affinity configuration for that tunnel interface.

To determine the exact Cisco vSmart Controllers that the tunnel interface has established control connections with, use the **show control affinity status** command:

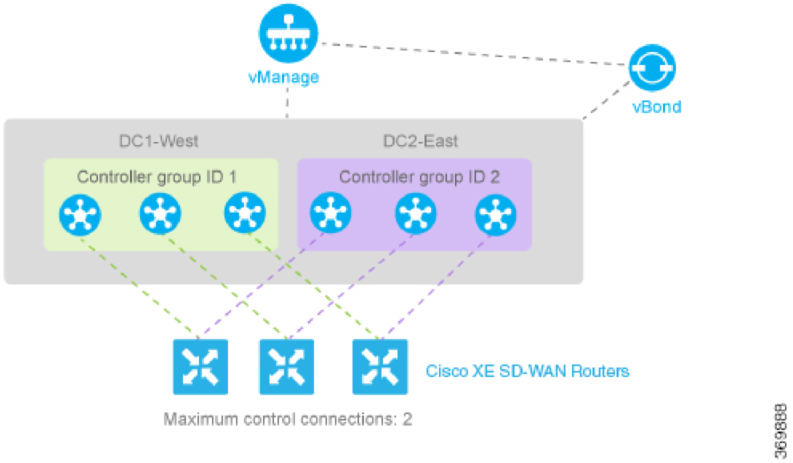
```
ISR4331-1# show sdwan control affinity status
ASSIGNED CONNECTED CONTROLLERS   - System IP( G),..  - System IP of the assigned vSmart
                                                             G is the group ID to which
the vSmart belongs to

UNASSIGNED CONNECTED CONTROLLERS - System IP( G),..  - System IP of the unassigned vSmart
                                                             G is the group ID to which
the vSmart belongs to


INDEX           INTERFACE          ASSIGNED   CONNECTED CONTROLLERS
                          UNASSIGNED CONNECTED CONTROLLERS
------------------------------------------------------------------------------------------
0         GigabitEthernet 0/0/1     10.255.2.120(  1)
```

The command output above shows that interface `GigabitEthernet 0/0/1` has control connections to the vSmart controller, 10.255.2.120,which is in group 1. If the interface were connected to a vSmart controller not in the controller group list, it would be listed in the Unassigned Connected Controllers column.

When a data center has multiple vSmart controllers, you can configure them to be in different controller groups. For example, if you configure them to be in two different controller groups, each Cisco IOS XE SD-WAN device can establish two control connections, one to each of the groups. While this configuration design is similar to what we discussed in the previous section, providing redundant control connections to the vSmart controllers, on subtle difference is that it provides fault isolation between the twoCisco vSmart Controller groups in the data center. The configuration for this scenario is almost identical to the configuration when Cisco vSmart Controllers are two data centers. The only difference is that here, two Cisco vSmart Controller groups are collocated in the same data center. See the configuration example in the next section.

### Configure Affinity to vSmart Controllers in Two Data Centers

You can use affinity to enable redundancy among data centers, for a network design in which multiple Cisco vSmart Controllers are spread across two or more data centers. Then, if the link between a Cisco IOS XE SD-WAN device and one of the data centers goes down, the Cisco vSmart Controllers in the second data center are available to continue servicing the overlay network. The figure below illustrates this scenario, showing three Cisco vSmart Controllers in each of two data centers. Each of the three Cisco IOS XE SD-WAN devices establishes a TLOC connection to one controller in the West data center and one in the East data center.



You configure the three vSmart controllers in DC1-West with controller group identifier 1:

```
vSmart-DC1(config)# system controller-group-id 1
```

The three vSmart controllers in DC2-East are in controller group 2:

```
vSmart-DC2(config)# system controller-group-id 2
```

We want all the Cisco IOS XE SD-WAN devices to have a maximum of two OMP sessions, and we want each tunnel interface to have a maximum of two control connections and to not exclude any controller groups. So the only configuration that needs to be done on the routers is to set the controller group list. We want Cisco IOS XE SD-WAN devices in the west to prefer Cisco vSmart Controllers in DC1-West over DC2-East:

```
ISR4331-West(config)#  system controller-group-list 1 2
```

Similarly, we want Cisco IOS XE SD-WAN devices in the east to prefer DC2-East:

```
ISR4331-East(config)# system controller-group-list 2 1
```

The software evaluates the controller group list in order, so with this configuration, the Cisco XE SD-WAN-West routers prefer Cisco vSmart Controller group 1 (which is the West data center), and the Cisco XE SD-WAN-East routers prefer Cisco vSmart Controller group 2.

You can fine-tune the controller group preference in other ways:

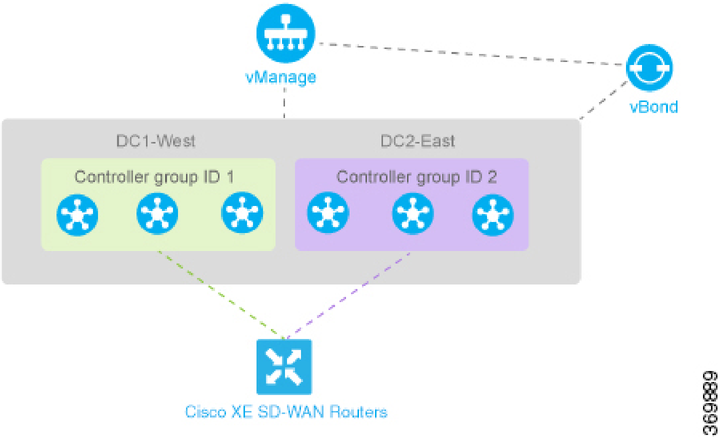
- Set the maximum number of OMP sessions allowed on the router to 2 (**system max-omp-sessions 1**). To illustrate how this works, let's look at a Cisco XE SD-WAN-West router. The router has only one tunnel interface, and that interface creates one control connection to Cisco vSmart Controller list 1. If all the Cisco vSmart Controllers in this group become unavailable, or if the connection between the router that the DC1-West data center goes down, the tunnel interface establishes one control connection to Cisco vSmart Controller list 2, because this group is listed in the **system controller-group-list** command. If all Cisco vSmart Controllers in both controller groups, or the connections to them, become unavailable, and if the vBond orchestrator also indicates that all these vSmart controllers are unreachable, the tunnel interface establishes a control connection to any other Cisco vSmart Controller in the overlay network if other controllers are present.

- Set the maximum number of control connections that the tunnel interface can establish to 1 ( **vpn 0 sdwan interface tunnel-interface max-control-connections 1** ). Because the software evaluates the controller group list in order, for a Cisco XE SD-WAN-West router, this configuration forces the tunnel interface to establish a control connection to Cisco vSmart Controller group 1. Again, if this controller group or data center becomes unreachable, the tunnel establishes a control connection with controller group 2, because this group is configured in the **system controller-group-list** command. And if neither controller group 1 or 2 is available, and if another Cisco vSmart Controller is present in the network, the tunnel interface establishes a control connection with that controller.

- Exclude the non-preferred Cisco vSmart Controller group for a particular tunnel. For example, for a Cisco XE SD-WAN-West router to prefer controller group 1, you configure **vpn 0 sdwan interface tunnel-interface exclude-controller-group-list 2** . As with the above configurations, if this controller group or data center becomes unreachable, the tunnel establishes a control connection with controller group 2, because this group is configured in the **system controller-group-list** command. And if neither controller group 1 or 2 is available, and if another Cisco vSmart Controller is present in the network, the tunnel interface establishes a control connection with that controller.

### Configure Redundant Control Connections on One Cisco IOS XE SD-WAN Device

When a router has two tunnel connections and the network has two (or more) data centers, you can configure redundant control connections from the Cisco IOS XE SD-WAN device to Cisco vSmart Controllers in two of the data centers. It is recommended that do this using the minimum number of OMP sessions—in this case, two. To do this, you configure one of the tunnel interfaces to go only to one of the data centers and the other to go only to the second. This configuration provides vSmart redundancy with the minimum number of OMP sessions.



On the Cisco IOS XE SD-WAN device router, define the controller group list and configure the maximum number of OMP sessions to be 2:

```
ISR4331(config)# system controller-group-list 1 2
ISR4331(config)#  system max-omp-sessions 2
```

For one of the tunnels, you can use the default affinity configuration (that is, there is nothing to configure) to have this tunnel prefer a Cisco vSmart Controller in group 1. You can also explicitly force this tunnel to prefer Cisco vSmart Controller group 1:

```
ISR4331(config-tunnel-interface-1)# max-control-connections 1
```

You do not need to configure **exclude-controller-group-list 2** , because the software evaluates the controller group list in order, starting with group 1. However, you could choose to explicitly exclude vSmart controller group 2.

Then, on the second tunnel, configure it to prefer a vSmart controller in group 2. As with the other tunnel, you limit the maximum number of control connections to 1. In addition, you have to exclude controller group 1 for this tunnel.

```
ISR4331(config-tunnel-interface-2)# max-control-connections 1
ISR4331(config-tunnel-interface-2)# exclude-controller-group-list 1
```